UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/197,275	11/20/2018	Jason K. Resch	CS00403	4290

89322 7590 06/09/2020
Garlick & Markison (PST)
100 Congress Avenue, Suite 2000
Austin, TX 78701

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2419	

NOTIFICATION DATE	DELIVERY MODE
06/09/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

MMURDOCK@TEXASPATENTS.COM
bpierotti@texaspatents.com

Notice of Abandonment	Application No.	Applicant(s)
	16/197,275	Resch et al.
	Examiner	**Art Unit**
	David García Cervetti	2419

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☑ Applicant's failure to timely file a proper reply to the Office letter mailed on 15 November 2019.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 to the final rejection. (A proper reply under 37 CFR 1.113 to a final rejection consists only of:(1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) if this is utility or plant application, a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. Note that RCEs are not permitted in design applications.)
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 8 below).
   (d) ☑ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $ _____ is insufficient. A balance of $ _____ is due.
   The issue fee required by 37CFR 1.18 is $ _____ . The publication fee, if required by 37 CFR 1.18(d), is $ _____ .
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record or other party authorized under 37 CFR 1.33 (b). See 37 CFR 1.138(b).

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34) upon the filing of a continuing application.

6. ☐ The decision by the Patent Trial and Appeal Board rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☐ The dismissal of the appeal in an application having no allowed claims. (When an appeal is dismissed in an application having no allowed claims the application stands abandoned. See MPEP 1215.04 subsections I-V for an explanation of the reasons why an appeal is dismissed.)

8. ☑ The reason(s) below:

   Contacted Attorney of Record, Patricia Markison Healy, at 808.283.3608 to verify and was informed that the Applicant decided to discontinue prosecution of the application and let it go abandoned.

/David Garcia Cervetti/ Primary Examiner, Art Unit 2419	

Petitions to revive under 37 CFR 1.137, or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 2
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/197,275	11/20/2018	Jason K. Resch	CS00403	4290

89322 7590 11/15/2019
Garlick & Markison (PST)
100 Congress Avenue, Suite 2000
Austin, TX 78701

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
11/15/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

MMURDOCK@TEXASPATENTS.COM
bpierotti@texaspatents.com

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No. 16/197,275	Applicant(s) Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 27 August 2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 20 November 2018 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed 8/27/2019 has been fully considered.

2. Claims 1-16 are pending and have been examined.

Notice of Pre-AIA or AIA Status

3. The present application is being examined under the pre-AIA first to invent provisions.

Response to Amendment

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. The objection to the claims is withdrawn.

6. Regarding the obviousness-type double patenting rejection, Examiner respectfully points out that the instant claims are analogous to the conflicting claims since they also require the dispersed storage error encoding, the randomly ordered/obfuscated data slices, and the auxiliary data. Applicant's arguments are not persuasive.

7. Regarding the rejection under 35 USC 103, the cited portions of Applicant's specification fall short of defining "dispersed storage error encoding", at most it broadly describes that error encoding could be forward error correction (FEC), information dispersal algorithm, or error correction coding, just as Casanova provides with the tracker mechanism to enable dispersal and reconstruction of a file and additional encoding/compression processing of fragments (par.42-50). Applicant's arguments are not persuasive.

8. Regarding the argument that Casanova does not tech auxiliary data (e.g., this is some type of extra data that does not include the file data), Examiner respectfully points out that Casanova provides a "file tracker" that reasonably corresponds to "some type of extra data that does not include the file data" (par.26-30, 34-45). Applicant's arguments are not persuasive.

Double Patenting

9. Claims 1-16 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of Patent Nos. 8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071,8885821, 8782494, 8856617, and 9128870. Although the conflicting claims are not identical, they are not patentably distinct from each other because

- "A method comprises: dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices; dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices; obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices; obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage" (claim 1, instant application) is analogous to
- "A method for execution by a processing module of a computing device, the method comprises: receiving a data object retrieval message regarding receiving a transmission from a particular source device; receiving, as the transmission, randomly ordered encoded slices from the particular source device; rearranging the randomly ordered encoded slices into first randomly ordered encoded data slices corresponding to data and a set of second randomly ordered encoded data slices corresponding to auxiliary data based on de-selection information; ordering the second randomly ordered encoded data slices into a set of encoded data slices in accordance with auxiliary data de-sequencing information; decoding the set of encoded data slices in accordance with operational parameters to produce auxiliary data; when the auxiliary data content corresponds to de-sequencing of the first randomly ordered encoded data slices, determining a pseudo random de-sequencing order for the first randomly ordered encoded data slices from the auxiliary data; ordering the first randomly ordered encoded data slices based on the pseudo-random de-sequencing order to produce a plurality of sets of encoded data slices; dispersed storage error decoding the plurality of sets of encoded data slices to produce a plurality of encrypted data segments; decrypting the plurality of encrypted data segments to produce a plurality of data segments; and aggregating the plurality of data segments to produce the data" (claim 1, patent 8959366) and analogous to
- "A method comprising: receiving a data segment of a data stream; encrypting the data segment to produce an encrypted data segment; dispersed storage error encoding the encrypted data segment to produce a set of encoded data slices, wherein a threshold number of the encoded data slices of the set of encoded data slices are needed to recover the encrypted data segment; dispersed storage error encoding auxiliary data to produce a set of encoded auxiliary data slices; generating a sequence of output slices to obscure the set of encoded data slices by interspersing the set of encoded auxiliary data slices within the set of encoded data slices; and sending the sequence of output slices for storage in a distributed storage network (DSN)" (claim 1, patent 10282564).

10. This is a provisional obviousness-type double patenting rejection because the conflicting claims of the instant application have not in fact been patented.

11. The claims of the conflicting patents and/or applications contain every element of claims 1-16 of the instant application and thus anticipate the claims of the instant application. Claims 1-16 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

12. "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species with that genus). "ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

13. "Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic claim. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly, absent a terminal

disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).

Claim Rejections - 35 USC § 103

14. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Casanova (20080126357), and further in view of Michaelsen (20050002531).

Regarding claims 1 and 9, Casanova teaches dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices; dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices (par.14-15, 22-31,51-60); and

outputting, by the computing device, the first and second sets of encoded data slices for storage (par.57-61).

Casanova does not expressly disclose, however Michaelsen teaches obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices; obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage (par.9-19, 105-135, 140-150).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Michaelsen to the system of Casanova.

One of ordinary skill in the art would have been motivated to perform such a modification to further increase complexity for unintended recipients to access content (Michaelsen, par.3-19, 100-150).

Regarding claims 2 and 10, Casanova/ Michaelsen teaches dispersed storage error encoding, by the computing device, the auxiliary data to produce a second set of encoded auxiliary data slices (Casanova, par.26-40, 55-60);

obfuscating, by the computing device, the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a

first set of further obfuscated encoded data slices; and obfuscating, by the computing device, the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices (Michaelsen, par.9-19, 105-135, 140-150).

Regarding claims 3 and 11, Casanova/ Michaelsen teaches wherein the auxiliary data comprises one or more of: null data; authentication information; a next pseudo random output sequencing order; a pseudo random output sequencing order identifier; a next outputting threshold; a random number generator output; an encryption key; a starting point for the pseudo random output sequencing order; a device identifier; a data identifier; a data type; a data size indicator; a priority indicator; a security indicator; and a performance indicator (Casanova, par.26-42, 55-60, Michaelsen, 120-130).

Regarding claims 4 and 12, Casanova/ Michaelsen teaches encrypting, by the computing device, the plurality of data segments to produce a plurality of encrypted data segments; and dispersed storage error encoding, by the computing device, the plurality of encrypted data segments to produce the plurality of sets of encoded data slices (Casanova, par.14, 26-42, 55-60).

Regarding claims 5 and 13, Casanova/ Michaelsen teaches encrypting, by the computing device, the auxiliary data to produce encrypted auxiliary data; and dispersed storage error encoding, by the computing device, the encrypted auxiliary data to produce the set of encoded auxiliary data slices (Casanova, par.14, 26-42, 55-60).

Regarding claims 6 and 14, Casanova/ Michaelsen teaches wherein the auxiliary data is encrypted via an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data (Casanova, par.14, 26-42, 55-60).

Regarding claims 7 and 15, Casanova/ Michaelsen teaches wherein the auxiliary data is encrypted via an all or nothing transformation to produce the encrypted auxiliary data and the plurality of data segments is encrypted via an all or nothing transformation to produce the plurality of encrypted data segments (Casanova, par. 14-15, 22-31,51-60, Michaelsen, 142-150).

Regarding claims 8 and 16, Casanova/ Michaelsen teaches wherein the obfuscating the first set of encoded data slices comprises: interspersing, by the computing device, the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output

sequencing order to produce the first set of obfuscated encoded data slices (Michaelsen, 14-20, 120-130, 142-150).

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

16. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Garcia Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Friday 8AM-5PM.

18. Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

19. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, SHEWAYE GELAGAY can be reached on (571)272-4219. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

20. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David Garcia Cervetti/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 1 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20070226145-A1	09-2007	Ishigaki; Yoshinobu	G06K17/0022	705/51
*	B	US-20070160198-A1	07-2007	Orsini; Rick	H04L9/085	380/28
*	C	US-20060177061-A1	08-2006	Orsini; Rick L.	G06F21/606	380/268
*	D	US-20020003881-A1	01-2002	REITMEIER, GLENN ARTHUR	H04L9/34	380/210
*	E	US-20020078227-A1	06-2002	Kronenberg, Sandy Craig	H04L29/06	709/237
*	F	US-20030028879-A1	02-2003	Gordon, Donald F.	H04N5/4401	725/39
*	G	US-20070100913-A1	05-2007	Sumner; Gary Steven	G06F11/1453	1/1
*	H	US-7457415-B2	11-2008	Reitmeier; Glenn Arthur	H04L9/34	348/E7.055
*	I	US-20090041235-A1	02-2009	Reitmeier; Glenn Arthur	H04L9/34	380/42
*	J	US-20080263113-A1	10-2008	Krishnaiyer; Rajesh Anantha	G06F16/1844	1/1
*	K	US-7991746-B2	08-2011	Krishnaiyer; Rajesh Anantha	G06F16/1844	707/664
*	L	US-5535239-A	07-1996	Padovani; Roberto	H04B1/707	370/209
*	M	US-5621799-A	04-1997	Katta; Noboru	H04N7/1675	348/E7.056

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	Pang et al., StegFS: A Steganographic File System, IEEE, 2003
*	V	Bella et al., Distributed Backup through Information Dispersal, Elsevier, 2006
*	W	Barr et al., pStore: A Secure Distributed Backup System, 2001
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 2 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080147821-A1	06-2008	Dietrich; Bradley W.	H04L63/104	709/216
*	B	US-20080222481-A1	09-2008	Huang; Cheng	H03M13/1191	714/752
*	C	US-20080222480-A1	09-2008	Huang; Cheng	H03M13/1191	714/752
*	D	US-20060212782-A1	09-2006	Li; Jin	H03M13/1575	714/784
*	E	US-20040117718-A1	06-2004	Manasse, Mark Steven	H03M13/1515	714/781
*	F	US-8626820-B1	01-2014	Levy; Richard S.	G06F11/1004	709/201
*	G	US-8560930-B2	10-2013	Li; Zongwang	H03M13/036	714/777
*	H	US-8522125-B1	08-2013	Feng; Jun	H03M13/293	714/801
*	I	US-7472334-B1	12-2008	Scott; Thomas P.	H03M13/151	714/785
*	J	US-20020046359-A1	04-2002	Boden, Scott T.	G06F12/1408	714/6.12
*	K	US-20070079083-A1	04-2007	Gladwin; S. Christopher	G06F21/6227	711/154
*	L	US-20070079082-A1	04-2007	Gladwin; S. Christopher	G06F11/1076	711/154
*	M	US-20070079081-A1	04-2007	Gladwin; S. Christopher	G06F21/6227	711/154

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 3 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20050131993-A1	06-2005	Fatula, Joseph John JR.	G06F9/5072	709/202
*	B	US-20040215998-A1	10-2004	Buxton, Robert F.	G06F11/1474	714/2
*	C	US-20040024963-A1	02-2004	Talagala, Nisha	G06F11/1076	711/114
*	D	US-20030018927-A1	01-2003	Gadir, Omar M.A.	G06F11/2005	714/4.11
*	E	US-20020166079-A1	11-2002	Ulrich, Thomas R.	G06F9/5083	714/6.12
*	F	US-20020062422-A1	05-2002	Butterworth, Henry Esmond	G06F11/0727	711/114
*	G	US-6826711-B2	11-2004	Moulton; Gregory Hagan	G06F11/1076	711/114
*	H	US-6718361-B1	04-2004	Basani; Vijay R.	H04L67/1095	707/999.01
*	I	US-6418539-B1	07-2002	Walker; Mark S.	G06F11/2058	714/5.1
*	J	US-5991414-A	11-1999	Garay; Juan Alberto	H04L9/302	380/30
*	K	US-6175571-B1	01-2001	Haddock; Stephen R.	H04L12/5601	370/423
*	L	US-6128277-A	10-2000	Bruck; Joshua	G06F11/1076	370/216
*	M	US-6058454-A	05-2000	Gerlach; Ralph John	G06F3/0607	710/10

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 4 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6012159-A	01-2000	Fischer; Michael	H03M13/13	714/755
*	B	US-5987622-A	11-1999	Lo Verso; Susan	G06F11/1076	714/6.1
*	C	US-5890156-A	03-1999	Rekieta; Thomas W.	G06F9/50	707/610
*	D	US-5809285-A	09-1998	Hilland; Jeffrey R.	G06F3/0608	703/25
*	E	US-5774643-A	06-1998	Lubbers; Clark E.	G06F11/1076	711/114
*	F	US-5485474-A	01-1996	Rabin; Michael O.	G06F11/004	714/762
*	G	US-4092732-A	05-1978	Ouchi; Norman Ken	G06F11/1076	714/5.11
*	H	US-9015301-B2	04-2015	Redlich; Ron M.	G06Q10/10	709/223
*	I	US-8904080-B2	12-2014	Martin; Don	G06F11/1456	710/20
*	J	US-7509420-B2	03-2009	Moulton; Gregory Hagan	H04L67/1097	709/203
*	K	US-7272602-B2	09-2007	Moulton; Gregory Hagan	G06F16/137	1/1
*	L	US-7103824-B2	09-2006	Halford; Robert	G06F11/1076	714/759
*	M	US-6690795-B1	02-2004	Richards; William James	H04N7/1675	348/E7.056

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 5 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080010218-A1	01-2008	Zank; Anthony E.	G06F21/64	705/75
*	B	US-20080192936-A1	08-2008	Bellwood; Thomas A.	H04N5/913	380/277
*	C	US-20060056519-A1	03-2006	Horowitz; Michael	H04N19/176	375/240.27
*	D	US-20050265349-A1	12-2005	Garg, Sachin	H04L29/06027	370/395.2
*	E	US-20020002675-A1	01-2002	BUSH, RONALD ROSCOE	G06Q20/102	713/160
*	F	US-7406595-B1	07-2008	Boyle, Jr.; Vincent Michael	H04L9/0637	708/521
*	G	US-7577689-B1	08-2009	Masinter; Larry	G06F11/1464	1/1
*	H	US-8392474-B2	03-2013	Franco; Lucas Goncalves	H04L51/00	707/679
*	I	US-9135456-B2	09-2015	O'Hare; Mark S.	G06F21/606	1/1
*	J	US-20090055547-A1	02-2009	Hudson; Michael D.	D01D5/423	709/231
*	K	US-20080320151-A1	12-2008	McCanne; Steven	H03M7/30	709/228
*	L	US-20060069719-A1	03-2006	McCanne; Steven	H04L67/2828	709/203
*	M	US-20120198302-A1	08-2012	Otterstedt; Jan	H03M13/13	714/755

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 6 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20100266122-A1	10-2010	Suzaki; Tomoyasu	H04L9/002	380/28
*	B	US-20080049930-A1	02-2008	You; Yong-Kuk	H04L9/0637	380/28
*	C	US-20060069964-A1	03-2006	Hayashi; Junichi	H04L1/0061	714/52
*	D	US-20050123271-A1	06-2005	Ichinose, Tsutomu	G11B20/00086	386/329
*	E	US-20040172549-A1	09-2004	Kojima, Tadashi	G11B20/00086	713/193
*	F	US-20040145661-A1	07-2004	Murakami, Tomochika	H04N1/32144	348/222.1
*	G	US-20030012372-A1	01-2003	Cheng, Siu Lung	H03M13/2957	380/28
*	H	US-20030002665-A1	01-2003	Sako, Yoichiro	G11B20/00086	380/37
*	I	US-9854332-B2	12-2017	Winograd; Joseph M.	H04N21/44204	1/1
*	J	US-9854331-B2	12-2017	Winograd; Joseph M.	H04N21/44204	1/1
*	K	US-6571212-B1	05-2003	Dent; Paul W.	H04L1/004	704/270.1
*	L	US-5910182-A	06-1999	Dent; Paul W.	H03M13/00	714/755
*	M	US-8275132-B2	09-2012	Buchen; Neil B.	H04N7/1675	380/202

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 7 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20070263864-A1	11-2007	BUCHEN; NEIL B.	H04N7/1675	380/201
*	B	US-20030123664-A1	07-2003	Pedlow, Leo M. JR.	H04N7/162	380/218
*	C	US-7707645-B2	04-2010	Haruki; Hiroyoshi	G06F21/57	713/193
*	D	US-20100172496-A1	07-2010	Furukawa; Jun	H04L9/0869	380/46
*	E	US-20060129801-A1	06-2006	Kang; Kyung-don	G06F21/10	713/153
*	F	US-20090177894-A1	07-2009	Orsini; Rick L.	G06F21/6209	713/193
*	G	US-20090097661-A1	04-2009	Orsini; Rick L.	H04L9/083	380/279
*	H	US-20100299313-A1	11-2010	ORSINI; RICK L.	H04L9/085	707/652
*	I	US-20100199089-A1	08-2010	Vysogorets; Mikhail	G06F21/34	713/168
*	J	US-20120066757-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/9
*	K	US-20120066756-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/9
*	L	US-20120066752-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/7
*	M	US-20120066517-A1	03-2012	Vysogorets; Mikhail	G06F21/34	713/193

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/197,275	Resch et al.
	Examiner	**Art Unit**
	David García Cervetti	2436

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06F21/85 G06F21/6218 G06F21/606 G06F21/72 G06F21/80 H04L9/0894 H04L9/3242 H04W12/0013 H04W12/02	11/06/2019	DGC

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
inventor name search, acm, ieee, springer, google, scholar, east history attached	11/06/2019	DGC

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/David Garcia Cervetti/ Primary Examiner, Art Unit 2436	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/197,275	Resch et al.
	Examiner	**Art Unit**
	David García Cervetti	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/26/2019	11/11/2019							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							

FNT-based **Reed-Solomon** erasure codes

A Soro, J Lacan - 2010 7th IEEE Consumer Communications ..., 2010 - ieeexplore.ieee.org
... of reliability and the persistence of the data following the **Information Dispersal Algorithm** (IDA) proposed by ... We have tested also the **Reed-Solomon** implementation by Rizzo [5], named ... Low Density Parity Check (LDPC) Staircase and Triangle Forward **Error** Correction (FEC ...
☆ 99 Cited by 27 Related articles All 15 versions

Information dispersal algorithm based on **Reed-Solomon** code [J]

HJ Wu, WW Chen - Journal of Computer Applications, 2010 - en.cnki.com.cn
... of Command Automation,PLA University of Science and Technology,Nanjing Jiangsu 210007,China). **Information Dispersal Algorithm**(IDA) based on **Reed-Solomon**(RS) code ... Nanjing University of Aero．＆Astro，Najing 210016);On the Undetected **Error** Probability of ...
☆ 99 Cited by 2 Related articles »

Asynchronous verifiable information dispersal

C Cachin, S Tessaro - 24th IEEE Symposium on Reliable ..., 2005 - ieeexplore.ieee.org
... With this background, we consider following **problem**: Some data has to be distributed by a ... The classic alternative, as proposed by Rabin [19], is an **information dispersal algorithm** (IDA): using an ... of the scheme are presented, in- cluding one that uses **error**-correcting codes ...
☆ 99 Cited by 70 Related articles All 15 versions

Fast **fault**-tolerant parallel communication and on-line maintenance for hypercubes using information dispersal

YD Lyuu - Mathematical systems theory, 1991 - Springer
... N-~°°gl°gJv~; however, this result holds by ignoring, in the analysis, the probability of routing **failure** due to ... 2. **Information Dispersal Algorithm** (IDA) ... anticipated by McEliece and Sarwate when they pointed out the relation between Shamir's scheme and **Reed-Solomon** codes [13 ...
☆ 99 Cited by 28 Related articles All 8 versions »

Fast **fault**-tolerant parallel communication for de bruijn and digit-exchange networks using information dispersal

YD Lyuu - Networks, 1993 - Wiley Online Library
... Ne(lo*lofl); however, this result holds by ignoring, in the analysis, the probability of routing **failure** due to ... 2. **INFORMATION DISPERSAL ALGORITHM** (IDA) ... McEliece and Sarwate when they pointed out the rela- tion between Shamir's scheme and the **Reed-Solomon** codes [171 ...
☆ 99 Cited by 9 Related articles All 5 versions »

An implementation of the Florida concatenated **Information Dispersal Algorithm/Reed-Solomon error** correction coding scheme

T Merrill - 1995 - University of Florida
☆ 99 »

Fast **fault**-tolerant parallel communication for de Bruijn networks using information dispersal

YD Lyuu - Proceedings of the Third IEEE Symposium on ..., 1991 - ieeexplore.ieee.org
... 1 -N-"(lOg'Og N); however, this result holds by ignoring, in the analysis, the probability of routing **failure** due to ... 2 **Information Dispersal Algorithm** (IDA) ... by McEliece and Sarwate when they pointed out the rela- tion between Shamir's scheme and the **Reed-Solomon** codes [ll] ...
☆ 99 Cited by 3 Related articles All 5 versions

Secret sharing made short

H Krawczyk - Annual International Cryptology Conference, 1993 - Springer
... outline the following simple information disper- sal scheme based on **Reed Solomon** erasure codes ... We assume a generic **information dispersal algorithm** that we denote by IDA, and which works ... schemes was presented by McElice and Sarwate [lo] where **error** correcting code ...
☆ 99 Cited by 396 Related articles All 14 versions »

Digital fountains: A survey and look forward

M Mitzenmacher - Information Theory Workshop, 2004 - ieeexplore.ieee.org
... spirit but iiiore expansive than the similar idea of the **information dispersal algorithm** [23, 271 ... More importantly, standard algorithms for decod- ing **Reed-Solomon** codes require quadratic time ... in preprocessing.) A natural approach for dealing with this **problem** involves encoding ...
☆ 99 Cited by 334 Related articles All 11 versions »

General information dispersal algorithms

P Béguin, A Cresti - Theoretical computer science, 1998 - Elsevier

... Moreover they can be applied to **fault**-tolerant transmission of information and to communication between processors in ... d = {A: IAI 2 m}. The algorithm described is a simple version of Rabin's **information dispersal algorithm**, and it is based on **Reed Solomon** erasure codes ...

☆ 99 Cited by 14 Related articles All 5 versions

Related searches

reed solomon **code** information dispersal algorithm

fermat number information dispersal algorithm

reliable communication information dispersal algorithm

information dispersal **parallel communication**

burst error **channel optimal** information dispersal

information dispersal fault **tolerance**

fast decoding of reed solomon **codes**

latency targets optimal information dispersal

distributed service optimal information dispersal

information dispersal **exchange networks**

information dispersal **remainder theorem**

parallel processing information dispersal **approach**

load balancing efficient dispersal **of** information

parallel algorithms information **dissemination**

information dispersal **low congestion**

information dispersal **bruijn networks**

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	"20190108366".pn.	US-PGPUB; USPAT	OR	OFF	2019/11/11 12:27
L2	0	"20080126357".pn. and (auxiliary metadata meta$1data)	US-PGPUB; USPAT	OR	OFF	2019/11/11 12:42
L3	1	"20080126357".pn. and (order sequence ordered ordering)	US-PGPUB; USPAT	OR	OFF	2019/11/11 12:42
L4	1	"20080126357".pn. and (order sequence ordered ordering track tracking tracker tracked)	US-PGPUB; USPAT	OR	ON	2019/11/11 12:45
L5	1	"20080126357".pn. and (error correct$)	US-PGPUB; USPAT	OR	ON	2019/11/11 13:06
L6	1	"20080126357".pn. and (error correct$ crc track tracker tracking tracked compres$)	US-PGPUB; USPAT	OR	ON	2019/11/11 13:20
L7	1	"20080126357".pn. and (error correct$ crc track tracker tracking tracked compres$ encrypt$ crypto$)	US-PGPUB; USPAT	OR	ON	2019/11/11 13:21
L8	1	"20080126357".pn. and (compact$)	US-PGPUB; USPAT	OR	ON	2019/11/11 13:26
S1	3986	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S2	1246	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S3	2045	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S4	49	("5126964" | "5930466" | "8046044" | "8046044" | "8225233" | "20060079755" | "20100156761" | "20120011474" | "3774161" | "3886359" | "4056846" | "4138721" | "4216526" | "4228468" | "4228495" | "4258273" | "4279199" | "4342916" | "4378022" | "4404684" | "4418383" | "4458203" | "4468748" | "4472818" | "4479205" | "4555763" | "4557019" | "4559597" | "4580215" | "4582491" | "4608977" | "4630193" | "4630202" | "4631585" | "4651096" | "4674046" | "4707661" | "4718432" | "4731839" | "4733187" | "4739308" | "4739352" | "4742480" | "4748887" | "4751587" | "4763279" | "4767992" |	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:57

		"4789929" | "4791590" | "4817187").PN.				
S5	44	("20110182424" | "20110182429" | "20110185193" | "20020016961" | "20030028879" | "20100266120" | "20100269008" | "20100287200" | "20110026842" | "20110029742" | "20110029809" | "20110055661" | "20110072210" | "20110072321" | "20110078080" | "20110078373" | "20110083053" | "20110055661" | "20110072210" | "20110072321" | "20110078080" | "20110078373" | "20110083053" | "20110107027" | "20110107165" | "20110107180" | "20110107181" | "20110107184" | "20110107185" | "20110107380" | "20110122523" | "20110125771" | "20110126026" | "20110126295" | "20110161655" | "20110161680" | "20110161681" | "20110161781" | "20110184997" | "20110185253" | "20110185258" | "20110213929" | "20110214011" | "20110225362" | "20110228931" | "20110231699" | "20110231733" | "20110261839" | "20110264717" | "20110264823").PN.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:57
S6	1	"20110185193".pn. and (aont transformation)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:49
S7	158	(aont nothing near4 transformation)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:50
S8	63	(aont nothing near4 transformation) and (encrypt$ crypto$)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:50
S9	63	(US-20120255035-$ or US-20120255034-$ or US-20120226904-$ or US-20120222134-$ or US-20120221856-$ or US-20120221855-$ or US-20120221854-$ or US-20120198241-$ or US-20120179916-$ or US-20120173883-$ or US-20120170750-$ or US-20120166818-$ or US-20120166815-$ or US-20120166576-$ or US-20120159197-$ or US-20120124366-$ or US-20120110346-$ or US-20120072723-$ or US-20120054747-$ or US-20110314346-$ or US-20110314154-$ or US-20110314072-$ or US-20110314058-$ or US-20110311051-$ or US-20110296440-$ or US-20110258439-$).did. or (US-20110246817-$ or US-20110246766-$ or US-20110202763-$ or US-20110202755-$ or US-20110185193-$ or US-20110182429-$ or US-20110182424-$ or US-20110107112-$ or US-20100299313-$ or US-20100269008-$ or US-20100268966-$ or US-20100266120-$ or US-20100266119-$ or US-20100098255-$ or US-20090177894-$ or US-20090158052-$ or US-20090097661-$ or US-20080183992-$ or US-20070226145-$ or US-20070219915-$ or US-20070160198-$ or US-	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:51

		20060177061-$ or US-20050118141-$ or US-20040141613-$).did. or (US-8320560-$ or US-8300828-$ or US-8271802-$ or US-8266438-$ or US-8135134-$ or US-8121294-$ or US-8060877-$ or US-8009830-$ or US-7913093-$ or US-7840487-$ or US-7457419-$ or US-7260820-$ or US-7220891-$).did.				
S10	63	S9 and S7	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:52
S11	138668	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:51
S12	138667	(desequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:52
S13	17416	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram frame)	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:52
S14	2808	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame)	US-PGPUB; USPAT	OR	ON	2012/12/09 14:53
S15	37	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering re-order)	US-PGPUB; USPAT	OR	ON	2012/12/09 14:54
S16	474	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order)	US-PGPUB; USPAT	OR	ON	2012/12/09 14:54
S17	3	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation disper$ near4 storage near4 error)	US-PGPUB; USPAT	OR	ON	2012/12/09 16:12
S18	3	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering	US-PGPUB; USPAT	OR	ON	2012/12/09 16:12

		reordering order re-order) and (nothing adj transformation disper$ near4 error)				
S19	338	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation error crc)	US-PGPUB; USPAT	OR	ON	2012/12/10 08:29
S20	205	dispers$ near5 storage near4 error	US-PGPUB; USPAT	OR	ON	2012/12/10 08:32
S23	174	dispers$ adj storage near4 error near5 (encrypt$ decrypt$ crypto$ encod$ decod$)	US-PGPUB; USPAT	OR	ON	2012/12/10 08:33
S24	5	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (dispers$ near4 storage)	US-PGPUB; USPAT	OR	ON	2012/12/10 12:43
S25	38	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (distribut$ near4 storage)	US-PGPUB; USPAT	OR	ON	2012/12/10 12:45
S26	9128	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:28
S27	980	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:28
S28	77	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (reorder$)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:29
S29	263	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble	US-PGPUB; USPAT	OR	ON	2013/03/24 21:55

		assembling)				
S30	260	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2013/03/24 22:11
S31	4186	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S32	1295	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S33	2124	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S34	1	"7457415".pn.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:28
S35	37	("4736420" | "4742544" | "4947447" | "5014310" | "5049990" | "5113443" | "5195134" | "5351299" | "5392072" | "5420866" | "5479512" | "5546461" | "5621799" | "5625416" | "5701391" | "5706346" | "5734755" | "5764994" | "5802520" | "5926624" | "6035068" | "6041160" | "6061451" | "6064748" | "6081785" | "6101195" | "6157606" | "6266299" | "6285774" | "6349088" | "6392705" | "6529553").PN. OR ("7457415").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/24 22:28
S36	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2013/03/24 23:22
S37	502	cleversafe.as.	US-PGPUB; USPAT	OR	ON	2014/05/15 08:43
S38	135	cleversafe.as.	USPAT	OR	ON	2014/05/15 08:44
S39	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 08:58
S40	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad	US-PGPUB; USPAT	OR	ON	2014/05/15 09:44

		@ad)<"20101128"				
S41	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:45
S42	132	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame slice) same (sequence sequencing index auxiliary metadata) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:46
S43	0	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame slice) and transmit$ near6 (index) near8 content and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:48
S44	2	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame slice) and transmit$ near6 (vector order) near8 content and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:49
S45	1669	G06F11/1008.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:09
S46	1294	G06F21/72.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:09
S47	1163	G06F21/80.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S48	1258	G06F21/85.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S49	743	H04L9/3242.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S50	742	(distributed dispersed) adj storage adj network	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:24
S51	405	(distributed dispersed) adj storage adj network.clm.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:24
S52	332	(distributed dispersed) adj storage adj network.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:25
S56	27	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and encrypted.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:27
S57	30	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch	US-PGPUB; USPAT	OR	ON	2014/10/05 11:27

		leggette).in.				
S58	5	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:30
S59	5365	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S60	1545	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S61	2686	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S62	1781	G06F11/1008.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S63	1402	G06F21/72.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S64	1185	G06F21/80.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S65	1332	G06F21/85.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S66	806	H04L9/3242.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S67	4	(G06F21/85 and H04N21/2347 and H04N21/222 and H04N21/8456 and H04L9/3242 and G06F21/72 and G06F21/80 and H04L67/1097 and H04L65/604 and G06F2211/1028 and H04W12/02 and G06F2221/2107 and G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:51
S68	23270	(G06F21/85 H04N21/2347 H04N21/222 H04N21/8456 H04L9/3242 G06F21/72 G06F21/80 H04L67/1097 H04L65/604 G06F2211/1028 H04W12/02 G06F2221/2107 G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:51
S72	1627	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:42
S73	39916	(G06F21/85 or G06F3/067 or G06F3/0647 or G06F11/1076 or G06F3/0619 or H04L67/1097 or G06F21/72 or H04N21/222 or G06F21/80 or H04N21/8456 or H04L9/3242 or H04N21/2347 or H04L65/604 or H04W12/02 or G06F2211/1028 or G06F11/1008 or G06F2221/2107).cpc.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:42
S74	5962	713/193.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S75	44	("20110214011" | "20110213928" |	US-	OR	OFF	2015/09/25

		"20110213929" | "20030225970" | "20060010290" | "20070294565" | "20110225451" | "20010026677" | "20050031042" | "20100260262" | "20100268692" | "20100332751" | "20110026842" | "20110029711" | "20110029742" | "20110029809" | "20110029836" | "20110055661" | "20110072210" | "20110078080" | "20110078373" | "20110078774" | "20110083053" | "20110055661" | "20110072210" | "20110078080" | "20110078373" | "20110078774" | "20110083053" | "20110106855" | "20110106904" | "20110106972" | "20110106973" | "20110107026" | "20110107027" | "20110107036" | "20110107078" | "20110107094" | "20110107113" | "20110107165" | "20110107180" | "20110107181" | "20110107182" | "20110107184" | "20110107185" | "20110107380" | "20110122523" | "20110125771" | "20110126026" | "20110126060").PN.	PGPUB; USPAT			21:43
S76	4000	380/28.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S77	549	380/268.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S78	1097	380/279.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S79	46	("7505535" | "7207224" | "7907722" | "7907722" | "8098952" | "9125609" | "4882737" | "5148479" | "5373372" | "5430830" | "5602638" | "5768159" | "7200233" | "7483058" | "7774272" | "7792067" | "7933218" | "8014479" | "8085283" | "7933218" | "8014479" | "8085283" | "8094813" | "8300809" | "8379523" | "8429414" | "8437870" | "8588423" | "8670430" | "8891370" | "8924983" | "8983787" | "9064438" | "3555184" | "3555195" | "3555204" | "3555251" | "3555255" | "3555259" | "3556007" | "3557308" | "3557314" | "3557349" | "3557354" | "3557355" | "3557357" | "3557673" | "3558811" | "3558820" | "3558823").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S80	4044	S75 S76	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S81	90	S75 S79	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S82	2450	714/763.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:46
S83	479	(desequencing de-sequencing de near3 sequencing sequencing interspersing)	US-PGPUB;	OR	ON	2015/09/25 21:53

		near5 (data slice) near8 stream	USPAT			
S84	609	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet) near8 stream	US-PGPUB; USPAT	OR	ON	2015/09/25 21:53
S85	499	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet) near8 stream and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/25 21:53
S86	105	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet segment part portion section) near8 stream and encrypt$ near5 (data slice packet segment part portion section)and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/25 21:54
S87	105	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet segment part portion section) near8 stream and encrypt$ near5 (data slice packet segment part portion section) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/25 21:54
S88	13930	reed adj solomon adj code	US-PGPUB; USPAT	OR	ON	2015/09/27 11:31
S89	0	reed adj solomon adj code and distribution adj matrix and identity adj matrix	US-PGPUB; USPAT	OR	ON	2015/09/27 11:33
S90	6	reed adj solomon adj code and distribution adj matrix	US-PGPUB; USPAT	OR	ON	2015/09/27 11:33
S93	26	reed adj solomon adj code and (distribution identity) adj matrix and galois and (disperse dispersed distributed) near6 storage	US-PGPUB; USPAT	OR	ON	2015/09/27 11:35
S94	1	"8959366".pn.	US-PGPUB; USPAT	OR	ON	2015/09/27 11:37
S95	33	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 11:57
S96	1752	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S97	666	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S98	237	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S99	1	distributed adj storage.clm. and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet	USPAT	OR	ON	2015/09/27 13:03

		segment)				
S100	11	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet segment)	USPAT	OR	ON	2015/09/27 13:04
S104	134	(dispersed distributed) adj storage adj network and encrypt$ near6 (data content) near6 (slice segment part portion section packet) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/27 13:12
S105	2814	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:12
S106	1346	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (slice segment part portion section packet)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:12
S107	1037	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (slice segment part portion section packet) and (error near3 (code encode coding encoding) parity near3 check)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:13
S108	39	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (random$ pseudorandom$) near8 (order ordering ordered reorder reordered reordering sequence sequencing) near6 (slice segment part portion section packet) and (error near3 (code encode coding encoding) parity near3 check)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:14
S109	1	"20140344645".pn. and readable	US-PGPUB; USPAT	OR	ON	2015/09/27 17:11
S110	1	"20140344645".pn. and (media medium)	US-PGPUB; USPAT	OR	ON	2015/09/27 17:12
S111	1	"20140344645".pn. and nothing	US-PGPUB; USPAT	OR	ON	2015/09/27 17:42
S112	0	"all or nothing"	US-PGPUB; USPAT	OR	ON	2015/09/27 17:43
S113	78	("20020062422" | "20020166079" | "20030018927" | "20030037261" | "20030065617" | "20030084020" | "20040024963" | "20040122917" | "20040215998" | "20040228493" | "20050100022" | "20050114594" | "20050125593" | "20050131993" |	US-PGPUB; USPAT	OR	ON	2015/09/27 17:51

		"20050132070" | "20050144382" | "20050229069" | "20060047907" | "20060136448" | "20060156059" | "20060224603" | "20070079081" | "20070079082" | "20070079083" | "20070088970" | "20070174192" | "20070214285" | "20070234110" | "20070283167" | "20090094251" | "20090094318" | "20100023524" | "4092732" | "5454101" | "5485474" | "5774643" | "5802364" | "5809285" | "5890156" | "5987622" | "5991414" | "6012159" | "6058454" | "6128277" | "6175571" | "6192472" | "6256688" | "6272658" | "6301604" | "6356949" | "6366995" | "6374336" | "6415373" | "6418539" | "6449688" | "6567948" | "6571282" | "6609223" | "6718361" | "6760808" | "6785768" | "6785783" | "6826711" | "6879596" | "7003688" | "7024451" | "7024609" | "7080101" | "7103824" | "7103915" | "7111115" | "7140044" | "7146644" | "7171493" | "7222133" | "7240236" | "7272613" | "7636724").PN.				
S114	338	("5485474").URPN.	USPAT	OR	OFF	2015/09/27 18:33
S115	1	"8626820".pn.	US-PGPUB; USPAT	OR	OFF	2015/09/27 20:43
S116	0	"20080263113".pn. and error	US-PGPUB; USPAT	OR	OFF	2016/03/18 21:55
S117	1	"20080263113".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/18 21:56
S118	5	dispersed near4 storage near4 error and encoding near4 auxiliary near4 data	US-PGPUB; USPAT	OR	OFF	2016/03/18 22:16
S119	43	distributed near4 storage and error near4 encoding and auxiliary near4 data	US-PGPUB; USPAT	OR	OFF	2016/03/18 22:20
S120	32	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 slice	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S121	36	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 (slice portion section part segment)	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S122	36	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 (slice portion section part segment fragment)	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S123	573	information adj dispersal and error adj encoding	US-PGPUB; USPAT	OR	ON	2016/03/18 22:34
S125	151	information adj dispersal and encrypt$ and error adj encoding and (@pd @prad @rlad @ptad @ad)< "20100128"	US-PGPUB; USPAT	OR	ON	2016/03/18 22:42
S126	5933	713/189.ccls.	US-	OR	OFF	2016/03/19

			PGPUB; USPAT			21:56
S127	1632	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2016/03/19 21:56
S128	2927	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2016/03/19 21:56
S129	30886	(G06F21/85 H04N21/2347 H04N21/222 H04N21/8456 H04L9/3242 G06F21/72 G06F21/80 H04L67/1097 H04L65/604 G06F2211/1028 H04W12/02 G06F2221/2107 G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2016/03/19 21:59
S130	1	"20080263113".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/24 09:47
S131	77	(intersper$ scatter$ intermix$) near6 (slice packet datagram) near8 (encrypted encoded)	US-PGPUB; USPAT	OR	ON	2016/03/24 10:03
S132	70	(intersper$ scatter$ intermix$) near6 (slice packet datagram) near8 (encrypted encoded) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/03/24 10:04
S133	23	(random$ pseudorandom$) near6 (order ordering ordered) near6 (slice packet datagram) near8 (encrypted encoded) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2016/03/24 10:29
S134	1	"8626820".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/24 10:42
S135	1284	information adj dispersal adj algorithm	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:32
S136	823	information adj dispersal adj algorithm and data near6 (slice slices portion section segment) near8 metadata	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:33
S137	334	information adj dispersal adj algorithm and data near6 (slice slices portion section segment) near8 metadata and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:33
S138	338	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:34
S139	305	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and error near6 (encoding encoded encode) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:34
S140	313	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and error near6 (encoding encoded encode) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/09/28 21:34
S141	47	threshold near8 (recover$ recreat$) near8 (share) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 15:49

S142	1	"6690795".pn.	US-PGPUB; USPAT	OR	ON	2016/10/10 16:28
S143	9	threshold near8 (recover$ recreat$) near8 (share) and reed adj solomon and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 16:31
S144	15	threshold near8 (recover$ recreat$) near8 (share) and (reed adj solomon fec error adj correct$) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 16:32
S145	5	jigdfs	US-PGPUB; USPAT	OR	ON	2016/10/10 16:54
S146	61384	(G06F21/85 or G06F11/1076 or G06F3/0647 or G06F3/0619 or G06F3/067 or H04L67/1097 or H04N21/2347 or H04N21/8456 or G06F21/72 or H04N21/222 or H04L9/3242 or G06F21/80 or H04L65/604 or H04W12/02 or G06F11/1008 or G06F2221/2107 or G06F2211/1028).cpc.	US-PGPUB; USPAT	OR	OFF	2018/02/13 09:53
S147	1	"7574579".pn.	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:09
S148	0	"7574579".pn. and error	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S149	1	"7574579".pn. and integrity	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S150	0	"7574579".pn. and (mac hmac)	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S151	1	"7574579".pn. and (code)	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S152	1	"20130272164".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 13:13
S153	1	"20170272942".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 13:13
S154	0	"20130272164".pn. and (pair pairing)	US-PGPUB; USPAT	OR	ON	2018/02/13 13:20
S155	1	"20170272942".pn. and (pair pairing)	US-PGPUB; USPAT	OR	ON	2018/02/13 13:21
S156	456	(dispersed distributed) adj storage adj network and encrypt$ near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 14:09
S157	278	error near6 (encode encoding encoded) near8 (encrypted) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 16:28
S158	466	error near6 (encode encoding encoded) near8 (encrypted) and (@pd @prad @rlad	US-PGPUB;	OR	ON	2018/02/13 16:28

		@ptad @ad)<"20140805"	USPAT			
S159	1	("20040172371").pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 17:08
S160	19	(encrypted) near6 interspersed near3 error and (@pd @prad @rlad @ptad @ad) <"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:09
S161	276	(encrypted) near6 integrity near3 code and (@pd @prad @rlad @ptad @ad) <"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:57
S162	185	(encrypted) near6 integrity near3 code and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:57
S163	32	(intersper$) near3 error near6 (correction correcting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 21:12
S164	38	(intersper$) near3 error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 21:13
S165	23	program near3 (id identifier) and (cervetti.xa. cervetti.xp.)	US-PGPUB; USPAT	OR	ON	2018/02/13 21:17
S166	1	program near3 (id identifier) and "20070263864".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 21:18
S167	1	program near3 (id identifier) and "20030123664".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 21:21
S168	12	program near3 (id identifier) and error and (cervetti.xa. cervetti.xp.)	US-PGPUB; USPAT	OR	ON	2018/02/13 21:22
S169	981	(distributed dispersed) adj storage adj network.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/02/16 13:11
S170	1	"8275132".pn.	US-PGPUB; USPAT	OR	OFF	2018/02/17 07:57
S171	5359	data near5 (dispersal dispersion dispersing dispersed) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/17 09:06
S173	76	data near5 (dispersal dispersion dispersing dispersed) near8 (encrypt$ crypto$) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/17 09:07
S174	480	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation error crc)	US-PGPUB; USPAT	OR	ON	2018/06/21 20:40
S175	214	(dispersed distributed disperse) adj storage adj network and (encrypt$ crypto$) near6 (data content) near6 (slice segment part	US-PGPUB; USPAT	OR	ON	2018/07/08 11:13

		portion section packet) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad)<"20100128"				
S176	548	(dispersed distributed) adj storage adj network and encrypt$ and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/06 15:15
S177	201	data near5 (dispersal dispersion dispersing dispersed) near8 (encrypt$ crypto$) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/08/06 17:09
S178	550	reed adj solomon adj code and (distribution identity) adj matrix	US-PGPUB; USPAT	OR	ON	2018/08/07 10:44
S179	0	rehm.xp.	US-PGPUB; USPAT	OR	ON	2018/08/07 10:50
S180	44	rehm.xa.	US-PGPUB; USPAT	OR	ON	2018/08/07 10:50
S181	663	(dispersed distributed) adj storage adj network and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/07 20:12
S182	1659	dispers$ near5 storage near4 error near5 (encrypt$ decrypt$ crypto$ encod$ decod$)	US-PGPUB; USPAT	OR	ON	2018/08/07 20:45
S183	1658	dispers$ near5 storage near4 error near5 (encod$ decod$)	US-PGPUB; USPAT	OR	ON	2018/08/07 20:45
S184	1	"10000000".pn.	US-PGPUB; USPAT	OR	ON	2018/08/07 20:57
S185	1116	speed near4 light near4 faster	US-PGPUB; USPAT	OR	ON	2018/08/07 20:59
S186	588	speed near4 light near4 faster and (@pd @prad @rlad @ptad @ad)>"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/07 21:00
S187	859	(distributed dispersed) adj storage adj network.clm. and error.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/08/07 22:01
S188	851	(distributed dispersed) adj storage adj network.clm. and error.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	OFF	2018/08/07 22:02
S189	312	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	OFF	2018/08/07 22:02
S190	859	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/08/07 22:17
S191	208	reed adj solomon adj code and (distribution identity) adj matrix and galois	US-PGPUB;	OR	ON	2018/08/08 09:02

			USPAT			
S192	401	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling)	US-PGPUB; USPAT	OR	OFF	2018/08/08 09:57
S193	46	laforgia.xa.	US-PGPUB; USPAT	OR	OFF	2018/08/08 21:17
S194	368	laforgia.xp.	US-PGPUB; USPAT	OR	OFF	2018/08/08 21:17
S195	248	information adj dispersal and error adj encoding and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/09 08:38
S196	8	("8677214" "9076138" "9021263" "8918897" "8744071" "8782494" "8856617" "9128870").pn.	USPAT	OR	OFF	2018/12/03 06:19
S199	94868	(G06F21/85 or G06F21/6218 or G06F21/606 or H04L9/0894 or H04W12/0013 or H04N21/222 or H04N21/2347 or H04N21/8456 or G06F11/1076 or G06F21/72 or G06F21/80 or H04L67/1097 or G06F3/0619 or G06F3/0647 or G06F3/067 or H04L9/3242 or G06F2221/2107 or G06F11/1008 or H04W12/02 or G06F2211/1028 or H04L65/604).cpc.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:12
S200	94868	(G06F21/85 G06F21/6218 G06F21/606 H04L9/0894 H04W12/0013 H04N21/222 H04N21/2347 H04N21/8456 G06F11/1076 G06F21/72 G06F21/80 H04L67/1097 G06F3/0619 G06F3/0647 G06F3/067 H04L9/3242 G06F2221/2107 G06F11/1008 H04W12/02 G06F2211/1028 H04L65/604).cpc.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:13
S201	2	"8959366".pn. "10282564".pn.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:56
S202	152	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation)	US-PGPUB; USPAT	OR	OFF	2019/06/26 09:20
S203	165	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation)	US-PGPUB; USPAT	OR	ON	2019/06/26 09:20
S205	121	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and error near6 (encode encoded encoding)	US-PGPUB; USPAT	OR	ON	2019/06/26 09:21
S206	23	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding).clm. and (obfuscate obfuscating obfuscated obfuscation).clm. and error near6 (encode	US-PGPUB; USPAT	OR	ON	2019/06/26 09:22

		encoded encoding).clm.				
S207	52	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and (data error information content) near6 (encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 09:36
S208	62	information near3 dispersal near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content) near6 (encode encoded encoding) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 09:46
S209	65	information near3 dispersal near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 09:47
S210	74	(data information) near3 (dispersal dispersing dispersion disperse dispersed) near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 10:01
S211	133	(data information) near3 (scater scattering scattered split splitting dispersal dispersing dispersion disperse dispersed) near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 10:03
S212	623	vmac	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S213	291	vmac and wireless	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S214	269	vmac and wireless and virtual$	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S215	3017	vmac vnic	US-PGPUB; USPAT	OR	ON	2019/06/26 10:11
S216	96	vmac and vnic	US-PGPUB; USPAT	OR	ON	2019/06/26 10:11
S217	2	("8327141" "20100199089").pn. and (data information) near3 (scater scattering scattered split splitting dispersal dispersing dispersion disperse dispersed) near3	US-PGPUB; USPAT	OR	ON	2019/06/26 11:37

		algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"				
S218	1913	dispersed adj storage adj error	US-PGPUB; USPAT	OR	ON	2019/06/26 12:08
S219	1654	dispersed adj storage adj error adj encoding	US-PGPUB; USPAT	OR	ON	2019/06/26 12:09
S220	17	dispersed adj storage adj error adj encoding and auxiliary adj data	US-PGPUB; USPAT	OR	ON	2019/06/26 12:09
S221	1653	dispersed adj storage adj error adj encoding and encrypt$	US-PGPUB; USPAT	OR	ON	2019/06/26 12:10
S222	75	dispersed adj storage adj error adj encoding and encrypt$ and (obfuscate obfuscation)	US-PGPUB; USPAT	OR	ON	2019/06/26 12:10
S223	4	dispersed adj storage adj error adj encoding and encrypt$ and (obfuscate obfuscation) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 12:10
S224	166	dispersed adj storage adj error adj encoding and encrypt$ and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 12:11
S225	154	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and data near6 (encode encoded encoding)	US-PGPUB; USPAT	OR	ON	2019/06/26 15:13
S226	224	reed adj solomon adj code and (distribution identity) adj matrix and galois	US-PGPUB; USPAT	OR	ON	2019/06/26 18:26
S227	2	("20080126357" "20050002531").pn.	US-PGPUB; USPAT	OR	ON	2019/06/26 21:11
S228	1	"20190108366".pn. and (other possible could)	US-PGPUB; USPAT	OR	OFF	2019/09/05 21:11
S229	1	"20190108366".pn. and (dispersed storage error encoding)	US-PGPUB; USPAT	OR	OFF	2019/09/05 21:17
S230	16494	(random randomly) near5 (delay delayed delaying)	US-PGPUB; USPAT	OR	OFF	2019/09/05 22:27
S231	204	(random randomly) near5 (delay delayed delaying) and sql	US-PGPUB; USPAT	OR	OFF	2019/09/05 22:27
S232	2	(random randomly) near5 (delay delayed delaying) and sql near5 injection	US-PGPUB; USPAT	OR	OFF	2019/09/05 22:28

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S69	8	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:27
S70	1	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:28
S71	1	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:30
S197	187	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling)	USPAT	OR	OFF	2018/12/03 08:30
S198	119	information adj dispersal and encrypt$ and error adj encoding and (@pd @prad @rlad @ptad @ad)< "20100128"	USPAT	OR	ON	2018/12/03 08:41

11/11/2019 1:40:46 PM
C:\Users\dcervetti\Documents\EAST\Workspaces\16-197-275-06-26-2019-14452182-09252015-12954880-12042012.wsp

FNT-based **Reed-Solomon** erasure codes

A Soro, J Lacan - 2010 7th IEEE Consumer Communications ..., 2010 - ieeexplore.ieee.org

... Abstract—This paper presents a new construction of Maximum-Distance Separable (MDS) **Reed-Solomon** erasure codes based on Fermat Number ... These codes can be used as the basic component of the **Information Dispersal Algorithm** (IDA) system used in a several P2P ...

