

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00215
Patent 10,452,854 B2

Before THOMAS L. GIANNETTI, JASON M. REPKO, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

REPKO, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Google LLC (“Petitioner”) filed a petition requesting *inter partes* review of claims 1–10 of U.S. Patent No. 10,452,854 B2 (Ex. 1001, “the ’854 patent”). Paper 2 (“Pet.”). Security First Innovations, LLC (“Patent Owner”) filed a Preliminary Response. Paper 9 (“Prelim. Resp.”).

To institute an *inter partes* review, we must determine “that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2018). For the reasons discussed below, Petitioner has shown a reasonable likelihood that it would prevail with respect to all claims challenged in the Petition. Thus, we institute an *inter partes* review.

A. Related Matters

According to the parties, the ’854 patent has been asserted in *Security First Innovations, LLC v. Google LLC*, No. 2:23-cv-00097 (E.D. Va.) (transferred from Alexandria Division, 1:23-cv-00329). Pet. xi; Paper 6, 1 (First Updated Mandatory Notices). Patent Owner further indicates that IPR2024-00212, IPR2024-00213, and IPR2024-00214 are related administrative matters. Paper 6, 1.

B. The ’854 Patent

The ’854 patent generally relates to securing data from unauthorized access or use. Ex. 1001, 1:25–26. The data to be secured is parsed, split, or separated into several parts. *Id.* at 2:47–49. The data is encrypted either before or after the parsing, splitting, or separating. *Id.* at 2:49–52. The encryption step can be repeated. *Id.* at 2:52–54.

In one embodiment, the ’854 patent describes a fault-tolerant scheme for “disaster recovery.” *Id.* at 70:26–39. This scheme allows the original data to be regenerated from less than the total number of data chunks. *See, e.g.,*

id. For example, the data can be divided into four portions and stored in four different locations. *Id.* at 70:33–38. To successfully recreate the original data, the fault-tolerant scheme only needs two of the four portions. *Id.* This is beneficial if the data at two locations is lost or otherwise corrupted. *Id.* Also, the fault-tolerant feature can be used to implement the “two-man rule,” in which two entities need to put their portions together to retrieve the original data. *Id.* at 70:40–47.

C. Claims

Of the challenged claims, only claim 1 is independent.

1. A method for securely storing a data set, the method comprising:

receiving an external key from an external storage system,

generating a plurality of data chunks based on the data set,
such that the data set can be reconstructed using at
least a minimum number of the plurality of data
chunks, wherein generating the data chunks
comprises:

distributing the data set into a plurality of shares,
wherein each of the shares comprises less than all
of the data set,

accessing a plurality of distinct encryption keys,

encrypting each of the shares with a respective one of
the plurality of distinct encryption keys,

performing an encryption operation based on the external
key to further secure the plurality of data chunks;
and

storing with the plurality of data chunks data indicative of
at least one of the distinct encryption keys on a
plurality of different storage devices.

Id. at 83:19–36.

D. Evidence

Name	Reference	Exhibit No.
Orsini	US 2004/0049687 A1, published Mar. 11, 2004	1005
Foster	US 2003/0200176 A1, published Oct. 23, 2003	1006
Hayhurst	US 2004/0216164 A1, published Oct. 28, 2004	1007

E. Asserted Grounds

Petitioner asserts that claims 1–10 would have been unpatentable on the following grounds. Pet. 3.

Claims Challenged	Pre-AIA ¹ 35 U.S.C. §	Reference(s)/Basis
1–10	102	Orsini
1–10	103(a)	Orsini
1–10	103(a)	Foster, Hayhurst

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art “would have had at least a bachelor’s degree in computer science, computer engineering, or a related field, with three years of experience in the area of securing data from unauthorized access or use.” Pet. 6 (citing Ex. 1003² ¶¶ 37–38). Petitioner also asserts that a “higher level of education may substitute for less experience.” *Id.*

Patent Owner does not respond to Petitioner’s assertions or argue for a definition of a person of ordinary skill in the art. *See* Prelim. Resp.

Here, we apply the skill level proposed by Petitioner. Pet. 6.

¹ Petitioner asserts the claims at issue have an effective filing date prior to March 16, 2013, the effective date of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”). Pet. 3. Here, we apply the pre-AIA versions of 35 U.S.C. §§ 102 and 103.

² Exhibit 1003 is the declaration of Samrat Bhattacharjee, Ph.D.

B. Denial for Failure to Comply with 37 C.F.R. § 42.104(b)(e)(3)

Under the Board’s rules, the petition must identify “[h]ow the challenged claim is to be construed.” 37 C.F.R. § 42.104(b)(3). In interpreting the claims here, we use the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2023).

In the related district-court proceeding, the parties have provided different proposed constructions for some terms. *See* Ex. 1064 (Petitioner’s proposed constructions), Ex. 1065 (Patent Owner’s proposed constructions). The Petition states that it presents alternative rationales based on each construction in each pair. *See* Pet. 8.

In Patent Owner’s view, “[t]he Board cannot apply a construction that [Petitioner] does not propose and that [Petitioner] insists is wrong.” Prelim. Resp. 55. That is, Patent Owner argues that in challenging the claims here (specifically, in addressing the limitation “generating a plurality of data chunks based on the data set such that the data set can be reconstructed using at least a minimum number of the plurality of chunks”), Petitioner must either follow its own construction proposed in the district-court proceeding or “acquiesce” to Patent Owner’s construction. *See id.* at 55–57. Because Petitioner does neither, Patent Owner encourages the Board to deny the Petition. *See id.* at 55–56 (citing *Samsung Elecs. v. Uniloc 2017 LLC*, IPR2020-00046, Paper 6 at 10 (PTAB Apr. 1, 2020); *Hologic, Inc. v. Enzo Life Sciences, Inc.*, IPR2018-00019, Paper 21 at 6 (PTAB Nov. 28, 2018)). We disagree.

In *Hologic*, the Board denied the Petition for failing to satisfy Rule 42.104(b)(3) because Petitioner expressly disagreed with all its proffered constructions. *Hologic*, Paper 21 at 6. Patent Owner cites another case in

which the Board came to a similar conclusion. Prelim. Resp. 55 (citing *CareFusion Corp. v. Baxter Int'l, Inc.*, IPR2016-01456, Paper at 7 (PTAB Feb. 6, 2017) (denying institution for failing to provide a sufficient statement of how the challenged claims are to be construed under 37 C.F.R. § 42.104(b)(3) because the petitioner expressly disagreed with the petition's constructions)).

But here, however, Petitioner does not insist any construction is incorrect. Rather, Petitioner merely presents alternative rationales for why the claims are unpatentable, stating that the Petition demonstrates “unpatentability regardless of which proposed construction is correct.” Pet. 8. Even though some stated rationales are based on Patent Owner's district-court construction, the Petition complies with the rule because it explains how the challenged claims are to be construed under the alternative challenges. See 37 C.F.R. § 42.104(b)(3). The rule “does not require Petitioner to express its subjective agreement regarding correctness of its proffered claim constructions or to take ownership of those constructions.” *Western Digital Corp. v. SPEX Techs.*, IPR2018-00084, Paper 14 at 11 (PTAB Apr. 25, 2018).

In *Samsung*, the Board denied the petition because it did not identify the corresponding structure in the means-plus-function terms as required by the rule.³ *Samsung*, Paper 6 at 6–7. The petitioner in *Samsung* expressly noted that the claims could not be properly construed. *Id.* The Board

³ “Where the claim to be construed contains a means-plus-function . . . limitation . . . the construction of the claim *must* identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function.” 37 C.F.R. § 42.104(b)(3) (emphasis added).

explained that the petitioner essentially requested that the Board declare the claims indefinite or “adopt constructions [the petitioner] expressly advocate[d] against.” *Id.* at 8. In denying institution, the Board found that the petition did not comply with 37 C.F.R. § 42.104(b)(3). *See id.* Patent Owner cites another case that came to a similar conclusion. *See* Prelim. Resp. 55 (citing *Toyota Motor Corp. v. Blitzsafe Texas, LLC*, IPR2016-00422, Paper 12 at 27 (PTAB July 6, 2016) (“Petitioner asserts that there is no corresponding structure, material, or acts in the Specification of the ’786 patent, and characterizes the means-plus-function element as indefinite.”)). But, unlike the limitations at issue in *Samsung* and *Toyota*, the limitations here are not in means-plus-function form, and the Petition does not contain an argument that the claims are indefinite.

Thus, we disagree that we should deny the Petition for failure to comply with 37 C.F.R. § 42.104(b)(3).

C. Claim Construction

“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

The Board applies the following constructions based on the record at this stage in the proceeding.

1. Order of Steps

In the related district-court proceeding, the parties disagree about whether the steps of the claims must be performed in the order written: Petitioner argues that the steps must be performed in order. Ex. 1064, 16.

Patent Owner states that it “has not adopted this position.” Prelim. Resp. 60 n.2.

In claim 1, the step of receiving the external key appears before the step of generating the data chunks. *See* Ex. 1001, 83:22–24. Here, the Petition “presents alternative mappings of the prior-art disclosures to both parties’ proposed constructions” from the related district-court proceeding. Pet. 8. For example, Petitioner argues that performing the steps in order would have been a conventional design choice or would have been met by consecutively encrypting multiple data sets. *Id.* at 82.