☆ 99 Cited by 27 Related articles All 15 versions

Information dispersal algorithm based on **Reed-Solomon** code [J]

HJ Wu, WW Chen - Journal of Computer Applications, 2010 - en.cnki.com.cn

Information Dispersal Algorithm (IDA) based on **Reed-Solomon** (RS) code can be used in high strong and reliable distributed storage system. The encoding/decoding speed is an important criterion for the availability of the RS code. Firstly the erasure principium of RS ...

☆ 99 Cited by 2 Related articles »

Asynchronous verifiable information dispersal

C Cachin, S Tessaro - 24th IEEE Symposium on Reliable ..., 2005 - ieeexplore.ieee.org

... data. The classic alternative, as proposed by Rabin [19], is an **information dispersal algorithm** (IDA): using an erasure code, the data is split into blocks, so that each server holds exactly one block, and so that only a subset of the blocks is needed in order to reconstruct the data ...

☆ 99 Cited by 70 Related articles All 15 versions

General information dispersal algorithms

P Béguin, A Cresti - Theoretical computer science, 1998 - Elsevier

... to reconstruct the file. Observe that in this case d = {A: IAI 2 m}. The algorithm described is a simple version of Rabin's **information dispersal algorithm**, and it is based on **Reed Solomon** erasure codes. The information f EF to ...

☆ 99 Cited by 14 Related articles All 5 versions

Scheme for information dispersal and reconstruction

MO Rabin - US Patent 5,485,474, 1996 - Google Patents

US5485474A - Scheme for information dispersal and reconstruction - Google Patents. Scheme for information dispersal and reconstruction. Download PDF Info. Publication number US5485474A. US5485474A US07/702,110 ...

☆ 99 Cited by 1165 Related articles All 2 versions »

Distributed backup through information dispersal

G Bella, C Pistagna, S Riccobene - Electronic Notes in Theoretical ..., 2006 - Elsevier

... This uses Cauchy **Reed Solomon** codes instead [6], which appear to be more space-efficient than other forward error-correction codes. 2.1 IDA In 1989, Rabin proposed IDA (**Information Dispersal Algorithm**) [9], an al- gorithm whose name explains the main goal ...

☆ 99 Cited by 7 Related articles All 5 versions

Secret sharing made short

H Krawczyk - Annual International Cryptology Conference, 1993 - Springer

... Remark: For completeness, we outline the following simple information disper- sal scheme based on **Reed Solomon** erasure codes ... We assume a generic **information dispersal algorithm** that we denote by IDA, and which works for parameters n (number of file fragments) and m ...

☆ 99 Cited by 396 Related articles All 14 versions »

Performance of balanced disk array schemes

WA Burkhard, KC Claffy... - [1991] Digest of Papers ..., 1991 - ieeexplore.ieee.org

... Performance of balanced disk array schemes. Abstract: The balanced **information dispersal algorithm** (BIDA) provides attractive reliability enhancements as well as modest performance gains for the storage of data at a number of storage sites ...

☆ 99 Cited by 4 Related articles All 2 versions

Grid Based Pervasive Distributed Storage

D Arias, J Sanabria, W Rivera - 2007 2nd International ..., 2007 - ieeexplore.ieee.org

... **Information dispersal algorithm** shows a better access reliability than the simple replication algorithm as shown in Figure 2. As a reference point, for an access reliability R = 0.9 when the probability of failure is p = 0.4 and m = 8, the ... IDA vs **Reed-Solomon** - Dispersal Operation ...

☆ 99 Cited by 4 Related articles All 8 versions

Digital fountains: A survey and look forward

M Mitzenmacher - Information Theory Workshop, 2004 - ieeexplore.ieee.org

... An alternative paradigm was introduced in [3], based on the idealized solution ofa dig- ital fountain (similar in spirit but iiiore expansive than the similar idea of the **information dispersal algorithm** [23, 271) ... DIGITAL FOUNTAIN CONSTRUCTIONS A. **REED-SOLOMON** CODES ...

☆ 99 Cited by 334 Related articles All 11 versions »

Related searches

reed solomon **code** information dispersal algorithm

fermat number information dispersal algorithm

cloud computing information dispersal algorithms

optimal information dispersal

fast decoding of reed solomon **codes**

information dispersal **remainder theorem**

efficient dispersal **of** information

information dispersal **latency targets**

information dispersal **burst error channel**

number theoretic transforms reed solomon **codes**

information dispersal **reliable communication**

information dispersal **computer networks**

distributed data storage information dispersal algorithms

high security information dispersal algorithm

storage system information dispersal algorithm

information dispersal **network overlays**

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/197,275	Filing Date 11/20/2018	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	08/27/2019	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 16	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/PEARLIE A FENNELL/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

1st Named Inventor:	Jason K. Resch	**Examiner:**	CERVETTI, DAVID GARCIA
Application No.:	16/197,275	**Art Unit:**	2436
Filing Date:	20 Nov 2018	**Docket No.:**	CS00403_END920165769 US09
Confirmation No.:	4290		
Title:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE		

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS

I. To authorize permission for Internet Communications.

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03).

I am the attorney or agent of record. Registration No. 73072.

RESPECTFULLY SUBMITTED,

By: /Patricia A. Markison/Reg. No. 73072
Patricia A. Markison

Garlick & Markison
100 Congress Avenue, Suite 2000
Austin, TX 78701
Phone: (808) 283-3608
E-mail: pmarkison@texaspatents.com

Electronic Acknowledgement Receipt

EFS ID:	36993179
Application Number:	16197275
International Application Number:	
Confirmation Number:	4290
Title of Invention:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE
First Named Inventor/Applicant Name:	Jason K. Resch
Customer Number:	89322
Filer:	Patricia A. Markison/Kimberly Brown
Filer Authorized By:	Patricia A. Markison
Attorney Docket Number:	CS00403
Receipt Date:	27-AUG-2019
Filing Date:	20-NOV-2018
Time Stamp:	15:50:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		CS00403_END920165769US09_NFOA_Response.pdf	165992 70ce8d6e908ae00e7a6c366f8d32843bddc97f89	yes	17

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	10
	Applicant Arguments/Remarks Made in an Amendment	11	16
	Internet Communications Authorized	17	17
Warnings:			
Information:			
	Total Files Size (in bytes):	165992	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Certification under 37 C.F.R. §1.8

Date of Mailing or Transmission: 8/27/2019

I hereby certify that I have caused the document indicated herein on the date indicated above to be transmitted via the Office electronic filing system in accordance with 37 C.F.R. §1.6(a)(4).

BY: /Kimberly Brown/ (Signature) **Name:** Kimberly Brown (Typed Name)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

1st Named Inventor:	Jason K. Resch	**Examiner:**	CERVETTI, DAVID GARCIA
Application No.:	16/197,275	**Art Unit:**	2436
Filing Date:	20 Nov 2018	**Docket No.:**	CS00403_END920165769 US09
Confirmation No.:	4290		
Title:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE		

RESPONSE TO NON-FINAL OFFICE ACTION

Date: 8/27/2019

United States Patent and Trademark Office
P. O. Box 1450
Alexandria, VA 22313-1450

In response to an office action dated July 02, 2019 regarding the above-captioned patent application, the Applicant respectfully submits the following amendment and response, which is being filed within three (3) months of the mailing date thereof.

The three (3) month due date for responding to the office action falls on October 02, 2019, and the Applicant respectfully asserts that this amendment and response being filed on or before October 02, 2019 is timely filed in accordance with M.P.E.P. §710.05, 35 U.S.C. §21, and 37 C.F.R. §1.7.

AMENDMENT TO THE CLAIMS

1. (Original) A method comprises:

dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices;

dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices;

obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices;

obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and

outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage.

2. (Original) The method of claim 1 further comprises:

dispersed storage error encoding, by the computing device, the auxiliary data to produce a second set of encoded auxiliary data slices;

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 47
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

obfuscating, by the computing device, the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices; and

obfuscating, by the computing device, the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

3. (currently amended) The method of claim 1, wherein the auxiliary data comprises one or more of:

null data;

authentication information;

a next pseudo random output sequencing order;

a pseudo random output sequencing order identifier;

a next outputting threshold;

a random number generator output;

an encryption key;

a starting point for the pseudo random output sequencing order;

a device identifier;

a data identifier;

a data type;

a data size ~~indictor~~ <u>indicator</u>;

a priority indicator;

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 48
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

a security indicator; and

a performance indicator.

4. (Original) The method of claim 1 further comprises:

encrypting, by the computing device, the plurality of data segments to produce a plurality of encrypted data segments; and

dispersed storage error encoding, by the computing device, the plurality of encrypted data segments to produce the plurality of sets of encoded data slices.

5. (Original) The method of claim 4 further comprises:

encrypting, by the computing device, the auxiliary data to produce encrypted auxiliary data; and

dispersed storage error encoding, by the computing device, the encrypted auxiliary data to produce the set of encoded auxiliary data slices.

6. (Original) The method of claim 5, wherein the auxiliary data is encrypted via an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data.

7. (Original) The method of claim 5, wherein the auxiliary data is encrypted via an all or nothing transformation to produce the encrypted auxiliary data and the plurality of data segments

is encrypted via an all or nothing transformation to produce the plurality of encrypted data segments.

8. (Original) The method of claim 1, wherein the obfuscating the first set of encoded data slices comprises:

interspersing, by the computing device, the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order to produce the first set of obfuscated encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 50
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

9. (Original) A computing device of a dispersed storage network (DSN), the computing device comprises:

an interface;

memory; and

a processing module operably coupled to the memory and the interface, wherein the processing module is operable to:

dispersed storage error encode a plurality of data segments to produce a plurality of sets of encoded data slices;

dispersed storage error encode auxiliary data to produce a set of encoded auxiliary data slices;

obfuscate a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices;

obfuscate a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and

output the first and second sets of obfuscated encoded data slices for storage.

10. (Original) The computing device of claim 9, wherein the processing module is further operable to:

dispersed storage error encode the auxiliary data to produce a second set of encoded auxiliary data slices;

obfuscate the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices; and

obfuscate the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

11. (currently amended) The computing device of claim 9, wherein the auxiliary data comprises one or more of:

null data;

authentication information;

a next pseudo random output sequencing order;

a pseudo random output sequencing order identifier;

a next outputting threshold;

a random number generator output;

an encryption key;

a starting point for the pseudo random output sequencing order;

a device identifier;

a data identifier;

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 52
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

a data type;

a data size ~~indictor~~ indicator;

a priority indicator;

a security indicator; and

a performance indicator.

12. (Original) The computing device of claim 9, wherein the processing module is further operable to:

encrypt the plurality of data segments to produce a plurality of encrypted data segments; and

dispersed storage error encode the plurality of encrypted data segments to produce the plurality of sets of encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 53
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

13. (Original) The computing device of claim 12, wherein the processing module is further operable to:

encrypt the auxiliary data to produce encrypted auxiliary data; and

dispersed storage error encode the encrypted auxiliary data to produce the set of encoded auxiliary data slices.

14. (currently amended) The computing device of claim 13, wherein the processing module is further operable to:

encrypt the auxiliary data <u>via</u> an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data.

15. (Original) The computing device of claim 13, wherein the processing module is further operable to:

encrypt the auxiliary data via an all or nothing transformation to produce the encrypted auxiliary data and encrypt the plurality of data segments via an all or nothing transformation to produce the plurality of encrypted data segments.

16. (Original) The computing device of claim 9, wherein the processing module is further operable to obfuscate the first set of encoded data slices by:

interspersing the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order to produce the first set of obfuscated encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 55
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

REMARKS/ARGUMENTS

1. In the above referenced Office Action:

   a. Status of the claims.

      - Claims 1-16 are pending;
      - Claims 1-16 are rejected;
      - Claims 3, 11 and 14 are objected to.

   b. Claims 3 and 11 have been objected to for informalities;

   c. Claim 14 has been objected to for informalities;

   d. Claims 1-16 have been provisionally rejected under the judicially created obviousness-type double patenting doctrine as being unpatentable over Patent No.'s (8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071, 8885821, 8782494, 8856617 and 9128870);

   e. Claims 1-16 have been rejected under 35 USC §103(a) as being unpatentable over Casanova (U.S. Pub. No. 2008/0126357) and further in view of Michaelsen (U.S. Pub. No. 2005/0002531).

The rejections and objections have been traversed. Applicant respectfully requests reconsideration of the allowability of claims 1-16.

2. Claims 3 and 11 have been objected to for informalities. The Applicant has amended claims 3 and 11 to overcome the present objection.

3. Claim 14 has been objected to for informalities. The Applicant has amended claim 14 to overcome the present objection.

4. Claims 1-16 have been provisionally rejected under the judicially created obviousness-type double patenting doctrine as being unpatentable over Patent No.'s (8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071, 8885821, 8782494, 8856617 and 9128870). The Applicant respectfully disagrees.

MPEP 804(II)(B)(2) states in part that:

"Any non-statutory double patenting rejection made under the obviousness analysis should make clear:

- (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and
- (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of, the invention defined in a claim in the patent.

When considering whether the invention defined in a claim of an application would have been an obvious variation of the invention defined in the claim of a patent, the disclosure of the patent may not be used as prior art. *General Foods Corp. v. Studiengesellschaft Kohle mbH*, 972 F.2d 1272, 1279, 23 USPQ2d 1839, 1846 (Fed. Cir. 1992)."

The M.P.E.P. requires that an obviousness-type double patenting rejection should make clear the differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and the reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of, the invention defined in a claim in the patent.

The Office Action has failed to make clear the differences between the inventions defined by the conflicting claims and the reasons why a person of ordinary skill in the art would conclude that the invention the reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of, the invention defined in a claim in the patent.

The Office Action only compares claim 1 of patent numbers 8959366 and 10282564 with claim 1 of the instant application and states that the claims of the conflicting patents and/or applications contain every element of claims 1-16 of the instant application and thus anticipate the claims of the instant application.

The Office Action fails to cite a claim from Patent No.'s 8677214, 9076138, 9021263, 8649521, 8918897, 8744071, 8885821, 8782494, 8856617 and 9128870 or make clear the

differences between the inventions defined in Patent No.'s 8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071, 8885821, 8782494, 8856617 and 9128870 and the current application as required by M.P.E.P 804. The Office Action also fails to provide reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of, the invention defined in a currently pending claim in the patent application as required by M.P.E.P. 804. As such, the Applicant requests that the rejection citing 8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071, 8885821, 8782494, 8856617 and 9128870 be withdrawn.

5. Claims 1-16 have been rejected under 35 USC §103(a) as being unpatentable over Casanova (U.S. Pub. No. 2008/0126357) and further in view of Michaelsen (U.S. Pub. No. 2005/0002531). The Applicant respectfully disagrees with this rejection and the reasoning thereof.

Casanova teaches at paragraphs 23-31 a distributed file system that operates by partitioning a file into a plurality of fragments, preferably encrypting each fragment, and storing the fragments at a plurality of remote nodes in a network. To assure reliability, each fragment is redundantly stored at a plurality of nodes. For example, a user initiates a request to save or transmit a file. In response to the request, the device partitions the file into a plurality of fragments. The device then transmits the fragments to a variety of remote storage nodes. Optionally, each fragment is encrypted. Preferably, the method and system of invention provides for secure storage of each file; however, the degree of security may vary, depending upon the particular file being saved or transmitted. If a user is storing or transmitting a financial file, for example, each fragment will preferably be encrypted.

Casanova further teaches at paragraphs 53-60 storage and retrieval of fragments where a sending node is configured to send fragments of a file to a plurality of storage nodes and a receiving node is configured to retrieve the segments from one or more of the storage nodes and to create a copy of the original file. The sending node includes a segmenter that segments the file into fragments, and an optional encrytor that encrypts each segment. If the receiving user wants to access the file, the receiving node extracts the information in the file tracker to create a tracking

table that corresponds to the original tracking table at the sending node. A gatherer component is configured to download each fragment in the tracking table by requesting the fragment from one of the identified storage units, SUIDs, assigned to the fragment. If the selected storage unit is not available, or is notable to send the requested fragment, the gatherer selects another storage unit from the list of SUIDs for the fragment and tries again until the fragment is received from at least one of the storage units. If the fragment had been encrypted at the sending node, it is correspondingly decrypted by a decryptor at the receiving node. A collator arranges the fragments in their proper order and provides a copy of the original file.

As such Casanova teaches a distributed file system where files are partitioned into fragments, optionally encrypted, and stored across multiple storage units. Casanova does not teach dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices.

The Applicant's specification defines dispersed storage error encoding in paragraphs 49-50 and paragraphs 63-74. In summary, dispersed storage error encoding involves partitioning a data file into segments, error encoding each segment (e.g., forward error correction (FEC), information dispersal algorithm, or error correction coding) and slicing each error encoded segment into a plurality of error coded (EC) data slices. For example, if a Reed-Solomon (or other FEC scheme) is used in an n/k system, then a data segment is divided into n slices, where k number of slices is needed to reconstruct the original data (i.e., k is the threshold). As a few specific examples, the n/k factor may be 5/3; 6/4; 8/6; 8/5; 16/10. In contrast, in Casanova, files are partitioned and optionally encrypted.

Further, Casanova does not teach dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices. In Casanova, the file is partitioned and stored. While fragments may be stored redundantly, this does not equate to dispersed storage error encoding auxiliary data (e.g., this is some type of extra data that does not include the file data) to produce a set of encoded auxiliary data slices.

Based on the above clarifications, the combination of Casanova and Michaelsen does not render the claims obvious. Therefore, the Applicant believes claims 1-16 overcome the present rejection.

CONCLUSION

For the foregoing reasons, the Applicant believes that claims 1-16 are in condition for allowance and respectfully requests that they be passed to allowance.

The Applicant hereby rescinds any disclaimer of claim scope made in the parent application or any predecessor application in relation to the instant application. The Examiner is advised that any such previous disclaimer and the prior art that it was made to avoid, may need to be revisited. Further, the claims in the instant application may be broader than those of a parent application. Moreover, the Examiner should also be advised that any disclaimer made in the instant application should not be read into or against the parent application.

No additional fees are believed to be due. In the event that additional fees are due or a credit for an overpayment is due, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment to Deposit Account No. 502126.

The Examiner is invited to contact the undersigned by e-mail if the Examiner believes that such a communication would advance the prosecution of the present invention.

RESPECTFULLY SUBMITTED,

By: /Patricia A. Markison/Reg. No. 73072
Patricia A. Markison

Garlick & Markison
100 Congress Avenue, Suite 2000
Austin, TX 78701
Phone: (808) 283-3608
E-mail: pmarkison@texaspatents.com

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 61
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/197,275	11/20/2018	Jason K. Resch	CS00403_END920165769US09	4290

89322 7590 07/02/2019
Garlick & Markison (PST)
100 Congress Avenue, Suite 2000
Austin, TX 78701

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
07/02/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

MMURDOCK@TEXASPATENTS.COM
bpierotti@texaspatents.com

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No. 16/197,275	Applicant(s) Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 20 November 2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 20 November 2018 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 11/26/18.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are pending and have been examined.

Notice of Pre-AIA or AIA Status

2. The present application is being examined under the pre-AIA first to invent provisions.

Claim Objections

3. Claims 3 and 11 are objected to because of the following informalities: "a data size indictor".

4. Claim 14 is objected to because of the following informalities: "encrypt the auxiliary data an encryption". The intended metes and bounds of the claim is unclear. Appropriate correction is required.

Double Patenting

5. Claims 1-16 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of Patent Nos. 8959366, 10282564, 8677214, 9076138, 9021263, 8649521, 8918897, 8744071,8885821, 8782494, 8856617, and 9128870. Although the conflicting claims are not identical, they are not patentably distinct from each other because

- "A method comprises: dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices; dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices; obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices; obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage" (claim 1, instant application) is analogous to
- "A method for execution by a processing module of a computing device, the method comprises: receiving a data object retrieval message regarding receiving a transmission from a particular source device; receiving, as the transmission, randomly ordered encoded slices from the particular source device; rearranging the randomly ordered encoded slices into first randomly ordered encoded data slices corresponding to data and a set of second randomly ordered encoded data slices corresponding to auxiliary data based on de-selection information; ordering the second randomly ordered encoded data slices into a set of encoded data slices in accordance with auxiliary data de-sequencing information; decoding the set of encoded data slices in accordance with operational parameters to produce auxiliary data; when the auxiliary data content corresponds to de-sequencing of the first randomly ordered encoded data slices, determining a pseudo random de-sequencing order for the first randomly ordered encoded data slices from the auxiliary data; ordering the first randomly ordered encoded data slices based on the pseudo-random de-sequencing order to produce a plurality of sets of encoded data slices; dispersed storage error decoding the plurality of sets of encoded data slices to produce a plurality of encrypted data segments; decrypting the plurality of encrypted data segments to produce a plurality of data segments; and aggregating the plurality of data segments to produce the data" (claim 1, patent 8959366) and analogous to
- "A method comprising: receiving a data segment of a data stream; encrypting the data segment to produce an encrypted data segment; dispersed storage error encoding the encrypted data segment to produce a set of encoded data slices, wherein a threshold number of the encoded data slices of the set of encoded data slices are needed to recover the encrypted data segment; dispersed storage error encoding auxiliary data to produce a set of encoded auxiliary data slices; generating a sequence of output slices to obscure the set of encoded data slices by interspersing the set of encoded auxiliary data slices within the set of encoded data slices; and sending the sequence of output slices for storage in a distributed storage network (DSN)" (claim 1, patent 10282564).

6. This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims of the instant application have not in fact been patented.

7. The claims of the conflicting patents and/or applications contain every element of claims 1-16 of the instant application and thus anticipate the claims of the instant application. Claims 1-16 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

8. "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species with that genus). "ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

9. "Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic claim. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Casanova (20080126357), and further in view of Michaelsen (20050002531).

Regarding claims 1 and 9, Casanova teaches dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices; dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices (par.14-15, 22-31,51-60); and

outputting, by the computing device, the first and second sets of encoded data slices for storage (par.57-61).

Casanova does not expressly disclose, however Michaelsen teaches obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices; obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage (par.9-19, 105-135, 140-150).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the teachings of Michaelsen to the system of Casanova.

One of ordinary skill in the art would have been motivated to perform such a modification to further increase complexity for unintended recipients to access content (Michaelsen, par.3-19, 100-150).

Regarding claims 2 and 10, Casanova/ Michaelsen teaches dispersed storage error encoding, by the computing device, the auxiliary data to produce a second set of encoded auxiliary data slices (Casanova, par.26-40, 55-60);

obfuscating, by the computing device, the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices; and obfuscating, by the computing device, the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices (Michaelsen, par.9-19, 105-135, 140-150).

Regarding claims 3 and 11, Casanova/ Michaelsen teaches wherein the auxiliary data comprises one or more of: null data; authentication information; a next pseudo random output sequencing order; a pseudo random output sequencing order identifier; a next outputting threshold; a random number generator output; an encryption key; a starting point for the pseudo random output sequencing order; a device identifier; a data identifier; a data type; a data size indictor; a priority indicator; a security indicator; and a performance indicator (Casanova, par.26-42, 55-60, Michaelsen, 120-130).

Regarding claims 4 and 12, Casanova/ Michaelsen teaches encrypting, by the computing device, the plurality of data segments to produce a plurality of encrypted data segments; and dispersed storage error encoding, by the computing device, the plurality of encrypted data segments to produce the plurality of sets of encoded data slices (Casanova, par.14, 26-42, 55-60).

Regarding claims 5 and 13, Casanova/ Michaelsen teaches encrypting, by the computing device, the auxiliary data to produce encrypted auxiliary data; and dispersed storage error encoding, by the computing device, the encrypted auxiliary data to produce the set of encoded auxiliary data slices (Casanova, par.14, 26-42, 55-60).

Regarding claims 6 and 14, Casanova/ Michaelsen teaches wherein the auxiliary data is encrypted via an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data (Casanova, par.14, 26-42, 55-60).

Regarding claims 7 and 15, Casanova/ Michaelsen teaches wherein the auxiliary data is encrypted via an all or nothing transformation to produce the encrypted auxiliary data and the plurality of data segments is encrypted via an all or nothing transformation to produce the plurality of encrypted data segments (Casanova, par. 14-15, 22-31,51-60, Michaelsen, 142-150).

Regarding claims 8 and 16, Casanova/ Michaelsen teaches wherein the obfuscating the first set of encoded data slices comprises: interspersing, by the computing device, the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order to produce the first set of obfuscated encoded data slices (Michaelsen, 14-20, 120-130, 142-150).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Garcia Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Friday 8AM-5PM.

13. Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

14. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, SHEWAYE GELAGAY can be reached on (571)272-4219. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

15. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David Garcia Cervetti/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 1 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20070226145-A1	09-2007	Ishigaki; Yoshinobu	G06K17/0022	705/51
*	B	US-20070160198-A1	07-2007	Orsini; Rick	H04L9/085	380/28
*	C	US-20060177061-A1	08-2006	Orsini; Rick L.	G06F21/606	380/268
*	D	US-20020003881-A1	01-2002	REITMEIER, GLENN ARTHUR	H04L9/34	380/210
*	E	US-20020078227-A1	06-2002	Kronenberg, Sandy Craig	H04L29/06	709/237
*	F	US-20030028879-A1	02-2003	Gordon, Donald F.	H04N5/4401	725/39
*	G	US-20070100913-A1	05-2007	Sumner; Gary Steven	G06F11/1453	1/1
*	H	US-7457415-B2	11-2008	Reitmeier; Glenn Arthur	H04L9/34	348/E7.055
*	I	US-20090041235-A1	02-2009	Reitmeier; Glenn Arthur	H04L9/34	380/42
*	J	US-20080263113-A1	10-2008	Krishnaiyer; Rajesh Anantha	G06F16/1844	1/1
*	K	US-7991746-B2	08-2011	Krishnaiyer; Rajesh Anantha	G06F16/1844	707/664
*	L	US-5535239-A	07-1996	Padovani; Roberto	H04B1/707	370/209
*	M	US-5621799-A	04-1997	Katta; Noboru	H04N7/1675	348/E7.056

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Pang et al., StegFS: A Steganographic File System, IEEE, 2003
	V	Bella et al., Distributed Backup through Information Dispersal, Elsevier, 2006
	W	Barr et al., pStore: A Secure Distributed Backup System, 2001
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 2 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080147821-A1	06-2008	Dietrich; Bradley W.	H04L63/104	709/216
*	B	US-20080222481-A1	09-2008	Huang; Cheng	H03M13/1191	714/752
*	C	US-20080222480-A1	09-2008	Huang; Cheng	H03M13/1191	714/752
*	D	US-20060212782-A1	09-2006	Li; Jin	H03M13/1575	714/784
*	E	US-20040117718-A1	06-2004	Manasse, Mark Steven	H03M13/1515	714/781
*	F	US-8626820-B1	01-2014	Levy; Richard S.	G06F11/1004	709/201
*	G	US-8560930-B2	10-2013	Li; Zongwang	H03M13/036	714/777
*	H	US-8522125-B1	08-2013	Feng; Jun	H03M13/293	714/801
*	I	US-7472334-B1	12-2008	Scott; Thomas P.	H03M13/151	714/785
*	J	US-20020046359-A1	04-2002	Boden, Scott T.	G06F12/1408	714/6.12
*	K	US-20070079083-A1	04-2007	Gladwin; S. Christopher	G06F21/6227	711/154
*	L	US-20070079082-A1	04-2007	Gladwin; S. Christopher	G06F11/1076	711/154
*	M	US-20070079081-A1	04-2007	Gladwin; S. Christopher	G06F21/6227	711/154

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 3 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20050131993-A1	06-2005	Fatula, Joseph John JR.	G06F9/5072	709/202
*	B	US-20040215998-A1	10-2004	Buxton, Robert F.	G06F11/1474	714/2
*	C	US-20040024963-A1	02-2004	Talagala, Nisha	G06F11/1076	711/114
*	D	US-20030018927-A1	01-2003	Gadir, Omar M.A.	G06F11/2005	714/4.11
*	E	US-20020166079-A1	11-2002	Ulrich, Thomas R.	G06F9/5083	714/6.12
*	F	US-20020062422-A1	05-2002	Butterworth, Henry Esmond	G06F11/0727	711/114
*	G	US-6826711-B2	11-2004	Moulton; Gregory Hagan	G06F11/1076	711/114
*	H	US-6718361-B1	04-2004	Basani; Vijay R.	H04L67/1095	707/999.01
*	I	US-6418539-B1	07-2002	Walker; Mark S.	G06F11/2058	714/5.1
*	J	US-5991414-A	11-1999	Garay; Juan Alberto	H04L9/302	380/30
*	K	US-6175571-B1	01-2001	Haddock; Stephen R.	H04L12/5601	370/423
*	L	US-6128277-A	10-2000	Bruck; Joshua	G06F11/1076	370/216
*	M	US-6058454-A	05-2000	Gerlach; Ralph John	G06F3/0607	710/10

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 4 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6012159-A	01-2000	Fischer; Michael	H03M13/13	714/755
*	B	US-5987622-A	11-1999	Lo Verso; Susan	G06F11/1076	714/6.1
*	C	US-5890156-A	03-1999	Rekieta; Thomas W.	G06F9/50	707/610
*	D	US-5809285-A	09-1998	Hilland; Jeffrey R.	G06F3/0608	703/25
*	E	US-5774643-A	06-1998	Lubbers; Clark E.	G06F11/1076	711/114
*	F	US-5485474-A	01-1996	Rabin; Michael O.	G06F11/004	714/762
*	G	US-4092732-A	05-1978	Ouchi; Norman Ken	G06F11/1076	714/5.11
*	H	US-9015301-B2	04-2015	Redlich; Ron M.	G06Q10/10	709/223
*	I	US-8904080-B2	12-2014	Martin; Don	G06F11/1456	710/20
*	J	US-7509420-B2	03-2009	Moulton; Gregory Hagan	H04L67/1097	709/203
*	K	US-7272602-B2	09-2007	Moulton; Gregory Hagan	G06F16/137	1/1
*	L	US-7103824-B2	09-2006	Halford; Robert	G06F11/1076	714/759
*	M	US-6690795-B1	02-2004	Richards; William James	H04N7/1675	348/E7.056

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 5 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20080010218-A1	01-2008	Zank; Anthony E.	G06F21/64	705/75
*	B	US-20080192936-A1	08-2008	Bellwood; Thomas A.	H04N5/913	380/277
*	C	US-20060056519-A1	03-2006	Horowitz; Michael	H04N19/176	375/240.27
*	D	US-20050265349-A1	12-2005	Garg, Sachin	H04L29/06027	370/395.2
*	E	US-20020002675-A1	01-2002	BUSH, RONALD ROSCOE	G06Q20/102	713/160
*	F	US-7406595-B1	07-2008	Boyle, Jr.; Vincent Michael	H04L9/0637	708/521
*	G	US-7577689-B1	08-2009	Masinter; Larry	G06F11/1464	1/1
*	H	US-8392474-B2	03-2013	Franco; Lucas Goncalves	H04L51/00	707/679
*	I	US-9135456-B2	09-2015	O'Hare; Mark S.	G06F21/606	1/1
*	J	US-20090055547-A1	02-2009	Hudson; Michael D.	D01D5/423	709/231
*	K	US-20080320151-A1	12-2008	McCanne; Steven	H03M7/30	709/228
*	L	US-20060069719-A1	03-2006	McCanne; Steven	H04L67/2828	709/203
*	M	US-20120198302-A1	08-2012	Otterstedt; Jan	H03M13/13	714/755

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 6 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20100266122-A1	10-2010	Suzaki; Tomoyasu	H04L9/002	380/28
*	B	US-20080049930-A1	02-2008	You; Yong-Kuk	H04L9/0637	380/28
*	C	US-20060069964-A1	03-2006	Hayashi; Junichi	H04L1/0061	714/52
*	D	US-20050123271-A1	06-2005	Ichinose, Tsutomu	G11B20/00086	386/329
*	E	US-20040172549-A1	09-2004	Kojima, Tadashi	G11B20/00086	713/193
*	F	US-20040145661-A1	07-2004	Murakami, Tomochika	H04N1/32144	348/222.1
*	G	US-20030012372-A1	01-2003	Cheng, Siu Lung	H03M13/2957	380/28
*	H	US-20030002665-A1	01-2003	Sako, Yoichiro	G11B20/00086	380/37
*	I	US-9854332-B2	12-2017	Winograd; Joseph M.	H04N21/44204	1/1
*	J	US-9854331-B2	12-2017	Winograd; Joseph M.	H04N21/44204	1/1
*	K	US-6571212-B1	05-2003	Dent; Paul W.	H04L1/004	704/270.1
*	L	US-5910182-A	06-1999	Dent; Paul W.	H03M13/00	714/755
*	M	US-8275132-B2	09-2012	Buchen; Neil B.	H04N7/1675	380/202

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/197,275	Applicant(s)/Patent Under Reexamination Resch et al.	
	Examiner David García Cervetti	Art Unit 2436	Page 7 of 7

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20070263864-A1	11-2007	BUCHEN; NEIL B.	H04N7/1675	380/201
*	B	US-20030123664-A1	07-2003	Pedlow, Leo M. JR.	H04N7/162	380/218
*	C	US-7707645-B2	04-2010	Haruki; Hiroyoshi	G06F21/57	713/193
*	D	US-20100172496-A1	07-2010	Furukawa; Jun	H04L9/0869	380/46
*	E	US-20060129801-A1	06-2006	Kang; Kyung-don	G06F21/10	713/153
*	F	US-20090177894-A1	07-2009	Orsini; Rick L.	G06F21/6209	713/193
*	G	US-20090097661-A1	04-2009	Orsini; Rick L.	H04L9/083	380/279
*	H	US-20100299313-A1	11-2010	ORSINI; RICK L.	H04L9/085	707/652
*	I	US-20100199089-A1	08-2010	Vysogorets; Mikhail	G06F21/34	713/168
*	J	US-20120066757-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/9
*	K	US-20120066756-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/9
*	L	US-20120066752-A1	03-2012	Vysogorets; Mikhail	G06F21/34	726/7
*	M	US-20120066517-A1	03-2012	Vysogorets; Mikhail	G06F21/34	713/193

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/197,275	Resch et al.
	Examiner	**Art Unit**
	David García Cervetti	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/26/2019								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/197,275	Resch et al.
	Examiner	**Art Unit**
	David García Cervetti	2436

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06F21/85 G06F21/6218 G06F21/606 G06F21/72 G06F21/80 H04L9/0894 H04L9/3242 H04W12/0013 H04W12/02	06/25/2019	DGC

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
inventor name search, acm, ieee, springer, google, scholar, east history attached	06/25/2019	DGC

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/David Garcia Cervetti/ Primary Examiner, Art Unit 2436	

Intra-file Security for a Distrilmted File System

SA Banachowski, ZNJ Peterson, EL Miller... - ... Conference on Mass ..., 2002 - academia.edu

... In such a **distributed file system**, s-nodes are stored physically near the blocks they describe ... 4 IFS Applications To support **encryption** of data within existing unencrypted files that have ... legacy applications, an IFS-capable copy program can be provided to **encrypt** the appropriale ...

☆ 99 Cited by 10 Related articles All 17 versions »

Cobalt: **Separating** Content Distribution from Authorization in Distributed File Systems.

K Veeraraghavan, A Myrick, J Flinn - FAST, 2007 - usenix.org

... a persistent query notifies standalone applications about modifica- tions to data stored in the **distributed file system** ... is an RSA signing key pair and a symmetric Key-**Encryption**-Key (KEK ... To avoid computationally-expensive public key **cryptography**, the symmetric KEK is used to ...

☆ 99 Cited by 9 Related articles All 11 versions »

The design and evaluation of a distributed reliable file system

D Peric, T Bocek, FV Hecht... - ... on Parallel and ..., 2009 - ieeexplore.ieee.org

... This value is then used as a key to **encrypt** the data of the block ... This is similar to IgorFS, but there is no **encryption** ... A. Access Pattern [27] shows an analysis of **distributed file system** traces in a corporate environment, which reports that "there are very evi- dent peak periods ...

☆ 99 Cited by 11 Related articles All 4 versions

Secure capabilities for a petabyte-scale object-based **distributed file system**

C Olson, EL Miller - Proceedings of the 2005 ACM workshop on Storage ..., 2005 - dl.acm.org

... 2.1 Ceph We are designing a **distributed file system**, Ceph, that uses network attached object storage devices ... The protocol uses symmetric **cryptography** to ensure pri- vacy and integrity for all ... the **metadata** server encrypts it with KMD, which is a symmetric **encryption** key known ...

☆ 99 Cited by 30 Related articles All 10 versions »

A novel **encryption** scheme for data deduplication system

C Wang, Z Qin, J Peng, J Wang - ... International Conference on ..., 2010 - ieeexplore.ieee.org

... The ESDS is a deterministic **encryption** algorithm and there exits a relationship between the ... WJ Bolosky, "Reclaiming space from duplicate files in a serverless **distributed file system**", in Proc ... [6) AJ Menezes, PC V Oorschot, and SA Vanstone, Handbook of Applied **Cryptography** ...

☆ 99 Cited by 27 Related articles All 2 versions

pStore: A secure peer-to-peer backup system

C Batten, K Barr, A Saraf, S Trepetin - Unpublished report, MIT ..., 2001 - 129.69.211.95

... 2.2 Versioning and Backup The existing distributed storage systems dis- cussed above are intended for sharing, archiving, or providing a **distributed file system** ... File blocks are **encrypted** using convergent **encryption** [2]. Convergent **encryption** uses a hash of the ...

☆ 99 Cited by 143 Related articles All 26 versions »

A survey of peer-to-peer storage techniques for distributed file systems

R Hasan, Z Anwar, W Yurcik... - ... Computing (ITCC'05 ..., 2005 - ieeexplore.ieee.org

... 4.6 Farsite Farsite [1] is a symbiotic, serverless, **distributed file system** ... After **encryption**, replicas of the file are made and they are distributed to other client machines ... It replaces physical security of a server in a locked room with virtual security: **cryptography**, randomized replication ...

☆ 99 Cited by 163 Related articles All 17 versions »

FARSITE: Federated, available, and reliable storage for an incompletely trusted environment

A Adya, WJ Bolosky, M Castro, G Cermak... - ACM SIGOPS ..., 2002 - dl.acm.org

... This paper describes Farsite, a serverless **distributed file system** that logically functions as a centralized ... disclose information, Farsite enforces read-access control via strong **cryptography**, as described ... Performing **encryption** on a block level enables a client to write an individual ...

☆ 99 Cited by 1159 Related articles All 40 versions

Peerstore: Better performance by relaxing in peer-to-peer backup

M Landers, H Zhang, KL Tan - ... . Fourth International Conference ..., 2004 - ieeexplore.ieee.org

... block content, h(C), is used as key for a symmetric cipher used to **encrypt** the block ... A security flaw PeerStore shares with all systems using convergent **encryption**, is al- lowing an attacker ... Feasibility of a serverless **distributed file system** deployed on an existing set of desktop pcs ...

☆ 99 Cited by 89 Related articles All 12 versions »

A Framework for Evaluating Storage System Security.

E Riedel, M Kallahalla, R Swaminathan - FAST, 2002 - usenix.org

… revocation requires immediate re-**encryption** of data … groups to authorize access, but there is no explicit decision on aggregating the keys used to **encrypt** data … directory keys), and encrypts only file data and file names; directory structures and other **metadata** are left un-**encrypted** …

Cited by 258 Related articles All 15 versions

Related searches

highly available distributed file system

content distribution distributed file systems

security and reliability distributed file systems

proxy caching distributed file systems

petabyte scale distributed file system

storage techniques distributed file systems

strong security distributed file systems

layered structure distributed file system

stackable vnode level encryption file system

user space file system

transparent cryptographic file system

cryptographic file system **for unix**

caching architecture distributed file **access**

internet file system **user management**

group sharing storage file systems

file system **architectures security module**

Selecting the right data distribution scheme for a survivable storage system

JJ Wylie - 2009 - kilthub.cmu.edu

... Symmetric key **encryption** (eg, triple-DES, AES) is a data distribution **algorithm** characterized by ... key using secret sharing, and stores the **encrypted information** using **information dispersal** [30 ... can be used instead of symmetric key **cryptography** to protect **information** confidentiality ...

☆ 99 Cited by 121 Related articles All 20 versions »

pStore: A secure peer-to-peer backup system

C Batten, K Barr, A Saraf, S Trepetin - Unpublished report, MIT ..., 2001 - 129.69.211.95

... The revised **algorithm** uses the FB hash, length, and offset **information** to make an efficient ... the ef- fective capacity for a user include data compression and **information dispersal algorithms** (as in [4 ... tion and actual file data through FB sharing but keeps version **information** and file ...

☆ 99 Cited by 143 Related articles All 26 versions »

POTSHARDS: secure long-term storage without **encryption**

MW Storer, KM Greenan, EL Miller, K Voruganti - 2008 - escholarship.org

... used by Mnemosyne [14] and CleverSafe [7] uses **encryption** followed by **information dispersal** (IDA) to ... how we use approximate pointers to recover data with no additional **information** beyond the ... Currently we use an XOR-based **algorithm** that produces n fragments from an ...

☆ 99 Cited by 91 Related articles All 10 versions »

Distributed Backup through **Information Dispersal**

G Bella, C Pistagna, S Riccobene - Electronic Notes in Theoretical ..., 2006 - Elsevier

... IDA is adopted to **disperse** the backup ... The retrieval protocol would tolerate the absence of the node from the network thanks to IDA's style of **dispersing** the fragments ... 84–95. [8] Lyuu, Y.-D., "**Information Dispersal** and Parallel Computation," Cambridge University Press, 1993 ...

☆ 99 Cited by 7 Related articles All 5 versions

Efficient security for Desktop Data Grid using **cryptographic** protocol

R Vaishnavi, J Anand ... - ... Conference on Control ..., 2009 - ieeexplore.ieee.org

... A security protocol (**cryptographic** protocol or **encryption** protocol) is an abstract or ... The second technique, the **information dispersal algorithm**, provides high availability and assurance of the ... Even though the use of **cryptography** and **Information Dispersal Algorithms** is not new ...

☆ 99 Cited by 2 Related articles All 2 versions

Providing security to the desktop data grid

J Luna, M Flouris, M Marazakis ... - 2008 IEEE International ..., 2008 - ieeexplore.ieee.org

... Even though the use of **cryptography** and **Information Dispersal Algorithms** is not new for securing data and meta- data in distributed ... We strongly believe in the security advantages of using the QoSec factor as an input to the **Information** Dis- persal **Algorithm**; however, the ...

☆ 99 Cited by 13 Related articles All 12 versions

Survivable Storage System"

JJ Wylie, M Bakkaloglu, V Pandurangan ... - IEEE Computer ..., 2001 - snake.cs.uidaho.edu

... possible data distribution schemes » <**algorithm**, parameters> – modeling the consequences of the schemes ... » store **encrypted** data using **information dispersal** » parameters are m, n, and k (key length) – Compression ... **Cryptographic algorithms** » eg MD5, SHA-1 ...

☆ 99 Cited by 4 Related articles All 6 versions »

Unidirectional Key Distribution Across Time and Space with Applications to RFID Security.

A Juels, R Pappu, B Parno - USENIX Security Symposium, 2008 - static.usenix.org

... this unidirectional model of key transport, we propose protocols for **dispersing** keys or ... The resulting ciphertext is shared using an **information- dispersal algorithm**, eg, Rabin's IDA [27] ... a casual attacker who only obtains a few emissions cannot reconstruct any tag **information** ...

☆ 99 Cited by 83 Related articles All 20 versions »

A survey of peer-to-peer content distribution technologies

S Androutsellis-Theotokis, D Spinellis - ACM computing surveys (CSUR), 2004 - dl.acm.org

... Different infras- tructures and **algorithms** have been developed to provide such services ... In order for such reputation **information** to be kept secure, up-to-date, and avail- able throughout the network, complex reputation ... 2003] A Distributed reputation management **algorithm** ...