“As a general rule, unless the steps of a method claim actually recite an order, the steps are not ordinarily construed to require one.” *Mformation Techs., Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398 (Fed. Cir. 2014) (cleaned up). But, as a matter of logic or grammar, the claim language may require the steps be performed in the order written. *See id.* at 1398–99. The specification may also directly or implicitly require an order. *Id.* at 1399.

As for the claim’s logic and grammar here, the chunk-generating steps do not refer to the external key received in the first step. Instead, those steps use the “distinct encryption keys” for encrypting the shares:

generating a plurality of data chunks based on the data set, such that the data set can be reconstructed using at least a minimum number of the plurality of data chunks, wherein generating the data chunks comprises:

distributing the data set into a plurality of shares, wherein each of the shares comprises less than all of the data set,

accessing a plurality of distinct encryption keys,

encrypting each of the shares with a respective one of the plurality of distinct encryption keys,

Ex. 1001, 83:22–31 (emphasis added). The external key received in the first step is used to perform the encryption on the generated data chunks:

performing an encryption operation *based on the external key* to further secure the plurality of data chunks; and

storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.

Id. at 83:32–36 (emphasis added). Because the claim recites that the external key is not used until the encryption operation on the data chunks, the claim’s logic and grammar do not indicate that the external key must be received before generating the data chunks.

Nor do we see any implicit or explicit requirement in the specification. A user or external system can provide the external key for encrypting the data chunks. *Id.* at 77:59–61, 79:15–19. According to one embodiment, the data chunks are encrypted with the external key after the data set has been first encrypted by another key and split into shares. *See id.* at 79:4–19. But the “order of the processes used may depend on the particular application or use,” among other factors. *Id.* at 79:39–45. Also, the specification does not describe a particular “encryption operation” that imposes an order on receiving the key and generating the data chunks. Rather, “any encryption process is suitable for use in the process of the present invention.” *Id.* at 53:56–57. Thus, we determine that the specification does not directly or implicitly require an order between receiving the external key and generating the data chunks.

At this stage and on this record, we construe claim 1 such that the external key can be received before or after the data chunks are generated.

2. “at least a minimum number”

Claim 1 recites, in part, “the data set can be reconstructed using *at least a minimum number* of the plurality of data chunks.” *Id.* at 83:23–24 (emphasis added).

Petitioner presents two alternative rationales for addressing this limitation. *See* Pet. 8, 73. One rationale is based on Petitioner’s proposed construction for a “minimum number of . . . data chunks”: “a predefined number of the lowest amount of the plurality of data chunks.” Ex. 1064, 13; Pet. 73; Prelim. Resp. 48. The other is based on Patent Owner’s proposed construction for that phrase: “a threshold number of chunks less than or equal to the total number of [data] chunks.” Ex. 1065, 9; Pet. 73.⁴ The difference between these two constructions is whether the recited “minimum number” is defined before creating the chunks so that fewer than all chunks can be used to retrieve the dataset. *See* Pet. 73 (giving the example of “90 of 100 data chunks”); Prelim. Resp. 48–49 (discussing redundant data).

At this stage, we disagree that the claims are limited to reconstructing the data set from fewer than all data chunks. This feature is found in the ’854 patent’s fault-tolerant scheme. *See, e.g.*, Ex. 1001, 70:26–39, 75:26–31, 77:52–55, 78:3–6, 78:57–58. The fault-tolerant scheme permits “disaster recovery.” *Id.* at 70:26–39. In the scheme, “out of m portions stored, n may be the minimum number of these m portions necessary to retrieve the original data, where $n \leq m$.” *Id.* For example, the data can be divided into four portions that are stored in different locations, but the system needs only two of the four to successfully recover the original data. *Id.* at 70:33–38.

⁴ In the district-court proceeding, Patent Owner also argues that “minimum number of the plurality of [data] chunks” does not need to be construed. Ex. 1065, 9.

Under this scheme, the data can be recovered even if two of the four portions are destroyed or otherwise compromised. *Id.*

“Any suitable value for n or m may be used.” *Id.* at 70:38–39. In fact, n could be equal to m . *See id.* at 70:26–39. In this case, restoring the original data set requires all shares. *See, e.g., id.* at 62:6–8, 73:49–74–6. The embodiment in Figures 33 and 34, for example, stores four shares and reconstructs the original data using all four. *Id.* at 73:49–74:6, Figs. 33, 34.

Claim 1 does not expressly recite that a fault-tolerant scheme must be used. *Id.* Rather, the claim recites “*at least* a minimum number,” which encompasses quantities larger than some minimum. *See* Ex. 1001, 83:23–24 (emphasis added). Thus, claim 1 covers the embodiments in which all data shares are used to restore the original data, not just the fault-tolerant scheme. *See, e.g., id.* at 70:26–39, 62:6–8, 73:49–74:6, Figs. 33, 34.

One of the Petition’s alternative constructions is based on the fault-tolerant scheme. *See* Pet. 73. In particular, Petitioner’s first alternative construction calls for “a predefined number.” Ex. 1064, 13; Pet. 73. But that term is not found in the claims. Ex. 1001, 83:23–24 (claim 1). According to the ’854 patent, “In *some* embodiments, the data may be split into a predefined number of shares.” *Id.* at 78:35–36 (emphasis added). The ’854 patent mentions the “predefined number of shares” only in connection with the embodiments that use the fault-tolerant scheme. *See, e.g., id.* at 77:50–51 (“split into the predefined number of shares with fault tolerance”), 78:1–2 (same), 78:19–20 (same), 78:25–26 (same), 79:41–42 (same). Because the claim is not limited to the fault-tolerant embodiments for the reasons discussed above, we determine that the claim does not require “a predefined number.”

In sum, we construe “the data set can be reconstructed using at least a minimum number of the plurality of data chunks” to encompass reconstructing the data set from all data chunks, but the claim is not limited to “a predefined number” of data chunks or reconstructing the data set with fewer than all data chunks.

3. “*storage devices*”

Claim 1 recites “storing with the plurality of data chunks data indicative of at least one of the distinct encryption keys on a plurality of different *storage devices*.” Ex. 1001, 83:34–36 (emphasis added).

Patent Owner argues that the recited “storage device” is for long-term storage: “a [person of ordinary skill in the art (POSITA or POSA)] reviewing the ’854 patent would not understand a ‘storage device’ to encompass something like Foster’s receiver (*e.g.*, a set-top box or a DVD player) because the examples of storage devices given in the ’854— ‘magnetic or optical disk, USB key drive, etc.’—are each devices primarily dedicated to long-term storage.” Prelim. Resp. 59.

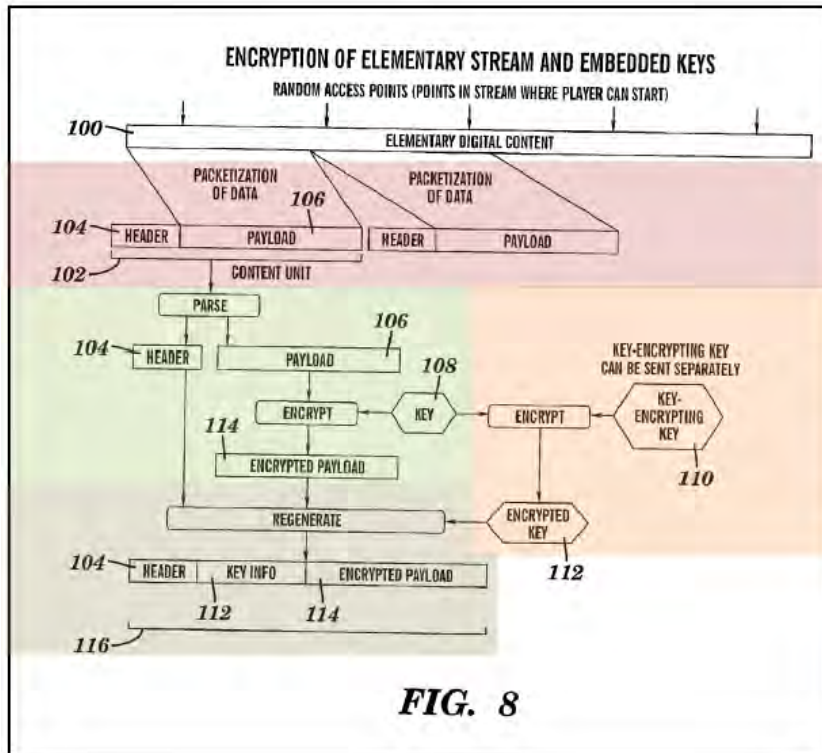
We note that claim 1 does not use the term “long-term.” Even so, we need not resolve whether the claim requires long-term storage at this stage because we disagree with Patent Owner that this feature distinguishes Foster or the system resulting from Petitioner’s proposed combination of Foster and Hayhurst. *See* § II.D.3 *infra*.

D. *Obviousness over Foster and Hayhurst*

Petitioner asserts that claims 1–10 are unpatentable as obvious over Foster and Hayhurst. Pet. 55–89.

1. Foster

Foster's system encrypts streaming content before transmitting it to a recipient. Ex. 1006 ¶ 2. Foster's Figure 8 is reproduced below with Petitioner's annotations. Pet. 56.



(1) Parcel content into pieces

(2) Encrypt pieces with keys

(3) Encrypt keys with KEK

(4) Encrypted pieces and keys for transmission/storage

Petitioner annotates Figure 8 with labels on four different parts of Foster's method: (1) parceling elementary digital content 100 into content units 102 containing header 104 and payload 106, (2) encrypting payload 106 with key 108, (3) encrypting key 108 with key-encrypting key (KEK) 110 to create encrypted key 112, and (4) using encrypted key 112 to regenerate header 104, key info 112, and encrypted payload 114. *Id.*; see also Ex. 1006 ¶ 64.

2. Hayhurst

Hayhurst relates to securely handling and storing electronic media, such as video-on-demand. Ex. 1007 ¶¶ 2, 8. Hayhurst's system segments the media for distribution to subscriber units. *Id.* ¶ 6. When a subscriber unit

requests a media file, another subscriber unit encrypts the file segments that it has and forwards them to the requesting subscriber. *Id.* ¶ 7. A main server then provides an encryption key to the requesting subscriber to unlock the media file. *Id.* According to Hayhurst, this method deters piracy because no single subscriber unit has all segments of the media file. *Id.* ¶ 8. Also, storing the segments on multiple subscriber units provides redundancy when one subscriber unit cannot provide a segment. *Id.* ¶ 9.

3. Claim 1

a. *Receiving the External Key and Generating the Data Chunks*

Claim 1 recites, in part,

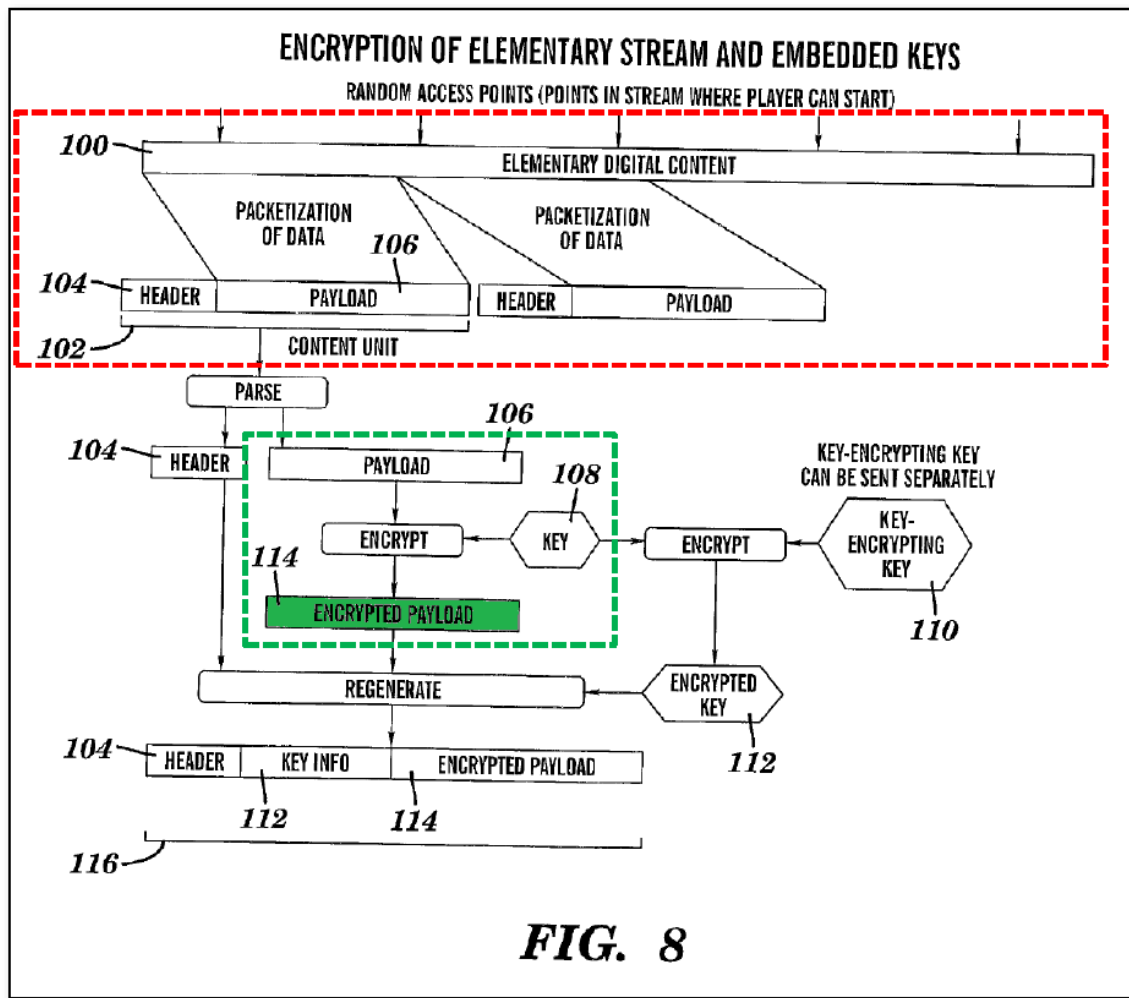
A method for securely storing a data set, the method comprising:
receiving an external key from an external storage system,
generating a plurality of data chunks based on the data set,
....

Ex. 1001, 83:22–24.

As for the receiving step, Petitioner refers to Figure 8 and asserts that Foster’s KEK 110 corresponds to the recited “external key” and database 426 corresponds to the recited “external storage system.” Pet. 68–71 (citing Ex. 1003 ¶¶ 195–200; Ex. 1006 ¶¶ 46, 77–79). Petitioner asserts that Foster teaches “receiving an external key from an external storage system,” as claimed, because “Foster’s computer uses a KEK from database 426’s key-storage system” and database 426 includes storage devices. *Id.* at 69–70 (citing Ex. 1003 ¶¶ 196, 199; Ex. 1006 ¶¶ 46, 77).

As for the data-chunk generating step, Petitioner asserts that Foster’s system generates a “plurality of data chunks based on the data set,” as claimed, because it generates encrypted payloads (the claimed “data chunks”) by encrypting payloads of digital content (the claimed “data set”).

Id. at 72. Petitioner annotates Foster’s Figure 8, below, to illustrate this argument. *Id.*



Petitioner adds a red box around Foster’s data packetization. *Id.* According to the Petition, the elementary digital content stream corresponds to the claimed “data set.” *Id.* at 71 (citing Ex. 1003 ¶¶ 201–202). Elementary digital content 100 is packetized to create content unit 102. Ex. 1006 ¶ 64. Content unit 102 contains header 104 and payload 106. *Id.* After parsing, the system encrypts payload 106 using tile key 108 to create encrypted payload 114. *Id.* Under Petitioner’s mapping, encrypted payload 114 (green) corresponds to the claimed “data chunks.” Pet. 72.

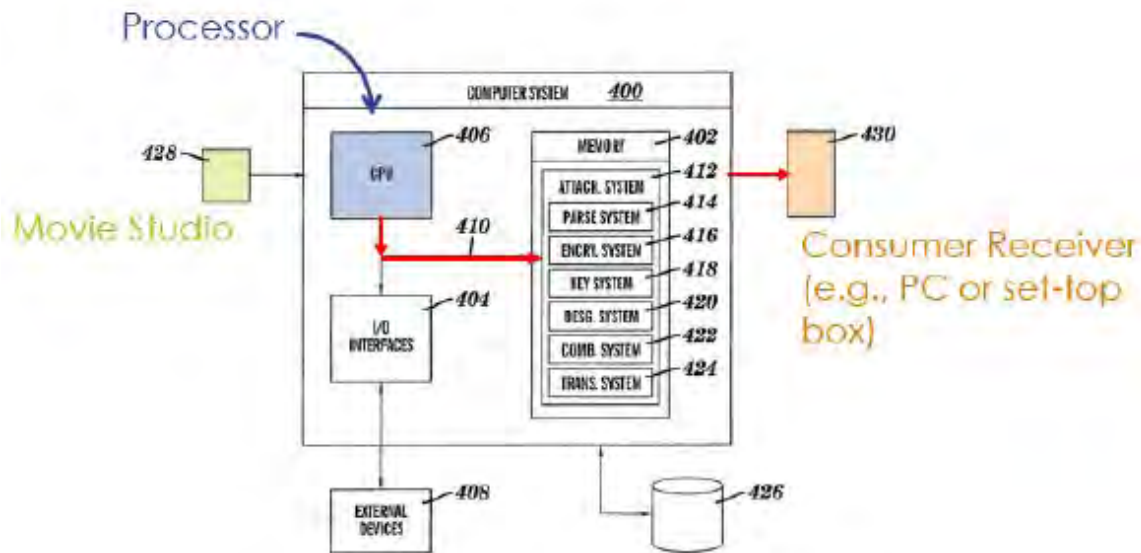
Patent Owner argues that Petitioner has not shown that Foster’s digital content is a “data set,” as claimed. Prelim. Resp. 41. According to Patent Owner, both parties agree that a “data set” must be “for storage.” *Id.* (citing Ex. 2020, 8 n.3; Pet. 65–66). Patent Owner argues that Foster’s definition of “content” does not mention storage: “Content—any data such as digital image, sound or binary data deliverable from a source to a recipient.” *Id.* (quoting Ex. 1006 ¶ 37⁵).