☆ 99 Cited by 1987 Related articles All 57 versions

Data privacy considerations in intensive care grids

T Solomonides - Global Healthgrid: E-Science Meets …, 2008 - books.google.com

… **encryption** mechanisms at the “Grid's edges”(there- fore disclosing the **encryption** key to the … in OceanStore [14], stored data are protected with redundancy and **cryptographic** mech- anisms … ap- proach is given by Cleversafe [3] via an **Information Dispersal Algorithm** (based on …

☆ 99 Cited by 7 Related articles All 13 versions

Related searches

cloud computing information dispersal algorithms

optimal information dispersal

information dispersal **latency targets**

information dispersal **reliable communication**

information dispersal **computer networks**

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 81
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16197275
Filing Date	2018-11-20
First Named Inventor	Jason K. Resch
Art Unit	
Examiner Name	
Attorney Docket Number	CS00403_END920165769US09

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4092732	A	1978-05-30	Ouchi	
	2	5485474	A	1996-01-16	Rabin	
	3	5535239		1996-07-09	Padovani et al.	
	4	5621799		1997-04-15	Katta et al.	
	5	5774643	A	1998-06-30	Lubbers et al.	
	6	5809285	A	1998-09-15	Hilland	
	7	5890156	A	1999-03-30	Rekieta et al.	
	8	5910182		1999-06-08	Dent et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	9	5987622	A	1999-11-16	Lo Verso et al.	
	10	5991414	A	1999-11-23	Garay et al.	
	11	6012159	A	2000-01-04	Fischer et al.	
	12	6058454	A	2000-05-02	Gerlach et al.	
	13	6128277	A	2000-10-03	Bruck et al.	
	14	6175571	B1	2001-01-16	Haddock et al.	
	15	6418539	B1	2002-07-09	Walker	
	16	6571212		2003-05-27	Dent	
	17	6690795		2004-02-10	Richards	
	18	6718361	B1	2004-04-06	Basani et al.	
	19	6826711	B2	2004-11-30	Moulton et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 83
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	20	7103824	B2	2006-09-05	Halford	
	21	7272602		2007-09-18	Moulton	
	22	7406595		2008-07-29	Boyle Jr. et al.	
	23	7457415		2008-11-25	Reitmeier et al.	
	24	7472334		2008-12-30	Scott et al.	
	25	7509420		2009-03-24	Moulton et al.	
	26	7577689		2009-08-18	Masinter et al.	
	27	7636724	B2	2009-12-22	de la Torre et al.	
	28	7707645		2010-04-27	Haruki et al.	
	29	7991746		2011-08-02	Krishnaiyer et al.	
	30	8275132		2012-09-25	Buchen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 84
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	31	8392474		2013-03-05	Franco et al.	
	32	8522125		2013-08-27	Feng et al.	
	33	8560930		2013-10-15	Li et al.	
	34	8626820		2014-01-07	Levy	
	35	8649521		2014-02-11	Grube et al.	
	36	8677214		2014-03-18	Grube et al.	
	37	8744071		2014-06-03	Leggette et al.	
	38	8782494		2014-07-15	Grube et al.	
	39	8856617		2014-10-07	Grube et al.	
	40	8885821		2014-11-11	Grube et al.	
	41	8904080		2014-12-02	Martin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	42	8918897		2014-12-23	Resch	
	43	8959336		2015-02-17	Lee	
	44	9015301		2015-04-21	Redlich et al.	
	45	9021263		2015-04-28	Resch et al.	
	46	9076138		2015-07-07	Resch	
	47	9128870		2015-09-08	Grube et al.	
	48	9135456		2015-09-15	OHare et al.	
	49	9854331		2017-12-26	Winograd et al.	
	50	9854332		2017-12-26	Winograd et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16197275
Filing Date	2018-11-20
First Named Inventor	Jason K. Resch
Art Unit	
Examiner Name	
Attorney Docket Number	CS00403_END920165769US09

	1	20020002675	A1	2002-01-03	BUSH	
	2	20020003881	A1	2002-01-10	REITMEIER et al.	
	3	20020046359	A1	2002-04-18	Boden	
	4	20020062422	A1	2002-05-23	Butterworth et al.	
	5	20020078227	A1	2002-06-20	Kronenberg	
	6	20020166079	A1	2002-11-07	Ulrich Thomas R. et al.	
	7	20030002665	A1	2003-01-02	Sako et al.	
	8	20030012372	A1	2003-01-16	Cheng	
	9	20030018927	A1	2003-01-23	Gadir Omar M.A. et al.	
	10	20030028879	A1	2003-02-06	Gordon Donald F. et al.	
	11	20030123664	A1	2003-07-03	Pedlow Leo M. JR. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 87
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	12	20040024963	A1	2004-02-05	Talagala et al.	
	13	20040117718	A1	2004-06-17	Manasse	
	14	20040145661	A1	2004-07-29	Murakami et al.	
	15	20040172549	A1	2004-09-02	Kojima et al.	
	16	20040215998	A1	2004-10-28	Buxton Robert F. et al.	
	17	20050123271	A1	2005-06-09	Ichinose et al.	
	18	20050131993	A1	2005-06-16	Fatula	
	19	20050265349	A1	2005-12-01	Garg et al.	
	20	20060056519	A1	2006-03-16	Horowitz et al.	
	21	20060069719	A1	2006-03-30	McCanne et al.	
	22	20060069964	A1	2006-03-30	Hayashi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 88
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	23	20060177061	A1	2006-08-10	Orsini et al.	
	24	20060212782	A1	2006-09-21	Li	
	25	20070079081	A1	2007-04-05	Gladwin et al.	
	26	20070079082	A1	2007-04-05	Gladwin et al.	
	27	20070079083	A1	2007-04-05	Gladwin et al.	
	28	20070100913	A1	2007-05-03	Sumner et al.	
	29	20070160198	A1	2007-07-12	Orsini et al.	
	30	20070226145	A1	2007-09-27	Ishigaki et al.	
	31	20070263864	A1	2007-11-15	BUCHEN et al.	
	32	20080010218	A1	2008-01-10	Zank	
	33	20080049930	A1	2008-02-28	You et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	34	20080147821	A1	2008-06-19	Dietrich et al.	
	35	20080192936	A1	2008-08-14	Bellwood et al.	
	36	20080222480	A1	2008-09-11	Huang et al.	
	37	20080222481	A1	2008-09-11	Huang et al.	
	38	20080263113	A1	2008-10-23	Krishnaiyer et al.	
	39	20080320151	A1	2008-12-25	McCanne et al.	
	40	20090041235	A1	2009-02-12	Reitmeier et al.	
	41	20090055547	A1	2009-02-26	Hudson et al.	
	42	20100266122	A1	2010-10-21	Suzaki et al.	
	43	20120198302	A1	2012-08-02	Otterstedt et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 90
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16197275
Filing Date	2018-11-20
First Named Inventor	Jason K. Resch
Art Unit	
Examiner Name	
Attorney Docket Number	CS00403_END920165769US09

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Aschenbrenner et al., Infrastructure for Interactivity- Decoupled Systems on the Loose, 2009, IEEE.	
	2	Bellare et al., Robust Computational Secret Sharing and a Unified Account of Classical Secret-Sharing Goals, Nov 2007, ACM.	
	3	BIAN, JigDFS: A Secure Distributed File System, 2009	
	4	Jensen et al., Resilia: a Safe and Secure Distributed Backup System for Small and Medium Enterprises, 2007, Springer.	
	5	KUBIATOWICZ, et al.; OceanStore: An Architecture for Global-Scale Persistent Storage; Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2000); November 2000; pp 1-12	
	6	Schuman et al., A Performance Comparison of Open-Source Erasure Coding Libraries for Storage Applications, Aug 2008,University of Tennessee.	
	7	Storer et al., Long-Term Threats to Secure Archives, Oct 2006, ACM.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 91
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

EXAMINER SIGNATURE			
Examiner Signature	/David Garcia Cervetti/	Date Considered	06/26/2019

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 92
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16197275
Filing Date	2018-11-20
First Named Inventor	Jason K. Resch
Art Unit	
Examiner Name	
Attorney Docket Number	CS00403_END920165769US09

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

X A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patricia A. Markison/	Date (YYYY-MM-DD)	2018-11-26
Name/Print	Patricia A. Markison	Registration Number	73072

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DGC/

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 94
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Selecting the right **data** distribution scheme for a survivable storage system
JJ Wylie - 2009 - kilthub.cmu.edu
... key **encryption** (eg, triple-DES, AES) is a **data** distribution **algorithm** characterized by ... Hybrid **data** distribution **algorithms** can be constructed by combining the **algorithms** already discussed ... using secret sharing, and stores the **encrypted** information using information **dispersal** [30 ...
☆ 99 Cited by 121 Related articles All 20 versions »

Providing security to the desktop **data** grid
J Luna, M Flouris, M Marazakis... - 2008 IEEE International ..., 2008 - ieeexplore.ieee.org
... 4], which imple- ments also an Information **Dispersal Algorithm** (based on the Reed-Solomon **algorithm**) for its open-source **Dispersed** Storage Project ... Even though the use of **cryptography** and Information **Dispersal Algorithms** is not new for securing **data** and meta- **data** in ...
☆ 99 Cited by 13 Related articles All 12 versions

Data embedding using phase **dispersion**
C Honsinger - 2000 - IET
... effect of convolving a message with a random phase carrier is to spatially **disperse** the message ... In this case we abandon the idea of tiling a **dispersed** message over the image and ... There are numerous applications of using binary **data** ranging from the interruption of a scanner ...
☆ 99 Cited by 57 Related articles All 16 versions »

A novel protocol for secure **data** storage in **Data** Grid
TS Muthu, R Masillamani - 2010 First International Conference ..., 2010 - ieeexplore.ieee.org
... fragmentation mechanism can also be used for storing long-lived **data** with high assurance: f is fragmented in just a few pieces (small m) and **dispersed** to a ... Even though the use of **cryptography** and Information **Dispersal Algorithms** is not new for securing **data** and **metadata** ...
☆ 99 Cited by 3 Related articles All 2 versions »

A novel protocol for secure **data** storage in **Data** Grid environment
TS Muthu, R Vadivel, A Ramesh... - Trendz in Information ..., 2010 - ieeexplore.ieee.org
... fragmentation mechanism can also be used for storing long-lived **data** with high assurance: f is fragmented in just a few pieces (small m) and **dispersed** to a ... Even though the use of **cryptography** and Information **Dispersal Algorithms** is not new for securing **data** and **metadata** ...
☆ 99 Cited by 3 Related articles

pStore: A secure peer-to-peer backup system
C Batten, K Barr, A Saraf, S Trepetin - Unpublished report, MIT ..., 2001 - 129.69.211.95
... The revised **algorithm** uses the FB hash, length, and offset information to make an efficient ... the ef- fective capacity for a user include **data** compression and information **dispersal algorithms** (as in [4 ... The delete chunk has the same identifier as the chunk to delete, but has no **data** ...
☆ 99 Cited by 143 Related articles All 26 versions »

Data privacy considerations in intensive care grids
T Solomonides - Global Healthgrid: E-Science Meets ..., 2008 - books.google.com
... A similar ap- proach is given by Cleversafe [3] via an Information **Dispersal Algorithm** (based on Page 205. 186 J. Luna et al./**Data** Privacy Considerations in Intensive Care Grids the Reed-Solomon **algorithm**) for its open-source **Dispersed** Storage Project ...
☆ 99 Cited by 7 Related articles All 13 versions

Efficient security for Desktop **Data** Grid using **cryptographic** protocol
R Vaishnavi, J Anand ... - ... Conference on Control ..., 2009 - ieeexplore.ieee.org
... The second technique, the information **dispersal algorithm**, provides high availability and assurance of the **data** in the Desktop **Data** Grid by means of **Data** ... Even though the use of **cryptography** and Information **Dispersal Algorithms** is not new for securing **data** and **metadata** ...
☆ 99 Cited by 2 Related articles All 2 versions

Data-centric privacy protocol for intensive care grids
J Luna, M Dikaiakos, M Marazakis ... - IEEE Transactions on ..., 2010 - ieeexplore.ieee.org
... and the fragmentation mechanisms (Table VI), we can observe that despite **encryption** costs in ... we run in a different subset of experiments several operation modes of the Information **Dispersal Algorithm** to find ... 8. **Data** throughput for the IDA mechanism with different values of n ...
☆ 99 Cited by 9 Related articles All 14 versions

Performance evaluation of a disaster recovery system and practical network system applications

Y Ueno, N Miyaho, S Suzuki... - 2010 Fifth International ..., 2010 - ieeexplore.ieee.org

... Discussion has also been provided on an effective shuffling **algorithm** using Mersenne Twister and "Fisher-Yates shuffle" to determine the **dispersed** location sites ... 215-218, Oct., 2007. [9] J. Yamato, M. Kan, and Y. Kikuchi, “Storage Based **Data** Protection for Disaster Recovery ...

☆ 99 Cited by 20 Related articles All 6 versions

Related searches

cryptographic **protocol desktop** data **grid**

Development of a Long Term Viable Dynamic **Data** Archive Format
RJ Allemang - sdrl.rhod.uc.edu
... simpler hashing/message digest type schemes (CRC32, MD5, et al.) should be preferable to **encoding** schemes (RS, et al.) because the **data** remains ASCII. For **error** detection purposes, each field may have an individual hash **coding** (CRC, et al.) attribute representing the ...
☆ 99 Related articles All 4 versions »

Multigig lossless **data** compression device
R Mehboob, SA Khan, Z Ahmed... - IEEE Transactions ..., 2010 - ieeexplore.ieee.org
... offices have to share voice, **data** and video information over a geographically **dispersed** locations making ... The **statistical** techniques are well suited for sources where **data** is predictable or consistent, but ... [2] PG Howard and JS Vitter, "Arithmetic **coding** for **data** compression," Proc ...
☆ 99 Cited by 10 Related articles All 5 versions

How standard is standardized MNC global environmental communication?
T Hunter, P Bansal - Journal of Business Ethics, 2007 - Springer
... In this study, we used the LISREL **statistical** package developed by Joreskog and Sorbom to perform a ... the final **coding** units used in the content analysis, as well as the loadings and **error** ... The **coding** units used in the construct validity tests and ultimately the **data** collection were ...
☆ 99 Cited by 86 Related articles All 15 versions »

Natural language watermarking via morphosyntactic alterations
HM Meral, B Sankur, AS Özsoy, T Güngör... - Computer Speech & ..., 2009 - Elsevier
... Edit distance is used to search for an **error**-tolerant watermark ... A **statistical** model that estimates the n-gram word strings for their synonym substitutions is proposed by Taskiran et al ... This is the steganography problem where **data** must be hidden in such a subtle way that it should ...
☆ 99 Cited by 86 Related articles All 9 versions

Multi-Level modeling and access control for **data** sharing in collaborative design
T Kim, CD Cera, WC Regli, H Choo, JH Han - Advanced Engineering ..., 2006 - Elsevier
... process in which multiple teams work on a design, often geographically **dispersed**, using heterogeneous ... geometric computation is needed, but simple handling of list or tree **data** structure is ... a representative vertex, and its position is computed using quadric **error** metric method ...
☆ 99 Cited by 41 Related articles All 5 versions

Practical experiences in using model-driven engineering to develop trustworthy computing systems
T Weigert, F Weil - IEEE International Conference on Sensor ..., 2006 - ieeexplore.ieee.org
... than planning when the design diagrams are interpreted consistently across geographically **dispersed** organizations ... Automation of labor-intensive and **error**-prone develop- ment tasks results in additional ... a 3X reduction in defects, which is also borne out by the **data**: In Figure 6 ...
☆ 99 Cited by 61 Related articles All 8 versions »

Botnets as a vehicle for online crime
N Ianelli, A Hackworth - CERT Coordination Center, 2005 - ijofcs.org
... By creating large, geographically **dispersed** botnets, attackers have been able to launch DDoS attacks ... FTP services make bots useful as malware download sites and **data** drops for spyware ... the bots useful as generic "bounces" through which attackers can **obfuscate** their true ...
☆ 99 Cited by 241 Related articles All 4 versions »

Visualization of **Statistical** Uncertainty
K Potter - 2006 - pdfs.semanticscholar.org
... While this is an effective measure of the **dispersion** of the **data**, there may be ... The moments of a distribution are **statistical** measures of certain characteristics, the most well known ... the quartiles give information about the location and variation changes in the **data**, while moments ...
☆ 99 Cited by 2 Related articles All 3 versions »

Privacy protected surveillance using secure visual object **coding**
K Martin, KN Plataniotis - ... on Circuits and Systems for Video ..., 2008 - ieeexplore.ieee.org
... Furthermore, some image details may be reconstructed through **error** concealment techniques [15] ... entities without the correct matching decryption key, kD, from correctly decrypting the **data**.1 The ... K is controlled by the user at the time of encryption/**encoding** to determine the ...
☆ 99 Cited by 62 Related articles All 5 versions

The new paradigm of flow cell sequencing

RA Holt, SJM Jones - Genome research, 2008 - genome.cshlp.org

… sheared human gDNA to microarrays containing oligonucleotide probes complementary to either **dispersed** short targets (6726 … could also be run twice on the same clusters to improve **error** rates …

Once generated, sequence **data** will need to be either compared with a reference …

☆ 99 Cited by 252 Related articles All 9 versions

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	("20080126357" "20050002531").pn.	US-PGPUB; USPAT	OR	ON	2019/06/26 21:11
S1	3986	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S2	1246	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S3	2045	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:55
S4	49	("5126964" | "5930466" | "8046044" | "8046044" | "8225233" | "20060079755" | "20100156761" | "20120011474" | "3774161" | "3886359" | "4056846" | "4138721" | "4216526" | "4228468" | "4228495" | "4258273" | "4279199" | "4342916" | "4378022" | "4404684" | "4418383" | "4458203" | "4468748" | "4472818" | "4479205" | "4555763" | "4557019" | "4559597" | "4580215" | "4582491" | "4608977" | "4630193" | "4630202" | "4631585" | "4651096" | "4674046" | "4707661" | "4718432" | "4731839" | "4733187" | "4739308" | "4739352" | "4742480" | "4748887" | "4751587" | "4763279" | "4767992" | "4789929" | "4791590" | "4817187").PN.	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:57
S5	44	("20110182424" | "20110182429" | "20110185193" | "20020016961" | "20030028879" | "20100266120" | "20100269008" | "20100287200" | "20110026842" | "20110029742" | "20110029809" | "20110055661" | "20110072210" | "20110072321" | "20110078080" | "20110078373" | "20110083053" | "20110055661" | "20110072210" | "20110072321" | "20110078080" | "20110078373" | "20110083053" | "20110107027" | "20110107165" | "20110107180" | "20110107181" | "20110107184" | "20110107185" | "20110107380" | "20110122523" | "20110125771" | "20110126026" | "20110126295" | "20110161655" | "20110161680" | "20110161681" | "20110161781" | "20110184997" | "20110185253" | "20110185258" | "20110213929" | "20110214011" | "20110225362" |	US-PGPUB; USPAT	OR	OFF	2012/12/08 21:57

		"20110228931" | "20110231699" | "20110231733" | "20110261839" | "20110264717" | "20110264823").PN.				
S6	1	"20110185193".pn. and (aont transformation)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:49
S7	158	(aont nothing near4 transformation)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:50
S8	63	(aont nothing near4 transformation) and (encrypt$ crypto$)	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:50
S9	63	(US-20120255035-$ or US-20120255034-$ or US-20120226904-$ or US-20120222134-$ or US-20120221856-$ or US-20120221855-$ or US-20120221854-$ or US-20120198241-$ or US-20120179916-$ or US-20120173883-$ or US-20120170750-$ or US-20120166818-$ or US-20120166815-$ or US-20120166576-$ or US-20120159197-$ or US-20120124366-$ or US-20120110346-$ or US-20120072723-$ or US-20120054747-$ or US-20110314346-$ or US-20110314154-$ or US-20110314072-$ or US-20110314058-$ or US-20110311051-$ or US-20110296440-$ or US-20110258439-$).did. or (US-20110246817-$ or US-20110246766-$ or US-20110202763-$ or US-20110202755-$ or US-20110185193-$ or US-20110182429-$ or US-20110182424-$ or US-20110107112-$ or US-20100299313-$ or US-20100269008-$ or US-20100268966-$ or US-20100266120-$ or US-20100266119-$ or US-20100098255-$ or US-20090177894-$ or US-20090158052-$ or US-20090097661-$ or US-20080183992-$ or US-20070226145-$ or US-20070219915-$ or US-20070160198-$ or US-20060177061-$ or US-20050118141-$ or US-20040141613-$).did. or (US-8320560-$ or US-8300828-$ or US-8271802-$ or US-8266438-$ or US-8135134-$ or US-8121294-$ or US-8060877-$ or US-8009830-$ or US-7913093-$ or US-7840487-$ or US-7457419-$ or US-7260820-$ or US-7220891-$).did.	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:51
S10	63	S9 and S7	US-PGPUB; USPAT	OR	OFF	2012/12/09 12:52
S11	138668	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:51
S12	138667	(desequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:52
S13	17416	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram frame)	US-PGPUB; USPAT	OR	OFF	2012/12/09 14:52
S14	2808	(desequenc$ de-sequenc$ de adj	US-	OR	ON	2012/12/09

		sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame)	PGPUB; USPAT			14:53
S15	37	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering re-order)	US-PGPUB; USPAT	OR	ON	2012/12/09 14:54
S16	474	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order)	US-PGPUB; USPAT	OR	ON	2012/12/09 14:54
S17	3	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation disper$ near4 storage near4 error)	US-PGPUB; USPAT	OR	ON	2012/12/09 16:12
S18	3	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation disper$ near4 error)	US-PGPUB; USPAT	OR	ON	2012/12/09 16:12
S19	338	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation error crc)	US-PGPUB; USPAT	OR	ON	2012/12/10 08:29
S20	205	dispers$ near5 storage near4 error	US-PGPUB; USPAT	OR	ON	2012/12/10 08:32
S23	174	dispers$ adj storage near4 error near5 (encrypt$ decrypt$ crypto$ encod$ decod$)	US-PGPUB; USPAT	OR	ON	2012/12/10 08:33
S24	5	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8	US-PGPUB; USPAT	OR	ON	2012/12/10 12:43

		(packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (dispers$ near4 storage)				
S25	38	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (distribut$ near4 storage)	US-PGPUB; USPAT	OR	ON	2012/12/10 12:45
S26	9128	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:28
S27	980	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:28
S28	77	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (reorder$)	US-PGPUB; USPAT	OR	ON	2013/03/24 15:29
S29	263	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling)	US-PGPUB; USPAT	OR	ON	2013/03/24 21:55
S30	260	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2013/03/24 22:11
S31	4186	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S32	1295	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S33	2124	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2013/03/24 22:24
S34	1	"7457415".pn.	US-	OR	OFF	2013/03/24

			PGPUB; USPAT			22:28
S35	37	("4736420" | "4742544" | "4947447" | "5014310" | "5049990" | "5113443" | "5195134" | "5351299" | "5392072" | "5420866" | "5479512" | "5546461" | "5621799" | "5625416" | "5701391" | "5706346" | "5734755" | "5764994" | "5802520" | "5926624" | "6035068" | "6041160" | "6061451" | "6064748" | "6081785" | "6101195" | "6157606" | "6266299" | "6285774" | "6349088" | "6392705" | "6529553").PN. OR ("7457415").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/24 22:28
S36	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2013/03/24 23:22
S37	502	cleversafe.as.	US-PGPUB; USPAT	OR	ON	2014/05/15 08:43
S38	135	cleversafe.as.	USPAT	OR	ON	2014/05/15 08:44
S39	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 08:58
S40	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20101128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:44
S41	24	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame) and (frame) near6 (sequence sequencing index auxiliary metadata) and (frame) near8 (assemble assembling) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:45
S42	132	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame slice) same (sequence sequencing index auxiliary metadata) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:46
S43	0	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame slice) and transmit$ near6 (index) near8 content and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2014/05/15 09:48
S44	2	(random randomly pseudorandom$ pseudo	US-	OR	ON	2014/05/15

		adj random$) near8 (order ordered ordering) near6 (frame slice) and transmit$ near6 (vector order) near8 content and (@pd @prad @rlad @ptad @ad)<"20100128"	PGPUB; USPAT			09:49
S45	1669	G06F11/1008.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:09
S46	1294	G06F21/72.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:09
S47	1163	G06F21/80.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S48	1258	G06F21/85.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S49	743	H04L9/3242.cpc.	US-PGPUB; USPAT	OR	ON	2014/05/15 10:10
S50	742	(distributed dispersed) adj storage adj network	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:24
S51	405	(distributed dispersed) adj storage adj network.clm.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:24
S52	332	(distributed dispersed) adj storage adj network.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:25
S56	27	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and encrypted.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:27
S57	30	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:27
S58	5	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:30
S59	5365	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S60	1545	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S61	2686	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2014/10/05 11:47
S62	1781	G06F11/1008.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S63	1402	G06F21/72.cpc.	US-	OR	ON	2014/10/05

			PGPUB; USPAT			11:48
S64	1185	G06F21/80.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S65	1332	G06F21/85.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S66	806	H04L9/3242.cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:48
S67	4	(G06F21/85 and H04N21/2347 and H04N21/222 and H04N21/8456 and H04L9/3242 and G06F21/72 and G06F21/80 and H04L67/1097 and H04L65/604 and G06F2211/1028 and H04W12/02 and G06F2221/2107 and G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:51
S68	23270	(G06F21/85 H04N21/2347 H04N21/222 H04N21/8456 H04L9/3242 G06F21/72 G06F21/80 H04L67/1097 H04L65/604 G06F2211/1028 H04W12/02 G06F2221/2107 G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2014/10/05 11:51
S72	1627	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:42
S73	39916	(G06F21/85 or G06F3/067 or G06F3/0647 or G06F11/1076 or G06F3/0619 or H04L67/1097 or G06F21/72 or H04N21/222 or G06F21/80 or H04N21/8456 or H04L9/3242 or H04N21/2347 or H04L65/604 or H04W12/02 or G06F2211/1028 or G06F11/1008 or G06F2221/2107).cpc.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:42
S74	5962	713/193.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S75	44	("20110214011" | "20110213928" | "20110213929" | "20030225970" | "20060010290" | "20070294565" | "20110225451" | "20010026677" | "20050031042" | "20100260262" | "20100268692" | "20100332751" | "20110026842" | "20110029711" | "20110029742" | "20110029809" | "20110029836" | "20110055661" | "20110072210" | "20110078080" | "20110078373" | "20110078774" | "20110083053" | "20110055661" | "20110072210" | "20110078080" | "20110078373" | "20110078774" | "20110083053" | "20110106855" | "20110106904" | "20110106972" | "20110106973" | "20110107026" | "20110107027" | "20110107036" | "20110107078" | "20110107094" | "20110107113" | "20110107165" | "20110107180" | "20110107181" | "20110107182" | "20110107184" | "20110107185" | "20110107380" | "20110122523" | "20110125771" |	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43

		"20110126026" | "20110126060").PN.				
S76	4000	380/28.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S77	549	380/268.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S78	1097	380/279.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:43
S79	46	("7505535" | "7207224" | "7907722" | "7907722" | "8098952" | "9125609" | "4882737" | "5148479" | "5373372" | "5430830" | "5602638" | "5768159" | "7200233" | "7483058" | "7774272" | "7792067" | "7933218" | "8014479" | "8085283" | "7933218" | "8014479" | "8085283" | "8094813" | "8300809" | "8379523" | "8429414" | "8437870" | "8588423" | "8670430" | "8891370" | "8924983" | "8983787" | "9064438" | "3555184" | "3555195" | "3555204" | "3555251" | "3555255" | "3555259" | "3556007" | "3557308" | "3557314" | "3557349" | "3557354" | "3557355" | "3557357" | "3557673" | "3558811" | "3558820" | "3558823").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S80	4044	S75 S76	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S81	90	S75 S79	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:44
S82	2450	714/763.ccls.	US-PGPUB; USPAT	OR	OFF	2015/09/25 21:46
S83	479	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice) near8 stream	US-PGPUB; USPAT	OR	ON	2015/09/25 21:53
S84	609	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet) near8 stream	US-PGPUB; USPAT	OR	ON	2015/09/25 21:53
S85	499	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet) near8 stream and ((@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/25 21:53
S86	105	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet segment part portion section) near8 stream and encrypt$ near5 (data slice packet segment part portion section)and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/25 21:54
S87	105	(desequencing de-sequencing de near3 sequencing sequencing interspersing) near5 (data slice packet segment part portion section) near8 stream and encrypt$ near5 (data slice packet segment part portion section) and (@pd @prad @rlad	US-PGPUB; USPAT	OR	ON	2015/09/25 21:54

		@ptad @ad)<"20100128"				
S88	13930	reed adj solomon adj code	US-PGPUB; USPAT	OR	ON	2015/09/27 11:31
S89	0	reed adj solomon adj code and distribution adj matrix and identity adj matrix	US-PGPUB; USPAT	OR	ON	2015/09/27 11:33
S90	6	reed adj solomon adj code and distribution adj matrix	US-PGPUB; USPAT	OR	ON	2015/09/27 11:33
S93	26	reed adj solomon adj code and (distribution identity) adj matrix and galois and (disperse dispersed distributed) near6 storage	US-PGPUB; USPAT	OR	ON	2015/09/27 11:35
S94	1	"8959366".pn.	US-PGPUB; USPAT	OR	ON	2015/09/27 11:37
S95	33	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 11:57
S96	1752	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S97	666	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment)	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S98	237	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/27 12:10
S99	1	distributed adj storage.clm. and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet segment)	USPAT	OR	ON	2015/09/27 13:03
S100	11	distributed adj storage and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (obfuscat$ obscur$ unintellig$) near6 (slice packet segment)	USPAT	OR	ON	2015/09/27 13:04
S104	134	(dispersed distributed) adj storage adj network and encrypt$ near6 (data content) near6 (slice segment part portion section packet) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2015/09/27 13:12
S105	2814	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:12
S106	1346	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (order ordering ordered reorder reordered reordering sequence	US-PGPUB; USPAT	OR	ON	2015/09/27 14:12

		sequencing) near6 (slice segment part portion section packet)				
S107	1037	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (slice segment part portion section packet) and (error near3 (code encode coding encoding) parity near3 check)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:13
S108	39	reed adj solomon and (disperse dispersed distributed) near6 (storage store storing stored) and (random$ pseudorandom$) near8 (order ordering ordered reorder reordered reordering sequence sequencing) near6 (slice segment part portion section packet) and (error near3 (code encode coding encoding) parity near3 check)	US-PGPUB; USPAT	OR	ON	2015/09/27 14:14
S109	1	"20140344645".pn. and readable	US-PGPUB; USPAT	OR	ON	2015/09/27 17:11
S110	1	"20140344645".pn. and (media medium)	US-PGPUB; USPAT	OR	ON	2015/09/27 17:12
S111	1	"20140344645".pn. and nothing	US-PGPUB; USPAT	OR	ON	2015/09/27 17:42
S112	0	"all or nothing"	US-PGPUB; USPAT	OR	ON	2015/09/27 17:43
S113	78	("20020062422" | "20020166079" | "20030018927" | "20030037261" | "20030065617" | "20030084020" | "20040024963" | "20040122917" | "20040215998" | "20040228493" | "20050100022" | "20050114594" | "20050125593" | "20050131993" | "20050132070" | "20050144382" | "20050229069" | "20060047907" | "20060136448" | "20060156059" | "20060224603" | "20070079081" | "20070079082" | "20070079083" | "20070088970" | "20070174192" | "20070214285" | "20070234110" | "20070283167" | "20090094251" | "20090094318" | "20100023524" | "4092732" | "5454101" | "5485474" | "5774643" | "5802364" | "5809285" | "5890156" | "5987622" | "5991414" | "6012159" | "6058454" | "6128277" | "6175571" | "6192472" | "6256688" | "6272658" | "6301604" | "6356949" | "6366995" | "6374336" | "6415373" | "6418539" | "6449688" | "6567948" | "6571282" | "6609223" | "6718361" | "6760808" | "6785768" | "6785783" | "6826711" | "6879596" | "7003688" | "7024451" | "7024609" | "7080101" | "7103824" | "7103915" | "7111115" | "7140044" | "7146644" | "7171493" | "7222133" | "7240236" | "7272613" |	US-PGPUB; USPAT	OR	ON	2015/09/27 17:51

		"7636724").PN.				
S114	338	("5485474").URPN.	USPAT	OR	OFF	2015/09/27 18:33
S115	1	"8626820".pn.	US-PGPUB; USPAT	OR	OFF	2015/09/27 20:43
S116	0	"20080263113".pn. and error	US-PGPUB; USPAT	OR	OFF	2016/03/18 21:55
S117	1	"20080263113".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/18 21:56
S118	5	dispersed near4 storage near4 error and encoding near4 auxiliary near4 data	US-PGPUB; USPAT	OR	OFF	2016/03/18 22:16
S119	43	distributed near4 storage and error near4 encoding and auxiliary near4 data	US-PGPUB; USPAT	OR	OFF	2016/03/18 22:20
S120	32	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 slice	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S121	36	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 (slice portion section part segment)	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S122	36	(distributed dispersed) near4 storage and error near4 encoding and auxiliary near4 data and data near4 (slice portion section part segment fragment)	US-PGPUB; USPAT	OR	ON	2016/03/18 22:21
S123	573	information adj dispersal and error adj encoding	US-PGPUB; USPAT	OR	ON	2016/03/18 22:34
S125	151	information adj dispersal and encrypt$ and error adj encoding and (@pd @prad @rlad @ptad @ad)< "20100128"	US-PGPUB; USPAT	OR	ON	2016/03/18 22:42
S126	5933	713/189.ccls.	US-PGPUB; USPAT	OR	OFF	2016/03/19 21:56
S127	1632	713/194.ccls.	US-PGPUB; USPAT	OR	OFF	2016/03/19 21:56
S128	2927	380/270.ccls.	US-PGPUB; USPAT	OR	OFF	2016/03/19 21:56
S129	30886	(G06F21/85 H04N21/2347 H04N21/222 H04N21/8456 H04L9/3242 G06F21/72 G06F21/80 H04L67/1097 H04L65/604 G06F2211/1028 H04W12/02 G06F2221/2107 G06F11/1008).cpc.	US-PGPUB; USPAT	OR	ON	2016/03/19 21:59
S130	1	"20080263113".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/24 09:47
S131	77	(intersper$ scatter$ intermix$) near6 (slice packet datagram) near8 (encrypted encoded)	US-PGPUB; USPAT	OR	ON	2016/03/24 10:03
S132	70	(intersper$ scatter$ intermix$) near6 (slice packet datagram) near8 (encrypted	US-PGPUB;	OR	ON	2016/03/24 10:04

		encoded) and (@pd @prad @rlad @ptad @ad)<"20100128"	USPAT			
S133	23	(random$ pseudorandom$) near6 (order ordering ordered) near6 (slice packet datagram) near8 (encrypted encoded) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2016/03/24 10:29
S134	1	"8626820".pn.	US-PGPUB; USPAT	OR	OFF	2016/03/24 10:42
S135	1284	information adj dispersal adj algorithm	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:32
S136	823	information adj dispersal adj algorithm and data near6 (slice slices portion section segment) near8 metadata	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:33
S137	334	information adj dispersal adj algorithm and data near6 (slice slices portion section segment) near8 metadata and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:33
S138	338	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:34
S139	305	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and error near6 (encoding encoded encode) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	OFF	2016/09/28 21:34
S140	313	(data information) near3 dispersal and data near6 (slice slices portion section segment) near8 metadata and error near6 (encoding encoded encode) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/09/28 21:34
S141	47	threshold near8 (recover$ recreat$) near8 (share) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 15:49
S142	1	"6690795".pn.	US-PGPUB; USPAT	OR	ON	2016/10/10 16:28
S143	9	threshold near8 (recover$ recreat$) near8 (share) and reed adj solomon and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 16:31
S144	15	threshold near8 (recover$ recreat$) near8 (share) and (reed adj solomon fec error adj correct$) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2016/10/10 16:32
S145	5	jigdfs	US-PGPUB; USPAT	OR	ON	2016/10/10 16:54
S146	61384	(G06F21/85 or G06F11/1076 or G06F3/0647 or G06F3/0619 or G06F3/067 or H04L67/1097 or H04N21/2347 or H04N21/8456 or G06F21/72 or H04N21/222 or H04L9/3242 or G06F21/80 or H04L65/604 or H04W12/02 or G06F11/1008 or G06F2221/2107 or G06F2211/1028).cpc.	US-PGPUB; USPAT	OR	OFF	2018/02/13 09:53

S147	1	"7574579".pn.	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:09
S148	0	"7574579".pn. and error	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S149	1	"7574579".pn. and integrity	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S150	0	"7574579".pn. and (mac hmac)	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S151	1	"7574579".pn. and (code)	US-PGPUB; USPAT	OR	OFF	2018/02/13 11:11
S152	1	"20130272164".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 13:13
S153	1	"20170272942".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 13:13
S154	0	"20130272164".pn. and (pair pairing)	US-PGPUB; USPAT	OR	ON	2018/02/13 13:20
S155	1	"20170272942".pn. and (pair pairing)	US-PGPUB; USPAT	OR	ON	2018/02/13 13:21
S156	456	(dispersed distributed) adj storage adj network and encrypt$ near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 14:09
S157	278	error near6 (encode encoding encoded) near8 (encrypted) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 16:28
S158	466	error near6 (encode encoding encoded) near8 (encrypted) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 16:28
S159	1	("20040172371").pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 17:08
S160	19	(encrypted) near6 interspersed near3 error and (@pd @prad @rlad @ptad @ad) <"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:09
S161	276	(encrypted) near6 integrity near3 code and (@pd @prad @rlad @ptad @ad) <"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:57
S162	185	(encrypted) near6 integrity near3 code and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/13 20:57
S163	32	(intersper$) near3 error near6 (correction correcting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 21:12
S164	38	(intersper$) near3 error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/13 21:13
S165	23	program near3 (id identifier) and	US-	OR	ON	2018/02/13

		(cervetti.xa. cervetti.xp.)	PGPUB; USPAT			21:17
S166	1	program near3 (id identifier) and "20070263864".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 21:18
S167	1	program near3 (id identifier) and "20030123664".pn.	US-PGPUB; USPAT	OR	ON	2018/02/13 21:21
S168	12	program near3 (id identifier) and error and (cervetti.xa. cervetti.xp.)	US-PGPUB; USPAT	OR	ON	2018/02/13 21:22
S169	981	(distributed dispersed) adj storage adj network.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/02/16 13:11
S170	1	"8275132".pn.	US-PGPUB; USPAT	OR	OFF	2018/02/17 07:57
S171	5359	data near5 (dispersal dispersion dispersing dispersed) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/02/17 09:06
S173	76	data near5 (dispersal dispersion dispersing dispersed) near8 (encrypt$ crypto$) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/02/17 09:07
S174	480	(desequenc$ de-sequenc$ de adj sequencing de adj sequence sequence sequencing) near5 order near8 (packet slice data message datagram segment block frame) and (encrypt$ crypto$) near8 (packet slice data message datagram segment block frame) near8 (ordering reordering order re-order) and (nothing adj transformation error crc)	US-PGPUB; USPAT	OR	ON	2018/06/21 20:40
S175	214	(dispersed distributed disperse) adj storage adj network and (encrypt$ crypto$) near6 (data content) near6 (slice segment part portion section packet) and (order ordering ordered reorder reordered reordering sequence sequencing) near6 (data content) near6 (slice segment part portion section packet) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/07/08 11:13
S176	548	(dispersed distributed) adj storage adj network and encrypt$ and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/06 15:15
S177	201	data near5 (dispersal dispersion dispersing dispersed) near8 (encrypt$ crypto$) and error near6 (correction correcting detection detecting) and (@pd @prad @rlad @ptad @ad)<"20140805"	US-PGPUB; USPAT	OR	ON	2018/08/06 17:09
S178	550	reed adj solomon adj code and (distribution identity) adj matrix	US-PGPUB; USPAT	OR	ON	2018/08/07 10:44
S179	0	rehm.xp.	US-PGPUB; USPAT	OR	ON	2018/08/07 10:50
S180	44	rehm.xa.	US-	OR	ON	2018/08/07

			PGPUB; USPAT			10:50
S181	663	(dispersed distributed) adj storage adj network and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/07 20:12
S182	1659	dispers$ near5 storage near4 error near5 (encrypt$ decrypt$ crypto$ encod$ decod$)	US-PGPUB; USPAT	OR	ON	2018/08/07 20:45
S183	1658	dispers$ near5 storage near4 error near5 (encod$ decod$)	US-PGPUB; USPAT	OR	ON	2018/08/07 20:45
S184	1	"10000000".pn.	US-PGPUB; USPAT	OR	ON	2018/08/07 20:57
S185	1116	speed near4 light near4 faster	US-PGPUB; USPAT	OR	ON	2018/08/07 20:59
S186	588	speed near4 light near4 faster and (@pd @prad @rlad @ptad @ad)>"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/07 21:00
S187	859	(distributed dispersed) adj storage adj network.clm. and error.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/08/07 22:01
S188	851	(distributed dispersed) adj storage adj network.clm. and error.clm. and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	OFF	2018/08/07 22:02
S189	312	distributed adj storage adj network and (random$ pseudorandom$ reorder$ order$) near6 (slice packet segment) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	OFF	2018/08/07 22:02
S190	859	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (grube markison resch leggette).in.	US-PGPUB; USPAT	OR	ON	2018/08/07 22:17
S191	208	reed adj solomon adj code and (distribution identity) adj matrix and galois	US-PGPUB; USPAT	OR	ON	2018/08/08 09:02
S192	401	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling)	US-PGPUB; USPAT	OR	OFF	2018/08/08 09:57
S193	46	laforgia.xa.	US-PGPUB; USPAT	OR	OFF	2018/08/08 21:17
S194	368	laforgia.xp.	US-PGPUB; USPAT	OR	OFF	2018/08/08 21:17
S195	248	information adj dispersal and error adj encoding and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2018/08/09 08:38
S196	8	("8677214" "9076138" "9021263" "8918897" "8744071" "8782494"	USPAT	OR	OFF	2018/12/03 06:19

		"8856617" "9128870").pn.				
S199	94868	(G06F21/85 or G06F21/6218 or G06F21/606 or H04L9/0894 or H04W12/0013 or H04N21/222 or H04N21/2347 or H04N21/8456 or G06F11/1076 or G06F21/72 or G06F21/80 or H04L67/1097 or G06F3/0619 or G06F3/0647 or G06F3/067 or H04L9/3242 or G06F2221/2107 or G06F11/1008 or H04W12/02 or G06F2211/1028 or H04L65/604).cpc.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:12
S200	94868	(G06F21/85 G06F21/6218 G06F21/606 H04L9/0894 H04W12/0013 H04N21/222 H04N21/2347 H04N21/8456 G06F11/1076 G06F21/72 G06F21/80 H04L67/1097 G06F3/0619 G06F3/0647 G06F3/067 H04L9/3242 G06F2221/2107 G06F11/1008 H04W12/02 G06F2211/1028 H04L65/604).cpc.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:13
S201	2	"8959366".pn. "10282564".pn.	US-PGPUB; USPAT	OR	OFF	2019/06/26 08:56
S202	152	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation)	US-PGPUB; USPAT	OR	OFF	2019/06/26 09:20
S203	165	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation)	US-PGPUB; USPAT	OR	ON	2019/06/26 09:20
S205	121	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and error near6 (encode encoded encoding)	US-PGPUB; USPAT	OR	ON	2019/06/26 09:21
S206	23	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding).clm. and (obfuscate obfuscating obfuscated obfuscation).clm. and error near6 (encode encoded encoding).clm.	US-PGPUB; USPAT	OR	ON	2019/06/26 09:22
S207	52	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and (data error information content) near6 (encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 09:36
S208	62	information near3 dispersal near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content) near6 (encode encoded encoding) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 09:46
S209	65	information near3 dispersal near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad)	US-PGPUB; USPAT	OR	ON	2019/06/26 09:47

		<"20100128"				
S210	74	(data information) near3 (dispersal dispersing dispersion disperse dispersed) near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 10:01
S211	133	(data information) near3 (scater scattering scattered split splitting dispersal dispersing dispersion disperse dispersed) near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 10:03
S212	623	vmac	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S213	291	vmac and wireless	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S214	269	vmac and wireless and virtual$	US-PGPUB; USPAT	OR	ON	2019/06/26 10:07
S215	3017	vmac vnic	US-PGPUB; USPAT	OR	ON	2019/06/26 10:11
S216	96	vmac and vnic	US-PGPUB; USPAT	OR	ON	2019/06/26 10:11
S217	2	("8327141" "20100199089").pn. and (data information) near3 (scater scattering scattered split splitting dispersal dispersing dispersion disperse dispersed) near3 algorithm and (obfuscate obfuscating obfuscated obfuscation) and (data error information content metadata auxiliary) near6 (encrypt encrypting encrypted encryption encode encoded encoding) and (@pd @prad @rlad @ptad @ad) <"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 11:37
S218	1913	dispersed adj storage adj error	US-PGPUB; USPAT	OR	ON	2019/06/26 12:08
S219	1654	dispersed adj storage adj error adj encoding	US-PGPUB; USPAT	OR	ON	2019/06/26 12:09
S220	17	dispersed adj storage adj error adj encoding and auxiliary adj data	US-PGPUB; USPAT	OR	ON	2019/06/26 12:09
S221	1653	dispersed adj storage adj error adj encoding and encrypt$	US-PGPUB; USPAT	OR	ON	2019/06/26 12:10
S222	75	dispersed adj storage adj error adj	US-	OR	ON	2019/06/26

		encoding and encrypt$ and (obfuscate obfuscation)	PGPUB; USPAT			12:10
S223	4	dispersed adj storage adj error adj encoding and encrypt$ and (obfuscate obfuscation) and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 12:10
S224	166	dispersed adj storage adj error adj encoding and encrypt$ and (@pd @prad @rlad @ptad @ad)<"20100128"	US-PGPUB; USPAT	OR	ON	2019/06/26 12:11
S225	154	(dispersed dispersing disperse dispersion) near6 (encode encoded encoding) and (obfuscate obfuscating obfuscated obfuscation) and data near6 (encode encoded encoding)	US-PGPUB; USPAT	OR	ON	2019/06/26 15:13
S226	224	reed adj solomon adj code and (distribution identity) adj matrix and galois	US-PGPUB; USPAT	OR	ON	2019/06/26 18:26

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S69	8	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:27
S70	1	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:28
S71	1	(distributed dispersed) adj storage adj network.clm. and error.clm. and data adj slice.clm. and (encrypted encrypt encrypting).clm. and (encode encoded encoding).clm. and (grube markison resch leggette).in.	USPAT	OR	ON	2014/10/05 11:30
S197	187	(random randomly pseudorandom$ pseudo adj random$) near8 (order ordered ordering) near6 (frame datagram packet slice content data information) and (frame datagram packet slice content data information) near6 (auxiliary metadata) and (frame datagram packet slice content data information) near8 (assemble assembling)	USPAT	OR	OFF	2018/12/03 08:30
S198	119	information adj dispersal and encrypt$ and error adj encoding and (@pd @prad @rlad @ptad @ad)<"20100128"	USPAT	OR	ON	2018/12/03 08:41

6/26/2019 9:20:12 PM
C:\Users\dcervetti\Documents\EAST\Workspaces\16-197-275-06-26-2019-14452182-09252015-12954880-12042012.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/197,275	11/20/2018	Jason K. Resch	CS00403_END920165769US09

CONFIRMATION NO. 4290

89322
Garlick & Markison (IBM)
100 Congress Avenue, Suite 2000
Austin, TX 78701

PUBLICATION NOTICE

OC000000107339287

Title:SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE

Publication No.US-2019-0108366-A1
Publication Date:04/11/2019

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
16/197,275	11/20/2018	2482	1720	CS00403_END920165769US09	16	2

CONFIRMATION NO. 4290

FILING RECEIPT

89322
Garlick & Markison (IBM)
106 E. 6th Street, Suite 900
Austin, TX 78701

OC000000104737092

Date Mailed: 12/31/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Jason K. Resch, Chicago, IL;
S. Christopher Gladwin, Chicago, IL;
Thomas F. Shirley JR., Wauwatosa, WI;
Gary W. Grube, Barrington Hills, IL;

Applicant(s)