Patent Owner makes a similar argument with respect to the claimed data chunks. *Id.* at 56–60. In particular, claim 1 recites “*storing* with the plurality of data chunks data indicative of at least one of the distinct encryption keys *on a plurality of different storage devices*.” Ex. 1001, 83:34–36 (emphasis added). According to Patent Owner, Foster does not store its data packets on storage devices, as required by this limitation. Prelim. Resp. 57. Patent Owner argues that Foster streams data to a receiver for immediate decoding and playback, not to a “storage device,” which is secure long-term storage. *Id.* In Patent Owner’s view, this is the fundamental difference between Foster and the claimed invention. *Id.* at 38–41, 57 (citing Ex. 2003 ¶¶ 82–84). Patent Owner argues that Foster’s receiver is not a storage device because it is not dedicated to long-term storage. *Id.* at 57–60 (citing Ex. 2003 ¶¶ 108–109).

We disagree that Petitioner has not sufficiently shown, at this stage, that Foster’s digital content is for storage or that its receiver is a storage device. Specifically, Petitioner argues that Foster’s receiver 430 stores the data chunks in its storage device. Pet. 80. Foster’s Figure 16, with the

⁵ Patent Owner quotes this sentence from paragraph 37 but cites paragraph 8.

annotations of Patent Owner's declarant, Aviel D. Rubin, Ph.D., is shown below. Ex. 2003 ¶ 83.



Annotated Figure 16 shows that the content is sent from movie studio 428 to computer system 400 to receiver 430. *Id.*

The record at this stage sufficiently supports Petitioner's argument that Foster's receiver 430 stores content that it receives. Pet. 65 (citing Ex. 1006 ¶¶ 4, 8, Fig. 8). According to Dr. Rubin's annotations, receiver 430 can be a personal computer (PC) or set-top box. Ex. 2003 ¶ 83 (labeling the receiver in Figure 16 as such). This is consistent with Foster. Ex. 1006 ¶¶ 49, 51 (describing PC 18 and a set-top box). Foster describes how the receiver stores encrypted content. *See id.* ¶¶ 8, 79. For example, Foster explains, "Once received, recipient 430 can then synchronously store the encrypted content." *Id.* ¶ 79, *cited in* Pet. 68–69. According to Foster, "The encrypted title key is then attached to the content packet and the header for synchronized transmission to, or *storage by a receiver.*" *Id.* ¶ 8 (emphasis added), *quoted in* Pet. 65. For at least the reason that Foster teaches a PC or

set-top box storing a version of the data set, Petitioner has sufficiently shown at this stage that Foster's data set is "for storage." *See* Pet. 65–66, 80–82.

At this stage, we credit Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 221–222) over Dr. Rubin's (Ex. 2003 ¶¶ 108–109) because it is better supported by the current record. In particular, we see no support for Dr. Rubin's testimony that Foster's receiver cannot provide long-term storage or is unlike the '854 patent's storage devices. *See* Ex. 2003 ¶¶ 108–109. For instance, we see little difference between Foster's PC 18 and the magnetic or optical disk, USB key drive, or other devices that Dr. Rubin claims are long-term storage devices. Ex. 1001, 67:16–19, *cited in* Ex. 2003 ¶¶ 108–109. PC 18 has "data storage." Ex. 1006 ¶ 75. Foster explains "optical media" or "magnetic media" are types of data storage. *Id.* Foster also states that the receiver stores data. *Id.* ¶ 8. In view of these parts of Foster, we credit Dr. Bhattacharjee's testimony that Foster's receiver has data storage (Ex. 1003 ¶¶ 221–222) over Dr. Rubin's testimony that Foster's devices are unlike those described in the '854 patent (Ex. 2003 ¶¶ 108–109), at this stage.

Even so, Petitioner does not rely on Foster alone. *See* Pet. 64, 80. Rather, in the Foster-Hayhurst combination, Foster's receiver performs the functions of Hayhurst's subscriber unit and incorporates its storage device to store the content on multiple devices. *See id.* According to Petitioner's obviousness rationale, Hayhurst's subscriber units store content:

POSAs understood that Foster's content units are individually accessible and agnostic to where and how they are stored compared to other content units, and thus were compatible with being stored on multiple, separate storage devices (like Hayhurst's subscriber storage devices).

Id. at 64–65.

Petitioner argues that there are benefits and advantages to “storing segmented content units on multiple devices in a distributed fashion.” *Id.* at 62. For example, Hayhurst stores the data on the subscriber units to deter piracy—i.e., no single subscriber unit has all the segments for a complete media file. Ex. 1007 ¶ 8. Also, because the segments are stored on multiple subscriber units, Hayhurst teaches that storing the content provides redundancy when one subscriber unit cannot provide a segment. *Id.* ¶ 9. In at least this way, Petitioner has sufficiently shown that content in the Foster-Hayhurst combination is “for storage.” Pet. 64–65.

Also, Patent Owner’s argument about Foster’s immediate decoding versus the ’854 patent’s long-term storage (Prelim. Resp. 38–41, 56–60) does not squarely address Petitioner’s proposal to use Foster’s receivers to store and distribute the content when combined with Hayhurst (Pet. 64–65). That is, Patent Owner’s arguments about storage amount to an individual attack on Foster without considering Petitioner’s reliance on Hayhurst’s teachings about storing content on the individual subscriber units. *See* Prelim. Resp. 38–41, 56–60. As discussed above, we see no difference between the devices used in the Foster-Hayhurst combination, e.g., magnetic or optical disks (Ex. 1006 ¶ 75), and those characterized by Patent Owner as “long term.” *See* Prelim. Resp. 59; Ex. 2003 ¶¶ 108–109 (citing Ex. 1001, 67:16–19). Thus, we disagree with Patent Owner that Petitioner’s combination does not generate a plurality of data chunks based on the data set or store the generated chunks. *See* Prelim. Resp. 38–41, 56–60.

In sum, Petitioner sufficiently shows that the Foster-Hayhurst combination renders obvious the recited data set, the step of “generating a plurality of data chunks based on the data set,” and the step of storing the generated chunks.

b. Order of Steps

As noted previously, in claim 1, the step of receiving the external key appears before the step of generating the data chunks. *See* Ex. 1001, 83:22–24. Petitioner argues that “Foster does not limit when it receives a KEK.” Pet. 82. As shown in Figure 8, Foster uses key 108 to create encrypted payload 114 (the “data chunks”) and encrypts key 108 using KEK 110 (the “external key”) to create the encrypted key 112. Ex. 1006, Fig. 8.

Patent Owner argues that, under Petitioner’s proposed claim construction in district court, the steps must be performed in order. Prelim. Resp. 60 (citing Ex. 1064, 16; Pet. 82). According to the Preliminary Response, “Patent Owner has not adopted this position and reserves the right to take a contrary position in District Court.” *Id.* at 60 n.2.

For the reasons discussed in § II.C.1, we disagree that the step of receiving the external key must be performed before the step of generating the data chunks. At this stage, Petitioner sufficiently shows that the Foster-Hayhurst combination teaches the recited receiving and generating steps for the reasons discussed in § II.D.3.a.

c. Data Chunks

Claim 1 recites, “generating a plurality of *data chunks* based on the data set . . . [and] storing with the plurality of *data chunks* data indicative of at least one of the distinct encryption keys on a plurality of different storage devices.” Ex. 1001, 83:22, 34–36 (emphasis added).

As discussed *supra*, Petitioner asserts that Foster’s encrypted payloads are the claimed “data chunks.” *See* Pet. 71–73. Patent Owner argues that Petitioner has not explained why Foster’s payloads are data chunks. Prelim. Resp. 42 (citing Pet. 72–74; Ex. 3003 ¶87). In Patent Owner’s view, Petitioner’s reasoning is conclusory. *Id.* According to Patent Owner, Foster’s

payloads are not data chunks because they are “payloads of packets that arise as a result of transmission according to the MPEG video compression standard.” *Id.* at 43. Patent Owner argues that packets are parsed into chunks but are not chunks themselves. *Id.* at 43–46. Patent Owner argues that the purpose of generating the data chunks is to secure the data. *Id.* at 46.

Patent Owner mischaracterizes Petitioner’s argument. Petitioner does not identify Foster’s payloads as the claimed data chunks. *See* Prelim. Resp. 42–46. Rather, Petitioner identifies payload 106 as the claimed “shares” and *encrypted* payload 114 as the “data chunks.” *See, e.g.,* Pet. 72 (“[T]he payloads ([1B1]’s ‘shares’) are encrypted to generate encrypted payloads, which are ‘a plurality of data chunks based on the data set,’ as claimed.”), 73 (“POSAs had reason to distribute Foster-Hayhurst’s ‘data set’ into encrypted payloads (‘data chunks’). . . .”) (emphasis in original). The two payloads are not the same: Payload 106 is the result of packetizing the elementary digital content 100, and encrypted payload 114 is generated by encrypting payload 106. *See, e.g.,* Ex. 1006, Fig. 6. Thus, even if the claim requires generating data chunks to secure the data, as Patent Owner argues (Prelim. Resp. 45–46), the record at this stage shows that Foster secures the digital content by generating encrypted payload 114 (Pet. 72–73).

Also, Patent Owner’s argument focuses on Foster individually, and does not address the combination of Foster and Hayhurst. Petitioner relies on the advantages of Hayhurst’s method to further secure the data. *See* Pet. 61–62. For example, Petitioner explains that Hayhurst teaches that one of the benefits of storing media-file segments, such as Foster’s content units, is to provide “a high level of security and a deterrence to piracy.” *Id.* at 62 (quoting Ex. 1007 ¶ 8). According to Hayhurst, the segmented and distributed storage of the content provides security and deterrence because

no one subscriber unit has more than one media segment, and a single segment has little value on its own. Ex. 1007 ¶ 8. Thus, Hayhurst also generates content segments to secure the data. *See id.* Thus, at this stage and on this record, we disagree with Patent Owner’s argument about the data chunks because it does not address Petitioner’s reliance on these teachings from Hayhurst, and amounts to an individual attack on Foster. *See* Prelim. Resp. 42–46.

Patent Owner argues that “Dr. Bhattacharjee’s conclusory testimony should be afforded little or no weight as it is precisely the sort of conclusory testimony rejected in” *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022) (precedential). Prelim. Resp. 42. We disagree that *Xerox* applies here. The testimony in *Xerox* was entitled to little weight because it restated the petition’s unsupported, conclusory assertions without adding supporting evidence or technical reasoning. *See Xerox*, Paper 9 at 15. By contrast, the Petition’s assertions here (Pet. 72–73), as well as Dr. Bhattacharjee’s testimony, are adequately supported by Foster and Hayhurst for all the reasons discussed above.

Patent Owner further argues that Foster’s packets do not correspond to the claimed chunks because Foster does not store them on storage devices. Prelim. Resp. 56–57. As discussed in § II.D.3.a, we disagree with Patent Owner’s argument that Foster does not teach storing the encrypted payloads, and further, find that Patent Owner’s argument is unavailing because it does not address Petitioner’s reliance on Hayhurst in combination with Foster. *See id.*

On this record, Petitioner sufficiently shows that the Foster-Hayhurst combination teaches or suggests generating and storing the data chunks as recited.

d. Reconstructing the Data Set

Claim 1 recites, in part, “the data set can be reconstructed using at least a minimum number of the plurality of data chunks.” Ex. 1001, 83:23–24. Petitioner shows that Foster teaches the claimed data set under Patent Owner’s proposed construction in the district-court proceeding: “a minimum number of the plurality of data chunks” is “a threshold number of chunks less than or equal to the total number of [data] chunks.” See Pet. 73 (citing Ex. 1065, 9).⁶ Under this construction, Petitioner argues that Foster’s system needs all encrypted content packets to access the entire elementary content stream. Pet. 73. Petitioner argues that this teaching follows from Foster’s statement that, “because each content packet can be encrypted with a different title key, a party who illicitly obtains a title key cannot access the entire stream.” *Id.* (quoting Ex. 1006 ¶ 71). According to the Petition, the content packets correspond to the recited data chunks, and accessing the entire stream corresponds to reconstructing the data set, as recited. *Id.*

Patent Owner does not present arguments specific to this rationale. See Prelim. Resp. On this record and at this stage, Petitioner shows that Foster’s elementary content stream (“data set”) can be reconstructed using at least a minimum number of the plurality of content packets (“data chunks”). Pet. 73. We credit Dr. Bhattacharjee’s testimony that Foster uses all encrypted content packets to reconstruct, or access, the original content stream. Ex. 1003 ¶¶ 204–206. This testimony is consistent with Foster’s explanation that the title keys are attached and transmitted with the content

⁶ In the district-court proceeding, Patent Owner alternatively argues that the claim limitation need not be construed. See Ex. 1065, 9.

packets that they encrypt, and the key cannot be used to decrypt the other content packets. Ex. 1006 ¶ 71.

e. Remaining Limitations

Apart from the arguments discussed above, Patent Owner does not present arguments specifically directed to the subject matter recited in the rest of the claim. *See* Prelim. Resp. Even so, Petitioner has the burden to show that the challenged claims are unpatentable. Thus, we have reviewed Petitioner’s arguments and evidence submitted in connection with the remaining limitations and find them to be sufficient at this stage and on this record.

From the current record, Petitioner has established a reasonable likelihood that it will prevail in demonstrating that at least independent claim 1 would have been obvious over Foster and Hayhurst. Because Petitioner has shown a reasonable likelihood of success in showing that claim 1 is unpatentable, we institute on all challenges and all claims challenged in the Petition. *See* 37 C.F.R. § 42.108(a) (“When instituting . . . review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

4. Claims 2–10

Petitioner contends that the subject matter recited in claims 2–10 would have been obvious over the Foster-Hayhurst combination. Pet. 82–89. Apart from the arguments discussed above, Patent Owner does not present arguments specifically directed to claims 2–10. *See* Prelim. Resp. Even so, Petitioner has the burden to show that the challenged claims are unpatentable. We have reviewed Petitioner’s arguments made in connection

with claims 2–10 and find them to be sufficient at this stage of the proceeding and on this record. *See* Pet. 82–89.

E. Anticipation and Obviousness over Orsini

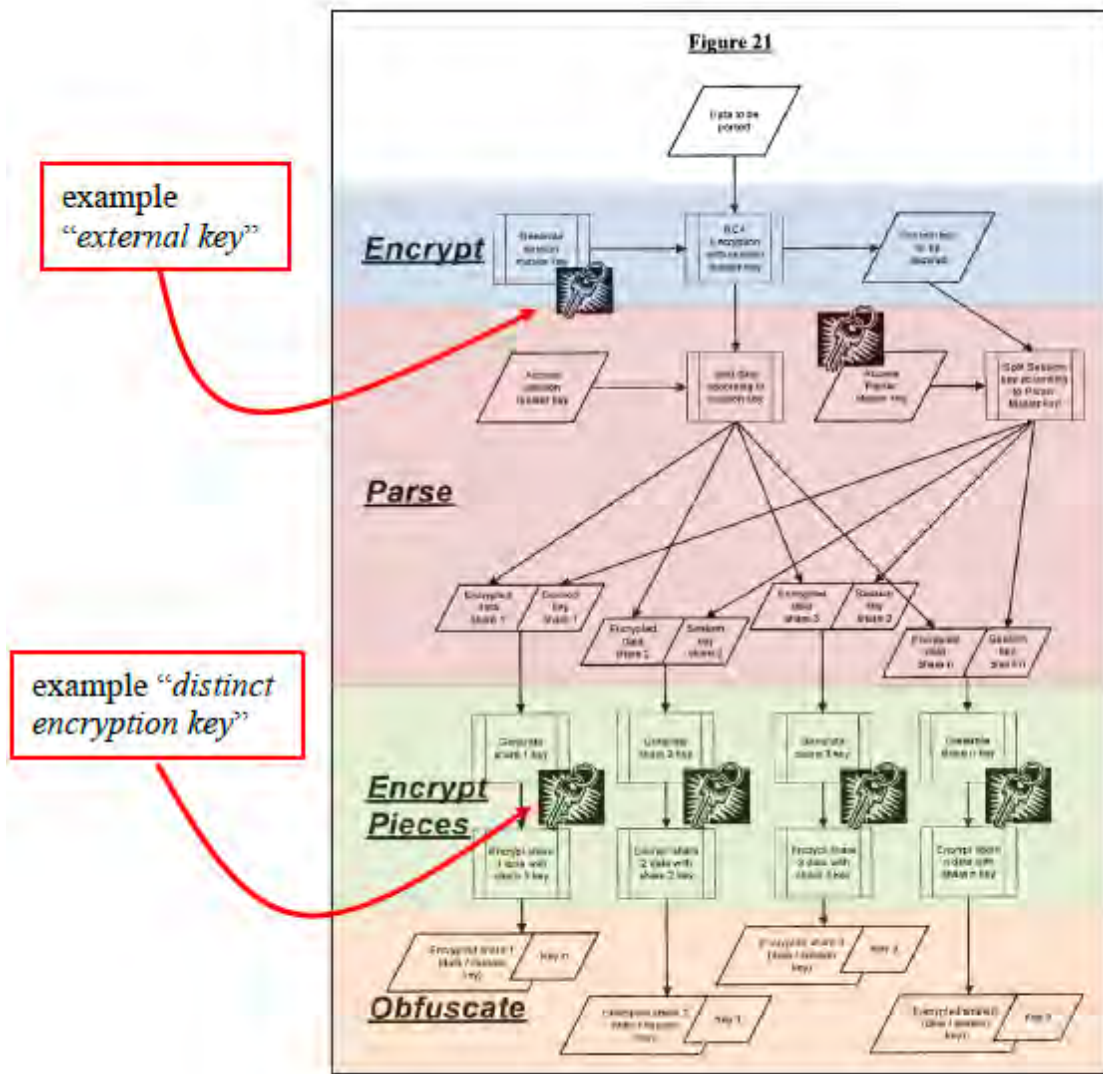
Petitioner asserts that claims 1–10 are unpatentable as anticipated by or obvious over Orsini. Pet. 8–54.

1. Orsini

Orsini and the '854 patent share three named inventors and contain overlapping disclosures and figures. *See id.* at 8 (noting that paragraphs 1–423 and figures 1–25 of Orsini are found in the '854 patent); Prelim. Resp. 1 (same). Like the '854 patent, Orsini is directed to a system for securing sensitive data from unauthorized access and use. Ex. 1005, Abstract.