International Business Machines Corporation, Armonk, NY;

Power of Attorney: The patent practitioners associated with Customer Number 89322

Domestic Priority data as claimed by applicant

This application is a CIP of 14/452,182 08/05/2014
which is a CON of 12/954,880 11/28/2010 PAT 8959366
which claims benefit of 61/299,245 01/28/2010

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 118
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

If Required, Foreign Filing License Granted: 12/27/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/197,275**

Projected Publication Date: 04/11/2019

Non-Publication Request: No

Early Publication Request: No
Title

SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE

Preliminary Class

375

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
16/197,275

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	16 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 460 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1720

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT A	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT A	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT A	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
AMENDMENT B	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
AMENDMENT B	Application Size Fee (37 CFR 1.16(s))									
AMENDMENT B	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16197275
Filing Date	2018-11-20
First Named Inventor	Jason K. Resch
Art Unit	
Examiner Name	
Attorney Docket Number	CS00403_END920165769US09

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4092732	A	1978-05-30	Ouchi	
	2	5485474	A	1996-01-16	Rabin	
	3	5535239		1996-07-09	Padovani et al.	
	4	5621799		1997-04-15	Katta et al.	
	5	5774643	A	1998-06-30	Lubbers et al.	
	6	5809285	A	1998-09-15	Hilland	
	7	5890156	A	1999-03-30	Rekieta et al.	
	8	5910182		1999-06-08	Dent et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	9	5987622	A	1999-11-16	Lo Verso et al.	
	10	5991414	A	1999-11-23	Garay et al.	
	11	6012159	A	2000-01-04	Fischer et al.	
	12	6058454	A	2000-05-02	Gerlach et al.	
	13	6128277	A	2000-10-03	Bruck et al.	
	14	6175571	B1	2001-01-16	Haddock et al.	
	15	6418539	B1	2002-07-09	Walker	
	16	6571212		2003-05-27	Dent	
	17	6690795		2004-02-10	Richards	
	18	6718361	B1	2004-04-06	Basani et al.	
	19	6826711	B2	2004-11-30	Moulton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	20	7103824	B2	2006-09-05	Halford	
	21	7272602		2007-09-18	Moulton	
	22	7406595		2008-07-29	Boyle Jr. et al.	
	23	7457415		2008-11-25	Reitmeier et al.	
	24	7472334		2008-12-30	Scott et al.	
	25	7509420		2009-03-24	Moulton et al.	
	26	7577689		2009-08-18	Masinter et al.	
	27	7636724	B2	2009-12-22	de la Torre et al.	
	28	7707645		2010-04-27	Haruki et al.	
	29	7991746		2011-08-02	Krishnaiyer et al.	
	30	8275132		2012-09-25	Buchen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	31	8392474		2013-03-05	Franco et al.	
	32	8522125		2013-08-27	Feng et al.	
	33	8560930		2013-10-15	Li et al.	
	34	8626820		2014-01-07	Levy	
	35	8649521		2014-02-11	Grube et al.	
	36	8677214		2014-03-18	Grube et al.	
	37	8744071		2014-06-03	Leggette et al.	
	38	8782494		2014-07-15	Grube et al.	
	39	8856617		2014-10-07	Grube et al.	
	40	8885821		2014-11-11	Grube et al.	
	41	8904080		2014-12-02	Martin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	42	8918897		2014-12-23	Resch	
	43	8959336		2015-02-17	Lee	
	44	9015301		2015-04-21	Redlich et al.	
	45	9021263		2015-04-28	Resch et al.	
	46	9076138		2015-07-07	Resch	
	47	9128870		2015-09-08	Grube et al.	
	48	9135456		2015-09-15	OHare et al.	
	49	9854331		2017-12-26	Winograd et al.	
	50	9854332		2017-12-26	Winograd et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	1	20020002675	A1	2002-01-03	BUSH	
	2	20020003881	A1	2002-01-10	REITMEIER et al.	
	3	20020046359	A1	2002-04-18	Boden	
	4	20020062422	A1	2002-05-23	Butterworth et al.	
	5	20020078227	A1	2002-06-20	Kronenberg	
	6	20020166079	A1	2002-11-07	Ulrich Thomas R. et al.	
	7	20030002665	A1	2003-01-02	Sako et al.	
	8	20030012372	A1	2003-01-16	Cheng	
	9	20030018927	A1	2003-01-23	Gadir Omar M.A. et al.	
	10	20030028879	A1	2003-02-06	Gordon Donald F. et al.	
	11	20030123664	A1	2003-07-03	Pedlow Leo M. JR. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	12	20040024963	A1	2004-02-05	Talagala et al.	
	13	20040117718	A1	2004-06-17	Manasse	
	14	20040145661	A1	2004-07-29	Murakami et al.	
	15	20040172549	A1	2004-09-02	Kojima et al.	
	16	20040215998	A1	2004-10-28	Buxton Robert F. et al.	
	17	20050123271	A1	2005-06-09	Ichinose et al.	
	18	20050131993	A1	2005-06-16	Fatula	
	19	20050265349	A1	2005-12-01	Garg et al.	
	20	20060056519	A1	2006-03-16	Horowitz et al.	
	21	20060069719	A1	2006-03-30	McCanne et al.	
	22	20060069964	A1	2006-03-30	Hayashi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	23	20060177061	A1	2006-08-10	Orsini et al.	
	24	20060212782	A1	2006-09-21	Li	
	25	20070079081	A1	2007-04-05	Gladwin et al.	
	26	20070079082	A1	2007-04-05	Gladwin et al.	
	27	20070079083	A1	2007-04-05	Gladwin et al.	
	28	20070100913	A1	2007-05-03	Sumner et al.	
	29	20070160198	A1	2007-07-12	Orsini et al.	
	30	20070226145	A1	2007-09-27	Ishigaki et al.	
	31	20070263864	A1	2007-11-15	BUCHEN et al.	
	32	20080010218	A1	2008-01-10	Zank	
	33	20080049930	A1	2008-02-28	You et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

	34	20080147821	A1	2008-06-19	Dietrich et al.	
	35	20080192936	A1	2008-08-14	Bellwood et al.	
	36	20080222480	A1	2008-09-11	Huang et al.	
	37	20080222481	A1	2008-09-11	Huang et al.	
	38	20080263113	A1	2008-10-23	Krishnaiyer et al.	
	39	20080320151	A1	2008-12-25	McCanne et al.	
	40	20090041235	A1	2009-02-12	Reitmeier et al.	
	41	20090055547	A1	2009-02-26	Hudson et al.	
	42	20100266122	A1	2010-10-21	Suzaki et al.	
	43	20120198302	A1	2012-08-02	Otterstedt et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Aschenbrenner et al., Infrastructure for Interactivity- Decoupled Systems on the Loose, 2009, IEEE.	
	2	Bellare et al., Robust Computational Secret Sharing and a Unified Account of Classical Secret-Sharing Goals, Nov 2007, ACM.	
	3	BIAN, JigDFS: A Secure Distributed File System, 2009	
	4	Jensen et al., Resilia: a Safe and Secure Distributed Backup System for Small and Medium Enterprises, 2007, Springer.	
	5	KUBIATOWICZ, et al.; OceanStore: An Architecture for Global-Scale Persistent Storage; Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2000); November 2000; pp 1-12	
	6	Schuman et al., A Performance Comparison of Open-Source Erasure Coding Libraries for Storage Applications, Aug 2008,University of Tennessee.	
	7	Storer et al., Long-Term Threats to Secure Archives, Oct 2006, ACM.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16197275
	Filing Date	2018-11-20
	First Named Inventor	Jason K. Resch
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CS00403_END920165769US09

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patricia A. Markison/	Date (YYYY-MM-DD)	2018-11-26
Name/Print	Patricia A. Markison	Registration Number	73072

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	34398262
Application Number:	16197275
International Application Number:	
Confirmation Number:	4290
Title of Invention:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE
First Named Inventor/Applicant Name:	Jason K. Resch
Customer Number:	89322
Filer:	Patricia A. Markison/Kimberly Brown
Filer Authorized By:	Patricia A. Markison
Attorney Docket Number:	CS00403_END920165769US09
Receipt Date:	26-NOV-2018
Filing Date:	
Time Stamp:	19:49:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	CS00403_END920165769US09_IDS.pdf	1037862 31df1f76fac2372cbeea2cc566b1cd3999a352ce	no	13

Warnings:

Information:	
Total Files Size (in bytes):	1037862

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT5247397

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
JASON K. RESCH	11/19/2018
S. CHRISTOPHER GLADWIN	11/19/2018
THOMAS F. SHIRLEY JR.	11/19/2018
GARY W. GRUBE	10/12/2018

RECEIVING PARTY DATA

Name:	INTERNATIONAL BUSINESS MACHINES CORPORATION
Street Address:	NEW ORCHARD ROAD
City:	ARMONK
State/Country:	NEW YORK
Postal Code:	10504

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	16197275

CORRESPONDENCE DATA

Fax Number: (888)708-9048

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Email: ktaylor@texaspatents.com
Correspondent Name: GARLICK & MARKISON
Address Line 1: 106 E. 6TH STREET, SUITE 900
Address Line 4: AUSTIN, TEXAS 78701

ATTORNEY DOCKET NUMBER:	CS00403_END920165769US09
NAME OF SUBMITTER:	KIMBERLY BROWN
SIGNATURE:	/KIMBERLY BROWN/
DATE SIGNED:	11/20/2018
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 3
source=CS00403_END920165769US09_Asg-Dec_signed#page1.tif
source=CS00403_END920165769US09_Asg-Dec_signed#page2.tif

source=CS00403_END920165769US09_Asg-Dec_signed#page3.tif

DECLARATION (37 C.F.R. § 1.63) FOR UTILITY PATENT APPLICATION USING AN APPLICATION DATA SHEET (37 C.F.R. § 1.76) AND ASSIGNMENT

Title of Invention: **SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE**

As a below named and undersigned inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked):

[X] United States application or PCT international application number 16/197,275 filed on 11/20/2018.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. § 1.56.

Whereas, I ("ASSIGNOR") have made certain inventions, improvements, and discoveries (herein referred to as the "Invention") disclosed in the above-identified patent application and further identified by the IBM Docket Number provided above in the header of this document;

Whereas, International Business Machines Corporation (herein referred to as the "ASSIGNEE"), a corporation of New York having a place of business at Armonk, New York, desires to acquire, and I desire to grant to the ASSIGNEE, my entire worldwide right, title, and interest in and to the Invention and in and to any and all patent applications and patents directed thereto;

Now, therefore, for good and valuable consideration, the receipt and sufficiency thereof being hereby acknowledged, I hereby sell or have sold, assign or have assigned, and otherwise transfer or have transferred to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the Invention, the above-identified United States patent application, and any and all other patent applications and patents for the Invention which may be applied for or granted therefor in the United States and in all foreign countries and jurisdictions, including all divisions, continuations, reissues, reexaminations, renewals, extensions, counterparts, substitutes, and extensions thereof, and all rights of priority resulting from the filing of such applications and granting of such patents. In addition, I hereby authorize and request the Director of the United States Patent and Trademark Office to issue any United States Patent, and foreign patent authorities to issue any foreign patent, granted for the Invention, to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the same to be held and enjoyed by the ASSIGNEE, its successors, legal representatives, and assigns to the full end of the terms for which any and all such patents may be granted, as fully and entirely as would have been held and enjoyed by me had this Assignment not been made; and I agree to execute any and all documents and instruments and perform all lawful acts reasonably related to recording this Assignment or perfecting title to the Invention and all related patents and applications, in the ASSIGNEE, its successors, legal

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 139
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of New York, and any disputes will be resolved in a New York state court or federal court sited in New York.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

(1) Legal Name of Inventor: Jason K. Resch

Signature: / Jason Resch / Date: 11-19-18

(2) Legal Name of Inventor: S. Christopher Gladwin

Signature: / / Date:

(3) Legal Name of Inventor: Thomas F. Shirley, Jr.

Signature: / Thomas F. Shirley / Date: 19 Nov 18

(4) Legal Name of Inventor: Gary W. Grube

Signature: / Gary W. Grube / Date: 10/12/2018

representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of New York, and any disputes will be resolved in a New York state court or federal court sited in New York.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

(1) Legal Name of Inventor: Jason K. Resch

Signature: / _____ / Date: _____

(2) Legal Name of Inventor: S. Christopher Gladwin

Signature: / Chris Gladwin / Date: 19 Nov 2018

(3) Legal Name of Inventor: Thomas F. Shirley, Jr.

Signature: / _____ / Date: _____

(4) Legal Name of Inventor: Gary W. Grube

Signature: / Gary W Grube / Date: 10/12/2018

Security First Innovations, LLC, Exhibit 2012
Scanned with CamScanner
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	**TBD**
Filing Date	**Herewith**
First Named Inventor	**Jason K. Resch**
Title	**SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE**
Art Unit	
Examiner Name	
Attorney Docket Number	**CS00403_END920165769US09**

SIGNATURE of Applicant or Patent Practitioner

Signature	**/Patricia A. Markison/**	Date (Optional)	**11/20/2018**
Name	**Patricia A. Markison**	Registration Number	**73,072**
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☒ *Total of **1** forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 89322

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

International Business Machines Corporation

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	4/6/2016
Name	Timothy M. Farrell, Reg. No. 37,321		
Title	Counsel, International Business Machines Corporation		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No.:	CS00403_END920165769US09
First Named Inventor:	Jason K. Resch
Filing Date:	Herewith
Title:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE

Date: 11/20/2018

United States Patent and Trademark Office
P. O. Box 1450
Alexandria, VA 22313-1450

The present application claims priority, as a continuation, continuation-in-part, or a divisional of U.S. Utility Application No. 14/452,182, filed 8/5/2014, co-pending, entitled "DISTRIBUTED STORAGE WITH AUXILIARY DATA INTERSPERSAL AND METHOD FOR USE THEREWITH," may also claim priority to one or more other applications and/or patents, and may be related to other applications and/or related patents, as detailed within the Application Data Sheet and/or the Specification of the present application along with any other applications and/or patents that claim priority from any of the foregoing (collectively, "Predecessor Applications").

The Examiner is advised that the prior art cited in the Predecessor Applications should be reviewed and cited during examination of the present application per the Manual of Patent Examining Procedure Section 904. The Examiner is advised that the rejections made, amendments made, and arguments made in the Predecessor Applications should be reviewed and considered during examination of the present application.

The Examiner is advised that any disclaimer that may be made in the present application should not be read into or against the Predecessor Applications or any patents issuing therefrom. Further, the Examiner is also advised that any disclaimer made in a Predecessor Application is not to be read into or against the present application.

RESPECTFULLY SUBMITTED,

By: /Patricia A. Markison/Reg. No. 73072
Patricia A. Markison

Garlick & Markison
106 E. 6th Street, Suite 900
Austin, TX 78701
Phone: (808) 283-3608
E-mail: pmarkison@texaspatents.com

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE
First Named Inventor/Applicant Name:	Jason K. Resch
Filer:	Patricia A. Markison/Kimberly Brown
Attorney Docket Number:	CS00403_END920165769US09

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1720**

Electronic Acknowledgement Receipt

EFS ID:	34368598
Application Number:	16197275
International Application Number:	
Confirmation Number:	4290
Title of Invention:	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE
First Named Inventor/Applicant Name:	Jason K. Resch
Customer Number:	89322
Filer:	Patricia A. Markison/Kimberly Brown
Filer Authorized By:	Patricia A. Markison
Attorney Docket Number:	CS00403_END920165769US09
Receipt Date:	20-NOV-2018
Filing Date:	
Time Stamp:	20:38:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1720
RAM confirmation Number	112118INTEFSW00006866090457
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	CS00403_END920165769US09_ADS.pdf	1793553 f794aa23c6e13080bf2c23302b18cafd19ecef10	no	9
Warnings:					
Information:					
2		CS00403_END920165769US09_Patent_Application.pdf	330405 749c4cbd10f9e827e2d0b79881fbb70ffed4e954	yes	51

Multipart Description/PDF files in .zip description

Document Description	Start	End
Abstract	51	51
Claims	45	50
Specification	1	44

Warnings:					
Information:					
3	Drawings-only black and white line drawings	CS00403_END920165769US09_Drawings.pdf	741137 eb909fa661eb6b84eaeab317cab6a6d59b861d7d	no	31
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Oath or Declaration filed	CS00403_END920165769US09_Asg-Dec_signed.pdf	2292018 d6c0fc5744276759e1b6ecf698e93b2219cd1564	no	3
Warnings:					
Information:					

5	Power of Attorney	CS00403_END920165769US09_POA.pdf	726072 d1ade8058c275fbfe4a22705d706888cc0196892	no	2
Warnings:					
Information:					
6	Transmittal Letter	CS00403_END920165769US09_AppStmt.pdf	68828 3f168fffea3e037d4a002ce6a478097c3b8afd24	no	1
Warnings:					
Information:					
7	Non Patent Literature	1_NPL_Jensen.pdf	2172361 a0a7fe9c4484a6025a8a7d0c3793305079bae3d5	no	16
Warnings:					
Information:					
8	Non Patent Literature	2_NPL18_Kubiatowicz.pdf	175466 577436dc0d6001f7a8c89751be0e3862ed6ddd9a	no	12
Warnings:					
Information:					
9	Non Patent Literature	3_NPL_Bian.pdf	1673016 f355cf4855bdde018d6605074943a3e83d1eee04	no	7
Warnings:					
Information:					
10	Non Patent Literature	4_NPL_Schuman.pdf	256347 cab9dba123c9b782e2685883fa1c365318442e61	no	13
Warnings:					
Information:					
11	Non Patent Literature	5_NPL_Bellare.pdf	414045 978bc2008cf74dae4ce23b80013f919ff18059b5	no	36
Warnings:					
Information:					

12	Non Patent Literature	6_NPL_Aschenbrenner.pdf	218179 86c79fa19d9086ca581c71f9954fe55e9db0ddcc	no	6
Warnings:					
Information:					
13	Non Patent Literature	7_NPL_Storer.pdf	242544 20360c1f80fe19edf59ab4c18e57c6c7c8ad20af	no	7
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	35334 3e05838fa5af2f0648133f3341e2f62037cfaaa0	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	11139305	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jason	K.	Resch	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	Chicago	State/Province	IL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	222 South Riverside Plaza, Ste. 170&182
Address 2	
City	Chicago
State/Province	IL
Postal Code	60606
Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	S.	Christopher	Gladwin	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	Chicago	State/Province	IL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	843 W. Webster Avenue
Address 2	
City	Chicago
State/Province	IL
Postal Code	60614
Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Thomas	F.	Shirley	Jr.

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

City	Wauwatosa	State/Province	WI	Country of Residence i	US

Mailing Address of Inventor:

Address 1	222 South Riverside Plaza, Ste. 170&182		
Address 2			
City	Chicago	State/Province	IL
Postal Code	60606	Country i	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Gary	W.	Grube	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	Barrington Hills	State/Province	IL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	2 Ridgecroft Lane		
Address 2			
City	Barrington Hills	State/Province	IL
Postal Code	60010	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	89322		
Email Address	PMARKISON@TEXASPATENTS.COM	Add Email	Remove Email

Application Information:

Title of the Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE		
Attorney Docket Number	CS00403_END920165769US09	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	31	Suggested Figure for Publication (if any)	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89322		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation in part of	14/452182	2014-08-05

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/452182	Continuation of	12/954880	2010-11-28	8959366	2015-02-17
Prior Application Status	Expired				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12/954880	Claims benefit of provisional	61/299245	2010-01-28		
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.					Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	International Business Machines Corporation		
Mailing Address Information For Applicant:			
Address 1	New Orchard Road		
Address 2			
City	Armonk	**State/Province**	NY
Country	US	Postal Code	10504
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Patricia A. Markison/			Date (YYYY-MM-DD)	2018-11-20
First Name	Patricia A.	Last Name	Markison	Registration Number	73072

Additional Signature may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CS00403_END920165769US09
	Application Number	
Title of Invention	SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ABSTRACT OF THE DISCLOSURE

A method includes dispersed storage error encoding a plurality of data segments to produce a plurality of sets of encoded data slices and dispersed storage error encoding auxiliary data to produce a set of encoded auxiliary data slices. The method further includes obfuscating a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices. The method further includes obfuscating a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices. The method further includes outputting the first and second sets of obfuscated encoded data slices for storage.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 160
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CLAIMS

What is claimed is:

1. A method comprises:

dispersed storage error encoding, by a computing device of a dispersed storage network (DSN), a plurality of data segments to produce a plurality of sets of encoded data slices;

dispersed storage error encoding, by the computing device, auxiliary data to produce a set of encoded auxiliary data slices;

obfuscating, by the computing device, a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices;

obfuscating, by the computing device, a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and

outputting, by the computing device, the first and second sets of obfuscated encoded data slices for storage.

2. The method of claim 1 further comprises:

dispersed storage error encoding, by the computing device, the auxiliary data to produce a second set of encoded auxiliary data slices;

obfuscating, by the computing device, the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices; and

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 161
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

obfuscating, by the computing device, the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

3. The method of claim 1, wherein the auxiliary data comprises one or more of:

null data;
authentication information;
a next pseudo random output sequencing order;
a pseudo random output sequencing order identifier;
a next outputting threshold;
a random number generator output;
an encryption key;
a starting point for the pseudo random output sequencing order;
a device identifier;
a data identifier;
a data type;
a data size indictor;
a priority indicator;
a security indicator; and
a performance indicator.

4. The method of claim 1 further comprises:

encrypting, by the computing device, the plurality of data segments to produce a plurality of encrypted data segments; and

dispersed storage error encoding, by the computing device, the plurality of encrypted data segments to produce the plurality of sets of encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 162
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

5. The method of claim 4 further comprises:

encrypting, by the computing device, the auxiliary data to produce encrypted auxiliary data; and

dispersed storage error encoding, by the computing device, the encrypted auxiliary data to produce the set of encoded auxiliary data slices.

6. The method of claim 5, wherein the auxiliary data is encrypted via an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data.

7. The method of claim 5, wherein the auxiliary data is encrypted via an all or nothing transformation to produce the encrypted auxiliary data and the plurality of data segments is encrypted via an all or nothing transformation to produce the plurality of encrypted data segments.

8. The method of claim 1, wherein the obfuscating the first set of encoded data slices comprises:

interspersing, by the computing device, the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order to produce the first set of obfuscated encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 163
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

9. A computing device of a dispersed storage network (DSN), the computing device comprises:

an interface;

memory; and

a processing module operably coupled to the memory and the interface, wherein the processing module is operable to:

dispersed storage error encode a plurality of data segments to produce a plurality of sets of encoded data slices;

dispersed storage error encode auxiliary data to produce a set of encoded auxiliary data slices;

obfuscate a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices;

obfuscate a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slice of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices; and

output the first and second sets of obfuscated encoded data slices for storage.

10. The computing device of claim 9, wherein the processing module is further operable to:

dispersed storage error encode the auxiliary data to produce a second set of encoded auxiliary data slices;

obfuscate the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices; and

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 164
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

obfuscate the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

11. The computing device of claim 9, wherein the auxiliary data comprises one or more of:

null data;
authentication information;
a next pseudo random output sequencing order;
a pseudo random output sequencing order identifier;
a next outputting threshold;
a random number generator output;
an encryption key;
a starting point for the pseudo random output sequencing order;
a device identifier;
a data identifier;
a data type;
a data size indictor;
a priority indicator;
a security indicator; and
a performance indicator.

12. The computing device of claim 9, wherein the processing module is further operable to:

encrypt the plurality of data segments to produce a plurality of encrypted data segments; and

dispersed storage error encode the plurality of encrypted data segments to produce the plurality of sets of encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 165
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

13. The computing device of claim 12, wherein the processing module is further operable to:

encrypt the auxiliary data to produce encrypted auxiliary data; and

dispersed storage error encode the encrypted auxiliary data to produce the set of encoded auxiliary data slices.

14. The computing device of claim 13, wherein the processing module is further operable to:

encrypt the auxiliary data an encryption methodology used to encrypt the plurality of data segments to produce the encrypted auxiliary data.

15. The computing device of claim 13, wherein the processing module is further operable to:

encrypt the auxiliary data via an all or nothing transformation to produce the encrypted auxiliary data and encrypt the plurality of data segments via an all or nothing transformation to produce the plurality of encrypted data segments.

16. The computing device of claim 9, wherein the processing module is further operable to obfuscate the first set of encoded data slices by:

interspersing the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order to produce the first set of obfuscated encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 166
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

TITLE OF APPLICATION

SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority pursuant to 35 U.S.C. § 120 as a continuation-in-part of U.S. Utility Application No. 14/452,182, entitled "DISTRIBUTED STORAGE WITH AUXILIARY DATA INTERSPERSAL AND METHOD FOR USE THEREWITH," filed 08/05/2014, which claims priority pursuant to 35 U.S.C. § 120 as a continuation of U.S. Utility Application No. 12/954,880, entitled "DE-SEQUENCING ENCODED DATA SLICES," filed 11/28/2010, issued as U.S. Patent No. 8,959,366 on 02/17/2015, which claims priority pursuant to 35 U.S.C. § 119(e) to U.S. Provisional Application No. 61/299,245, entitled "SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE," filed 01/28/2010, all of which are hereby incorporated herein by reference in their entirety and made part of the present U.S. Utility Patent Application for all purposes.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable.

INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC

[0003] Not Applicable.

BACKGROUND OF THE INVENTION

TECHNICAL FIELD OF THE INVENTION

[0004] This invention relates generally to computer networks and more particularly to dispersing error encoded data.

DESCRIPTION OF RELATED ART

[0005] Computing devices are known to communicate data, process data, and/or store data. Such computing devices range from wireless smart phones, laptops, tablets, personal computers (PC), work stations, and video game devices, to data centers that support millions of web searches, stock trades, or on-line purchases every day. In general, a computing device includes a central

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 167
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

processing unit (CPU), a memory system, user input/output interfaces, peripheral device interfaces, and an interconnecting bus structure.

[0006] As is further known, a computer may effectively extend its CPU by using "cloud computing" to perform one or more computing functions (e.g., a service, an application, an algorithm, an arithmetic logic function, etc.) on behalf of the computer. Further, for large services, applications, and/or functions, cloud computing may be performed by multiple cloud computing resources in a distributed manner to improve the response time for completion of the service, application, and/or function. For example, Hadoop is an open source software framework that supports distributed applications enabling application execution by thousands of computers.

[0007] In addition to cloud computing, a computer may use "cloud storage" as part of its memory system. As is known, cloud storage enables a user, via its computer, to store files, applications, etc. on an Internet storage system. The Internet storage system may include a RAID (redundant array of independent disks) system and/or a dispersed storage system that uses an error correction scheme to encode data for storage.

[0008] Additional layers of security may be required when dispersed storage error encoding data for distributed storage depending on the type of data and/or user.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

[0009] Figure 1 is a schematic block diagram of an embodiment of a computing system in accordance with the invention;

[0010] Figure 2 is a schematic block diagram of an embodiment of a computing core in accordance with the invention;

[0011] Figure 3 is a schematic block diagram of an embodiment of a distributed storage processing unit in accordance with the invention;

[0012] Figure 4 is a schematic block diagram of an embodiment of a grid module in accordance with the invention;

[0013] Figure 5 is a diagram of an example embodiment of error coded data slice creation in accordance with the invention;

[0014] Figure 6 is another schematic block diagram of another embodiment of a computing system in accordance with the invention;

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 168
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0015] Figure 7 is another schematic block diagram of an embodiment of a dispersed storage (DS) processing module in accordance with the invention;

[0016] Figure 8A is a schematic block diagram of an embodiment of a storage module in accordance with the invention;

[0017] Figures 8B-8E are diagrams illustrating examples of sequencing and selecting encoded data slices in accordance with the invention;

[0018] Figure 9 is a flowchart illustrating an example of encoding data to produce encoded data slices in accordance with the invention;

[0019] Figure 10 is a flowchart illustrating an example of decoding encoded data slices to produce data in accordance with the invention;

[0020] Figure 11 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0021] Figure 12 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0022] Figure 13 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0023] Figure 14 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0024] Figure 15 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0025] Figure 16 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0026] Figure 17 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0027] Figure 18 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0028] Figure 19 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0029] Figure 20 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 169
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0030] Figure 21 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0031] Figure 22 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0032] Figure 23 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0033] Figure 24 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention;

[0034] Figure 25 is a flowchart illustrating another example of encoding data to produce encoded data slices in accordance with the invention;

[0035] Figure 26 is a flowchart illustrating another example of decoding encoded data slices to produce data in accordance with the invention; and

[0036] Figure 27 is a schematic block diagram of an embodiment of a computing device of the distributed or dispersed storage network (DSN) in accordance with the invention; and

[0037] Figure 28 is a flowchart illustrating an example of secure data transmission utilizing distributed storage in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0038] Figure 1 is a schematic block diagram of a computing system 10 that includes one or more of a first type of user devices 12, one or more of a second type of user devices 14, at least one distributed storage (DS) processing unit 16, at least one DS managing unit 18, at least one storage integrity processing unit 20, and a distributed storage network (DSN) memory 22 coupled via a network 24. The network 24 may include one or more wireless and/or wire lined communication systems; one or more private intranet systems and/or public internet systems; and/or one or more local area networks (LAN) and/or wide area networks (WAN).

[0039] The DSN memory 22 includes a plurality of distributed storage (DS) units 36 for storing data of the system. Each of the DS units 36 includes a processing module and memory and may be located at a geographically different site than the other DS units (e.g., one in Chicago, one in Milwaukee, etc.). The processing module may be a single processing device or a plurality of processing devices. Such a processing device may be a microprocessor, micro-controller, digital signal processor, microcomputer, central processing unit, field programmable gate array,

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 170
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

programmable logic device, state machine, logic circuitry, analog circuitry, digital circuitry, and/or any device that manipulates signals (analog and/or digital) based on hard coding of the circuitry and/or operational instructions. The processing module may have an associated memory and/or memory element, which may be a single memory device, a plurality of memory devices, and/or embedded circuitry of the processing module. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any device that stores digital information. Note that if the processing module includes more than one processing device, the processing devices may be centrally located (e.g., directly coupled together via a wired and/or wireless bus structure) or may be distributedly located (e.g., cloud computing via indirect coupling via a local area network and/or a wide area network). Further note that when the processing module implements one or more of its functions via a state machine, analog circuitry, digital circuitry, and/or logic circuitry, the memory and/or memory element storing the corresponding operational instructions may be embedded within, or external to, the circuitry comprising the state machine, analog circuitry, digital circuitry, and/or logic circuitry. Still further note that, the memory element stores, and the processing module executes, hard coded and/or operational instructions corresponding to at least some of the steps and/or functions illustrated in Figures 1–26.

[0040] Each of the user devices 12 – 14, the DS processing unit 16, the DS managing unit 18, and the storage integrity processing unit 20 may be a portable computing device (e.g., a social networking device, a gaming device, a cell phone, a smart phone, a personal digital assistant, a digital music player, a digital video player, a laptop computer, a handheld computer, a video game controller, and/or any other portable device that includes a computing core) and/or a fixed computing device (e.g., a personal computer, a computer server, a cable set-top box, a satellite receiver, a television set, a printer, a fax machine, home entertainment equipment, a video game console, and/or any type of home or office computing equipment). Such a portable or fixed computing device includes a computing core 26 and one or more interfaces 30, 32, and/or 33. An embodiment of the computing core 26 will be described with reference to Figure 2.

[0041] With respect to the interfaces, each of the interfaces 30, 32, and 33 includes software and/or hardware to support one or more communication links via the network 24 and/or directly. For example, interfaces 30 support a communication link (wired, wireless, direct, via a LAN, via the network 24, etc.) between the first type of user device 14 and the DS processing unit 16. As

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 171
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

another example, DSN interface 32 supports a plurality of communication links via the network 24 between the DSN memory 22 and the DS processing unit 16, the first type of user device 12, and/or the storage integrity processing unit 20. As yet another example, interface 33 supports a communication link between the DS managing unit 18 and any one of the other devices and/or units 12, 14, 16, 20, and/or 22 via the network 24.

[0042] In general and with respect to data storage, the system 10 supports three primary functions: distributed network data storage management, distributed data storage and retrieval, and data storage integrity verification. In accordance with these three primary functions, data can be distributedly stored in a plurality of physically different locations and subsequently retrieved in a reliable and secure manner regardless of failures of individual storage devices, failures of network equipment, the duration of storage, the amount of data being stored, attempts at hacking the data, etc.

[0043] The DS managing unit 18 performs distributed network data storage management functions, which include establishing distributed data storage parameters, performing network operations, performing network administration, and/or performing network maintenance. The DS managing unit 18 establishes the distributed data storage parameters (e.g., allocation of virtual DSN memory space, distributed storage parameters, security parameters, billing information, user profile information, etc.) for one or more of the user devices 12-14 (e.g., established for individual devices, established for a user group of devices, established for public access by the user devices, etc.). For example, the DS managing unit 18 coordinates the creation of a vault (e.g., a virtual memory block) within the DSN memory 22 for a user device (for a group of devices, or for public access). The DS managing unit 18 also determines the distributed data storage parameters for the vault. In particular, the DS managing unit 18 determines a number of slices (e.g., the number that a data segment of a data file and/or data block is partitioned into for distributed storage) and a read threshold value (e.g., the minimum number of slices required to reconstruct the data segment).

[0044] As another example, the DS managing module 18 creates and stores, locally or within the DSN memory 22, user profile information. The user profile information includes one or more of authentication information, permissions, and/or the security parameters. The security parameters may include one or more of encryption/decryption scheme, one or more encryption keys, key generation scheme, and data encoding/decoding scheme.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 172
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0045] As yet another example, the DS managing unit 18 creates billing information for a particular user, user group, vault access, public vault access, etc. For instance, the DS managing unit 18 tracks the number of times user accesses a private vault and/or public vaults, which can be used to generate a per-access bill. In another instance, the DS managing unit 18 tracks the amount of data stored and/or retrieved by a user device and/or a user group, which can be used to generate a per-data-amount bill.

[0046] The DS managing unit 18 also performs network operations, network administration, and/or network maintenance. As at least part of performing the network operations and/or administration, the DS managing unit 18 monitors performance of the devices and/or units of the system 10 for potential failures, determines the devices' and/or units' activation status, determines the devices' and/or units' loading, and any other system level operation that affects the performance level of the system 10. For example, the DS managing unit 18 receives and aggregates network management alarms, alerts, errors, status information, performance information, and messages from the devices 12-14 and/or the units 16, 20, 22. For example, the DS managing unit 18 receives a simple network management protocol (SNMP) message regarding the status of the DS processing unit 16.

[0047] The DS managing unit 18 performs the network maintenance by identifying equipment within the system 10 that needs replacing, upgrading, repairing, and/or expanding. For example, the DS managing unit 18 determines that the DSN memory 22 needs more DS units 36 or that one or more of the DS units 36 needs updating.

[0048] The second primary function (i.e., distributed data storage and retrieval) begins and ends with a user device 12 - 14. For instance, if a second type of user device 14 has a data file 38 and/or data block 40 to store in the DSN memory 22, it sends the data file 38 and/or data block 40 to the DS processing unit 16 via its interface 30. As will be described in greater detail with reference to Figure 2, the interface 30 functions to mimic a conventional operating system (OS) file system interface (e.g., network file system (NFS), flash file system (FFS), disk file system (DFS), file transfer protocol (FTP), web-based distributed authoring and versioning (WebDAV), etc.) and/or a block memory interface (e.g., small computer system interface (SCSI), internet small computer system interface (iSCSI), etc.). In addition, the interface 30 may attach a user identification code (ID) to the data file 38 and/or data block 40.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 173
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0049] The DS processing unit 16 receives the data file 38 and/or data block 40 via its interface 30 and performs a distributed storage (DS) process thereon (e.g., an error coding dispersal storage function). The DS processing 34 begins by partitioning the data file 38 and/or data block 40 into one or more data segments, which is represented as Y data segments. For example, the DS processing 34 may partition the data file 38 and/or data block 40 into a fixed byte size segment (e.g., 2^1 to 2^n bytes, where n =>2) or a variable byte size (e.g., change byte size from segment to segment, or from groups of segments to groups of segments, etc.).

[0050] For each of the Y data segments, the DS processing 34 error encodes (e.g., forward error correction (FEC), information dispersal algorithm, or error correction coding) and slices (or slices then error encodes) the data segment into a plurality of error coded (EC) data slices 42 - 48, which is represented as X slices per data segment. The number of slices (X) per segment, which corresponds to a number of pillars n, is set in accordance with the distributed data storage parameters and the error coding scheme. For example, if a Reed-Solomon (or other FEC scheme) is used in an n/k system, then a data segment is divided into n slices, where k number of slices is needed to reconstruct the original data (i.e., k is the threshold). As a few specific examples, the n/k factor may be 5/3; 6/4; 8/6; 8/5; 16/10.

[0051] For each slice 42 – 48, the DS processing unit 16 creates a unique slice name and appends it to the corresponding slice 42 - 48. The slice name includes universal DSN memory addressing routing information (e.g., virtual memory addresses in the DSN memory 22) and user-specific information (e.g., user ID, file name, data block identifier, etc.).

[0052] The DS processing unit 16 transmits the plurality of EC slices 42 – 48 to a plurality of DS units 36 of the DSN memory 22 via the DSN interface 32 and the network 24. The DSN interface 32 formats each of the slices for transmission via the network 24. For example, the DSN interface 32 may utilize an internet protocol (e.g., TCP/IP, etc.) to packetize the slices 42 – 48 for transmission via the network 24.

[0053] The number of DS units 36 receiving the slices 42 – 48 is dependent on the distributed data storage parameters established by the DS managing unit 18. For example, the DS managing unit 18 may indicate that each slice is to be stored in a different DS unit 36. As another example, the DS managing unit 18 may indicate that like slice numbers of different data segments are to be stored in the same DS unit 36. For example, the first slice of each of the data segments is to be stored in a first DS unit 36, the second slice of each of the data segments is to be stored in a second

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 174
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

DS unit 36, etc. In this manner, the data is encoded and distributedly stored at physically diverse locations to improve data storage integrity and security. Further examples of encoding the data segments will be provided with reference to one or more of Figures 2 – 26.

[0054] Each DS unit 36 that receives a slice 42 – 48 for storage translates the virtual DSN memory address of the slice into a local physical address for storage. Accordingly, each DS unit 36 maintains a virtual to physical memory mapping to assist in the storage and retrieval of data.

[0055] The first type of user device 12 performs a similar function to store data in the DSN memory 22 with the exception that it includes the DS processing. As such, the device 12 encodes and slices the data file and/or data block it has to store. The device then transmits the slices 11 to the DSN memory via its DSN interface 32 and the network 24.

[0056] For a second type of user device 14 to retrieve a data file or data block from memory, it issues a read command via its interface 30 to the DS processing unit 16. The DS processing unit 16 performs the DS processing 34 to identify the DS units 36 storing the slices of the data file and/or data block based on the read command. The DS processing unit 16 may also communicate with the DS managing unit 18 to verify that the user device 14 is authorized to access the requested data.

[0057] Assuming that the user device is authorized to access the requested data, the DS processing unit 16 issues slice read commands to at least a threshold number of the DS units 36 storing the requested data (e.g., to at least 10 DS units for a 16/10 error coding scheme). Each of the DS units 36 receiving the slice read command, verifies the command, accesses its virtual to physical memory mapping, retrieves the requested slice, or slices, and transmits it to the DS processing unit 16.

[0058] Once the DS processing unit 16 has received a read threshold number of slices for a data segment, it performs an error decoding function and de-slicing to reconstruct the data segment. When Y number of data segments has been reconstructed, the DS processing unit 16 provides the data file 38 and/or data block 40 to the user device 14. Note that the first type of user device 12 performs a similar process to retrieve a data file and/or data block.

[0059] The storage integrity processing unit 20 performs the third primary function of data storage integrity verification. In general, the storage integrity processing unit 20 periodically retrieves slices 45, and/or slice names, of a data file or data block of a user device to verify that

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 175
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

one or more slices have not been corrupted or lost (e.g., the DS unit failed). The retrieval process mimics the read process previously described.

[0060] If the storage integrity processing unit 20 determines that one or more slices is corrupted or lost, it rebuilds the corrupted or lost slice(s) in accordance with the error coding scheme. The storage integrity processing unit 20 stores the rebuild slice, or slices, in the appropriate DS unit(s) 36 in a manner that mimics the write process previously described.

[0061] Figure 2 is a schematic block diagram of an embodiment of a computing core 26 that includes a processing module 50, a memory controller 52, main memory 54, a video graphics processing unit 55, an input/output (IO) controller 56, a peripheral component interconnect (PCI) interface 58, an IO interface 60, at least one IO device interface module 62, a read only memory (ROM) basic input output system (BIOS) 64, and one or more memory interface modules. The memory interface module(s) includes one or more of a universal serial bus (USB) interface module 66, a host bus adapter (HBA) interface module 68, a network interface module 70, a flash interface module 72, a hard drive interface module 74, and a DSN interface module 76. Note the DSN interface module 76 and/or the network interface module 70 may function as the interface 30 of the user device 14 of Figure 1. Further note that the IO device interface module 62 and/or the memory interface modules may be collectively or individually referred to as IO ports.

[0062] The processing module 50 may be a single processing device or a plurality of processing devices. Such a processing device may be a microprocessor, micro-controller, digital signal processor, microcomputer, central processing unit, field programmable gate array, programmable logic device, state machine, logic circuitry, analog circuitry, digital circuitry, and/or any device that manipulates signals (analog and/or digital) based on hard coding of the circuitry and/or operational instructions. The processing module 50 may have an associated memory and/or memory element, which may be a single memory device, a plurality of memory devices, and/or embedded circuitry of the processing module 50. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any device that stores digital information. Note that if the processing module 50 includes more than one processing device, the processing devices may be centrally located (e.g., directly coupled together via a wired and/or wireless bus structure) or may be distributedly located (e.g., cloud computing via indirect coupling via a local area network and/or a wide area network). Further note that when the processing module 50

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 176
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

implements one or more of its functions via a state machine, analog circuitry, digital circuitry, and/or logic circuitry, the memory and/or memory element storing the corresponding operational instructions may be embedded within, or external to, the circuitry comprising the state machine, analog circuitry, digital circuitry, and/or logic circuitry. Still further note that, the memory element stores, and the processing module 50 executes, hard coded and/or operational instructions corresponding to at least some of the steps and/or functions illustrated in Figures 1- 26.

[0063] Figure 3 is a schematic block diagram of an embodiment of a dispersed storage (DS) processing module 34 of user device 12 and/or of the DS processing unit 16. The DS processing module 34 includes a gateway module 78, an access module 80, a grid module 82, and a storage module 84. The DS processing module 34 may also include an interface 30 and the DSnet interface 32 or the interfaces 68 and/or 70 may be part of user device 12 or of the DS processing unit 16. The DS processing module 34 may further include a bypass/feedback path between the storage module 84 to the gateway module 78. Note that the modules 78-84 of the DS processing module 34 may be in a single unit or distributed across multiple units.

[0064] In an example of storing data, the gateway module 78 receives an incoming data object that includes a user ID field 86, an object name field 88, and the data object field 40 and may also receive corresponding information that includes a process identifier (e.g., an internal process/application ID), metadata, a file system directory, a block number, a transaction message, a user device identity (ID), a data object identifier, a source name, and/or user information. The gateway module 78 authenticates the user associated with the data object by verifying the user ID 86 with the managing unit 18 and/or another authenticating unit.

[0065] When the user is authenticated, the gateway module 78 obtains user information from the management unit 18, the user device, and/or the other authenticating unit. The user information includes a vault identifier, operational parameters, and user attributes (e.g., user data, billing information, etc.). A vault identifier identifies a vault, which is a virtual memory space that maps to a set of DS storage units 36. For example, vault 1 (i.e., user 1's DSN memory space) includes eight DS storage units (X=8 wide) and vault 2 (i.e., user 2's DSN memory space) includes sixteen DS storage units (X=16 wide). The operational parameters may include an error coding algorithm, the width n (number of pillars X or slices per segment for this vault), a read threshold T, a write threshold, an encryption algorithm, a slicing parameter, a compression algorithm, an integrity

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 177
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

check method, caching settings, parallelism settings, and/or other parameters that may be used to access the DSN memory layer.

[0066] The gateway module 78 uses the user information to assign a source name 35 to the data. For instance, the gateway module 78 determines the source name 35 of the data object 40 based on the vault identifier and the data object. For example, the source name may contain a file identifier (ID), a vault generation number, a reserved field, and a vault identifier (ID). As another example, the gateway module 78 may generate the file ID based on a hash function of the data object 40. Note that the gateway module 78 may also perform message conversion, protocol conversion, electrical conversion, optical conversion, access control, user identification, user information retrieval, traffic monitoring, statistics generation, configuration, management, and/or source name determination.

[0067] The access module 80 receives the data object 40 and creates a series of data segments 1 through Y 90-92 in accordance with a data storage protocol (e.g., file storage system, a block storage system, and/or an aggregated block storage system). The number of segments Y may be chosen or randomly assigned based on a selected segment size and the size of the data object. For example, if the number of segments is chosen to be a fixed number, then the size of the segments varies as a function of the size of the data object. For instance, if the data object is an image file of 4,194,304 eight bit bytes (e.g., 33,554,432 bits) and the number of segments Y = 131,072, then each segment is 256 bits or 32 bytes. As another example, if segment sized is fixed, then the number of segments Y varies based on the size of data object. For instance, if the data object is an image file of 4,194,304 bytes and the fixed size of each segment is 4,096 bytes, the then number of segments Y = 1,024. Note that each segment is associated with the same source name.

[0068] The grid module 82 receives the data segments and may manipulate (e.g., compression, encryption, cyclic redundancy check (CRC), etc.) each of the data segments before performing an error coding function of the error coding dispersal storage function to produce a pre-manipulated data segment. After manipulating a data segment, if applicable, the grid module 82 error encodes (e.g., Reed-Solomon, Convolution encoding, Trellis encoding, etc.) the data segment or manipulated data segment into X error coded data slices 42-44.

[0069] The value X, or the number of pillars (e.g., X = 16), is chosen as a parameter of the error coding dispersal storage function. Other parameters of the error coding dispersal function include a read threshold T, a write threshold W, etc. The read threshold (e.g., T = 10, when X =

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 178
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

16) corresponds to the minimum number of error-free error coded data slices required to reconstruct the data segment. In other words, the DS processing module 34 can compensate for X-T (e.g., 16-10 = 6) missing error coded data slices per data segment. The write threshold W corresponds to a minimum number of DS storage units that acknowledge proper storage of their respective data slices before the DS processing module indicates proper storage of the encoded data segment. Note that the write threshold is greater than or equal to the read threshold for a given number of pillars (X).

[0070] For each data slice of a data segment, the grid module 82 generates a unique slice name 37 and attaches it thereto. The slice name 37 includes a universal routing information field and a vault specific field and may be 48 bytes (e.g., 24 bytes for each of the universal routing information field and the vault specific field). As illustrated, the universal routing information field includes a slice index, a vault ID, a vault generation, and a reserved field. The slice index is based on the pillar number and the vault ID and, as such, is unique for each pillar (e.g., slices of the same pillar for the same vault for any segment will share the same slice index). The vault specific field includes a data name, which includes a file ID and a segment number (e.g., a sequential numbering of data segments 1-Y of a simple data object or a data block number).

[0071] Prior to outputting the error coded data slices of a data segment, the grid module may perform post-slice manipulation on the slices. If enabled, the manipulation includes slice level compression, encryption, CRC, addressing, tagging, and/or other manipulation to improve the effectiveness of the computing system.

[0072] When the error coded data slices of a data segment are ready to be outputted, the grid module 82 determines which of the DS storage units 36 will store the EC data slices based on a dispersed storage memory mapping associated with the user's vault and/or DS storage unit attributes. The DS storage unit attributes may include availability, self-selection, performance history, link speed, link latency, ownership, available DSN memory, domain, cost, a prioritization scheme, a centralized selection message from another source, a lookup table, data ownership, and/or any other factor to optimize the operation of the computing system. Note that the number of DS storage units 36 is equal to or greater than the number of pillars (e.g., X) so that no more than one error coded data slice of the same data segment is stored on the same DS storage unit 36. Further note that EC data slices of the same pillar number but of different segments (e.g., EC data

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 179
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

slice 1 of data segment 1 and EC data slice 1 of data segment 2) may be stored on the same or different DS storage units 36.