2. Claim 1

According to Petitioner, “claim 1 performs the same encryption steps illustrated in Orsini’s Figure 21 but does not require (or exclude) encrypting the data set before splitting it into shares.” Pet. 14. Petitioner argues that this encryption step would occur after Orsini’s “encrypt pieces” step, as shown in the figures below. *Id.*



Petitioner argues that Orsini’s Figure 21 has four steps: encrypt, parse, encrypt pieces, and obfuscate. *Id.* at 10. This method uses a session master key and multiple share keys. *Id.* According to Petitioner’s mapping, the session master key corresponds to the claimed external key, and the multiple share keys correspond to distinct encryption keys, as labeled above. *Id.*

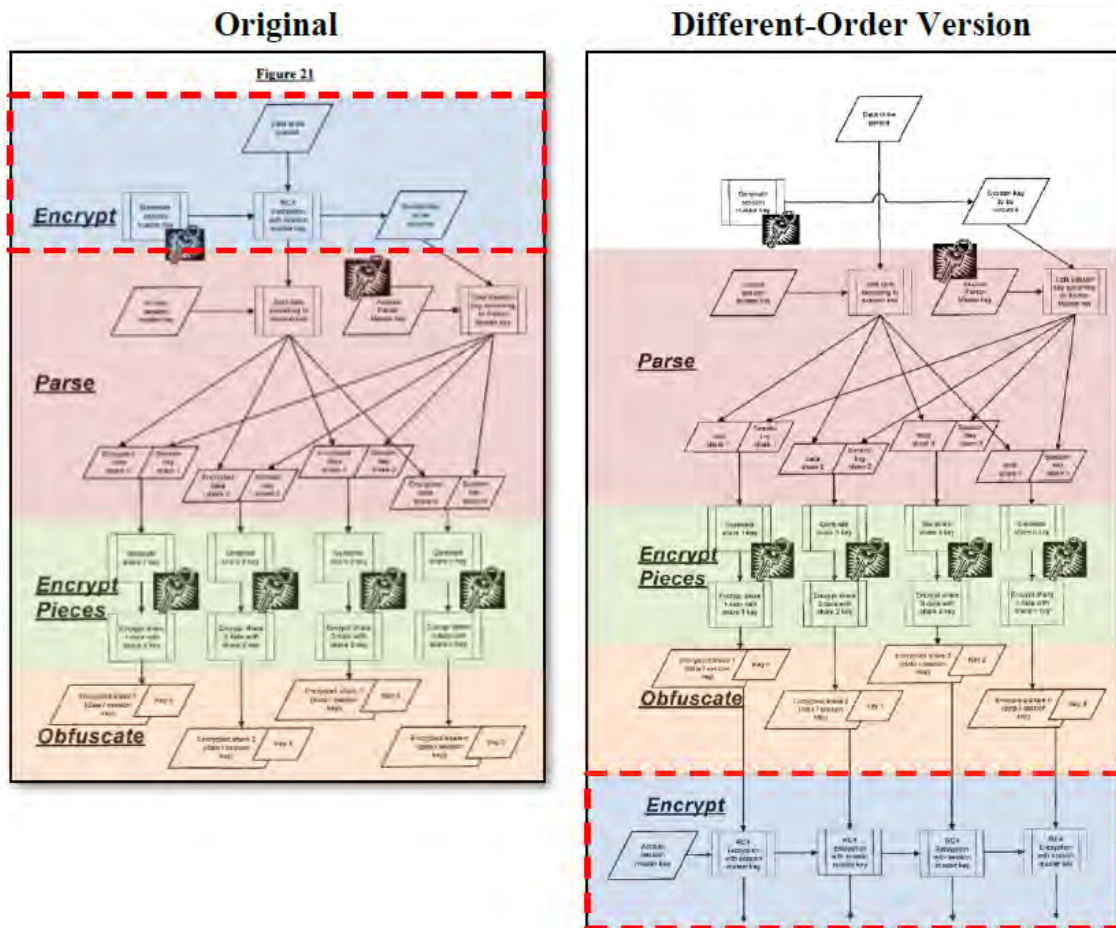
Petitioner gives the label “[1C]” to the claimed step of “performing an encryption operation based on the external key to further secure the plurality of data chunks.” *Id.* at 32. Petitioner argues that Orsini discloses, teaches, or suggests limitation [1C]. *See id.* at 33–48.

a. Anticipation

Petitioner argues that “Orsini discloses ‘that certain steps of the methods described herein may be performed *in different order, or repeated multiple times*, as desired.’” *Id.* at 14 (citing Ex. 1005 ¶ 301) (emphasis in original). Petitioner argues that one “certain step” could be the first encryption step. *Id.* at 33 (citing Ex. 1003 ¶¶ 110–11). Petitioner presents three different rationales: one based on the different order, another based on repeating the steps, and a third based on encrypting with a public key. *Id.* at 14, 36, 38.

i. Different Order

Petitioner illustrates its “different-order Orsini embodiment that meets claim 1” using the figures below. *Id.* at 15.



In the Different-Order Version (right), the second encryption further secures the data chunks using Orsini’s session master key, which Petitioner maps to the claimed “external key.” *Id.* at 34. That is, unlike Orsini’s Original Figure 21 (left), Petitioner’s Different-Order Version lacks an initial encrypt step. *See id.* Instead, there is an encryption step after the obfuscate step. *Id.*

We agree, however, with Patent Owner that Petitioner has not shown that Orsini anticipates claim 1 based on the Different-Order Version. Prelim. Resp. 8–21. “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Here, Petitioner does not identify where Orsini expressly or inherently describes the Different-Order Version. *See* Pet. 33–35. Instead, Petitioner argues that Orsini “teaches” or “suggests” reordering some steps. *Id.* For example, Petitioner argues that Orsini teaches that “certain steps” can be reordered, and Orsini’s parsing processes design “suggests and reinforces” reordering the steps. *See id.* at 14 (citing Ex. 1005 ¶ 301), 33 (citing Ex. 1005 ¶¶ 279, 301). For at least this reason, Petitioner has not shown that Orsini discloses the Different-Order Version. *Id.* at 34.

Even so, the Different-Order Version goes beyond mere reordering. *See id.* Rather, Petitioner’s Different-Order Version changes what is being encrypted compared to Orsini’s Figure 21. *See id.* Specifically, by moving the data set encryption steps from the beginning of Figure 21 to after the obfuscating step, the encrypt step is applied to the individual chunks instead of the entire data set. Prelim. Resp. 12.

Also, we agree with Patent Owner that “[t]hat ‘certain’ steps can be repeated, would not necessarily indicate that the chunks, each encrypted

with a separate share key, would be again encrypted using the session master key (the encryption operation Petitioner contends would be reordered/repeated).” *Id.* at 16. Dr. Rubin explains why reordering the steps in the way that Petitioner proposes would have been pointless:

Indeed, a [person of ordinary skill in the art] would recognize that encryption with the alleged external key would not be an appropriate step to repeat or reorder because it is parsed along with the data set into portions and those portions are then encrypted. Consequently, encrypting the shares with the alleged external key (*i.e.*, the session master key) would render the splitting and encryption of the alleged external key pointless.

Ex. 2003 ¶¶ 52–53. Dr. Bhattacharjee does not fully explain why the key that is parsed and encrypted is then used to further secure the data.

Ex. 1003 ¶¶ 110–111. Thus, we credit Dr. Rubin’s testimony (Ex. 2003 ¶¶ 52–53) over Dr. Bhattacharjee’s (Ex. 1003 ¶¶ 110–111) on this issue. For this additional reason, Petitioner has not shown that Orsini discloses the Different-Order Version. *See* Pet. 33–35.

Thus, we determine that Petitioner has not shown that Orsini discloses limitation [1C] by performing the steps in a different order. *See id.*

ii. Repeated Steps

Petitioner argues that Orsini discloses embodiments in which encrypted data shares (the claimed “data chunks”) are encrypted an additional time using a different algorithm. *Id.* at 36 (citing Ex. 1003 ¶ 115). Petitioner argues that Orsini’s dependent claims recite using “a different encryption algorithm.” *Id.* (citing Ex. 1005, claims 12, 29, 39). According to Petitioner, Orsini’s claimed embodiment that uses a “different encryption algorithm” performs encryption with the external key:

One different algorithm performed after encrypting the ‘shares’ (thus, after generating ‘data chunks’) that would have been

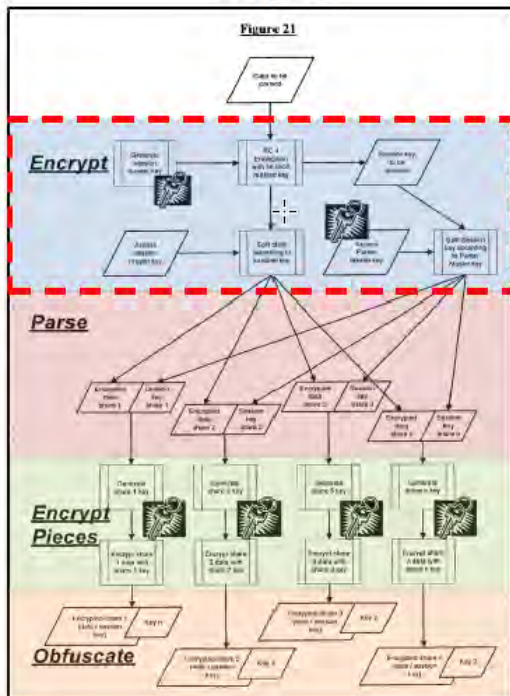
obvious to [skilled artisans] includes using a single encryption key to further encrypt all data chunks with that key, similar to using the session master key to encrypt the entire data set originally before splitting it.

Id. (emphases in original).

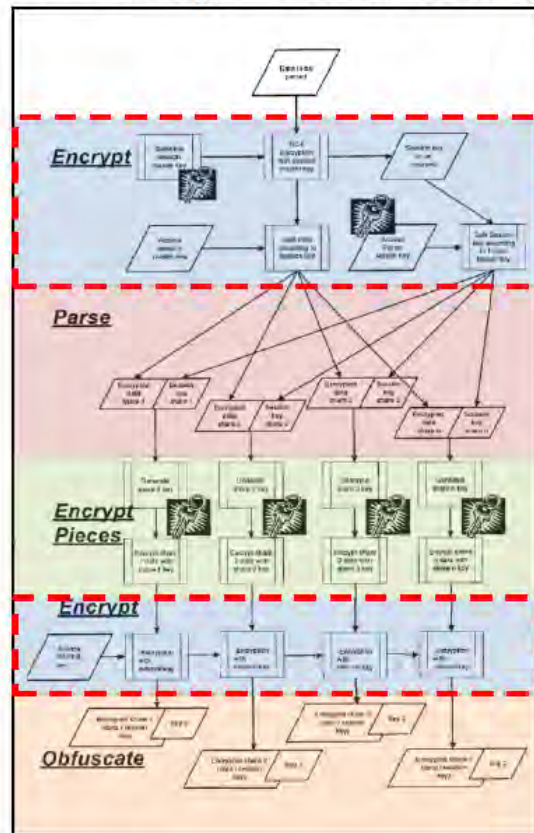
That is, on this record, the only support for Petitioner's conclusions is Orsini's statement that "the methods described herein may be . . . repeated multiple times" (Ex. 1005 ¶ 301), Orsini's claims reciting "a different encryption algorithm" (*see id.*, claims 12, 29, 39), and Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 115–116). Petitioner does not identify anything from Orsini that explains how the algorithms are different. *See* Pet. 35–38. Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 115–116) is entitled to little weight on this issue because Dr. Bhattacharjee merely repeats the Petition's conclusory assertions without adding supporting evidence or technical reasoning. *See Xerox*, Paper 9 at 15. For at least this reason, we agree with Patent Owner that Petitioner does not sufficiently support its reasoning about repeating Orsini's steps. *See* Prelim. Resp. 17–18.

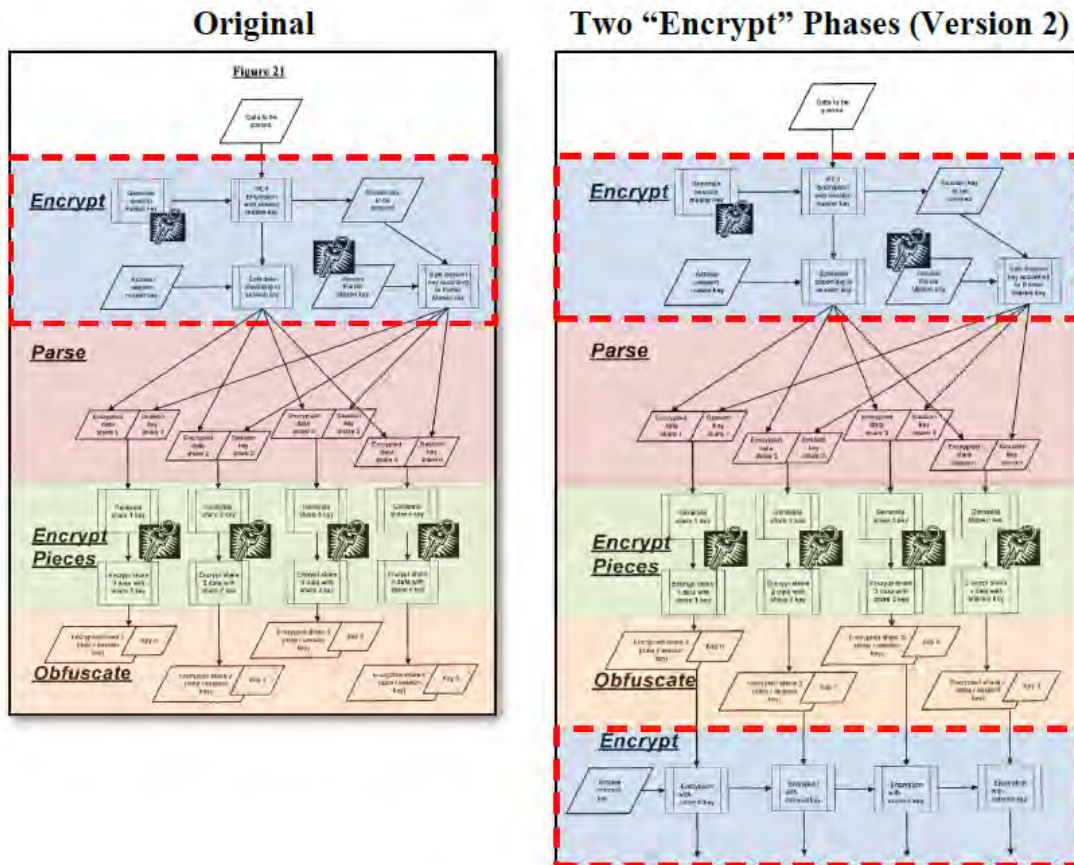
Apart from that issue, the Petition's Two-Encrypt-Phases rationale is deficient for reasons similar to those for the Different-Order rationale: Petitioner does not sufficiently explain or support its arguments about Orsini's session master key and common key. *See* § II.E.2.a.i *supra*. Two versions of Petitioner's Two Encrypt Phases are shown below. Pet. 37–38.

Original



Two "Encrypt" Phases (Version 1)





In either version, Orsini’s method would have an additional encryption step. *See id.* That is, Version 1 would “(1) encrypt the original data set with a session master key, (2) split the data into shares, (3) encrypt the data shares with distinct share keys, (4) encrypt each encrypted share (the ‘data chunk’) with a common key,^[7] and (5) obfuscate the encrypted shares.” *Id.* at 36. Version 2 obfuscates before it encrypts. *Id.*

According to Petitioner, the common key used in step (4) “would have been, or had reason to be, an ‘external key,’” as recited in claim 1. *Id.* As noted above, the additional encryption uses an algorithm that is somehow

⁷ According to Orsini, the sender and receiver of a message share a single common key that is used to encrypt and decrypt a message. Ex. 1005 ¶ 168.

different, according to Petitioner. *Id.* Thus, Petitioner argues that its Two Encrypt Phases discloses limitation [1C]. *See id.*

The claim recites “performing an encryption operation *based on the external key* to further secure the plurality of data chunks.” Ex. 1001, 83:32–33. Yet Orsini divides the session master key into pieces that are integrated into the shares before it encrypts the pieces. Ex. 1005, Fig. 21. Dr. Rubin testifies that, if the same session master key were used again in a repeated encryption step, these steps would be rendered pointless. Ex. 2003 ¶¶ 52–53. Petitioner does not adequately explain how the “different algorithm” would manage the session master key in the Two-Encrypt-Phases rationale. *See* Pet. 35–40. And the cited parts of Orsini—the claims and a few statements—provide little guidance on how the different encryption algorithm works. Ex. 1005 ¶ 301, claims 12, 29, 39; Pet. 35. For at least this reason, Petitioner has not shown that Orsini anticipates the claim by repeating encryption steps. *See* Pet. 35–38.

Also, even if Orsini repeats the method, both versions of Petitioner’s Two Encrypt Phases go beyond mere repetition. *See id.* For example, Patent Owner points out that if the session master key were somehow used in an encryption operation to “further secure” the chunks, then “[t]his would require complex changes to Figure 21’s method due to the need for external key management and would further remove the benefits of securely storing and transporting the session master key within the encrypted shares.” Prelim. Resp. 6–7 (Ex. 2003 ¶ 42). Dr. Rubin explains that “by the time the dataset is to be ‘further secured’ as required by claim 1, the session master key in Orsini is buried within encrypted shares, and any further use of it would entirely undermine the prior steps in Orsini’s method.” Ex. 2003 ¶ 42. We credit Dr. Rubin’s testimony (Ex. 2003 ¶ 42) over Dr. Bhattacharjee’s

(Ex. 1003 ¶¶ 114–116) because it is better supported by Orsini’s Figure 21. For this additional reason, Petitioner has not shown that Orsini anticipates claim 1 under its Two-Encrypt-Phases rationale. *See* Pet. 35–38.

iii. Encrypting with a Public Key

Petitioner argues that Orsini’s public encryption keys are “external keys.” *Id.* at 38. According to Petitioner, Orsini discloses encrypting data with the session key and encrypting that session key with the user’s public key. *Id.* at 39 (quoting Ex. 1005 ¶ 172). According to Petitioner, Orsini’s session key can be the session master key, and encrypting the session master key with a public key meets limitation [1C]. *Id.*