[0073] The storage module 84 performs an integrity check on the outbound encoded data slices and, when successful, identifies a plurality of DS storage units based on information provided by the grid module 82. The storage module 84 then outputs the encoded data slices 1 through X of each segment 1 through Y to the DS storage units 36. Each of the DS storage units 36 stores its EC data slice(s) and maintains a local virtual DSN address to physical location table to convert the virtual DSN address of the EC data slice(s) into physical storage addresses.

[0074] In an example of a read operation, the user device 12 and/or 14 sends a read request to the DS processing unit 16, which authenticates the request. When the request is authentic, the DS processing unit 16 sends a read message to each of the DS storage units 36 storing slices of the data object being read. The slices are received via the DSnet interface 32 and processed by the storage module 84, which performs a parity check and provides the slices to the grid module 82 when the parity check was successful. The grid module 82 decodes the slices in accordance with the error coding dispersal storage function to reconstruct the data segment. The access module 80 reconstructs the data object from the data segments and the gateway module 78 formats the data object for transmission to the user device.

[0075] Figure 4 is a schematic block diagram of an embodiment of a grid module 82 that includes a control unit 73, a pre-slice manipulator 75, an encoder 77, a slicer 79, a post-slice manipulator 81, a pre-slice de-manipulator 83, a decoder 85, a de-slicer 87, and/or a post-slice de-manipulator 89. Note that the control unit 73 may be partially or completely external to the grid module 82. For example, the control unit 73 may be part of the computing core at a remote location, part of a user device, part of the DS managing unit 18, or distributed amongst one or more DS storage units.

[0076] In an example of write operation, the pre-slice manipulator 75 receives a data segment 90-92 and a write instruction from an authorized user device. The pre-slice manipulator 75 determines if pre-manipulation of the data segment 90-92 is required and, if so, what type. The pre-slice manipulator 75 may make the determination independently or based on instructions from the control unit 73, where the determination is based on a computing system-wide predetermination, a table lookup, vault parameters associated with the user identification, the type

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 180
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

of data, security requirements, available DSN memory, performance requirements, and/or other metadata.

[0077] Once a positive determination is made, the pre-slice manipulator 75 manipulates the data segment 90-92 in accordance with the type of manipulation. For example, the type of manipulation may be compression (e.g., Lempel-Ziv-Welch, Huffman, Golomb, fractal, wavelet, etc.), signatures (e.g., Digital Signature Algorithm (DSA), Elliptic Curve DSA, Secure Hash Algorithm, etc.), watermarking, tagging, encryption (e.g., Data Encryption Standard, Advanced Encryption Standard, etc.), adding metadata (e.g., time/date stamping, user information, file type, etc.), cyclic redundancy check (e.g., CRC32), and/or other data manipulations to produce the pre-manipulated data segment.

[0078] The encoder 77 encodes the pre-manipulated data segment 92 using a forward error correction (FEC) encoder (and/or other type of erasure coding and/or error coding) to produce an encoded data segment 94. The encoder 77 determines which forward error correction algorithm to use based on a predetermination associated with the user's vault, a time based algorithm, user direction, DS managing unit direction, control unit direction, as a function of the data type, as a function of the data segment 92 metadata, and/or any other factor to determine algorithm type. The forward error correction algorithm may be Golay, Multidimensional parity, Reed-Solomon, Hamming, Bose Ray Chauduri Hocquenghem (BCH), Cauchy-Reed-Solomon, or any other FEC encoder. Note that the encoder 77 may use a different encoding algorithm for each data segment 92, the same encoding algorithm for the data segments 92 of a data object, or a combination thereof.

[0079] The encoded data segment 94 is of greater size than the data segment 92 by the overhead rate of the encoding algorithm by a factor of X/T, where X is the width or number of slices, and T is the read threshold. In this regard, the corresponding decoding process can accommodate at most X-T missing EC data slices and still recreate the data segment 92. For example, if X=16 and T=10, then the data segment 92 will be recoverable as long as 10 or more EC data slices per segment are not corrupted.

[0080] The slicer 79 transforms the encoded data segment 94 into EC data slices in accordance with the slicing parameter from the vault for this user and/or data segment 92. For example, if the slicing parameter is X = 16, then the slicer 79 slices each encoded data segment 94 into 16 encoded slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 181
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0081] The post-slice manipulator 81 performs, if enabled, post-manipulation on the encoded slices to produce the EC data slices. If enabled, the post-slice manipulator 81 determines the type of post-manipulation, which may be based on a computing system-wide predetermination, parameters in the vault for this user, a table lookup, the user identification, the type of data, security requirements, available DSN memory, performance requirements, control unit directed, and/or other metadata. Note that the type of post-slice manipulation may include slice level compression, signatures, encryption, CRC, addressing, watermarking, tagging, adding metadata, and/or other manipulation to improve the effectiveness of the computing system.

[0082] In an example of a read operation, the post-slice de-manipulator 89 receives at least a read threshold number of EC data slices and performs the inverse function of the post-slice manipulator 81 to produce a plurality of encoded slices. The de-slicer 87 de-slices the encoded slices to produce an encoded data segment 94. The decoder 85 performs the inverse function of the encoder 77 to recapture the data segment 90-92. The pre-slice de-manipulator 83 performs the inverse function of the pre-slice manipulator 75 to recapture the data segment 90-92.

[0083] Figure 5 is a diagram of an example of slicing an encoded data segment 94 by the slicer 79. In this example, the encoded data segment 94 includes thirty-two bits, but may include more or less bits. The slicer 79 disperses the bits of the encoded data segment 94 across the EC data slices in a pattern as shown. As such, each EC data slice does not include consecutive bits of the data segment 94 reducing the impact of consecutive bit failures on data recovery. For example, if EC data slice 2 (which includes bits 1, 5, 9, 13, 17, 25, and 29) is unavailable (e.g., lost, inaccessible, or corrupted), the data segment can be reconstructed from the other EC data slices (e.g., 1, 3 and 4 for a read threshold of 3 and a width of 4).

[0084] Figure 6 is a schematic block diagram of another embodiment of a computing system that includes a source user device 12, a plurality of destination user devices 1-D 12, a plurality of wireless modules 102-108, a dispersed storage (DS) processing unit 16, and a dispersed storage network (DSN) memory 22. Each of user devices 12 includes a computing core 26 and a DSN interface 32, wherein the computing core 26 includes a DS processing 34. Each of the wireless modules 102-108 may be portable devices (e.g., cell phone, tablet computer, radio, etc.) or fixed devices (e.g., access point, cellular base station, a radio site, etc.) and each includes a radio frequency transceiver and baseband processing circuitry. The wireless modules 102-108 operate in accordance with one or more wireless industry standards including, but not limited to, universal

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 182
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

mobile telecommunications system (UMTS), global system for mobile communications (GSM), long term evolution (LTE), wideband code division multiplexing (WCDMA), IEEE 802.11, IEEE 802.16.

[0085] Note that a wireless broadcast service is provided by the wireless module 102 by way of a common wireless resource including but not limited to a common frequency division multiplexing frequency (e.g., channel), a common time division multiplexing slot, a common code division multiplexing code, and/or a common frequency hopping sequence. In an example, all slice pillars produced from a common data object are transmitted as wireless signals of a common wireless resource. In another example, each slice pillar produced from the same data object is transmitted as wireless signals via two or more wireless resources (e.g., two or more frequencies).

[0086] In an example of operation, the source user device 12 is contained in a mobile vehicle (e.g., an aircraft, a ship, a truck, etc.) and is operable to securely transmit audio/video (A/V) data (e.g., a live video stream, an image file, a video file, an audio file, a text file, a text communication, etc.) to one or more of the destination user devices and/or to the DSN memory 22. In this example, the source user device 12 receives the audio/video data from an A/V source (e.g., one or more digital cameras, one or more microphones, etc.) and the DS processing module 34 encrypts the A/V data. The DS processing module 34 then partitions the encrypted data into data segments and encodes each of the data segments using a dispersed storage error encoding function to produce a plurality of sets of encoded data slices. Note that a set of encoded data slices corresponds to a data segment of the encrypted data.

[0087] As the DS processing module 34 is producing sets of encoded data slices, it stores them until a threshold number of encoded data slices are stored. Once a threshold number of encoded data slices are stored, the DS processing module 34 outputs encoded data slices to the DSN interface in accordance with a pseudo-random sequencing order. The pseudo-random sequencing order ensures that the encoded data slices of a set of encoded data slices are not outputted sequentially, but are outputted in a random order with encoded data slices of other sets to add further security to the transmission of the A/V data. For example, the pseudo-random sequencing order randomly orders the data segments prior to dispersal storage error encoding and then randomly orders the encoded data slices. As another example, the pseudo-random sequencing order randomly orders the encoded data slices.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 183
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0088] The wireless module 102 converts the randomly ordered encoded data slices into outbound RF signals in accordance with one or more standardized wireless communication protocols or a proprietary wireless communication protocol. For example, the baseband circuitry of the wireless module 102 converts an encoded data slice (a portion or an encoded data slice or multiple encoded data slices) into an outbound symbol stream. The RF transceiver of the wireless module converts the outbound symbol stream into an outbound RF signal.

[0089] At least one of the other wireless modules 104-108 receives the outbound RF signals of wireless module 102 and determines whether it is a destination. For example, the RF signals include destination address information, which the receiving wireless modules interpret to determine whether they are destinations. As another example, the RF signals include source address information, which the receiving wireless modules interpret to determine whether they are destinations for the source.

[0090] When a wireless module 104-108 is a destination, it converts the RF signals into the encoded data slices 110 and provides them to the corresponding DS unit (e.g., user device 12 or DS processing unit 16). The corresponding DS unit uses a pseudo-random de-sequencing order to re-order the received encoded data slices into sets of encoded data slices. The corresponding DS unit then decodes the set of encoded data slices using a dispersal storage error decoding function to produce the data segments, which are decrypted to re-produce the A/V data. To ensure security of the A/V data transmission, the pseudo-random sequencing/de-sequencing order and the dispersal storage error encoding/decoding function is securely communicated between the source user device 12 and the corresponding destination unit(s) (e.g., destination user devices and/or the DS processing unit).

[0091] Figure 7 is a schematic block diagram of another embodiment of a dispersed storage (DS) processing module 34 coupled to the DSnet interface 32 and the processing module 50. The processing module 50 is coupled to one or more data sources (e.g., camera, microphone, text messaging input, etc.) and the DSnet interface 32 is coupled to a wireless module 102. The DS processing module includes a storage module 138, a plurality of interfaces 114-118, a plurality of gateway modules 78, a plurality of access modules 80, and a plurality of grid modules 82. The interface modules 114-118, the gateway modules 78, the access modules 89, and the grid modules 82 are arranged in sets for processing different data (e.g., data 140 – 144), which includes A/V data from one or more data sources (e.g., cameras, computer, microphones, etc.) and/or auxiliary

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 184
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

data 144 (e.g., null data, authentication information, a next pseudo random output sequencing order, a pseudo random output sequencing order identifier, a next outputting threshold, a random number generator output, an encryption key, a starting point for the pseudo random output sequencing order, a device identifier, a data identifier, a data type, a data size indictor, a priority indicator, a security indicator, and/or a performance indicator).

[0092] In a first example of operation, one or more of the data sources provides data to the processing module 50 and/or directly to the DS processing module 34. For example, a first digital camera provides a stream of video directly to interface 114 of the DS processing module 50 and a second camera provides A/V data to the processing module 50 for A/V processing (e.g., video encoding, video decoding, compression, aspect ratio conversion, etc.). The processing module 50 provides the processed A/V data to interface 116 of the DS processing module 34. The processing module, or an auxiliary data source, may also generate auxiliary data 144, which is provided to interface 118 of the DS processing module 34.

[0093] Each set of gateway, access, and grid modules 78, 80, and 82 perform their corresponding functions on the data 140, 142, or auxiliary data 144, to produce one or more sets of slices 146-150. For instance and as discussed with reference to one or more of Figures 1-5, the gateway module 78 accommodates a file system of a data source (e.g., a computing core) by translating a computer file system to a virtual dispersed storage network (DSN) addressing (e.g., a source name). The access module 80 converts the data 140 – 144 into sequential data segments (e.g., segment 1, segment 2, segment 3, etc.). Alternatively, the access module 80 converts the data 140-144 into non-sequential data segments (e.g., segment 4, segment 1, segment 3, etc.) in accordance with a segment sequence sequencing/de-sequencing order. The grid module 82 encrypts and dispersal storage error encodes a data segment into a set of encoded data slices in a sequential order (e.g., pillar 0 slice 1, pillar 0 slice 2 etc., pillar 1 slice 1, pillar 1 slice 2 etc.). Alternatively, the grid module 82 encrypts and dispersal storage error encodes data segments into sets of encoded data slices and outputs the encoded data slices in accordance with the pseudo random sequencing/de-sequencing order (e.g., pillar 4 slice 8, pillar 2 slice 3 etc., pillar 5 slice 4, pillar 0 slice 2 etc.).

[0094] The storage module 138 receives the sets of encoded data slices 146-150 and outputs encoded data slices in accordance with the pseudo random sequencing/de-sequencing order. The random outputting of encoded data slices may be done in combination with the segment

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 185
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

sequencing performed by the access module 80, in combination with encoded data slice output randomize sequencing performed by the grid module 82, done without the sequencing performed by the access module or grid module, and/or a combination thereof.

[0095] As an example of the pseudo random sequencing/de-sequencing order, the storage module selects ten slices from set 1 (e.g., a set from the sets 146) followed by five slices from set 2 (e.g., a set from sets 148) followed by one slice from set 3 (e.g., a set from sets 150) etc. The storage module 138 may determine the random sequence and the starting point for the random sequence via a selection sequence generator and a seed. The seed and/or the identity of the random sequence may be included in the auxiliary data, may be embedded in the data 140, 142, and/or may be communicated using another secure mechanism.

[0096] In a second example of operation, the storage module 138 receives randomly ordered encoded data slices 110 and outputs sets of encoded data slices in accordance with the pseudo random sequencing/de-sequencing order. The grid module 82 decodes the set of encoded data slices 146-150 in accordance with a dispersal storage error decoding function to produce encrypted data segments, which it decrypts to produce data segments. Alternatively, the grid module 82 may re-order the sets of slices in accordance with the pseudo random sequencing/de-sequencing order prior to dispersal storage error decoding.

[0097] The access module 80 converts the data segments into the data 140-144. Alternatively, the access module 80 reorders the data segments in accordance with a segment sequence sequencing/de-sequencing order and then produces the data. The gateway module 78 translates the virtual dispersed storage network (DSN) addressing (e.g., a source name) into a computer file system name. The processing module 50 receives the data 140-144, processes it, and/or provides it to a data destination (e.g., a video monitor, a speaker, DSN memory, etc.).

[0098] Figure 8A is a schematic block diagram of an embodiment of a storage module 138 that includes a plurality of sequencers 160-164, a plurality of sequence generators 166-170, a plurality of de-sequencers 172-176, a plurality of de-sequence generators 178-182, a selector 184, a selection sequence generator 188, a de-selector 186, and a de-selection de-sequence generator 190.

[0099] In an example of operation, the storage module 138 receives sets of encoded data slices 192-196 from the plurality of grid modules 82. Each sequencer 160-162 converts its sets of encoded data slices into randomly ordered sets of encoded data slices accordance with a pseudo

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 186
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

random segment and/or slice sequence generated by the corresponding sequence generators 166-170. For instance, the sequence generators generate a random sequence based on a seed that reorders the corresponding sets of encoded data slices, reorders slices within a set of slices, and/or reorders slices and sets of slices. Alternatively, the sequence generator generates a null sequence such that the sequencer outputs the encoded data slices in the order they were received (i.e., first in, first out).

[0100] The selector 184 selects slices from sequencers 160-164 in accordance with a selection sequence. The selection sequence generator 188 generates the selection sequence in accordance with the pseudo random sequencing/de-sequencing order. As a specific example, the select sequence generator 188 generates a selection sequence that causes the selector 184 to select ten slices from sequencer 160, then five slices from sequencer 162, and then three slices from sequencer 164, which are subsequently outputted as output sequenced slices 204.

[0101] In another example of operation, the de-selector 186 receives input sequenced slices 206 and provides them to the de-sequencers 172-176 in accordance with a de-sequence order. The de-selection de-sequence generator 190 generates the de-sequence order in accordance with the pseudo random sequencing/de-sequencing order. As a specific example, the de-selection de-sequence generator 190 generates the de-sequence order such that the de-selector 186 sends ten slices of the input sequenced slices 206 to de-sequencer 172, the five slices to de-sequencer 174, and then three slices to de-sequencer 176.

[0102] Each of the de-sequencers 172-176 produces sets of encoded data slices as ordered output slices 198-202 in accordance with a slice and/or segment de-sequence order that is generated by a corresponding de-sequence generator 178-182. For instance, the de-sequence generators generate a random sequence based on a seed that reorders the received slices into sets of encoded data slices. Alternatively, the de-sequence generator generates a null sequence such that the de-sequencer outputs the encoded data slices in the order they were received (i.e., first in, first out).

[0103] The segment and/or slice sequence/de-sequence order may be part of the pseudo random sequencing/de-sequencing order. In addition, each pair of sequence generators and de-sequence generators may generate the same sequence/de-sequence order or different sequence/de-sequence orders. Further, the pseudo random sequencing/de-sequencing order includes one or more of one or more slice sequence/de-sequence orders, a selection sequence/de-sequence, a

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 187
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

sequence/de-sequence seed determination, one or more sequence/de-sequence seeds. Still further, the pseudo random sequencing/de-sequencing order may be determined based on one or more of a performance indicator, a security indicator, a security indicator, sequence information, a key, a user device identifier (ID), a lookup, a list, a command, a predetermination, a message, an algorithm, a data object, a data object ID, a data type, a data size, and a hash of the data. Even further, the pseudo random sequencing/de-sequencing order may be generated by any one of a variety of pseudo random number generation techniques that may be implemented in software, programmable logic, and/or a state machine.

[0104] Figure 8B is a diagram illustrating an example of pseudo random sequencing/de-sequencing of encoded data slices within the storage module 138 for two different data streams (e.g., data 1 and data 2). In this example, an encrypted data segment is dispersal storage error encoded into five encoded data slices. For instance, data segment 1 of data 1 is encoded into five encoded data slices (e.g., data 1, segment 1, slice 1, through data 1, segment 1, slice 5).

[0105] For pseudo random sequencing, the storage module 138 receives the encoded data slices of data 1 and data 2, stores them, and when a threshold number (e.g., X times the pillar width, which, for this example is 6 times 5 = 30) applies the pseudo random sequencing order to randomize the outputting of the encoded data slices. In this example, the pseudo random sequencing/de-sequencing order randomized encoded data slices are sequenced and selected to produce slices in order of data 2, segment 2, slice 3 followed by data 1, segment 1, slice 3, followed by data 1, segment 2, slice 1, followed by data 2, segment 3, slice 2, followed by data 2, segment 1, slice 4, etc.

[0106] For pseudo random de-sequencing, the storage module 138 receives the randomized encoded data slices 209, stores them until a threshold number are stored, and then applies the pseudo random de-sequencing order to reproduce the encoded data slices 205 of data 1 and the encoded data slices 207 of data 2. The storage module 138 may output the de-sequenced encoded data slices are they are de-sequenced or store a data segment's worth of slices and then send the set of encoded data slices.

[0107] Figure 8C is a diagram illustrating an example of pseudo random sequencing/de-sequencing of encoded data slices within the storage module 138 for two different data streams (e.g., data 1 and data 2, which may be auxiliary data). In this example, the access module 80 of the DS processing module 34 randomized the data segments prior to the grid module 82 dispersal

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 188
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

storage error encoding the data segments. The randomizing of the data segments may be different for each data path or it may be the same.

[0108] In the present example, the data segments of the first data path are randomized using a first segment sequence to produce, for three data segments, a randomized data segment order of 3, 1, 2. The data segments of the second data path are randomized using a second segment sequence to produce, for three data segments, a randomized data segment order of 2, 1, 3. The storage module 138 randomizes and de-randomizes the encoded data slices of the randomized data segments using the pseudo random sequencing/de-sequencing order as previously discussed.

[0109] Figure 8D is a diagram illustrating an example of pseudo random sequencing/de-sequencing of encoded data slices within the storage module 138 for two different data streams (e.g., data 1 and data 2). In this example, the grid module 82 of the DS processing module 80 randomized the encoded data slices for each data segment it dispersal storage error encodes. The randomizing of the encoded data slices may be different for each data path or it may be the same. The randomizing of the encoded data slices may also be the same or different for each data segment.

[0110] In the present example, each of the data segments of the first and second data paths are randomized using the same sequence to produce, for five encoded data slices per data segment, a randomized encoded data segment order of 2, 1, 5, 4, 3. The storage module 138 randomizes and de-randomizes the randomized encoded data slices using the pseudo random sequencing/de-sequencing order as previously discussed.

[0111] Figure 8E is a diagram illustrating an example of pseudo random sequencing/de-sequencing of encoded data slices within the storage module 138 for two different data streams (e.g., data 1 and data 2). In this example, an encrypted data segment is dispersal storage error encoded into five encoded data slices, but, for at least some of the data segments, less than all of the encoded data slices will be outputted. For instance, the first encoded data slice of data segment 1 of data 1 will not be outputted; the fourth encoded data slice of data segment 2 of data 1 will not be outputted; the second and fifth encoded data slices of data segment 3 of data 1 will not be outputted; the second encoded data slice of data segment 1 of data 2 will not be outputted; and the third encoded data slice of data segment 2 of data 2 will not be outputted.

[0112] For pseudo random sequencing, the storage module 138 receives the encoded data slices of data 1 and data 2, stores them, and a threshold number applies the pseudo random

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 189
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

sequencing order to randomize the outputting of the encoded data slices. When the storage module 138 reaches one of the encoded data slices that is not to be outputted, it outputs a null data slice or repeats one of the other encoded data slices.

[0113] For pseudo random de-sequencing, the storage module 138 receives the randomized encoded data slices 209, stores them until a threshold number are stored, and then applies the pseudo random de-sequencing order to reproduce the encoded data slices 205 of data 1 and the encoded data slices 207 of data 2, less the omitted encoded data slices. When the storage module 138 outputs a set of encoded data slices that includes one or more omitted encoded data slices, it may output the set without the omitted encoded data slice(s) or it may output a null data slice in the place of the omitted encoded data slice.

[0114] The examples of Figures 8B – 8E are equally applicable for data from a single source. In this instance, the pseudo random sequencing/de-sequencing order is applied to sets of encoded data slices of data segments of data from a single source.

[0115] Figure 9 is a flowchart illustrating an example of encoding data to produce encoded data slices. The method begins with step 210 where a processing module receives a store data object message from one or more of a computing core, a user device, a dispersed storage (DS) processing unit, a storage integrity processing unit, a DS managing unit, a DS unit, and a process or function of a user device. The store data object message includes a requester identifier (ID) (e.g., a source user device ID), a target ID (e.g., a destination user device ID), a data object name, data, a data stream (e.g., a video stream), sequence information, a key (e.g., an encryption key), a priority indicator, a security indicator, and/or a performance indicator.

[0116] The method continues at step 212 where the processing module determines one or more sets of error coding dispersal storage function parameters regarding the data of the data object message and for auxiliary data. For example, one set of error coding dispersal storage function parameters may be determined for the data and another set may be determined for the auxiliary data. As another example, the same error coding dispersal storage function parameters are determined for both the data and the auxiliary data.

[0117] The method continues at step 214 where the processing module segments the data in accordance with the error coding dispersal storage function parameters. The processing module segments the data into data segments, which may be outputted in a variety of ways. For example, the processing module outputs the data segments in the order in which they were created (i.e.,

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 190
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

sequentially). As another example, the processing module outputs the data segments in accordance with a segment sequencing order (i.e., pseudo randomly non-sequential).

[0118] The method continues at step 216 where the processing module dispersed storage error encodes the data segments to produce sets of encoded data slices (e.g., one set per data segment). The processing module may output the sets of encoded data slices in a variety of ways. For example, the processing module outputs the encoded data slices of a set in the order in which they were created (i.e., sequentially). As another example, the processing module outputs the encoded data slices of a set in accordance with a segment sequencing order (i.e., pseudo randomly non-sequential). As yet another example, the processing module outputs a threshold number of a set of encoded data slices (e.g., a read threshold, a write threshold, a decode threshold, etc.). As a further example, the processing module buffers a set of encoded data slices in two buffers: the first including a threshold number of encoded data slices and the second including the remaining encoded data slices. In this example, the processing module outputs the encoded data slices of the first buffer and outputs zero to all of the encoded data slices of the second buffer.

[0119] At step 216, the processing module may also generate a slice name for each encoded data slice of a set. The processing module determines slice information for a set of encoded data slices and encrypts the slice information to produce the slice name, which may be buffered.

[0120] The method continues at step 218 where the processing module determines a pseudo-random sequencing order and/or sequence information. For example, the processing module determines a pseudo-random sequencing order associated with algorithm 3AC (e.g. a pseudo random number generation algorithm), a sequence seed of 1F46D8EA39B based on a calculating a hash over requester ID 5F02D77B, and a key of 34D8AB90, which was embedded in the sequencing information.

[0121] The method continues at step 220 where the processing module sequences the outputting of encoded data slices in accordance with the pseudo-random sequencing order. For example, the processing module buffers encoded data slices of the sets until a threshold number have been buffered. When a threshold number of slices have been buffered, the processing module outputs the encoded data slices based on the pseudo-random sequencing order; example of which were discussed with reference to Figures 8B - 8E.

[0122] The method continues at step 222 where the processing module dispersal storage error encodes auxiliary data using the parameters determined at step 212 to produce one or more sets of

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 191
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

encoded auxiliary data slices. The auxiliary data, which may be encrypted using one or more the encrypting functions discussed herein prior to dispersal storage error encoding, includes null data, authentication information, a next pseudo random output sequencing order, a pseudo random output sequencing order identifier, a next outputting threshold, a random number generator output, an encryption key, a starting point for the pseudo random output sequencing order, a device identifier, a data identifier, a data type, a data size indictor, a priority indicator, a security indicator, and/or a performance indicator. For example, a video stream is the data of steps 214 & 216 and a next pseudo random output sequencing order is the auxiliary data.

[0123] The method continues at step 224 where the processing module determines auxiliary data sequence information (i.e., a pseudo-random sequencing order). The method continues at step 226 where the processing module sequences outputting of the encoded auxiliary data slices, which may be similar to sequencing the outputting of the encoded data slices.

[0124] The method continues at step 228 where the processing module determines selection information, which includes a pseudo random output sequencing order, a selection algorithm ID, a de-selection algorithm ID, a seed generation algorithm ID, a key, an ID, a hash algorithm, and/or a sequence seed. The method continues at step 230 where the processing module selects encoded data slices and encoded auxiliary data slices to produce output sequenced slices in accordance with the selection information. The method continues at step 232 where processing module transmits the output sequenced slices to one or more destinations via a wired and/or wireless network.

[0125] In addition, at step 232, the processing module may compare an ingress number of encoded data slices being buffered to an egress number of encoded data slices being outputted within a given time interval when a number of buffered encoded data slices compares favorably to the threshold. Next, the processing module adjusts the dispersed storage error encoding of the data segment such that the comparing of the ingress number to the egress number is favorable with respect to an underflow threshold when the comparing of the ingress number to the egress number is unfavorable with respect to the underflow threshold. Alternatively, the processing module may adjust the dispersed storage error encoding of the data segment such that the comparing of the ingress number to the egress number is favorable with respect to an overflow threshold when the comparing of the ingress number to the egress number is unfavorable with respect to the overflow threshold.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 192
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0126] Figure 10 is a flowchart illustrating an example of decoding encoded data slices to produce data. The method begins with step 234 where a processing module receives a retrieve data object message from one or more of a computing core, a user device, a dispersed storage (DS) processing unit, a storage integrity processing unit, a DS managing unit, a DS unit, and a process or function of a user device). The retrieve data object message includes one or more of a requester identifier (ID) (e.g., a source user device ID), a target ID (e.g., a destination user device ID), a data object name, a data object, sequence information, a key (e.g., an encryption key), a priority indicator, a security indicator, and a performance indicator.

[0127] The method continues at step 236 where the processing module determines error coding dispersal stored function parameters as previously discussed. The method continues at step 238 where the processing module obtains at least an ordering threshold number of encoded data slices to produce obtained encoded data slices from a user device, from DSN memory, etc.

[0128] The method continues at step 240 where the processing module determines de-selection information, which is the compliment to the selection information and is determined in a similar fashion. The method continues at step 242 where the processing module de-selects input sequenced slices (e.g., the received randomized encoded data slices) in accordance with the de-selection information. For example, this separates randomized encoded data slices from the randomized encoded auxiliary data slices.

[0129] The method continues at step 244 where the processing module determines auxiliary data de-sequence information, which is complimentary to the auxiliary data sequence information. The method continues at step 246 where the processing module de-sequences the sequenced (i.e., randomized) encoded auxiliary data slices to produce de-sequenced encoded auxiliary data slices. The method continues at step 248 where the processing module recreates the auxiliary data from the de-sequenced encoded auxiliary data slices in accordance with the auxiliary error coding dispersal storage function parameters. If the auxiliary data was encrypted, this step further includes decrypting the auxiliary data.

[0130] The method continues at step 250 where the processing module processes the auxiliary data in accordance with one or more of the auxiliary error coding dispersal storage function parameters, a flag, a command, a lookup, and the de-sequence information. For example, the processing module discards at least some of the auxiliary data when the de-sequence information indicates that the auxiliary data contains random numbers. In another example, the processing

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 193
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

module subsequently de-sequences sequenced encoded data slices of a sequence seed contained within the auxiliary data when the de-sequence information indicates that the auxiliary data contains the sequence seed. In another example, the processing module subsequently de-sequences sequenced encoded data slices of desired data utilizing de-sequence information contained within the auxiliary data when the de-sequence information indicates that the auxiliary data contains the de-sequence information.

[0131] The method continues at step 252 where the processing module determines data de-sequence information, which is complimentary to the data sequence information. The method continues at step 254 where the processing module orders (e.g., de-sequences) the randomized encoded data slices based on the pseudo-random de-sequencing order to produce a plurality of sets of encoded data slices. The method continues at step 256 where the processing module dispersed storage error decodes the plurality of sets of encoded data slices to produce a plurality of data segments in accordance with the error coding dispersal storage function parameters.

[0132] The method continues at step 258 where the processing module aggregates the plurality of data segments to produce the data (e.g., a data stream or one or more data objects). The processing module may aggregate the plurality of data segments by ordering them in accordance with a data segment order of the pseudo-random de-sequencing order. The method continues at step 260 where the processing module sends the data to a requester.

[0133] Figure 11 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes many similar steps to Figure 9. The method begins with steps 210 – 214 of Figure 9 and then continues with step 268 where, in order of receiving data segments, the processing module encrypts a data segment to produce an encrypted data segment. The processing module may encrypt the data segment using one or more encrypting functions, which include an all or nothing transformation (AONT), a stored encryption key and an encryption algorithm, a random encryption and an encryption algorithm, an encryption key associated with at least one recipient and an encryption algorithm, an obfuscating method, and/or a null encryption method.

[0134] As a specific example, the processing module encrypts the data segment utilizing an all or nothing transformation (AONT) to produce an encrypted data segment. The processing module then calculates a hash of the encrypted data segment utilizing a hash function (e.g., secure hash function SHA-256, SHA-512 etc.), which may use a secret key. The processing module truncates

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 194
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

the encrypted data hash to match the number of bits of the secret key, or other key. The processing module calculates an exclusive OR (XOR) of the key and the (truncated) encrypted data hash to produce a masked key. The processing module appends the masked key to the encrypted data segment, which is subsequently dispersal storage error encoded.

[0135] The method continues at step 270 where the processing module dispersed storage error encodes the encrypted data segments to sets of encoded data slices. The method concludes with steps 218 – 232 of Figure 9.

[0136] Figure 12 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps to the flowchart of Figure 10. The method begins with steps 234-256 of Figure 10 and then continues with step 312 where the processing module decrypts the encrypted data segments of step 256 to produce a plurality of data segments. The decrypting includes the complement of the encrypting function used to encrypt the data segments.

[0137] For example, if the data segments were encrypted using the AONT encryption method, the processing module utilizes the AONT method to decrypt the encrypted data segment packages. As a more specific example, the processing module uses the AONT method and a key (e.g., a random key) to decrypt each encrypted data segment based on the random key used to decrypt at least one encrypted auxiliary data segment associated with the auxiliary data. The method concludes with steps 258 – 260 of Figure 10.

[0138] Figure 13 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes many similar steps to Figure 9. The method begins with steps 210 – 214 of Figure 9 and then continues with step 324 where the processing module determines a data segment type (e.g., content) of a data segment. The data segment type includes one or more of a file header, a video header, routing information, addressing information, compression information, source information, destination information, video, text, music, speech, audio, telemetry, control information, a command, a request, status information, a random number, a sequence seed, a key, a private key, a shared key, a secret key, a public key, and an image. Such a determination may be based on one or more of the data segment, a data segment type determination algorithm, the error coding dispersal storage function parameters, a requester identifier (ID), a vault lookup, a data object name, a data object, a data stream, sequence

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 195
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

information, a key, a priority indicator, a security indicator, a command, a predetermination, a message, a performance indicator, and information received in the store data object message.

[0139] The method continues at step 326, where, in order of receiving the data segments, the processing module selects an encryption method based on the data type (e.g., data segment type) and encrypts the data segment using the selected encryption method to produce an encrypted data segment. Such a selection of the encryption method may be based on one or more of the data segment type, the data segment, an encryption method determination algorithm, the error coding dispersal storage function parameters, a requester ID, a vault lookup, a data object name, a data object, a data stream, sequence information, a key, a priority indicator, a security indicator, a command, a predetermination, a message, the performance indicator, and information received in the store data object message.

[0140] For example, the processing module encrypts the data segment utilizing an all or nothing transformation (AONT) encryption method when the data segment type indicates that the type is a video header and the security indicator indicates to encrypt video headers. In another example, the processing module determines not to encrypt the data segment when the data segment type indicates that the type is routine status information and the security indicator indicates to not encrypt routine status information. In another example, the processing module selects the encryption method to include encrypting the data segment utilizing a key based on a calculation of a hash value (e.g., secure hash function SHA-256, SHA-512 etc.) over a key of the day, a source user ID, and a current time value. The method concludes with steps 218 – 232 of Figure 10.

[0141] Figure 14 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps to the flowchart of Figure 10. The method begins with steps 234-256 of Figure 10 and then continues with step 370 where the processing module determines a data segment type of a data segment. The processing module may determine the data segment type based on one or more of the data segment type extracted from the auxiliary data, from the sets of encoded data slices, from the encrypted data segments, the encrypted data segment, a data segment type determination algorithm, the error coding dispersal storage function parameters, a requester ID, a vault lookup, a data object name, a data object, a data stream, sequence information, a key, a priority indicator, a security indicator, a command, a predetermination, a message, a performance indicator, and information received in the store data object message.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 196
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0142] The method continues at step 372 where the processing module selects a decryption method based on the data segment type and decrypts the encrypted data segments utilizing the decryption method to produce the plurality of data segments. Note that the decryption method may vary from encrypted data segment to encrypted data segment. The method concludes with steps 258 and 260 of Figure 10.

[0143] Figure 15 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9 and 11. The method begins with steps 210-214 of Figure 9, step 268 of Figure 11, and steps 216-220 of Figure 9. The method continues at step 392 where the processing module scrambles auxiliary data segments to produce scrambled auxiliary data segments utilizing a low processing utilization scrambling algorithm. The low processing utilization scrambling algorithm may include one or more of rearranging auxiliary data segment bits in accordance with a predetermined bit rearranging method, inverting all of the auxiliary data segment bits, inverting a portion of the auxiliary data segment bits in accordance with a predetermined method, and rearranging a portion of the auxiliary data segment bits in accordance with the predetermined bit rearranging method and inverting a portion of the auxiliary data segment bits in accordance with a predetermined bit inversion method. The processing module then dispersed storage error encodes the scrambled auxiliary data segments to produce encoded auxiliary data slices in accordance with auxiliary error coding dispersal storage function parameters as previously discussed. The method concludes with steps 224 – 232 of Figure 9.

[0144] Figure 16 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10 and 12. The method begins with steps 234 -246 of Figure 10 and continues with step 418 where the processing module dispersed storage error decodes the de-sequenced encoded auxiliary data slices to produce scrambled auxiliary data segments. The processing module de-scrambles (e.g., the compliment of the scrambling) the scrambled auxiliary data segments to produce auxiliary data segments in accordance with a de-scrambling algorithm. The processing module aggregates the auxiliary data segments to produce the auxiliary data. The method concludes with steps 250-256 of Figure 10, step 312 of Figure 12, and steps 258 – 260 of Figure 10.

[0145] Figure 17 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9 and 11. The

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 197
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

method begins with steps 210-214 of Figure 9 and continues at step 440 where the processing module determines an obfuscating method based on one or more of the error coding dispersal storage functions parameters, a requester identifier (ID), a vault lookup, a data object name, a data object, a data stream, sequence information, a key, a priority indicator, a security indicator, a command, a predetermination, a message, information in the store data object message, and a performance indicator. The obfuscating method may include one or more of adding random bits (e.g., creation of a new data segment that contains all of the bits of at least one receive data segment of the received data segments and new random bits), inverting bits of the received data segment, and replacing a portion of the bits of the received data segment with bits produced from a obfuscation calculation based on the portion of bits of the received data segment (e.g., a logical XOR of the data segment bits with a key). The method concludes with step 268 of Figure 11 and sets 216 – 232 of Figure 9.

[0146] Figure 18 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10 and 12. The method begins with steps 234 -256 of Figure 10 and step 312 of Figure 12. The method continues at step 488 where the processing module determines a de-obfuscating method (e.g., the compliment of the obfuscating method). The processing module may determine the de-obfuscating method may be based on one or more of the error coding dispersal storage function parameters, a requester identifier (ID), a vault lookup, a data object name, a data object, a data stream, sequence information, a key, a priority indicator, a security indicator, a command, a predetermination, a message, information in the store data object message, and a performance indicator. The method concludes with steps 258 – 260 of Figure 10.

[0147] Figure 19 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9 and 11. The method begins with steps 210-214 of Figure 9 and continues at step 500 where the processing module determines a secret key. Such a determination may be based on one or more of retrieval from a memory, a list, a lookup, a command, a message, a predetermination, and a calculation. Note that the processing module may determine a secret key for each data segment of the received data segments. In an example, the processing module calculates the secret key by hashing a key of the day, a user device identifier (ID), and a current date value.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 198
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0148] The processing module encrypts the data segment in accordance with encryption algorithm utilizing the secret key to produce an encrypted data segment as a data segment of the received data segments. The processing module may determine a second key based on one or more of retrieval from a memory, a list, a lookup, a command, a message, a predetermination, and a calculation. For example, the processing module determines the second key as a public key from a lookup subsequent to receiving the public key and storing it in a memory. The processing module encrypts the secret key in accordance with the error coding dispersal storage option parameters utilizing the second key to produce an encrypted secret key and appends the encrypted secret key to an associated encrypted data segment and/or to one or more encoded data slices of the associated encrypted data segment. The method concludes with step 268 of Figure 11 and steps 216 – 232 of Figure 9.

[0149] Figure 20 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10 and 12. The method begins with steps 234 -256 of Figure 10 and step 312 of Figure 12. The method continues at step 548 where the processing module extracts an encrypted secret key from the encrypted data segment and/or from at least one of the encoded data slices of the encrypted data segment. The processing module determines a second key based on one or more of a retrieval from a memory, a list, a lookup, a command, a message, a predetermination, and a calculation.

[0150] The processing module decrypts the encrypted secret key in accordance with the error coding dispersal storage function parameters (e.g., a specified decryption algorithm) utilizing the second key to produce a received secret key. The processing module determines a secret key based on one or more of the received secret key, retrieval from a memory, a list, a lookup, a command, a message, a predetermination, and a calculation. The processing module decrypts each of the further encrypted data segment (e.g., after the AONT method) in accordance with the error coding dispersal storage function parameters (e.g., a decryption algorithm) utilizing the corresponding secret key. The method concludes with steps 258 – 260 of Figure 10.

[0151] Figure 21 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9 and 11. The method begins with steps 210-214 of Figure 9, step 268 of Figure 11, and steps 216 – 218 of Figure 9. The method continues at step 566 where the processing module determines a sequence seed based on one or more of the sequence information, a seed generation algorithm, a hash function, a

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 199
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

received key, a stored key, a calculated key, a data type (e.g., video, audio, telemetry, commands, status information, etc.), a requester identifier (ID), a vault lookup, a data object name, a data object, a data stream, received sequence information (e.g., part of the request message), the error coding dispersal storage function parameters, information received in the store data object request message, a calculation, a priority indicator, a security indicator, a list, a command, a predetermination, a message, a previous seed, a last seed, a previous seed, and a performance indicator. For example, the processing module determines the sequence seed to include a calculated (e.g., hash) value of 1F46D8EA39B based on a hash over a source user device 5F02D77B, a key 34D8AB90, a sequence algorithm 3AC, and a video data type. The method concludes with steps 220 – 234 of Figure 9.

[0152] Figure 22 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10 and 12. The method begins with steps 234 -252 of Figure 10 and continues at step 602 where the processing module determines a de-sequence seed based on one or more of the de-sequence information, a seed generation algorithm, a hash function, a received key, a stored key, a calculated key, a data type (e.g., video, audio, telemetry, commands, status information, etc.), a requester identifier (ID), a vault lookup, a data object name, auxiliary data, a received sequence information (e.g., part of the request message), the error coding dispersal storage function parameters, information received in the retrieve data object request message, a calculation, a priority indicator, a security indicator, a list, a command, a predetermination, a message, a previous seed, a last seed, and a performance indicator. For example, the processing module determines the de-sequence seed to include a calculated (e.g., hash) value of 1F46D8EA39B based on a hash over a source user device 5F02D77B, a key 34D8AB90, a sequence algorithm 3AC, and a video data type.

[0153] The method continues at step 254 where the processing module orders the encoded data slices based on a pseudo-random de-sequencing order using the de-sequence seed. The method concludes with step 256 of Figure 10, 312 of Figure 12 and steps 258 – 260 of Figure 10.

[0154] Figure 23 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9 and 11. The method begins with steps 210-214 of Figure 9, step 268 of Figure 11, and steps 216 – 218 of Figure 9. The method continues at step 626 where the processing module determines a sequence seed, an encryption key or seed, which it appends to one or more data segments. In this step, the processing

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 200
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

module encrypts the sequence seed utilizing the encryption key to produce an encrypted sequence seed. Note that the encryption key may be varied from data segment to data segment. Alternatively, or in addition to, the processing module may include the sequence seed as data of the auxiliary data. The method concludes with steps 220 – 232 of Figure 9.

[0155] Figure 24 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10 and 12. The method begins with steps 234 -252 of Figure 10 and continues at step 662 where the processing module extracts an appended encrypted sequence seed from one or more of an auxiliary data segment, and encoded auxiliary data slice, and an encoded and sliced to produce an encrypted de-sequence seed. The processing module decrypts the encrypted de-sequence seed in accordance utilizing a private key (e.g., of a public/private key pair of an associated destination user device) to produce a decrypted de-sequence seed. In an example, the processing module determines the de-sequence seed to include a value of 1F46D8EA39B based on the decrypted de-sequence seed. In another example, the processing module determines the de-sequence seed to include a calculated (e.g., hash) value of 1F46D8EA39B based on a hash over a source user device 5F02D77B, a key 34D8AB90, a sequence algorithm 3AC, and a video data type.

[0156] The method continues at step 254 where the processing module orders the encoded data slices based on a pseudo-random de-sequencing order utilizing the de-sequence seed. The method concludes with step 256 of Figure 10, step 312 of Figure 12, and steps 258-260 of Figure 10.

[0157] Figure 25 is another flowchart illustrating another example of encoding data to produce encoded data slices, which includes similar steps from the flowcharts of Figures 9, 11, and 21. The method begins with steps 210-214 of Figure 9, step 268 of Figure 11, steps 216 – 218 of Figure 9, step 566 of Figure 21, and steps 220-230 of Figure 9. The method continues at step 700 where processing module sends the output sequenced slices to a dispersed storage (DS) processing unit (e.g., that may have requested slices and that may have provided a sequence seed and other information) for storage in at least one dispersed storage network (DSN) memory. In an example, the processing module sends first buffered encoded data slices and, at most, some second buffered encoded data slices of second buffered encoded data slices to the DSN memory for storage therein. Note that the output sequenced slices may be communicated from the source user device to the DS processing unit via one or more wireless modules utilizing wireless signals.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 201
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0158] Figure 26 is another flowchart illustrating another example of decoding encoded data slices to produce data, which includes similar steps from the flowcharts of Figures 10, 12, and 22. The method begins with steps 234 -252 of Figure 10, step 602 of Figure 22, steps 254 – 256 of Figure 9, and step 312 of Figure 12. The method continues at step 730 where the processing module aggregates the plurality of data segments to produce a data stream or data object and determines second error coding dispersal storage function parameters based on one or more of information in the retrieve data object message, a user device ID, a DS processing unit ID, a vault lookup, a predetermination, a command, and a message. The processing module dispersed storage error and codes the data stream or data object to produce a plurality of sets of re-encoded data slices in accordance with the second error coding dispersal storage parameters. The method continues at step 732 where the processing module sends slices to the DSN memory for storage therein in accordance with the slice storage format. For example, the processing module sends the obtained encoded data slices to the DSN memory for storage therein when the processing module determines that the slice storage format includes storing information in the format of the obtained encoded data slices (e.g., path A). In another example, the processing module sends the plurality of sets of encoded data slices to the DSN memory for storage therein when the processing module determines that the slice storage format includes storing information in the format of the plurality of the encoded data slices (e.g., path C). In another example, the processing module dispersed storage error encodes the plurality of data segments to produce the plurality of sets of re-encoded data slices and sends the plurality of sets of re-encoded data slices to the DSN memory for storage therein when the processing module determines that the slice storage format includes storing information in the format of re-encoded data slices.

[0159] It is noted that terminologies as may be used herein such as bit stream, stream, signal sequence, etc. (or their equivalents) have been used interchangeably to describe digital information whose content corresponds to any of a number of desired types (e.g., data, video, speech, text, graphics, audio, etc. any of which may generally be referred to as 'data').

[0160] As may be used herein, the terms "substantially" and "approximately" provides an industry-accepted tolerance for its corresponding term and/or relativity between items. For some industries, an industry-accepted tolerance is less than one percent and, for other industries, the industry-accepted tolerance is 10 percent or more. Other examples of industry-accepted tolerance range from less than one percent to fifty percent. Industry-accepted tolerances correspond to, but

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 202
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

are not limited to, component values, integrated circuit process variations, temperature variations, rise and fall times, thermal noise, dimensions, signaling errors, dropped packets, temperatures, pressures, material compositions, and/or performance metrics. Within an industry, tolerance variances of accepted tolerances may be more or less than a percentage level (e.g., dimension tolerance of less than +/- 1%). Some relativity between items may range from a difference of less than a percentage level to a few percent. Other relativity between items may range from a difference of a few percent to magnitude of differences.

[0161] Figure 27 is a schematic block diagram of an embodiment of a computing device (e.g., user device 12 or DS processing unit 16) of the distributed or dispersed storage network (DSN). When a computing device 734 has data to store it disperse storage error encodes the data in accordance with a dispersed storage error encoding process based on dispersed storage error encoding parameters. The dispersed storage error encoding parameters include an encoding function (e.g., information dispersal algorithm, Reed-Solomon, Cauchy Reed-Solomon, systematic encoding, non-systematic encoding, on-line codes, etc.), a data segmenting protocol (e.g., data segment size, fixed, variable, etc.), and per data segment encoding values. The per data segment encoding values include a total, or pillar width, number (T) of encoded data slices per encoding of a data segment i.e., in a set of encoded data slices); a decode threshold number (D) of encoded data slices of a set of encoded data slices that are needed to recover the data segment; a read threshold number (R) of encoded data slices to indicate a number of encoded data slices per set to be read from storage for decoding of the data segment; and/or a write threshold number (W) to indicate a number of encoded data slices per set that must be accurately stored before the encoded data segment is deemed to have been properly stored. The dispersed storage error encoding parameters may further include slicing information (e.g., the number of encoded data slices that will be created for each data segment) and/or slice security information (e.g., per encoded data slice encryption, compression, integrity checksum, etc.).

[0162] In the present example, Cauchy Reed-Solomon has been selected as the encoding function; the data segmenting protocol is to divide the data object into fixed sized data segments; and the per data segment encoding values include: a pillar width of 5, a decode threshold of 3, a read threshold of 4, and a write threshold of 4. In accordance with the data segmenting protocol, the computing device 734 divides the data (e.g., a file (e.g., text, video, audio, etc.), a data object, or other data arrangement) into a plurality of fixed sized data segments (e.g., 1 through Y of a fixed

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 203
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

size in range of Kilo-bytes to Tera-bytes or more). The number of data segments created is dependent of the size of the data and the data segmenting protocol.

[0163] The computing device 734 then disperse storage error encodes the plurality of data segments using the selected encoding function (e.g., Cauchy Reed-Solomon) to produce a plurality of sets of encoded data slices (EDSs). The computing device 734 may encrypt one or more of the plurality of data segments using one or more encrypting functions, which include an all or nothing transformation (AONT), a stored encryption key and an encryption algorithm, a random encryption and an encryption algorithm, an encryption key associated with at least one recipient and an encryption algorithm, an obfuscating method, and/or a null encryption method.

[0164] Computing device 734 dispersed storage error encodes an auxiliary data segment 738 of auxiliary data 736 (e.g., null data, authentication information, a next pseudo random output sequencing order, a pseudo random output sequencing order identifier, a next outputting threshold, a random number generator output, an encryption key, a starting point for the pseudo random output sequencing order, a device identifier, a data identifier, a data type, a data size indictor, a priority indicator, a security indicator, and/or a performance indicator) to produce a set of encoded auxiliary data slices (EADSs 1_1 through 5_1).

[0165] The computing device 734 may encrypt the auxiliary data 736 using one or more encrypting functions, which include an all or nothing transformation (AONT), a stored encryption key and an encryption algorithm, a random encryption and an encryption algorithm, an encryption key associated with at least one recipient and an encryption algorithm, an obfuscating method, and/or a null encryption method. The auxiliary data may be encrypted via an encryption methodology used to encrypt the plurality of encrypted data segments.

[0166] The computing device 734 obfuscates a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices. The obfuscating the first set of encoded data slices may include interspersing the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order. In this example, encoded auxiliary data slices EADS 1_1 and EADS 3_1 of the first set of encoded auxiliary data slices are interspersed within the first set of encoded data slices to create the first set of obfuscated encoded data slices (EDSs).

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 204
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0167] The computing device 734 obfuscates a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices. The obfuscating the second set of encoded data slices may include interspersing the at least one other encoded auxiliary data slices within the second set of encoded data slices in accordance with a pseudo random output sequencing order. In this example, encoded auxiliary data slices EADS 2_1 and EADS 4_1 of the first set of encoded auxiliary data slices are interspersed within the second set of encoded data slices to create the second set of obfuscated encoded data slices (EDSs).

[0168] Computing device 734 may further dispersed storage error encode the auxiliary data 736 to produce a second set of encoded auxiliary data slices. The computing device 734 obfuscates the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices. The computing device 734 may also obfuscate the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

[0169] Computing device 734 outputs the first and second sets of obfuscated (and/or further obfuscated) encoded data slices for storage.

[0170] Figure 28 is a flowchart illustrating an example of secure data transmission utilizing distributed storage. The method begins with step 740 where a computing device (e.g., user device 12 or DS processing unit 16) of the DSN disperse storage error encodes a plurality of data segments to produce a plurality of sets of encoded data slices (EDSs). The computing device may encrypt one or more of the plurality of data segments using one or more encrypting functions, which include an all or nothing transformation (AONT), a stored encryption key and an encryption algorithm, a random encryption and an encryption algorithm, an encryption key associated with at least one recipient and an encryption algorithm, an obfuscating method, and/or a null encryption method.

[0171] The method continues with step 742 where the computing device dispersed storage error encodes an auxiliary data segment of auxiliary data (e.g., null data, authentication information, a next pseudo random output sequencing order, a pseudo random output sequencing order identifier, a next outputting threshold, a random number generator output, an encryption key, a starting point for the pseudo random output sequencing order, a device identifier, a data identifier,

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 205
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

a data type, a data size indictor, a priority indicator, a security indicator, and/or a performance indicator) to produce a set of encoded auxiliary data slices (EADSs).

[0172] The computing device may encrypt the auxiliary data using one or more encrypting functions, which include an all or nothing transformation (AONT), a stored encryption key and an encryption algorithm, a random encryption and an encryption algorithm, an encryption key associated with at least one recipient and an encryption algorithm, an obfuscating method, and/or a null encryption method. The auxiliary data may be encrypted via an encryption methodology used to encrypt the plurality of encrypted data segments.

[0173] The method continues with step 744 where the computing device obfuscates a first set of encoded data slices of the plurality of sets of encoded data slices using at least one encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a first set of obfuscated encoded data slices. The obfuscating the first set of encoded data slices may include interspersing the at least one encoded auxiliary data slices within the first set of encoded data slices in accordance with a pseudo random output sequencing order.

[0174] The method continues with step 746 where the computing device obfuscates a second set of encoded data slices of the plurality of sets of encoded data slices using at least one other encoded auxiliary data slices of the set of encoded auxiliary data slices to produce a second set of obfuscated encoded data slices. The obfuscating the second set of encoded data slices may include interspersing the at least one other encoded auxiliary data slices within the second set of encoded data slices in accordance with a pseudo random output sequencing order.

[0175] The computing device may further dispersed storage error encode the auxiliary data to produce a second set of encoded auxiliary data slices. The computing device obfuscates the first set of obfuscated encoded data slices using at least one encoded auxiliary data slices of the second set of encoded auxiliary data slices to produce a first set of further obfuscated encoded data slices. The computing device may also obfuscate the second set of obfuscated encoded data slices using at least one other encoded auxiliary data slice of the second set of encoded auxiliary data slices to produce a second set of further obfuscated encoded data slices.

[0176] The method continues with step 748 where the computing device outputs the first and second sets of obfuscated (and/or further obfuscated) encoded data slices for storage.

[0177] As may also be used herein, the term(s) “configured to”, “operably coupled to”, “coupled to”, and/or “coupling” includes direct coupling between items and/or indirect coupling

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 206
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

between items via an intervening item (e.g., an item includes, but is not limited to, a component, an element, a circuit, and/or a module) where, for an example of indirect coupling, the intervening item does not modify the information of a signal but may adjust its current level, voltage level, and/or power level. As may further be used herein, inferred coupling (i.e., where one element is coupled to another element by inference) includes direct and indirect coupling between two items in the same manner as "coupled to".

[0178] As may even further be used herein, the term "configured to", "operable to", "coupled to", or "operably coupled to" indicates that an item includes one or more of power connections, input(s), output(s), etc., to perform, when activated, one or more its corresponding functions and may further include inferred coupling to one or more other items. As may still further be used herein, the term "associated with", includes direct and/or indirect coupling of separate items and/or one item being embedded within another item.

[0179] As may be used herein, the term "compares favorably", indicates that a comparison between two or more items, signals, etc., provides a desired relationship. For example, when the desired relationship is that signal 1 has a greater magnitude than signal 2, a favorable comparison may be achieved when the magnitude of signal 1 is greater than that of signal 2 or when the magnitude of signal 2 is less than that of signal 1. As may be used herein, the term "compares unfavorably", indicates that a comparison between two or more items, signals, etc., fails to provide the desired relationship.

[0180] As may be used herein, one or more claims may include, in a specific form of this generic form, the phrase "at least one of a, b, and c" or of this generic form "at least one of a, b, or c", with more or less elements than "a", "b", and "c". In either phrasing, the phrases are to be interpreted identically. In particular, "at least one of a, b, and c" is equivalent to "at least one of a, b, or c" and shall mean a, b, and/or c. As an example, it means: "a" only, "b" only, "c" only, "a" and "b", "a" and "c", "b" and "c", and/or "a", "b", and "c".

[0181] As may also be used herein, the terms "processing module", "processing circuit", "processor", "processing circuitry", and/or "processing unit" may be a single processing device or a plurality of processing devices. Such a processing device may be a microprocessor, micro-controller, digital signal processor, microcomputer, central processing unit, field programmable gate array, programmable logic device, state machine, logic circuitry, analog circuitry, digital circuitry, and/or any device that manipulates signals (analog and/or digital) based on hard coding

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 207
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

of the circuitry and/or operational instructions. The processing module, module, processing circuit, processing circuitry, and/or processing unit may be, or further include, memory and/or an integrated memory element, which may be a single memory device, a plurality of memory devices, and/or embedded circuitry of another processing module, module, processing circuit, processing circuitry, and/or processing unit. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any device that stores digital information. Note that if the processing module, module, processing circuit, processing circuitry, and/or processing unit includes more than one processing device, the processing devices may be centrally located (e.g., directly coupled together via a wired and/or wireless bus structure) or may be distributedly located (e.g., cloud computing via indirect coupling via a local area network and/or a wide area network). Further note that if the processing module, module, processing circuit, processing circuitry and/or processing unit implements one or more of its functions via a state machine, analog circuitry, digital circuitry, and/or logic circuitry, the memory and/or memory element storing the corresponding operational instructions may be embedded within, or external to, the circuitry comprising the state machine, analog circuitry, digital circuitry, and/or logic circuitry. Still further note that, the memory element may store, and the processing module, module, processing circuit, processing circuitry and/or processing unit executes, hard coded and/or operational instructions corresponding to at least some of the steps and/or functions illustrated in one or more of the Figures. Such a memory device or memory element can be included in an article of manufacture.

[0182] One or more embodiments have been described above with the aid of method steps illustrating the performance of specified functions and relationships thereof. The boundaries and sequence of these functional building blocks and method steps have been arbitrarily defined herein for convenience of description. Alternate boundaries and sequences can be defined so long as the specified functions and relationships are appropriately performed. Any such alternate boundaries or sequences are thus within the scope and spirit of the claims. Further, the boundaries of these functional building blocks have been arbitrarily defined for convenience of description. Alternate boundaries could be defined as long as the certain significant functions are appropriately performed. Similarly, flow diagram blocks may also have been arbitrarily defined herein to illustrate certain significant functionality.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 208
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0183] To the extent used, the flow diagram block boundaries and sequence could have been defined otherwise and still perform the certain significant functionality. Such alternate definitions of both functional building blocks and flow diagram blocks and sequences are thus within the scope and spirit of the claims. One of average skill in the art will also recognize that the functional building blocks, and other illustrative blocks, modules and components herein, can be implemented as illustrated or by discrete components, application specific integrated circuits, processors executing appropriate software and the like or any combination thereof.

[0184] In addition, a flow diagram may include a "start" and/or "continue" indication. The "start" and "continue" indications reflect that the steps presented can optionally be incorporated in or otherwise used in conjunction with one or more other routines. In addition, a flow diagram may include an "end" and/or "continue" indication. The "end" and/or "continue" indications reflect that the steps presented can end as described and shown or optionally be incorporated in or otherwise used in conjunction with one or more other routines. In this context, "start" indicates the beginning of the first step presented and may be preceded by other activities not specifically shown. Further, the "continue" indication reflects that the steps presented may be performed multiple times and/or may be succeeded by other activities not specifically shown. Further, while a flow diagram indicates a particular ordering of steps, other orderings are likewise possible provided that the principles of causality are maintained.

[0185] The one or more embodiments are used herein to illustrate one or more aspects, one or more features, one or more concepts, and/or one or more examples. A physical embodiment of an apparatus, an article of manufacture, a machine, and/or of a process may include one or more of the aspects, features, concepts, examples, etc. described with reference to one or more of the embodiments discussed herein. Further, from figure to figure, the embodiments may incorporate the same or similarly named functions, steps, modules, etc. that may use the same or different reference numbers and, as such, the functions, steps, modules, etc. may be the same or similar functions, steps, modules, etc. or different ones.

[0186] While the transistors in the above described figure(s) is/are shown as field effect transistors (FETs), as one of ordinary skill in the art will appreciate, the transistors may be implemented using any type of transistor structure including, but not limited to, bipolar, metal oxide semiconductor field effect transistors (MOSFET), N-well transistors, P-well transistors, enhancement mode, depletion mode, and zero voltage threshold (VT) transistors.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 209
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[0187] Unless specifically stated to the contra, signals to, from, and/or between elements in a figure of any of the figures presented herein may be analog or digital, continuous time or discrete time, and single-ended or differential. For instance, if a signal path is shown as a single-ended path, it also represents a differential signal path. Similarly, if a signal path is shown as a differential path, it also represents a single-ended signal path. While one or more particular architectures are described herein, other architectures can likewise be implemented that use one or more data buses not expressly shown, direct connectivity between elements, and/or indirect coupling between other elements as recognized by one of average skill in the art.

[0188] The term "module" is used in the description of one or more of the embodiments. A module implements one or more functions via a device such as a processor or other processing device or other hardware that may include or operate in association with a memory that stores operational instructions. A module may operate independently and/or in conjunction with software and/or firmware. As also used herein, a module may contain one or more sub-modules, each of which may be one or more modules.

[0189] As may further be used herein, a computer readable memory includes one or more memory elements. A memory element may be a separate memory device, multiple memory devices, or a set of memory locations within a memory device. Such a memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any device that stores digital information. The memory device may be in a form a solid-state memory, a hard drive memory, cloud memory, thumb drive, server memory, computing device memory, and/or other physical medium for storing digital information.

[0190] While particular combinations of various functions and features of the one or more embodiments have been expressly described herein, other combinations of these features and functions are likewise possible. The present disclosure is not limited by the particular examples disclosed herein and expressly incorporates these other combinations.

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 210
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

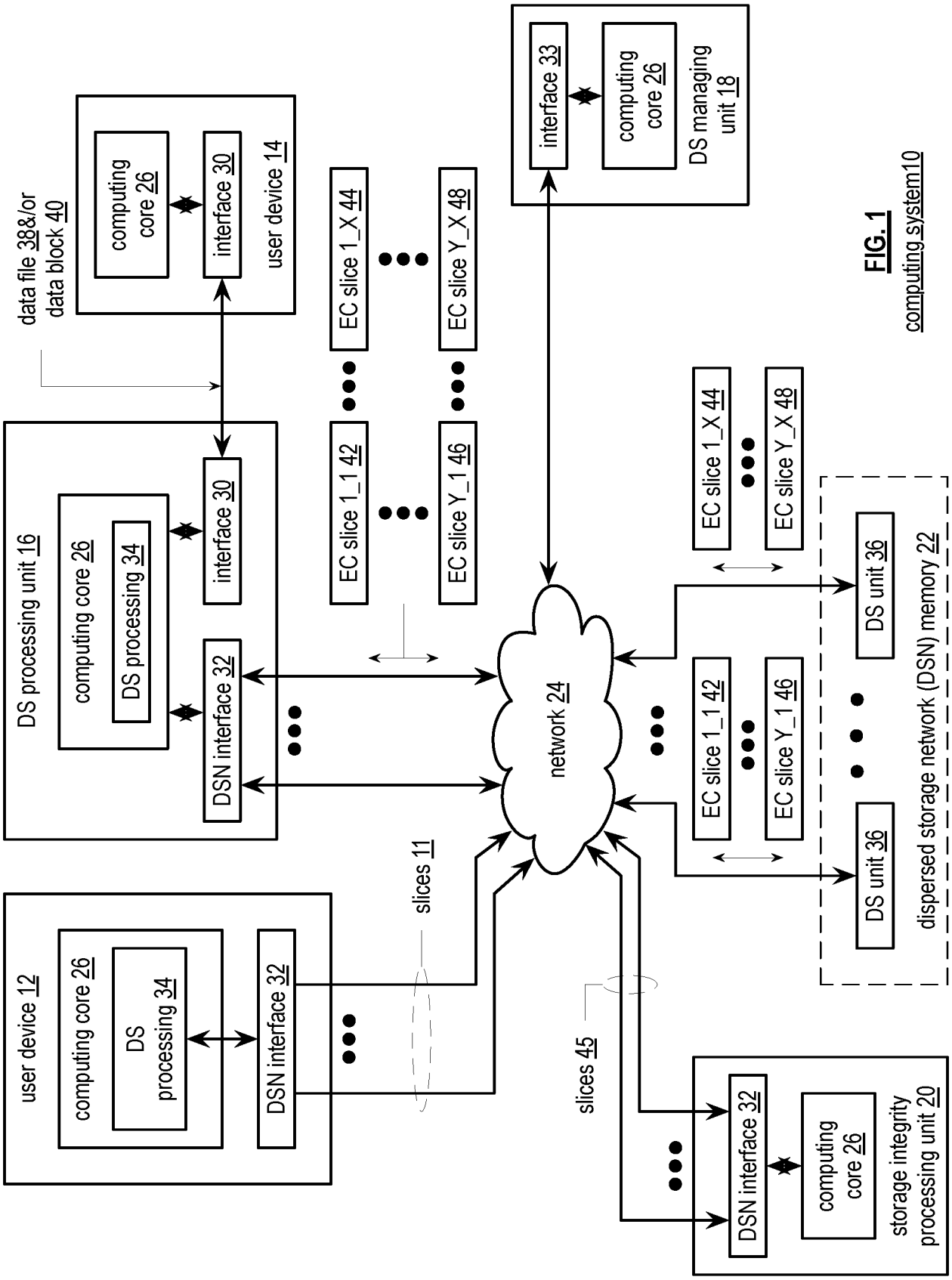

FIG. 1
computing system10

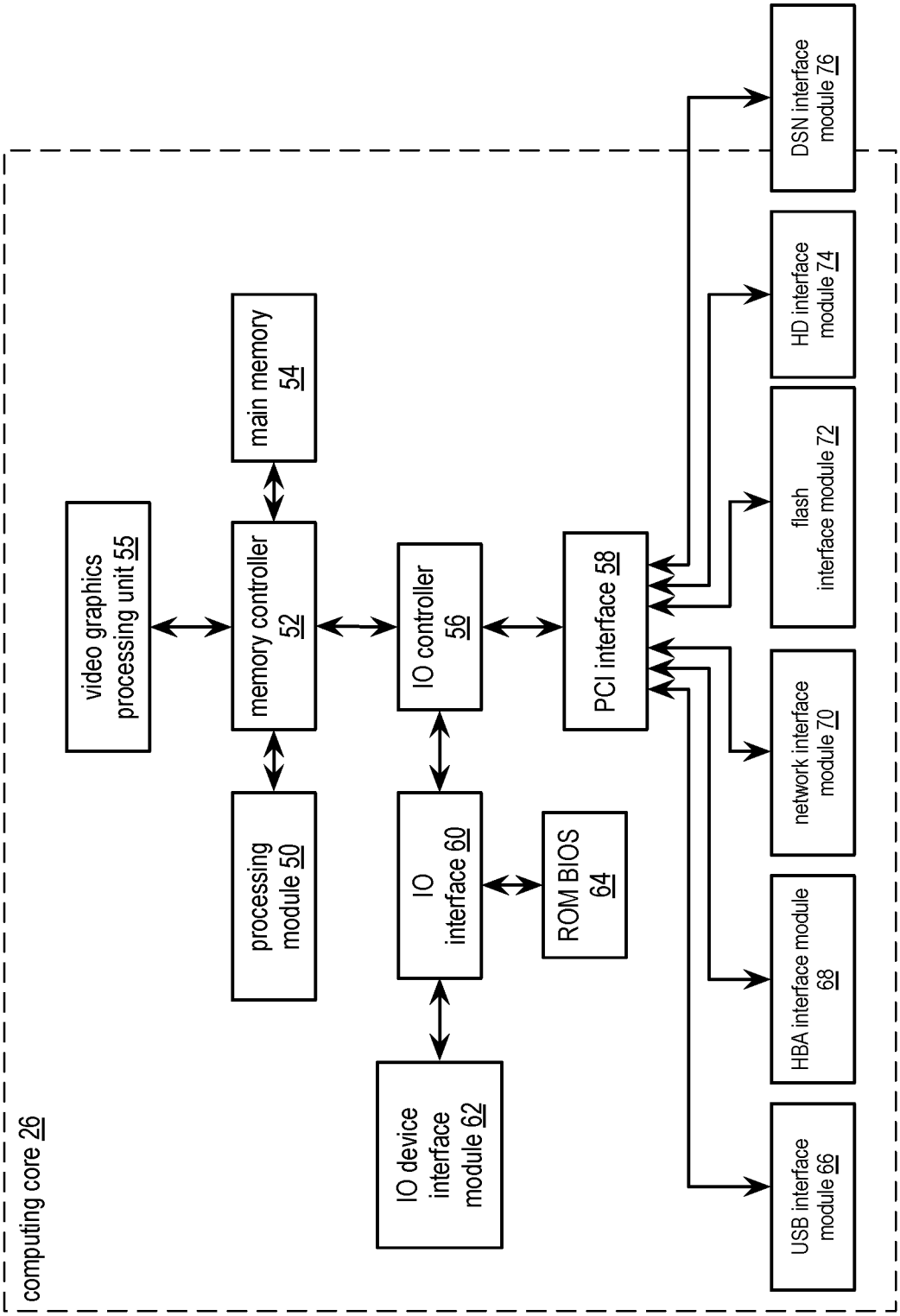
computing core 26
video graphics processing unit 55
main memory 54
memory controller 52
processing module 50
IO controller 56
IO interface 60
ROM BIOS 64
IO device interface module 62
PCI interface 58
DSN interface module 76
HD interface module 74
flash interface module 72
network interface module 70
HBA interface module 68
USB interface module 66

FIG.2

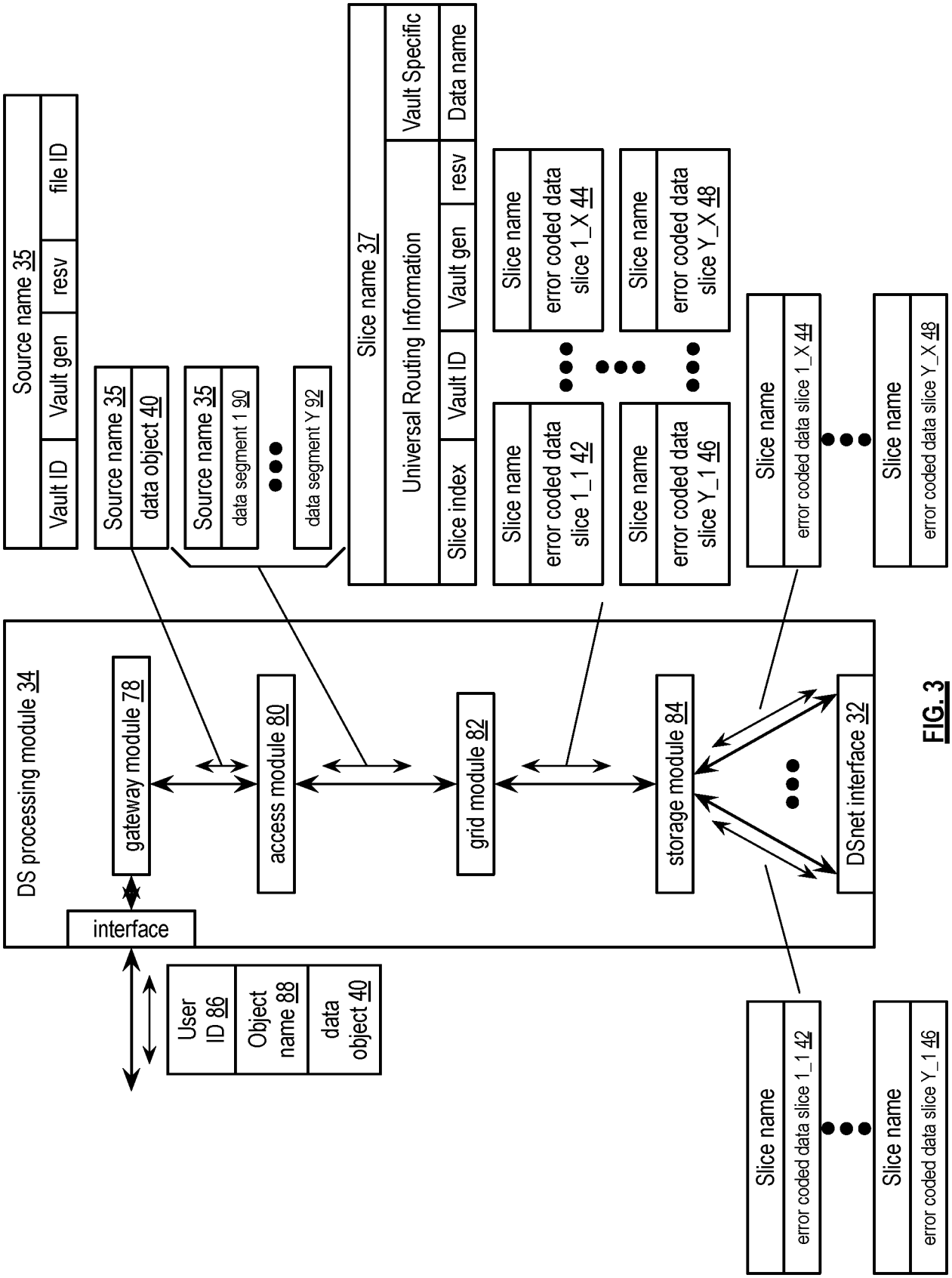
Source name 35
Vault ID
Vault gen
resv
file ID
Source name 35
data object 40
Source name 35
data segment 1 90
data segment Y 92
Slice name 37
Universal Routing Information
Slice index
Vault ID
Vault gen
resv
Vault Specific
Data name
Slice name
error coded data slice 1_X 44
Slice name
error coded data slice Y_X 48
Slice name
error coded data slice 1_1 42
Slice name
error coded data slice Y_1 46
Slice name
error coded data slice 1_X 44
Slice name
error coded data slice Y_X 48
DS processing module 34
gateway module 78
access module 80
grid module 82
storage module 84
DSnet interface 32
interface
User ID 86
Object name 88
data object 40
Slice name
error coded data slice 1_1 42
Slice name
error coded data slice Y_1 46

FIG. 3

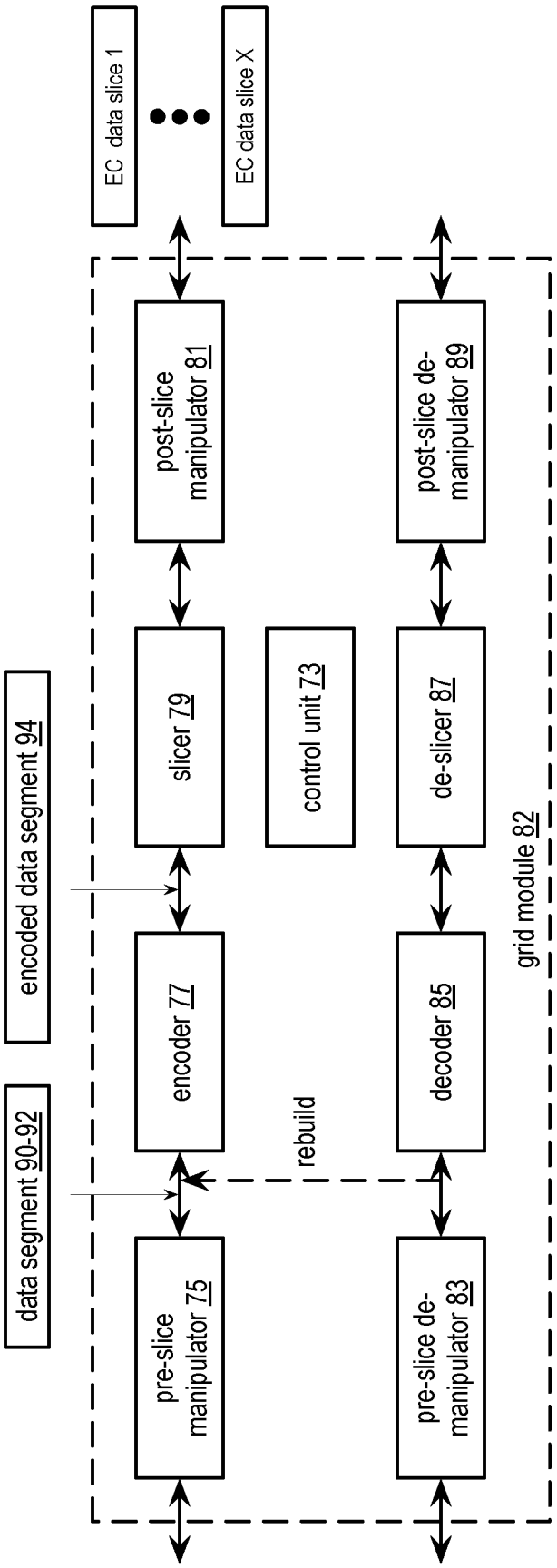
EC data slice 1
EC data slice X
encoded data segment 94
data segment 90-92
post-slice manipulator 81
slicer 79
encoder 77
pre-slice manipulator 75
control unit 73
rebuild
post-slice de-manipulator 89
de-slicer 87
decoder 85
pre-slice de-manipulator 83
grid module 82

FIG. 4

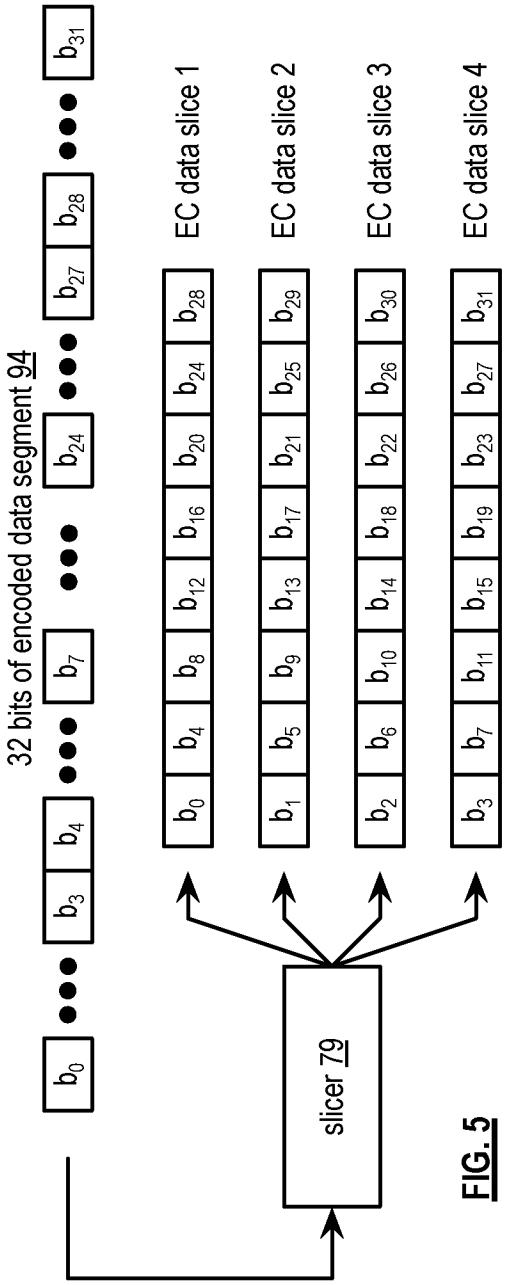
32 bits of encoded data segment 94
b0 b3 b4 b7 b24 b27 b28 b31
EC data slice 1
b0 b4 b8 b12 b16 b20 b24 b28
EC data slice 2
b1 b5 b9 b13 b17 b21 b25 b29
EC data slice 3
b2 b6 b10 b14 b18 b22 b26 b30
EC data slice 4
b3 b7 b11 b15 b19 b23 b27 b31
slicer 79

FIG. 5

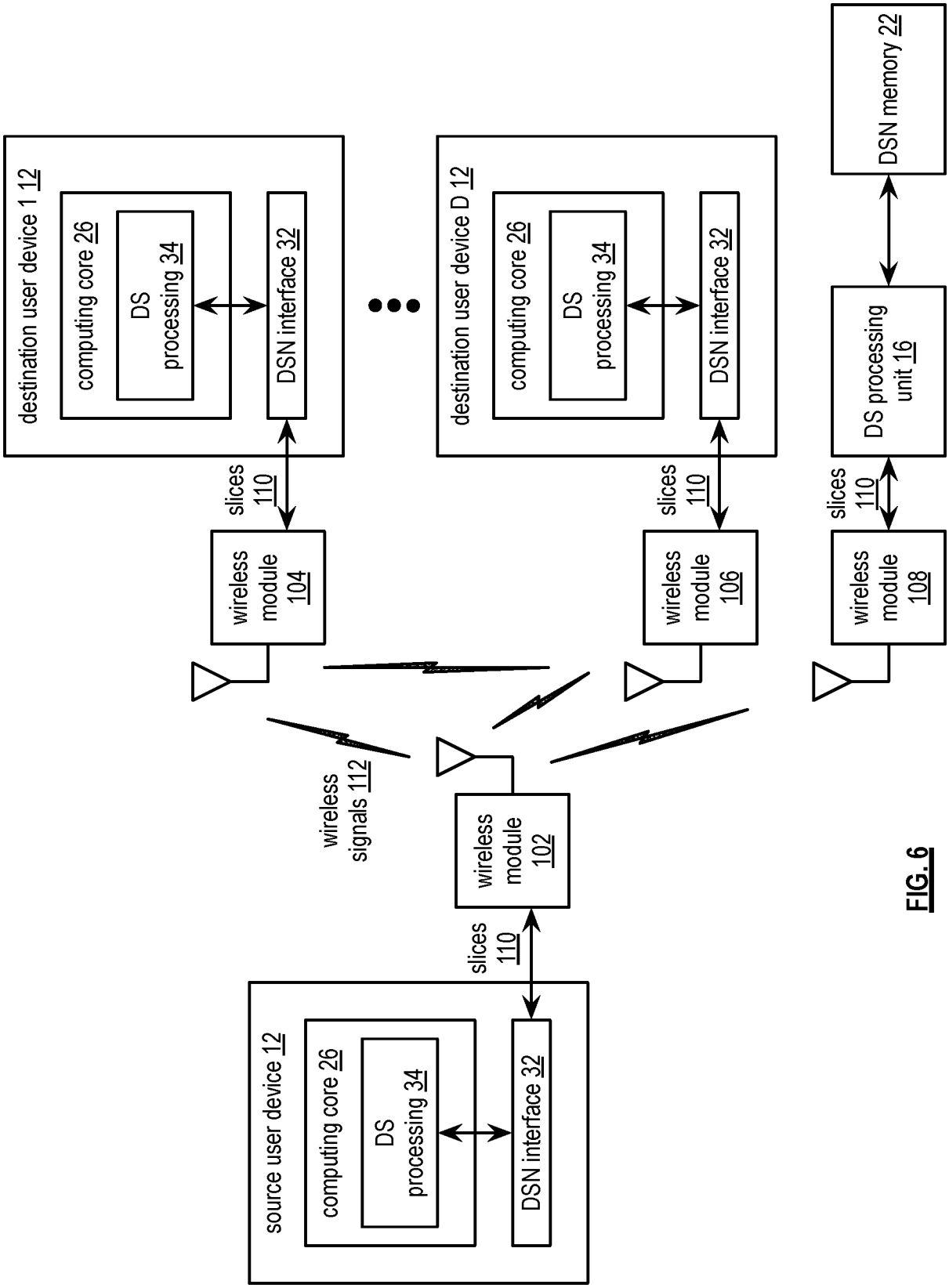
destination user device 1 12
computing core 26
DS processing 34
DSN interface 32
slices 110
wireless module 104
destination user device D 12
computing core 26
DS processing 34
DSN interface 32
slices 110
wireless module 106
DSN memory 22
DS processing unit 16
slices 110
wireless module 108
wireless signals 112
wireless module 102
slices 110
source user device 12
computing core 26
DS processing 34
DSN interface 32

FIG. 6

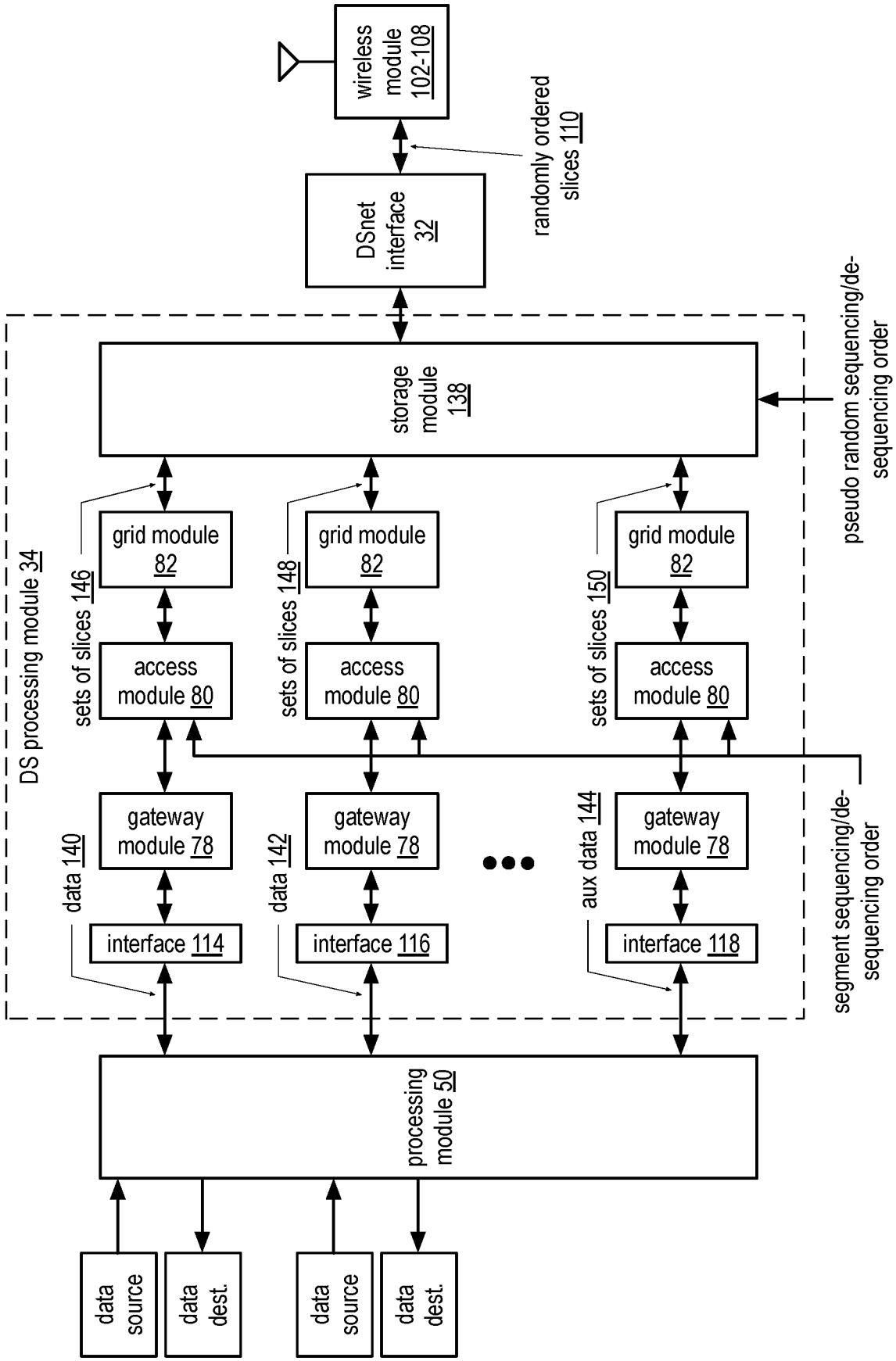
wireless module 102-108
randomly ordered slices 110
DSnet interface 32
storage module 138
pseudo random sequencing/de-sequencing order
DS processing module 34
sets of slices 146
sets of slices 148
sets of slices 150
grid module 82
access module 80
gateway module 78
data 140
data 142
aux data 144
interface 114
interface 116
interface 118
segment sequencing/de-sequencing order
processing module 50
data source
data dest.
data source
data dest.

FIG. 7

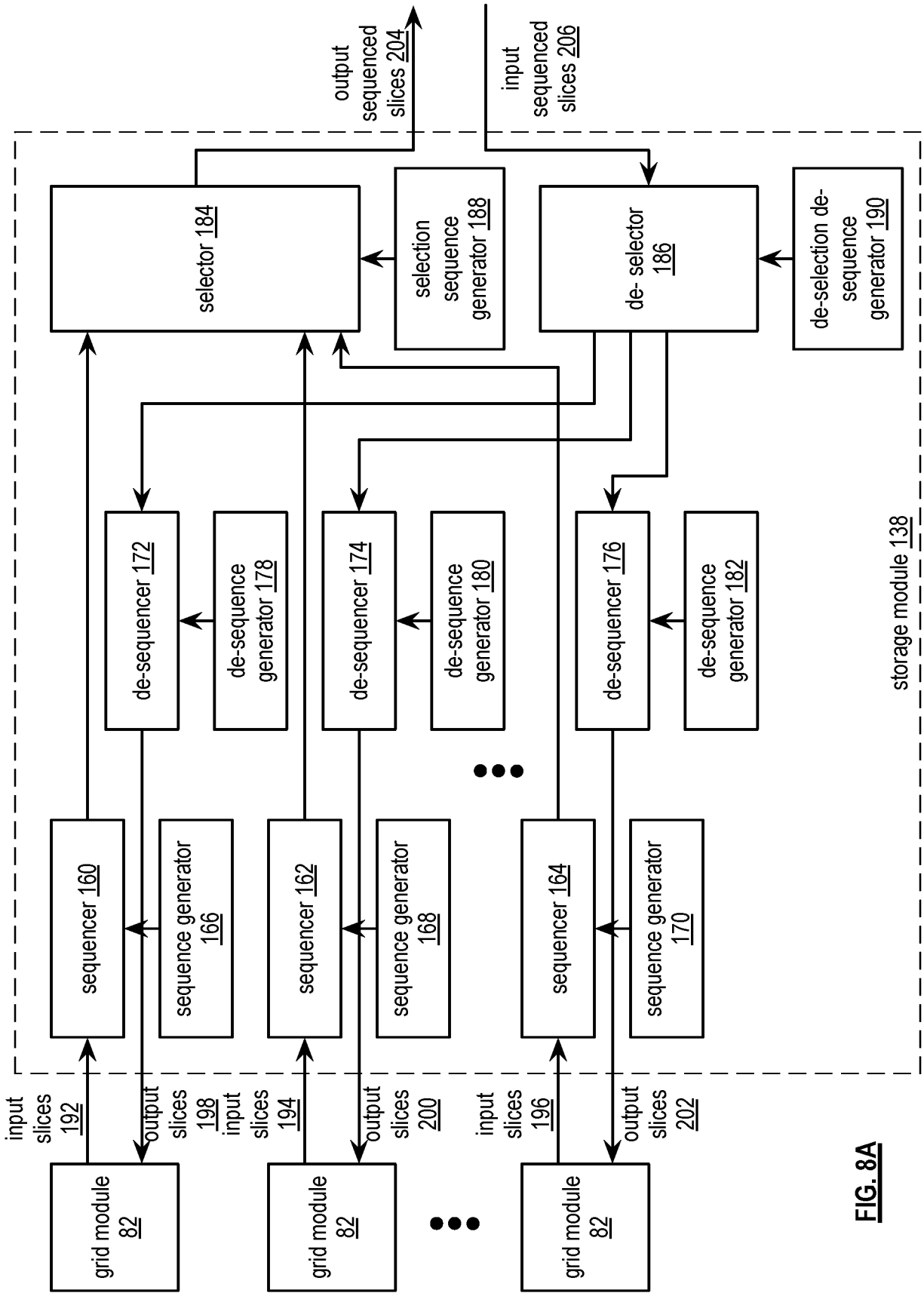
output sequenced slices 204
input sequenced slices 206
selector 184
selection sequence generator 188
de- selector 186
de-selection de-sequence generator 190
de-sequencer 172
de-sequence generator 178
de-sequencer 174
de-sequence generator 180
de-sequencer 176
de-sequence generator 182
storage module 138
sequencer 160
sequence generator 166
sequencer 162
sequence generator 168
sequencer 164
sequence generator 170
input slices 192
output slices 198
input slices 194
output slices 200
input slices 196
output slices 202
grid module 82
grid module 82
grid module 82

FIG. 8A

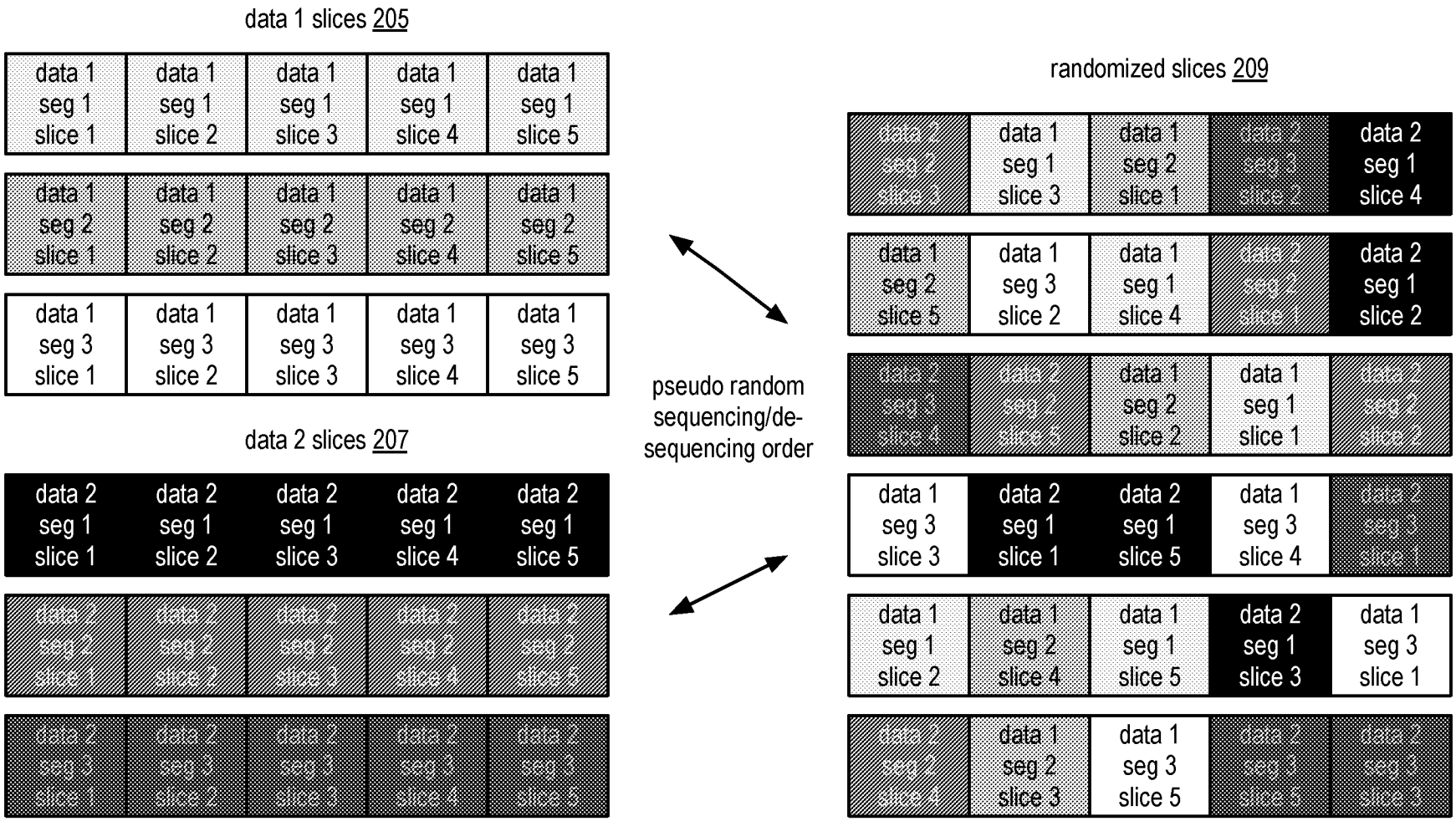
data 1 slices 205
data 1 seg 1 slice 1
data 1 seg 1 slice 2
data 1 seg 1 slice 3
data 1 seg 1 slice 4
data 1 seg 1 slice 5
data 1 seg 2 slice 1
data 1 seg 2 slice 2
data 1 seg 2 slice 3
data 1 seg 2 slice 4
data 1 seg 2 slice 5
data 1 seg 3 slice 1
data 1 seg 3 slice 2
data 1 seg 3 slice 3
data 1 seg 3 slice 4
data 1 seg 3 slice 5
data 2 slices 207
data 2 seg 1 slice 1
data 2 seg 1 slice 2
data 2 seg 1 slice 3
data 2 seg 1 slice 4
data 2 seg 1 slice 5
data 2 seg 2 slice 1
data 2 seg 2 slice 2
data 2 seg 2 slice 3
data 2 seg 2 slice 4
data 2 seg 2 slice 5
data 2 seg 3 slice 1
data 2 seg 3 slice 2
data 2 seg 3 slice 3
data 2 seg 3 slice 4
data 2 seg 3 slice 5
pseudo random sequencing/de-sequencing order
randomized slices 209
data 2 seg 2 slice 3
data 1 seg 1 slice 3
data 1 seg 2 slice 1
data 2 seg 3 slice 4
data 2 seg 1 slice 4
data 1 seg 2 slice 5
data 1 seg 3 slice 2
data 1 seg 1 slice 4
data 2 seg 2 slice 1
data 2 seg 1 slice 2
data 2 seg 3 slice 4
data 2 seg 2 slice 3
data 1 seg 2 slice 2
data 1 seg 1 slice 1
data 2 seg 2 slice 2
data 1 seg 3 slice 3
data 2 seg 1 slice 1
data 2 seg 1 slice 5
data 1 seg 3 slice 4
data 2 seg 3 slice 1
data 1 seg 1 slice 2
data 1 seg 2 slice 4
data 1 seg 1 slice 5
data 2 seg 1 slice 3
data 1 seg 3 slice 1
data 2 seg 2 slice 4
data 1 seg 2 slice 3
data 1 seg 3 slice 5
data 2 seg 3 slice 5
data 2 seg 3 slice 3