As Patent Owner points out, the public key is not shown in Figure 21. Prelim. Resp. 19–20. Rather, Petitioner combines the features from multiple embodiments to arrive at the claimed invention. *See* Pet. 38–39. Yet “it is not enough that the prior art reference discloses part of the claimed invention, which an ordinary artisan might supplement to make the whole, or that it includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention.” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). “[D]ifferences between the prior art reference and a claimed invention, however slight, invoke the question of obviousness, not anticipation.” *Id.* Thus, Petitioner has not shown that Orsini anticipates claim 1 under its public-key rationale. *See* Pet. 38–39.

b. Obviousness

Petitioner argues that the skilled artisan “had multiple reasons to implement Orsini to perform [1C] in view of POSAs’ background knowledge.” Pet. 39. Petitioner presents four alternative obviousness rationales. *Id.* at 39–48. Petitioner argues that a person of ordinary skill in the art had reason to (1) re-encrypt the data chunks with an external key,

(2) re-encrypt data chunks with an externally-received group key, (3) reorder data within each chunk based on an external key, or (4) encrypt distinct encryption keys with an externally stored KEK. *Id.*

i. Re-encrypting with External Key

Petitioner argues that a person of ordinary skill in the art “would have been motivated to reorder and/or repeat certain specific steps by encrypting already-encrypted data chunks with the same encryption key, and would have understood that doing so would provide additional security and efficiency benefits.” *Id.* at 40. According to Petitioner, “Re-encrypting data chunks with a common external encryption key was also a known solution to the known problem of how to further secure data using encryption, and thus was obvious.” *Id.*

Here, Petitioner’s rationale is deficient for all the reasons discussed above in §§ II.E.2.a.i and ii. Petitioner’s additional reasoning that the proposed modification would “provide additional security and efficiency benefits” is unsupported and conclusory. *Id.* Providing additional security is recited in the claim limitation itself: “performing an encryption operation based on the external key *to further secure* the plurality of data chunks.” Ex. 1001, 83:32–33 (emphasis added). In this way, Petitioner’s obviousness rationale is circular and does nothing more than restate the claim language. Pet. 39–40 (citing Ex. 1003 ¶¶ 120–22). Also, Petitioner does not explain why repeating or reordering steps would be efficient. *Id.* And, for the reasons discussed in §§ II.E.2.a.i and ii, we disagree that reordering and repeating Orsini’s steps in the way that Petitioner describes was a “known solution.” *Id.* at 40.

The Bhattacharjee Declaration largely repeats the Petition’s conclusory assertions, adding scant supporting evidence and technical

reasoning. *See* Ex. 1003 ¶¶ 121–123, *cited in* Pet. 39–40. According to Dr. Bhattacharjee, a person of ordinary skill in the art “would have understood that encrypting multiple smaller chunks of data with the same encryption key would have been computationally easier than encrypting the single larger data set before splitting it into shares.” *Id.* ¶ 121. But Dr. Bhattacharjee provides no supporting citations or additional technical reasoning for this statement. *See id.* According to Dr. Bhattacharjee, “This further encryption step would have also provided greater security by re-encrypting the data chunks a second time.” *Id.* As with the statement in the Petition, saying the purpose of further encryption is to provide “greater security” adds little to the obviousness rationale because it merely restates the claimed feature itself. *See* Ex. 1001, 83:32–33. Thus, we do not credit Dr. Bhattacharjee’s testimony (Ex. 1003 ¶¶ 121–123) on this issue.

In sum, on the current record, we agree with Patent Owner that Petitioner’s reason to modify Orsini is based on impermissible hindsight. Prelim. Resp. 37. Thus, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale based on re-encrypting the data chunks with an external key. Pet. 39–40.

ii. *Re-encrypting with Externally Received Group Key*

Petitioner argues that a person of ordinary skill in the art had reason to re-encrypt data chunks with an externally received *group* key. Pet. 40. In this rationale, Petitioner relies upon Orsini’s embodiments “in which ‘access to secured data can be limited to just those who are permitted or required to have access only to the portion they are working on, while others, such as managers or executives, may have access to all of the secured data.’” *Id.* (quoting Ex. 1005 ¶ 412). According to Petitioner, the conventional implementation of these embodiments uses a group-level encryption key,

citing several other references. *Id.* at 41 (citing Ex. 1003 ¶ 124; Ex. 1018, 5:19–35; Ex. 1029, 6:55–8:57; Ex. 1033, 8:31–41; Ex. 1034 ¶ 33).

Petitioner claims that it would have been “obvious to use known technique[s] to improve similar devices.” *Id.* (citing *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007)). Petitioner, though, provides no explanation why the additional cited references were “similar.” *Id.* Nor does Petitioner explain how the cited prior art would have been used to modify Orsini. *Id.* Thus, it is not apparent how Petitioner intends to rely on these references in its challenge. *Id.* Generally, the challenge based on re-encrypting with a group key (*id.*) lacks an articulated rationale. “Absent some articulated rationale, a finding that a combination of prior art would have been ‘common sense’ or ‘intuitive’ is no different than merely stating the combination ‘would have been obvious.’” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). On this record, we agree with Patent Owner that Petitioner’s reason to modify Orsini by re-encrypting the external group key is entirely based on impermissible hindsight. Prelim. Resp. 37.

Thus, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale based on re-encrypting data chunks with an externally received group key. Pet. 40.

iii. Reordering Data

Petitioner argues that a person of ordinary skill in the art “had reason to add additional security to Orsini’s encrypted shares (‘data chunks’) by cryptographically reordering/shuffling the data within each ‘data chunk.’” Pet. 41. Petitioner claims that this is a “conventional cryptographic operation to secure the data,” expressly taught by Orsini, or rendered obvious by

Orsini. *Id.* at 41–42 (citing Ex. 1003 ¶¶ 126–27; Ex. 1005 ¶ 281; Ex. 1030 ¶ 2).

For the reasons discussed in § II.E.2.a.i, we disagree with Petitioner’s assertion that Orsini’s statement about performing steps in a different order means that Orsini discloses the method of claim 1. *See id.* at 42 (citing Ex. 1003 ¶ 126).

As for whether this reordering would have been obvious, the Petition lacks an articulated rationale. *See id.* at 41–42. So Petitioner’s obviousness rationale is deficient for the same reasons discussed in § II.E.2.b.ii. For example, Petitioner states that a person of ordinary skill would have understood the benefits of reordering but fails to identify or analyze any specific benefit. *Id.* On this record, we agree with Patent Owner that Petitioner’s reason to modify Orsini to cryptographically reorder or shuffle the data is entirely based on impermissible hindsight. Prelim. Resp. 37.

Thus, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale about cryptographically reordering or shuffling the data. Pet. 41–42.

iv. *Encrypting the Distinct Encryption Keys with Externally-Stored KEK*

Petitioner argues that a person of ordinary skill in the art had reason to encrypt the distinct encryption keys with an externally stored KEK. Pet. 43–45.

Petitioner argues that Orsini discloses or renders obvious encrypting session keys with a public-key encryption key. *Id.* at 43. For the reasons discussed in § II.E.2.a.iii, Petitioner’s arguments about the public-key encryption key are deficient. In particular, Orsini does not show a public key in Figure 21. *See* Prelim. Resp. 19–20. Petitioner’s argument about the public-key encryption key is based on the features from multiple

embodiments. *See* Pet. 38–39. Yet Petitioner does not provide a sufficient rationale for combining these multiple embodiments. *See id.*

Petitioner’s analysis in § VI.B.b.iv of the Petition does not remedy the deficiencies in Petitioner’s analysis of the public-key encryption key. *See* § II.E.2.a.iii *supra*. Rather, the reasoning in § VI.B.b.iv depends on the Petition’s analysis about Orsini disclosing or rendering obvious encrypting session keys with a public-key encryption key. *See* Pet. 43 (citing Ex. 1005 ¶ 172). Thus, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale about encrypting the distinct encryption keys with an externally stored KEK. *See* § II.E.2.a.iii *supra*.

3. Conclusion

For all the reasons discussed above, Petitioner has not shown a reasonable likelihood of prevailing as to the unpatentability of claim 1 under its challenge based on Orsini.

Claims 2–10 depend from claim 1. At this stage and on this record, we determine that Petitioner’s analysis for claims 2–10 does not remedy the deficiencies with respect to claim 1. *See* Pet. 48–54. Thus, for the same reasons discussed in connection with the challenge to claim 1, Petitioner has not shown a reasonable likelihood of prevailing as to the unpatentability of claims 2–10 under its challenge based on Orsini.

III. CONCLUSION

Petitioner has shown a reasonable likelihood of prevailing as to the unpatentability of at least one of the challenged claims under its challenge based on the Foster-Hayhurst combination. Thus, we institute an *inter partes* review on all claims challenged in the Petition and on all grounds in the petition.

IV. ORDER

It is

ORDERED that, under 35 U.S.C. § 314(a), an *inter partes* review of claims 1–10 of the '854 patent is instituted for all grounds in the Petition; and

FURTHER ORDERED that, under 35 U.S.C. § 314(a), *inter partes* review of the '854 patent is instituted on this Decision's entry date, and under 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is given of the trial's institution.

FOR PETITIONER:

Elisabeth H. Hunt
Gregory S. Nieberg
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
gnieberg-ptab@wolfgreenfield.com

FOR PATENT OWNER:

Stephen J. Elliott
Andrei Iancu
SULLIVAN & CROMWELL LLP
elliotts@sullcrom.com
iancua@sullcrom.com

Kenneth Weatherwax
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com