FIG. 8B

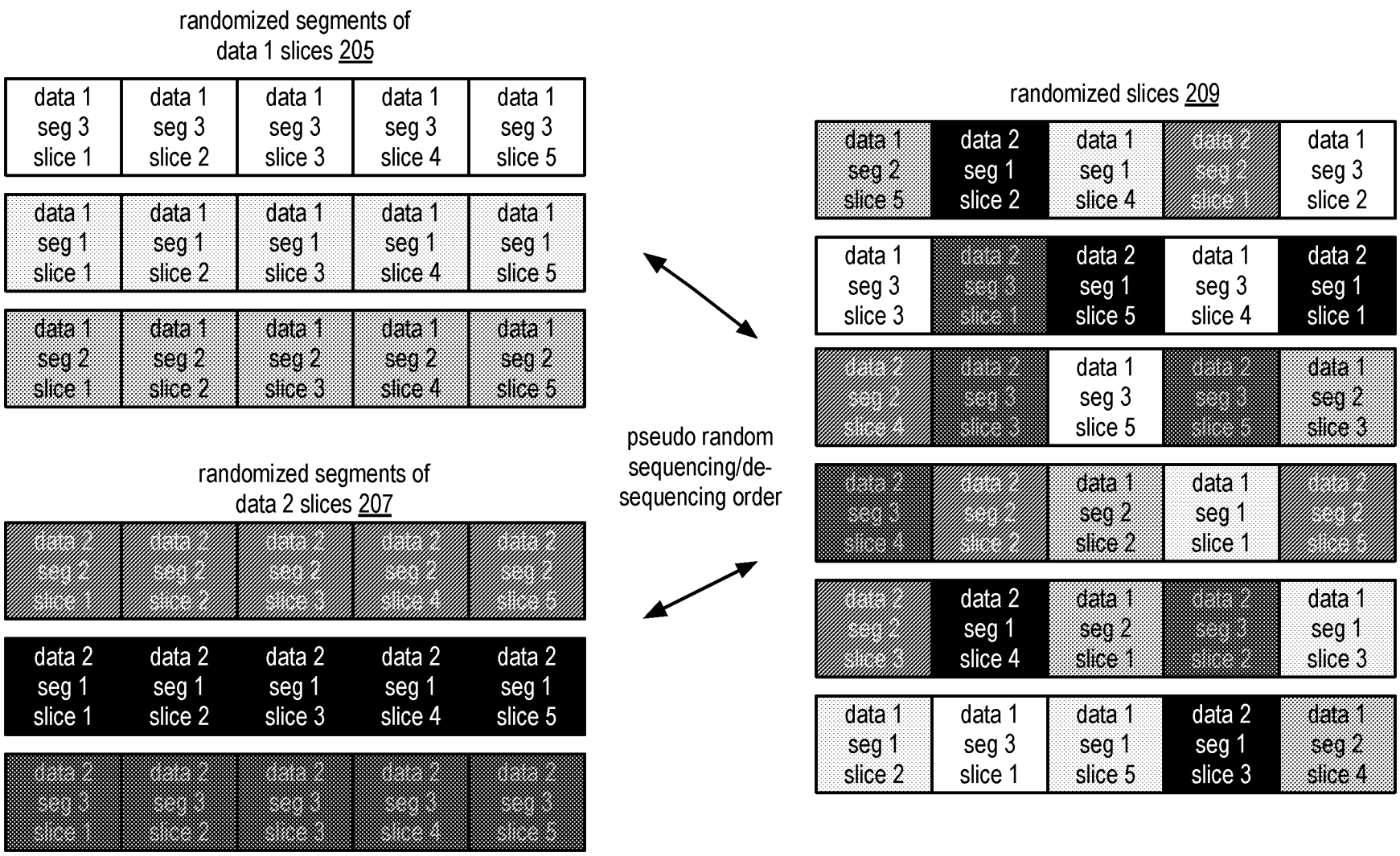
randomized segments of
data 1 slices 205
randomized segments of
data 2 slices 207
pseudo random
sequencing/de-
sequencing order
randomized slices 209

FIG. 8C

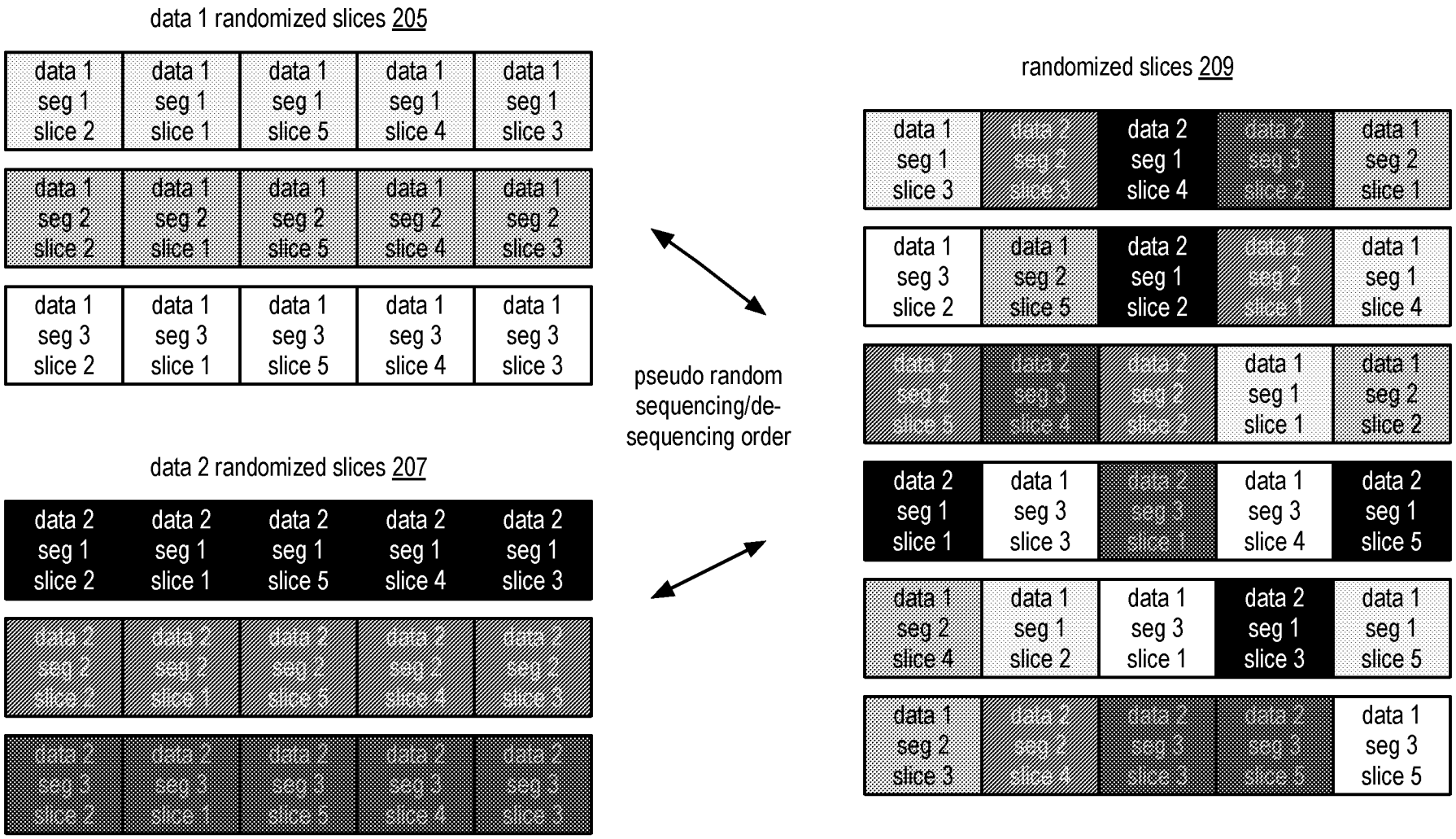
data 1 randomized slices 205
data 1 seg 1 slice 2
data 1 seg 1 slice 1
data 1 seg 1 slice 5
data 1 seg 1 slice 4
data 1 seg 1 slice 3
data 1 seg 2 slice 2
data 1 seg 2 slice 1
data 1 seg 2 slice 5
data 1 seg 2 slice 4
data 1 seg 2 slice 3
data 1 seg 3 slice 2
data 1 seg 3 slice 1
data 1 seg 3 slice 5
data 1 seg 3 slice 4
data 1 seg 3 slice 3
data 2 randomized slices 207
data 2 seg 1 slice 2
data 2 seg 1 slice 1
data 2 seg 1 slice 5
data 2 seg 1 slice 4
data 2 seg 1 slice 3
pseudo random sequencing/de-sequencing order
randomized slices 209
data 1 seg 1 slice 3
data 2 seg 1 slice 4
data 1 seg 2 slice 1
data 1 seg 3 slice 2
data 1 seg 2 slice 5
data 2 seg 1 slice 2
data 1 seg 1 slice 4
data 1 seg 1 slice 1
data 1 seg 2 slice 2
data 2 seg 1 slice 1
data 1 seg 3 slice 3
data 1 seg 3 slice 4
data 2 seg 1 slice 5
data 1 seg 2 slice 4
data 1 seg 1 slice 2
data 1 seg 3 slice 1
data 2 seg 1 slice 3
data 1 seg 1 slice 5
data 1 seg 2 slice 3
data 1 seg 3 slice 5

FIG. 8D

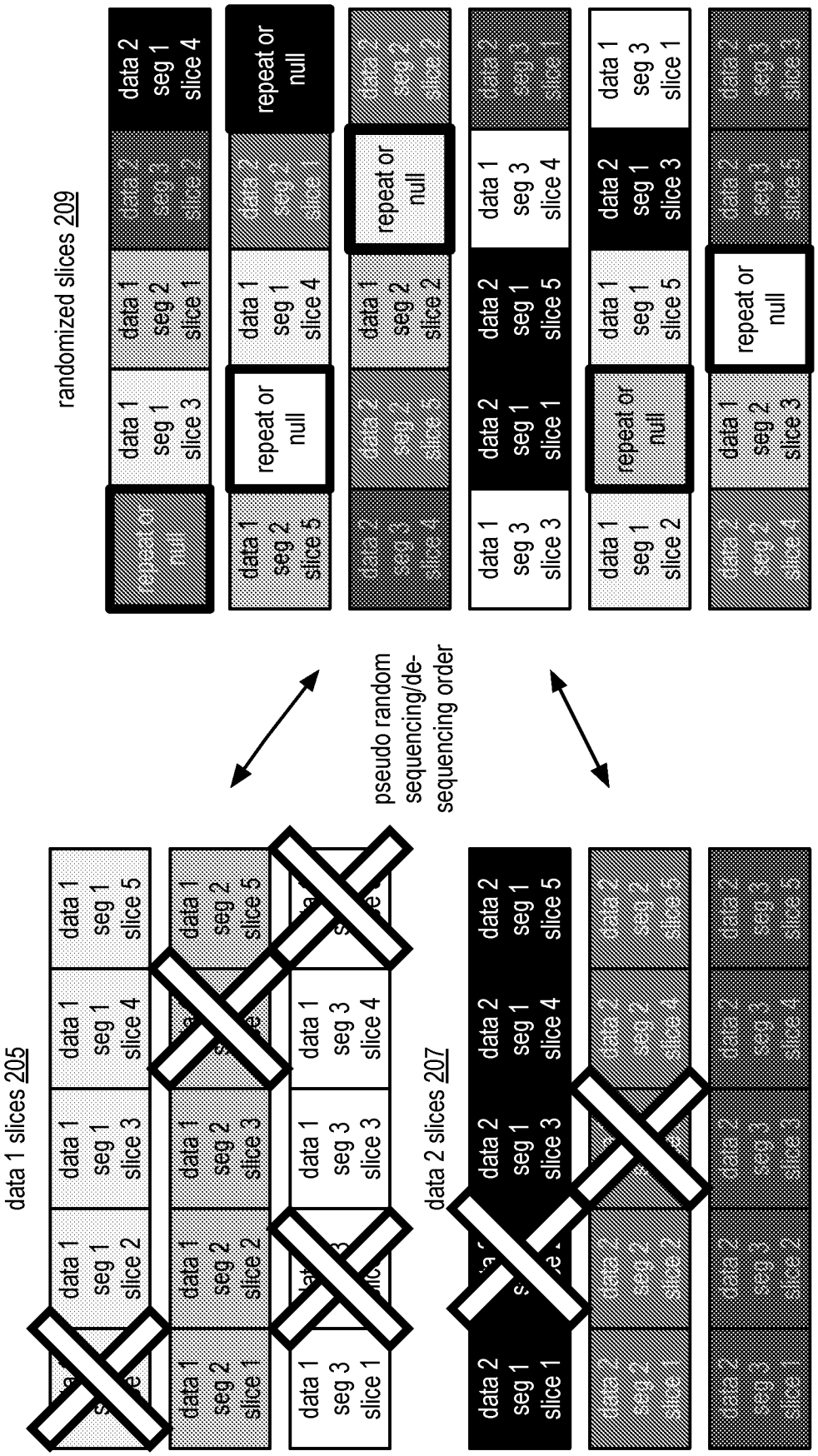
randomized slices 209
data 1 slices 205
data 2 slices 207
pseudo random sequencing/de-sequencing order
data 1 seg 1 slice 1
data 1 seg 2 slice 1
data 1 seg 1 slice 2
data 1 seg 2 slice 2
data 1 seg 1 slice 3
data 1 seg 2 slice 3
data 1 seg 1 slice 4
data 1 seg 3 slice 3
data 1 seg 3 slice 4
data 1 seg 1 slice 5
data 1 seg 2 slice 5
data 2 seg 1 slice 1
data 2 seg 1 slice 3
data 2 seg 1 slice 4
data 2 seg 1 slice 5
data 2 seg 1 slice 4
data 1 seg 1 slice 1
data 1 seg 2 slice 5
data 1 seg 1 slice 4
data 1 seg 2 slice 2
data 1 seg 3 slice 3
data 2 seg 1 slice 1
data 2 seg 1 slice 5
data 1 seg 3 slice 4
data 1 seg 1 slice 2
data 2 seg 1 slice 3
data 1 seg 1 slice 5
data 1 seg 3 slice 1
data 2 seg 1 slice 4
data 1 seg 2 slice 3
repeat or null
repeat or null
repeat or null
repeat or null

FIG. 8E

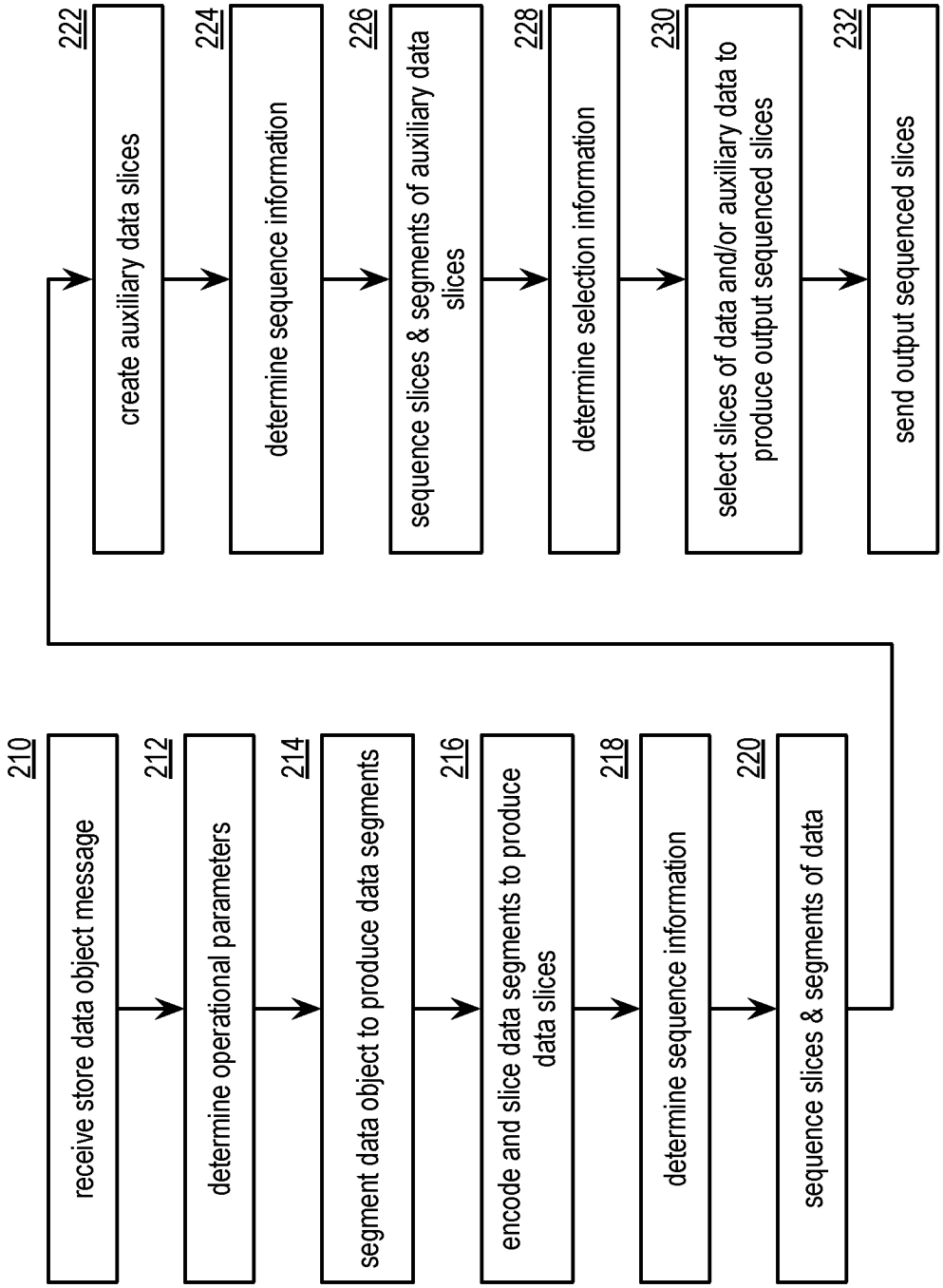
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
216
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 9

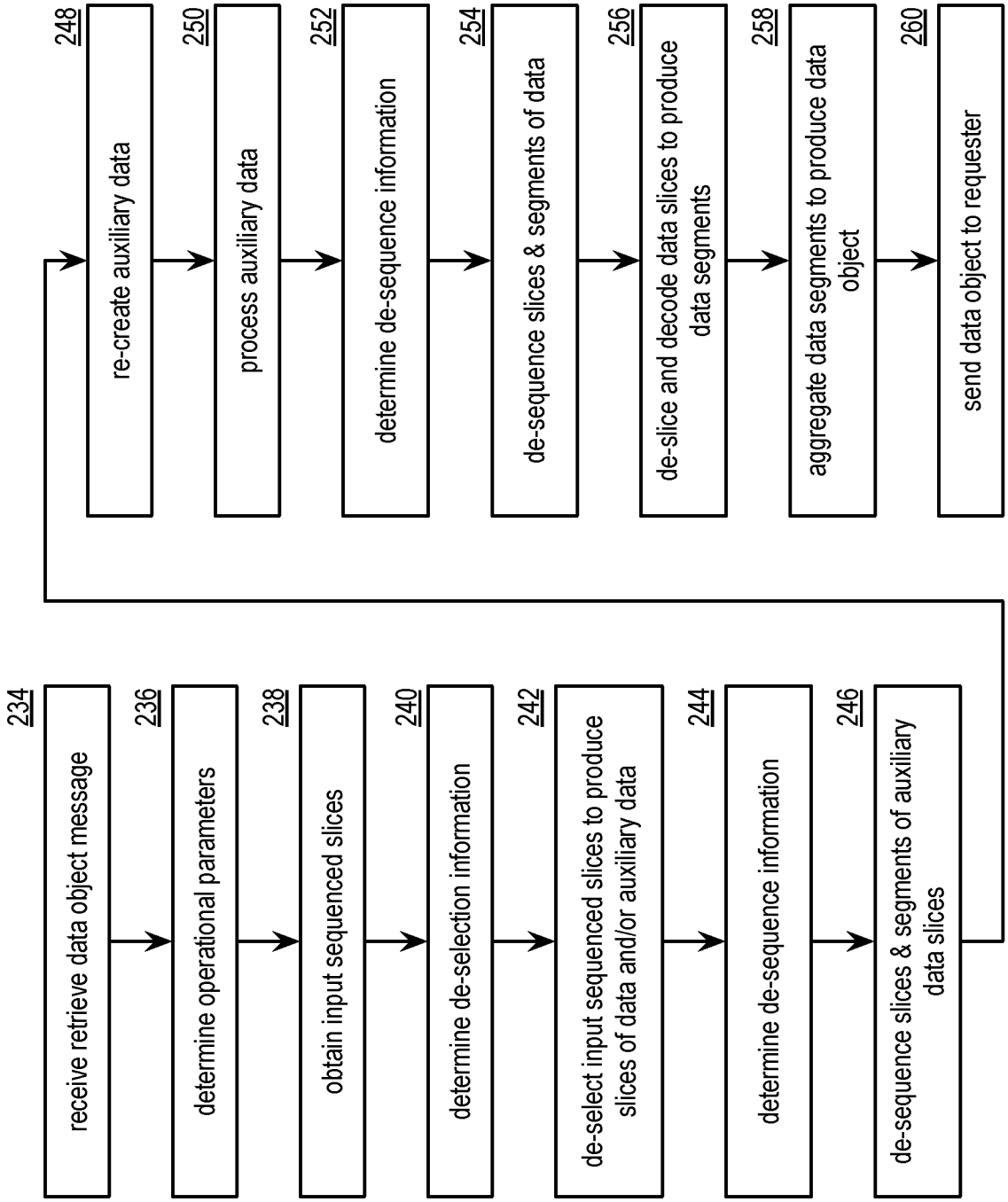
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 10

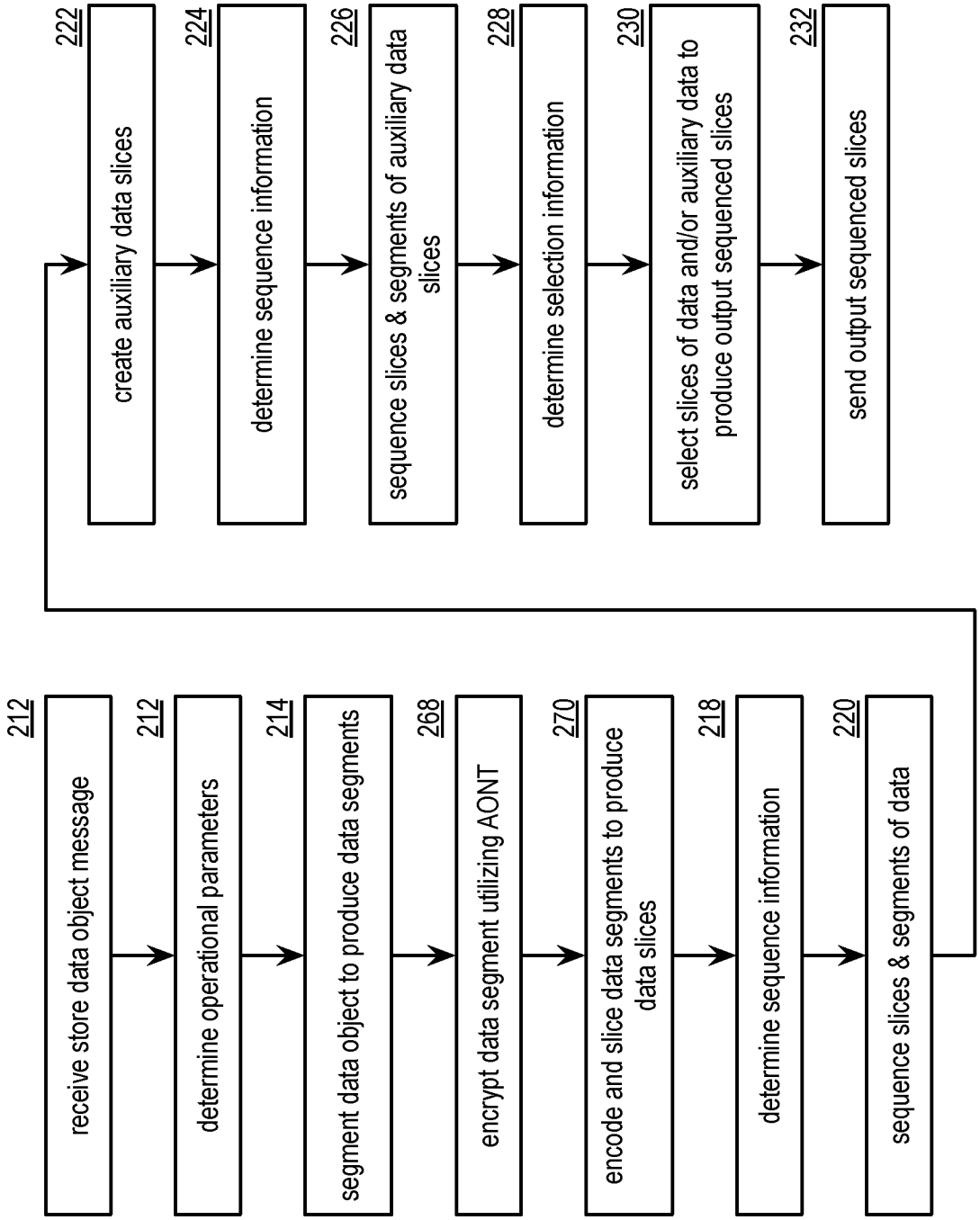
212
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
268
encrypt data segment utilizing AONT
270
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 11

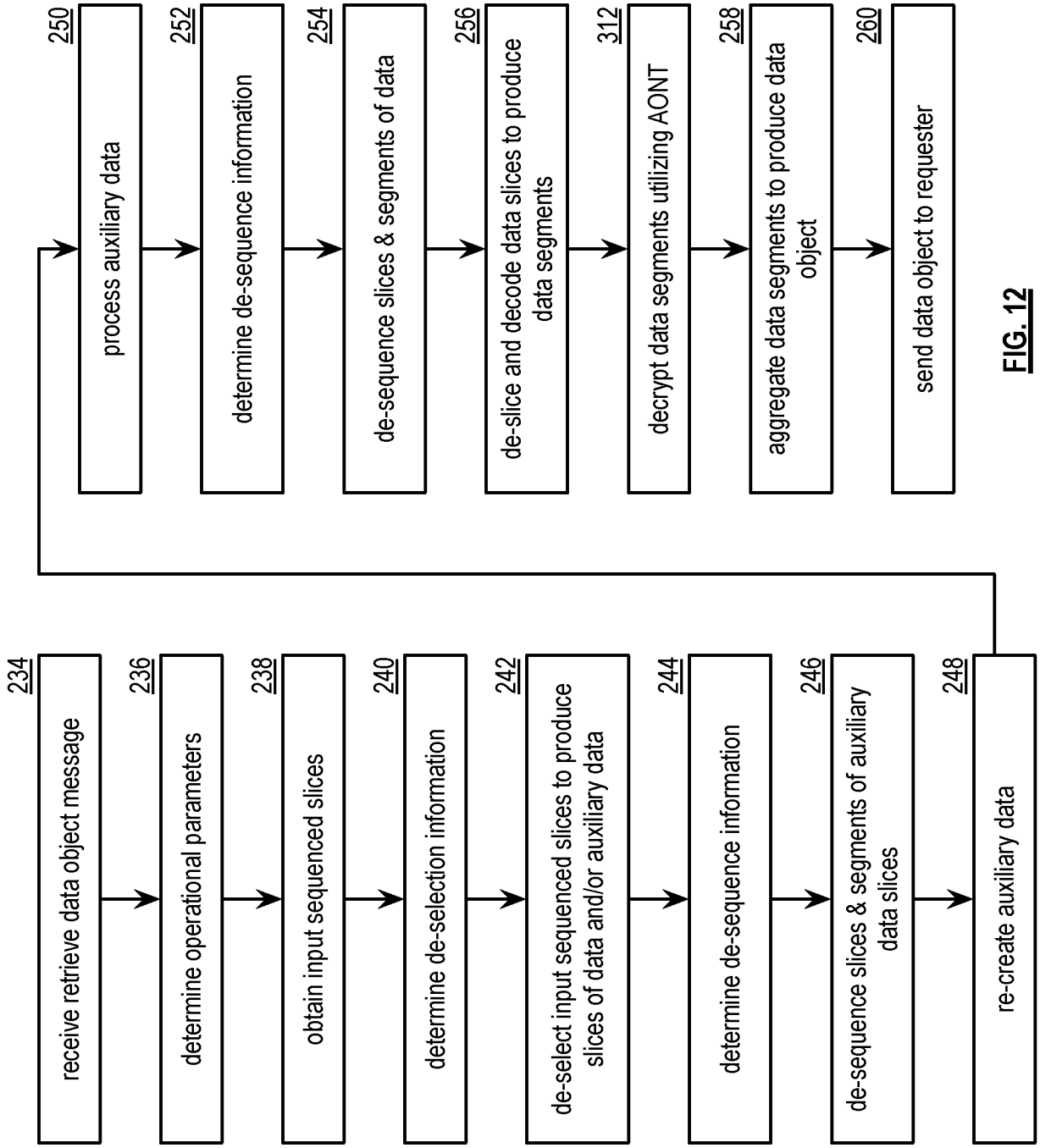
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 12

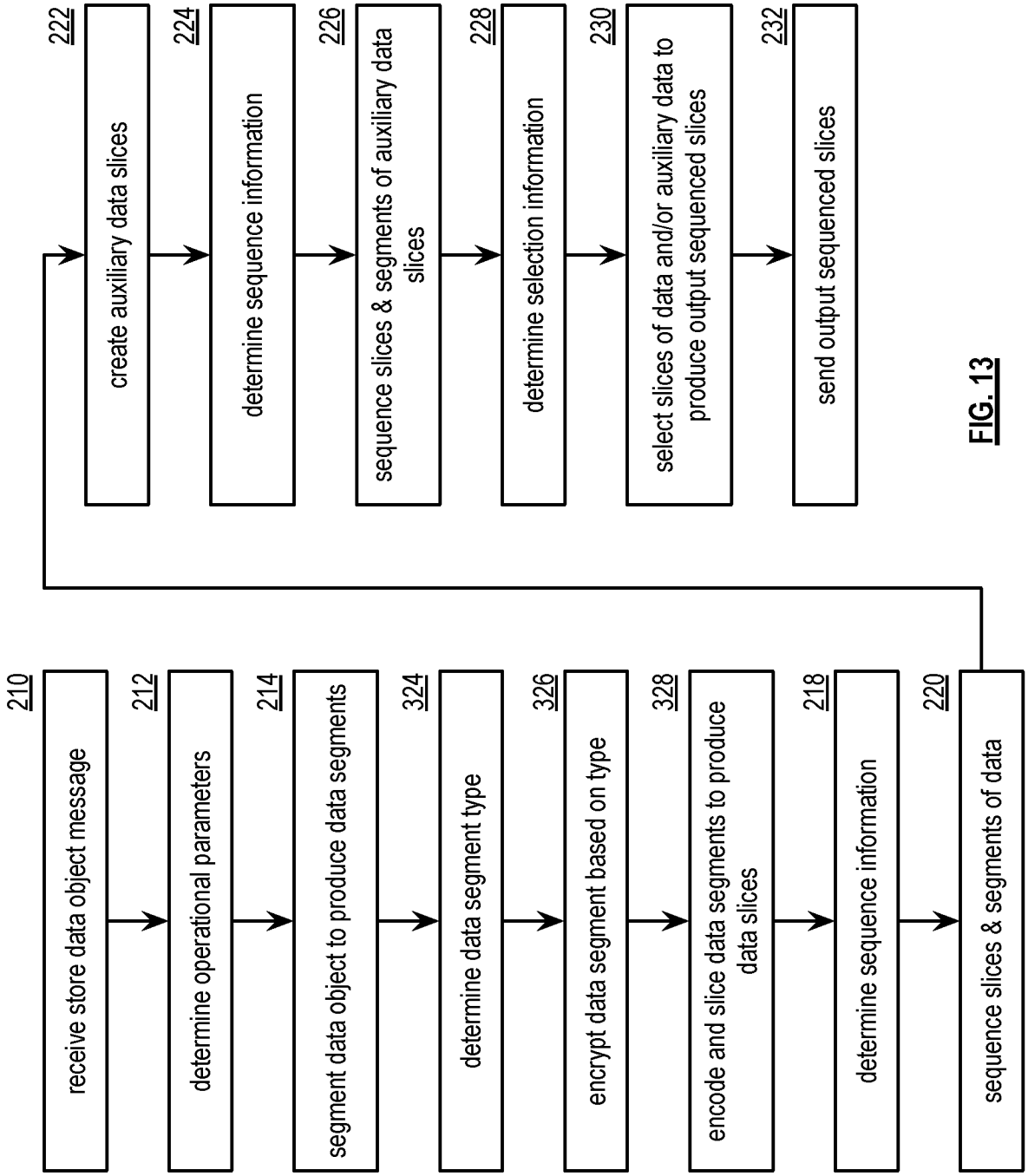
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
324
determine data segment type
326
encrypt data segment based on type
328
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 13

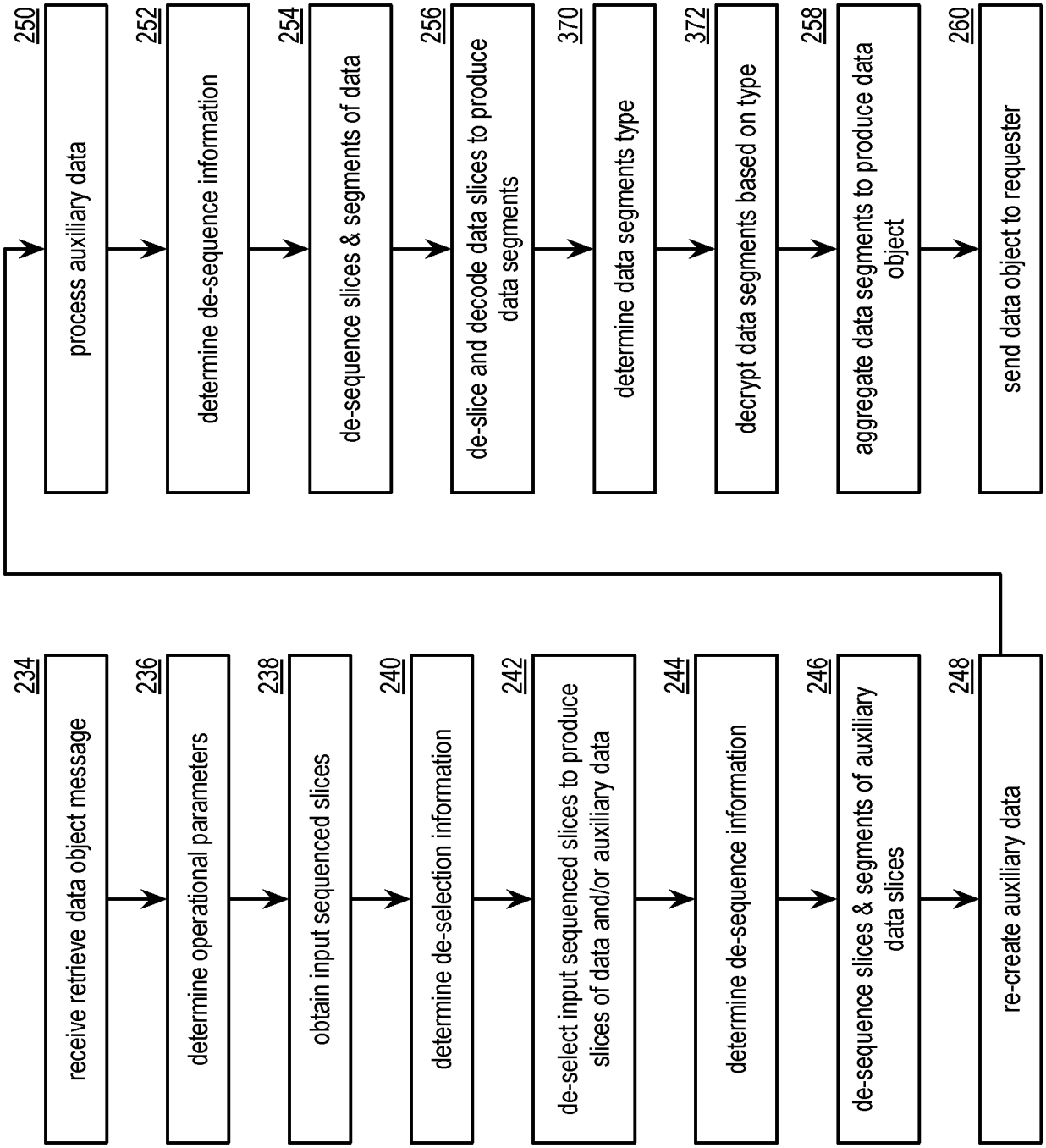
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
370
determine data segments type
372
decrypt data segments based on type
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 14

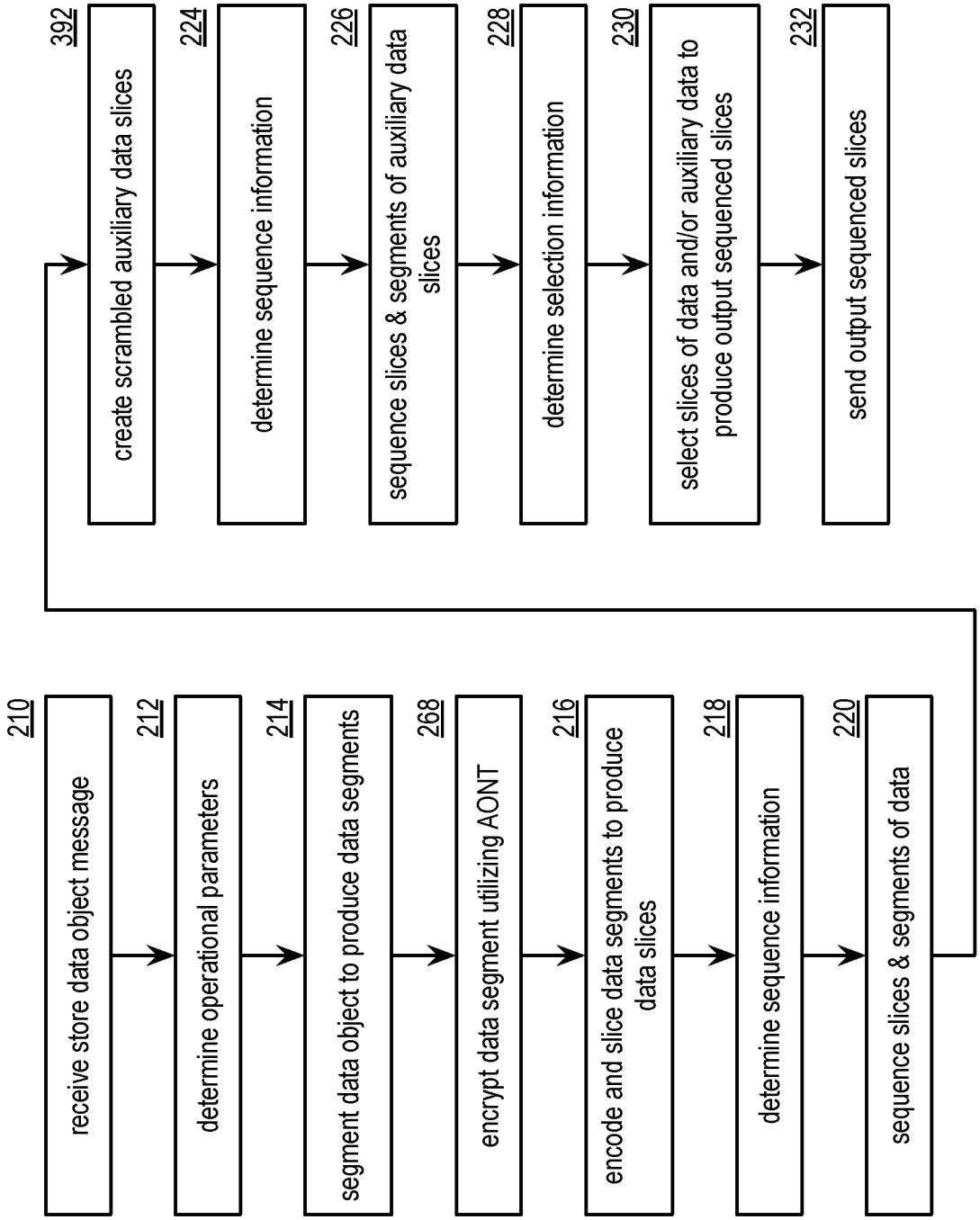
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
392
create scrambled auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 15

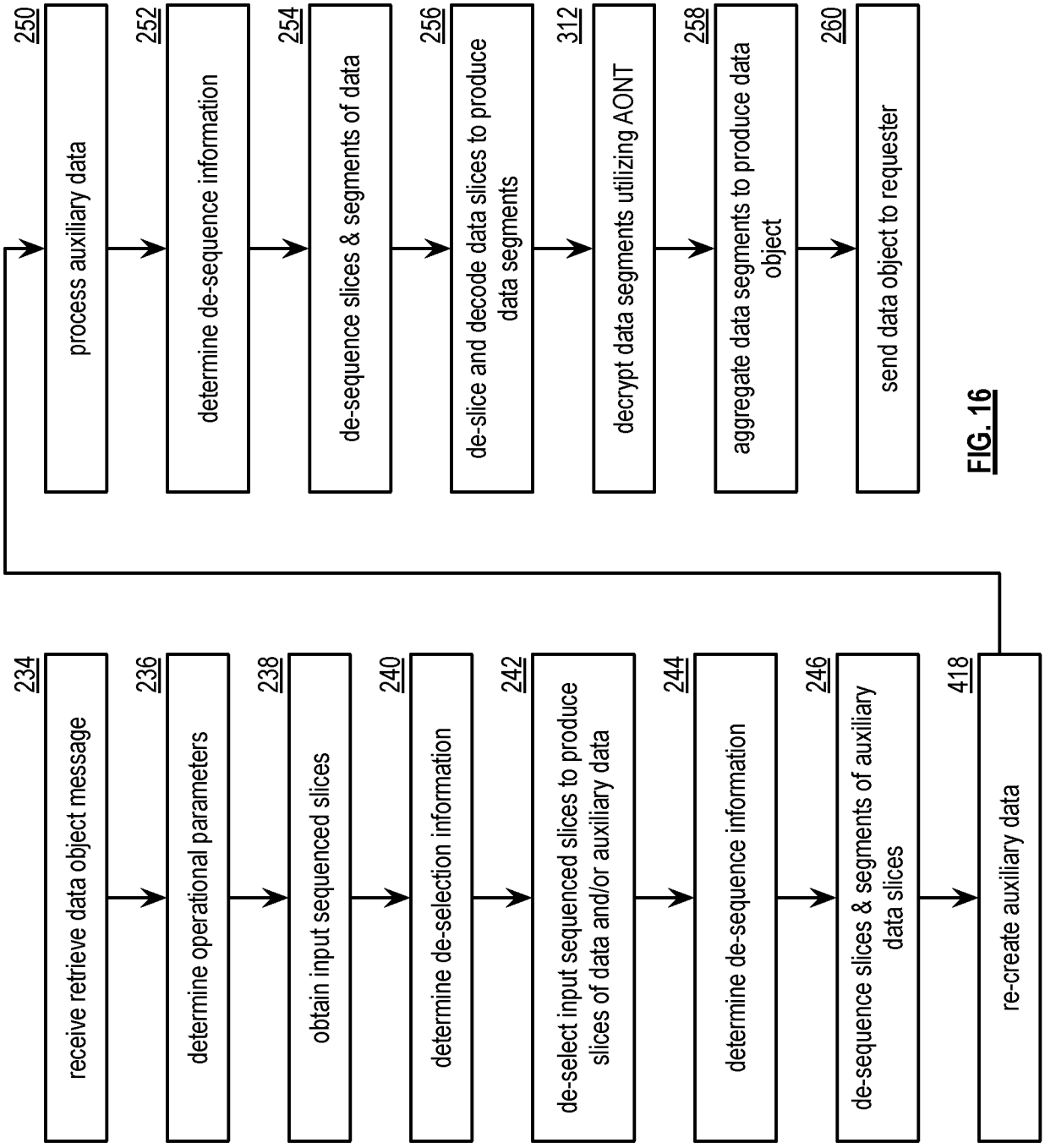
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
418
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 16

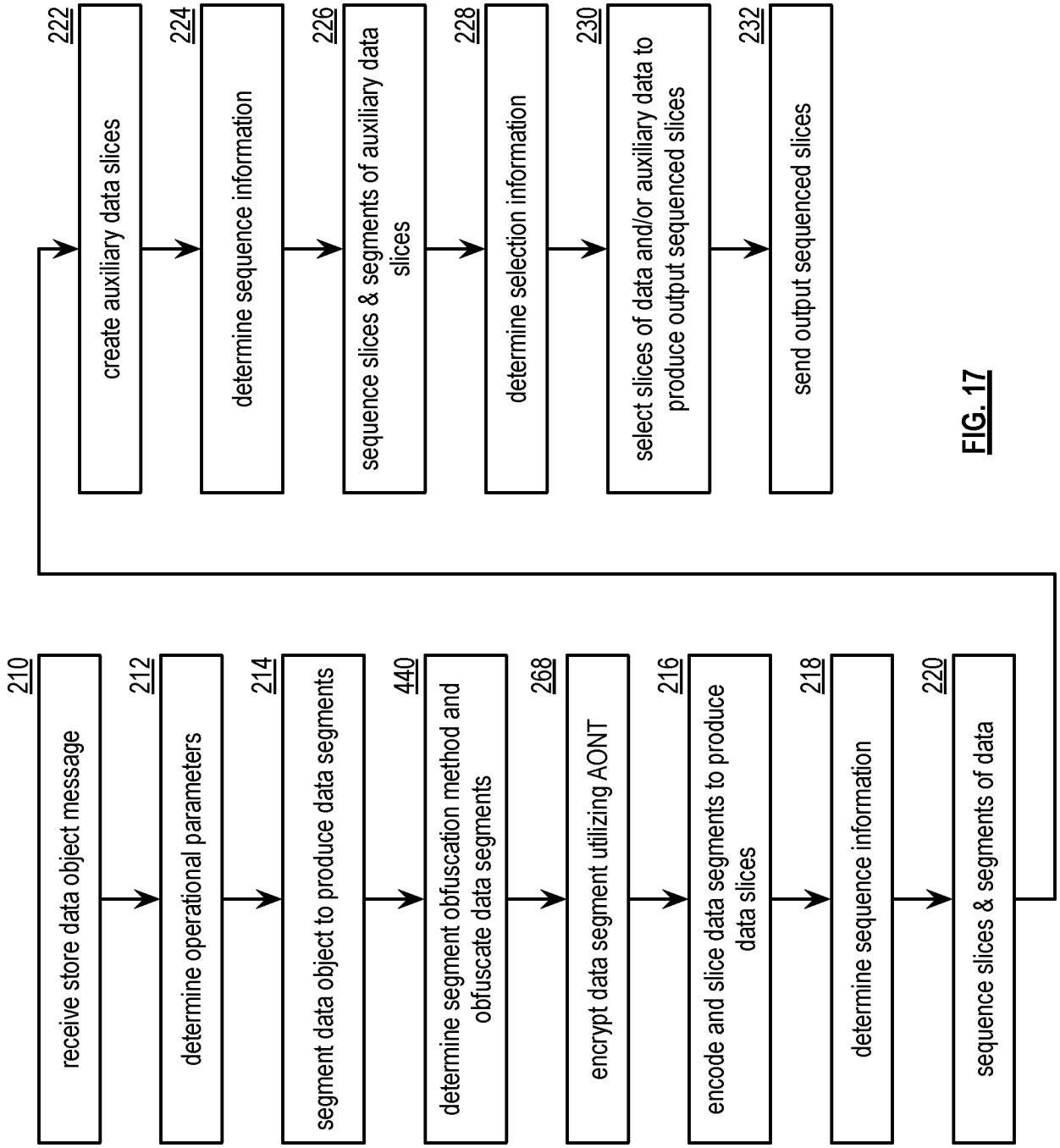
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
440
determine segment obfuscation method and obfuscate data segments
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 17

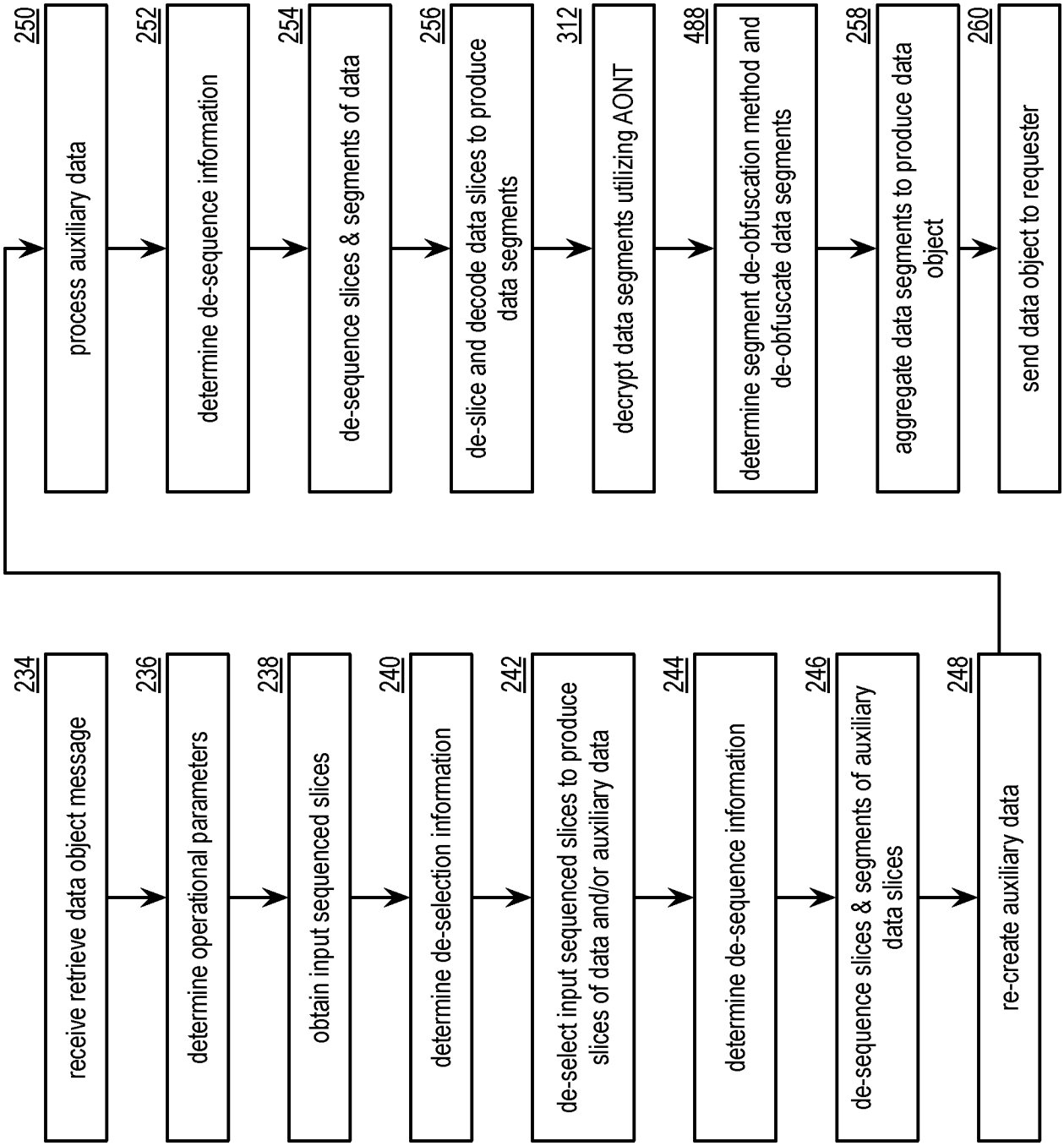
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
488
determine segment de-obfuscation method and de-obfuscate data segments
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 18

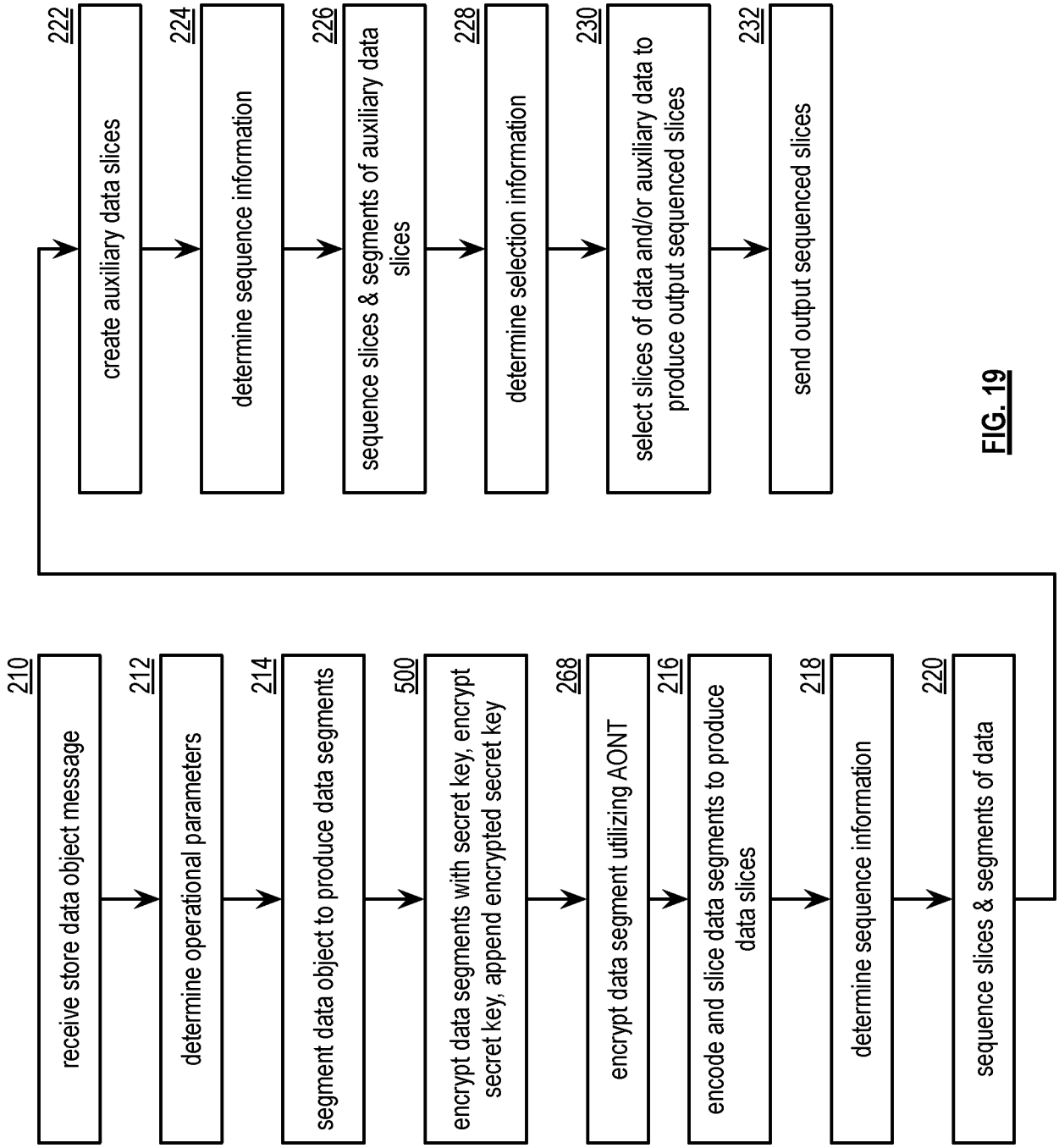
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
500
encrypt data segments with secret key, encrypt secret key, append encrypted secret key
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 19

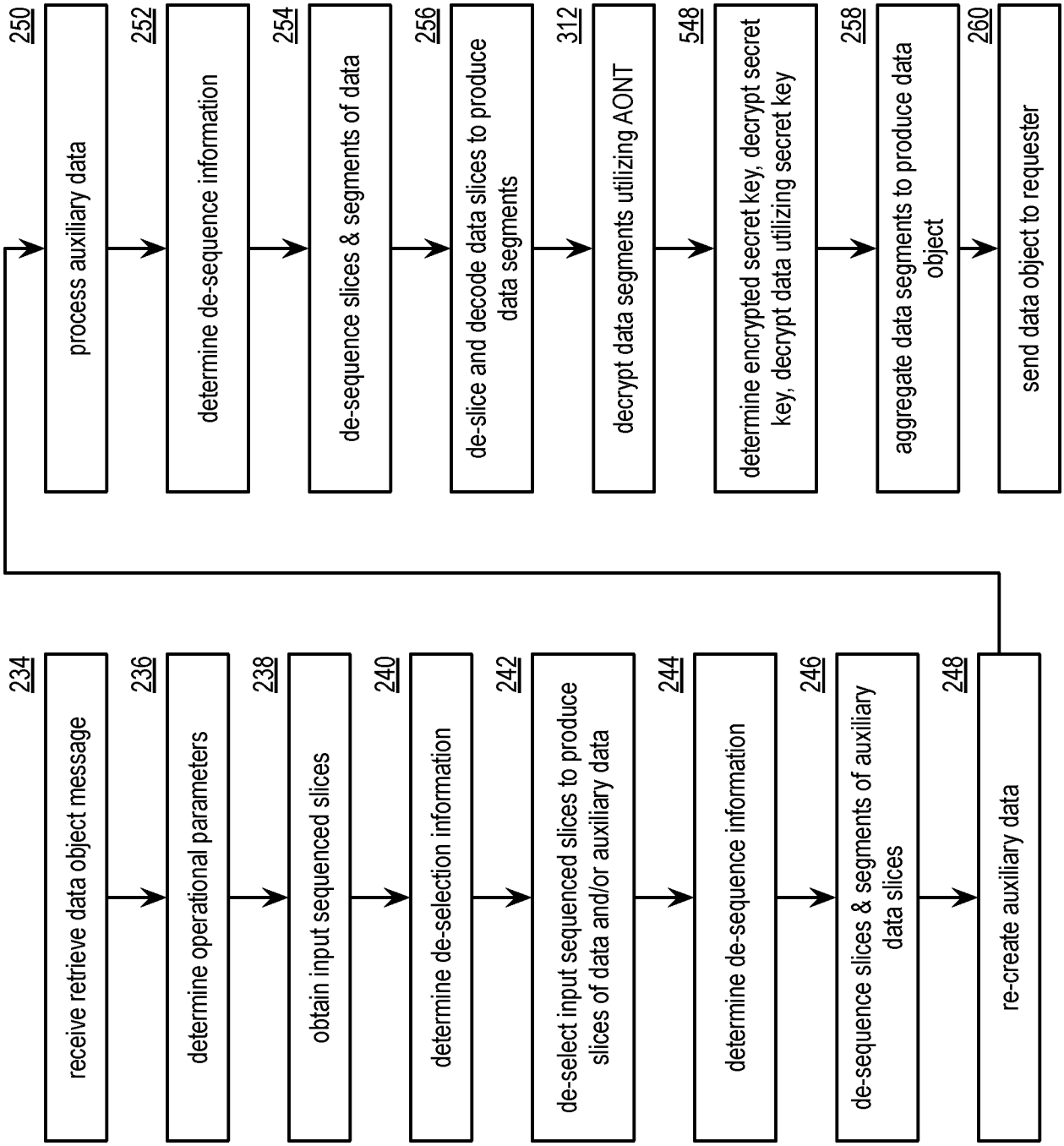
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
548
determine encrypted secret key, decrypt secret key, decrypt data utilizing secret key
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 20

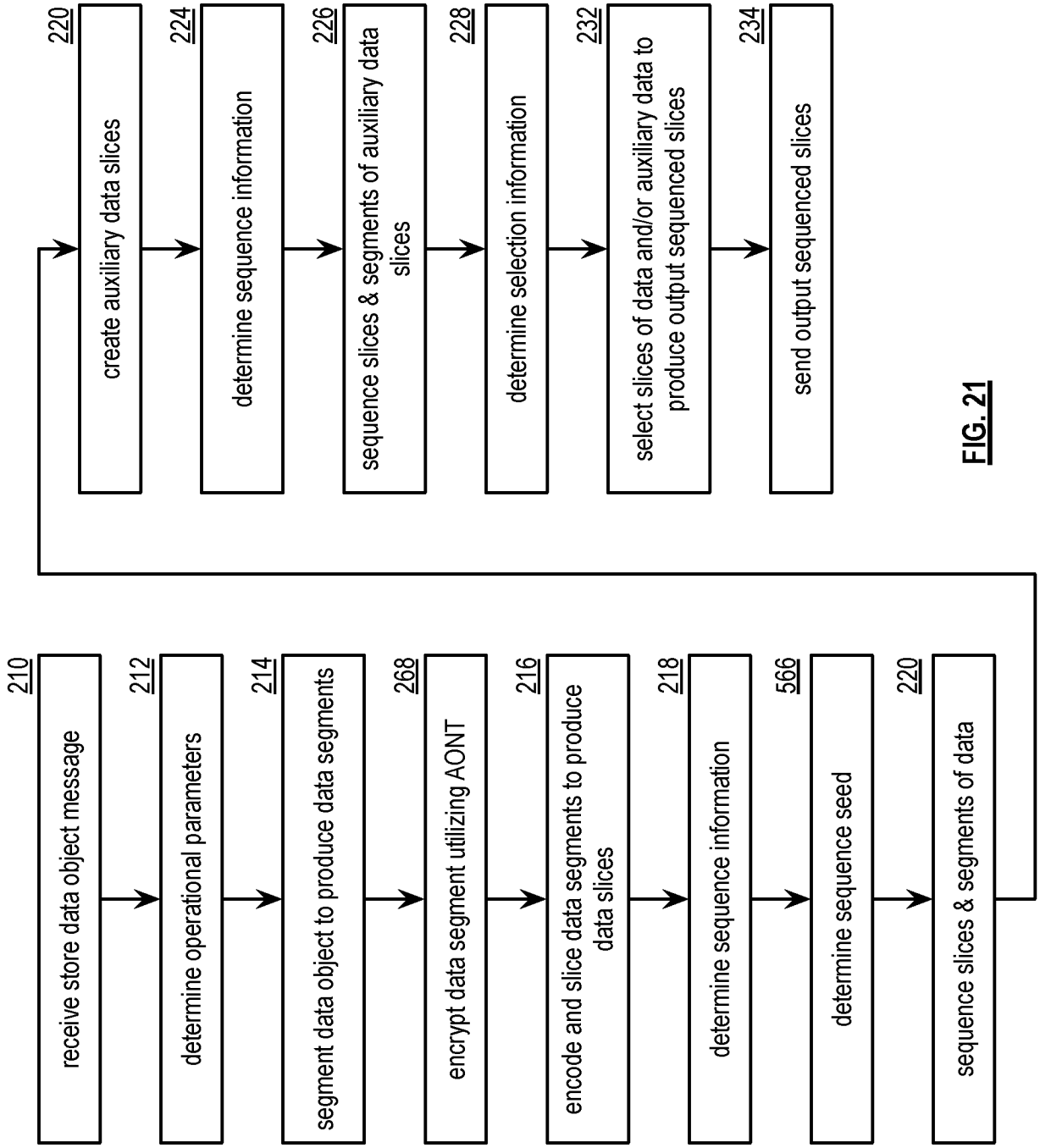
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
566
determine sequence seed
220
sequence slices & segments of data
220
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
232
select slices of data and/or auxiliary data to produce output sequenced slices
234
send output sequenced slices

FIG. 21

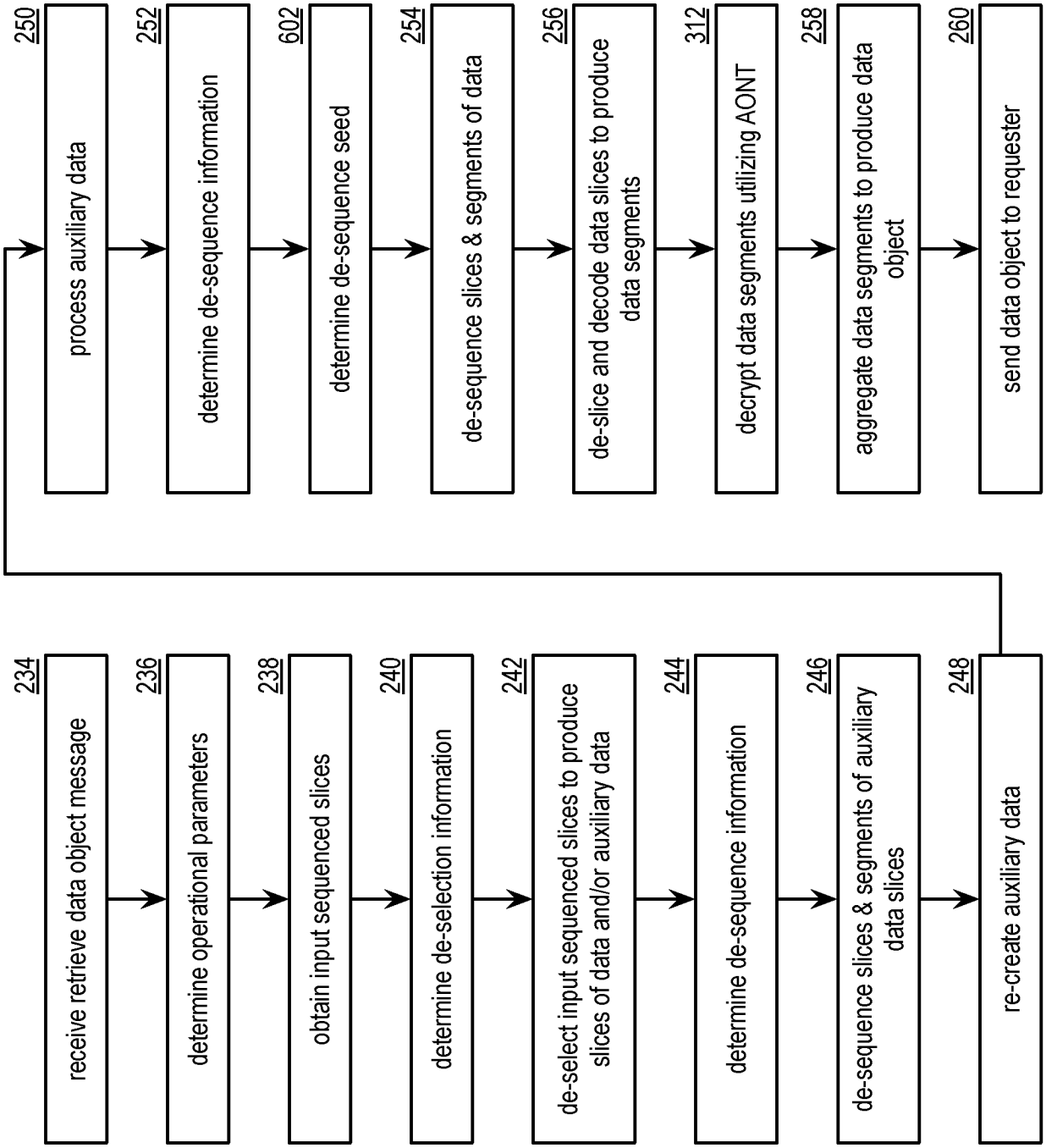
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
602
determine de-sequence seed
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 22

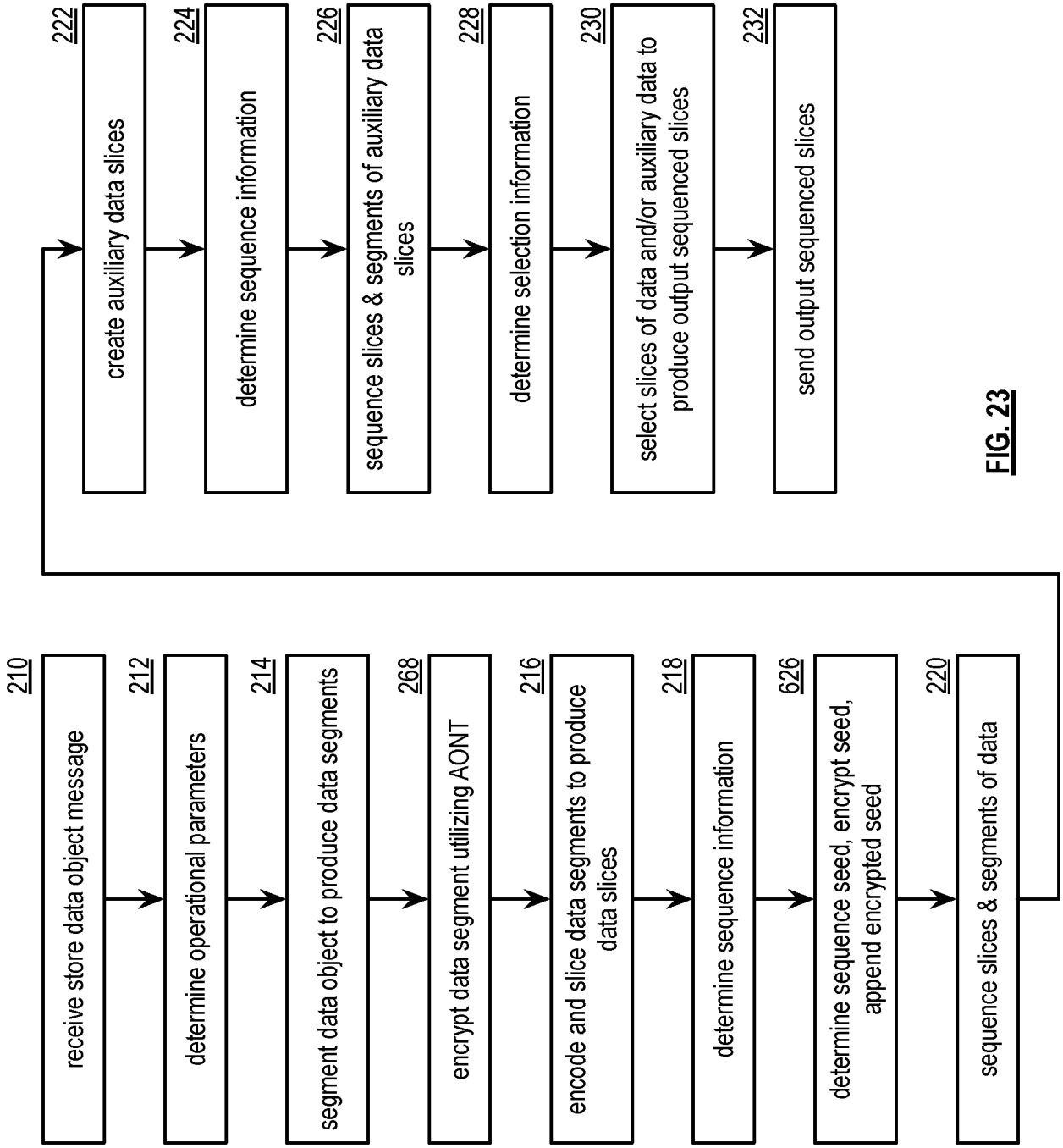
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
626
determine sequence seed, encrypt seed, append encrypted seed
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
232
send output sequenced slices

FIG. 23

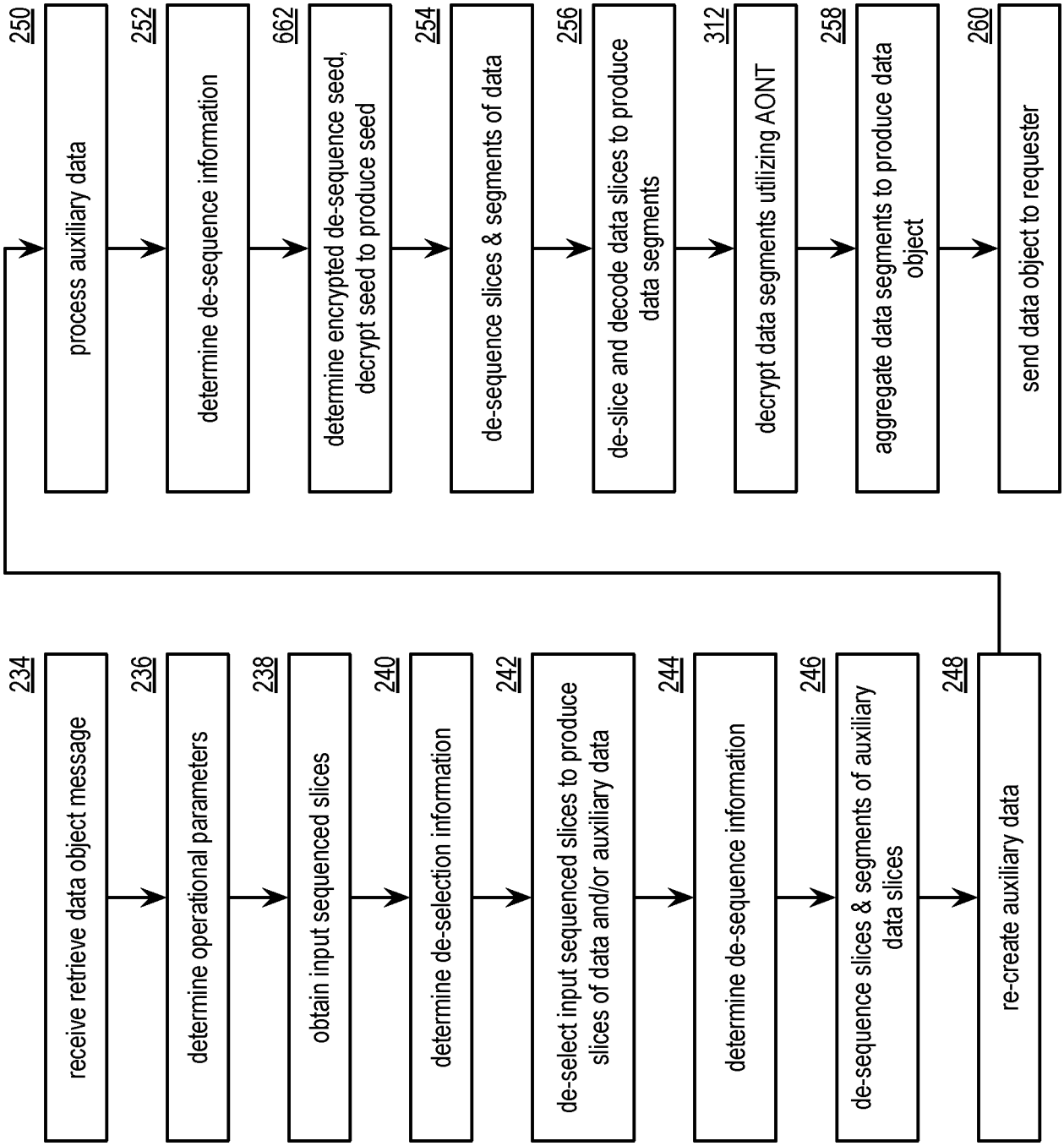
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data
250
process auxiliary data
252
determine de-sequence information
662
determine encrypted de-sequence seed, decrypt seed to produce seed
254
de-sequence slices & segments of data
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
258
aggregate data segments to produce data object
260
send data object to requester

FIG. 24

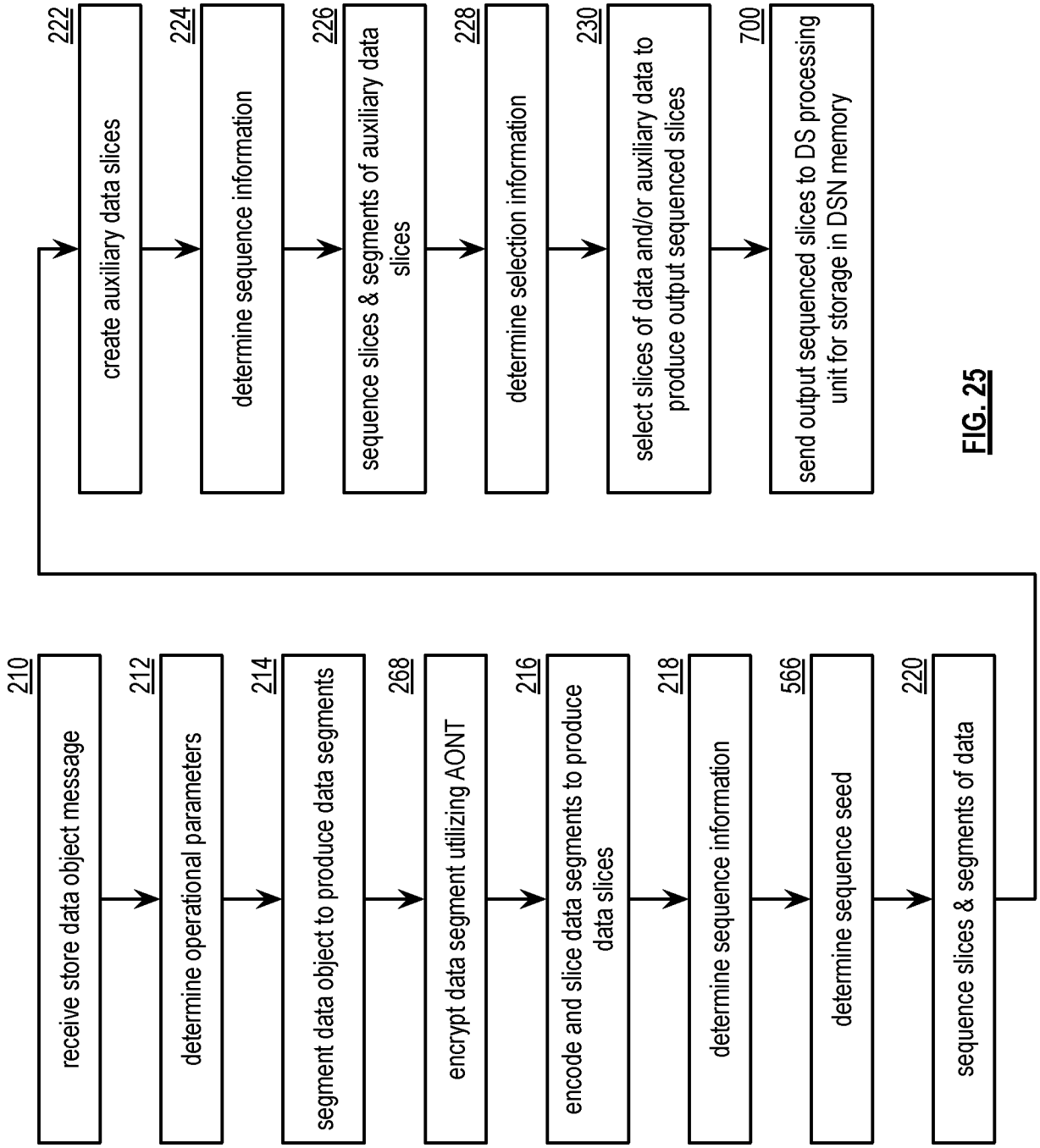
210
receive store data object message
212
determine operational parameters
214
segment data object to produce data segments
268
encrypt data segment utilizing AONT
216
encode and slice data segments to produce data slices
218
determine sequence information
566
determine sequence seed
220
sequence slices & segments of data
222
create auxiliary data slices
224
determine sequence information
226
sequence slices & segments of auxiliary data slices
228
determine selection information
230
select slices of data and/or auxiliary data to produce output sequenced slices
700
send output sequenced slices to DS processing unit for storage in DSN memory

FIG. 25

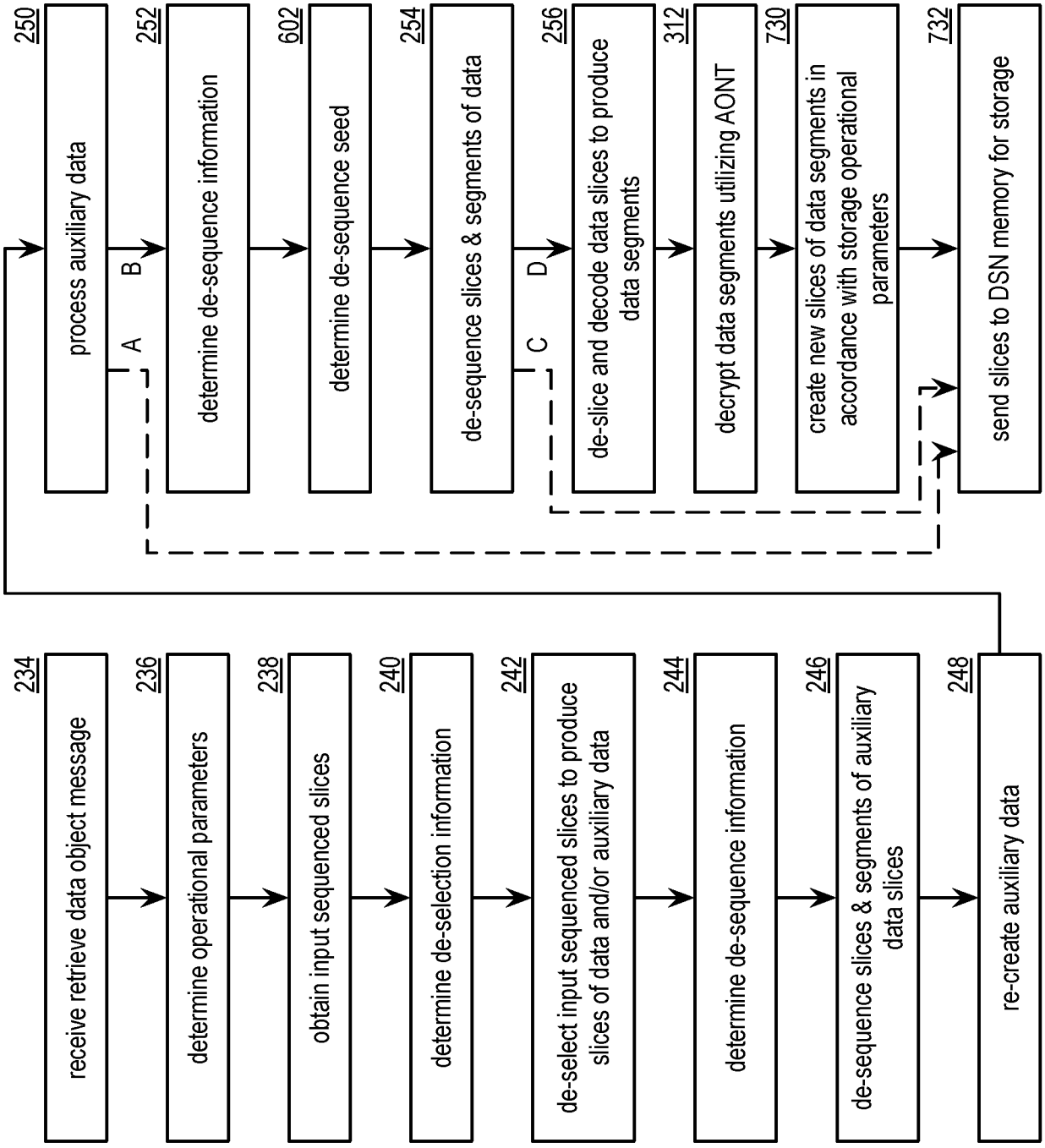
250
process auxiliary data
A
B
252
determine de-sequence information
602
determine de-sequence seed
254
de-sequence slices & segments of data
C
D
256
de-slice and decode data slices to produce data segments
312
decrypt data segments utilizing AONT
730
create new slices of data segments in accordance with storage operational parameters
732
send slices to DSN memory for storage
234
receive retrieve data object message
236
determine operational parameters
238
obtain input sequenced slices
240
determine de-selection information
242
de-select input sequenced slices to produce slices of data and/or auxiliary data
244
determine de-sequence information
246
de-sequence slices & segments of auxiliary data slices
248
re-create auxiliary data

FIG. 26

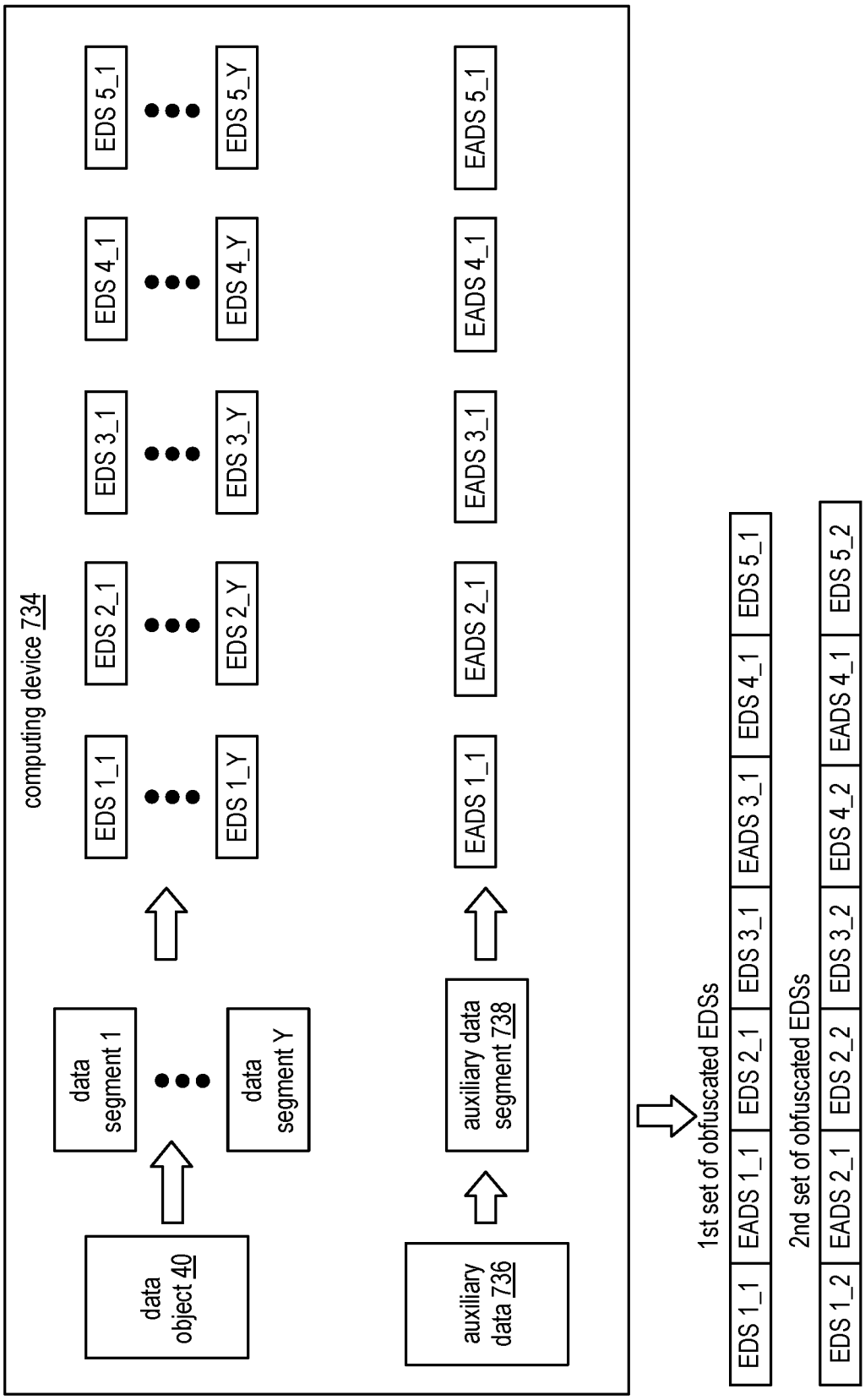
computing device 734
data object 40
data segment 1
data segment Y
EDS 1_1
EDS 1_Y
EDS 2_1
EDS 2_Y
EDS 3_1
EDS 3_Y
EDS 4_1
EDS 4_Y
EDS 5_1
EDS 5_Y
auxiliary data 736
auxiliary data segment 738
EADS 1_1
EADS 2_1
EADS 3_1
EADS 4_1
EADS 5_1
1st set of obfuscated EDSs
EDS 1_1
EADS 1_1
EDS 2_1
EDS 3_1
EADS 3_1
EDS 4_1
EDS 5_1
2nd set of obfuscated EDSs
EDS 1_2
EADS 2_1
EDS 2_2
EDS 3_2
EDS 4_2
EADS 4_1
EDS 5_2

FIG. 27

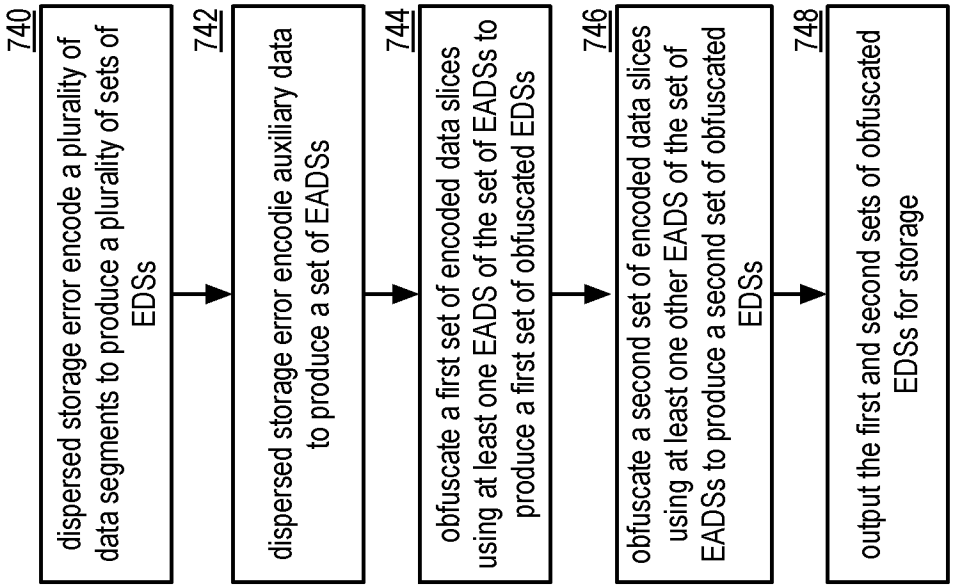
740
dispersed storage error encode a plurality of data segments to produce a plurality of sets of EDSs
742
dispersed storage error encodie auxiliary data to produce a set of EADSs
744
obfuscate a first set of encoded data slices using at least one EADS of the set of EADSs to produce a first set of obfuscated EDSs
746
obfuscate a second set of encoded data slices using at least one other EADS of the set of EADSs to produce a second set of obfuscated EDSs
748
output the first and second sets of obfuscated EDSs for storage

FIG. 28

DECLARATION (37 C.F.R. § 1.63) FOR UTILITY PATENT APPLICATION USING AN APPLICATION DATA SHEET (37 C.F.R. § 1.76) AND ASSIGNMENT

Title of Invention: **SECURE DATA TRANSMISSION UTILIZING DISTRIBUTED STORAGE**

As a below named and undersigned inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked):

☐ United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. § 1.56.

Whereas, I ("ASSIGNOR") have made certain inventions, improvements, and discoveries (herein referred to as the "Invention") disclosed in the above-identified patent application and further identified by the IBM Docket Number provided above in the header of this document;

Whereas, International Business Machines Corporation (herein referred to as the "ASSIGNEE"), a corporation of New York having a place of business at Armonk, New York, desires to acquire, and I desire to grant to the ASSIGNEE, my entire worldwide right, title, and interest in and to the Invention and in and to any and all patent applications and patents directed thereto;

Now, therefore, for good and valuable consideration, the receipt and sufficiency thereof being hereby acknowledged, I hereby sell or have sold, assign or have assigned, and otherwise transfer or have transferred to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the Invention, the above-identified United States patent application, and any and all other patent applications and patents for the Invention which may be applied for or granted therefor in the United States and in all foreign countries and jurisdictions, including all divisions, continuations, reissues, reexaminations, renewals, extensions, counterparts, substitutes, and extensions thereof, and all rights of priority resulting from the filing of such applications and granting of such patents. In addition, I hereby authorize and request the Director of the United States Patent and Trademark Office to issue any United States Patent, and foreign patent authorities to issue any foreign patent, granted for the Invention, to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the same to be held and enjoyed by the ASSIGNEE, its successors, legal representatives, and assigns to the full end of the terms for which any and all such patents may be granted, as fully and entirely as would have been held and enjoyed by me had this Assignment not been made; and I agree to execute any and all documents and instruments and perform all lawful acts reasonably related to recording this Assignment or perfecting title to the Invention and all related patents and applications, in the ASSIGNEE, its successors, legal

Security First Innovations, LLC, Exhibit 2012
Page 2012 - 242
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of New York, and any disputes will be resolved in a New York state court or federal court sited in New York.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

(1) Legal Name of Inventor: Jason K. Resch

Signature: / Jason Resch / Date: 11-19-18

(2) Legal Name of Inventor: S. Christopher Gladwin

Signature: / / Date: _____

(3) Legal Name of Inventor: Thomas F. Shirley, Jr.

Signature: / [illegible] / Date: 19 Nov 18

(4) Legal Name of Inventor: Gary W. Grube

Signature: / Gary W Grube / Date: 10/12/2018

representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of New York, and any disputes will be resolved in a New York state court or federal court sited in New York.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

(1) Legal Name of Inventor: Jason K. Resch

Signature: / _____ / Date: _____

(2) Legal Name of Inventor: S. Christopher Gladwin

Signature: / _____ / Date: 19 Nov 2018

(3) Legal Name of Inventor: Thomas F. Shirley, Jr.

Signature: / _____ / Date: _____

(4) Legal Name of Inventor: Gary W. Grube

Signature: / _____ / Date: 10/12/2018

Security First Innovations, LLC, Exhibit 2012
Scanned with CamScanner
IPR2025-01201, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

DocCode – SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 16197275 Document Date: 11/20/2018

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via eDAN using the Supplemental Content tab, or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: August 26, 2013