

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00214
Patent 11,068,609 B2

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

BELISLE, *Administrative Patent Judge*.

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

I. INTRODUCTION

Google LLC (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting an *inter partes* review of claims 1–10 (“Challenged Claims”) of U.S. Patent No. 11,068,609 B2 (Ex. 1001, “the ’609 patent”). Security First Innovations, LLC (“Patent Owner”) filed a Preliminary Response. Paper 10 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b) (2018); 37 C.F.R. § 42.4(a) (2023). We may not institute an *inter partes* review “unless . . . 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). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential). When instituting *inter partes* 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. 37 C.F.R. § 42.108(a).

Applying those standards, and upon consideration of the information presented in the Petition and Preliminary Response, we determine that Petitioner has demonstrated a reasonable likelihood of success in proving that at least one claim of the ’609 patent is unpatentable. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a). Accordingly, we institute an *inter partes* review as to all Challenged Claims of the ’609 patent on all grounds raised in the Petition.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner and Patent Owner each identify itself as a real party in interest. Pet. ix; Paper 4, 1. Petitioner also states: “Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.” Pet. ix n.1.

B. *Related Matters*

According to the parties, the ’609 patent has been asserted in *Security First Innovations, LLC v. Google LLC*, No. 2:23-cv-00097 (E.D. Va.) (Norfolk Division) (transferred from Alexandria Division, 1:23-cv-00329) (“District Court Case”). Pet. x; Paper 4, 1; Paper 7, 1.

The parties also indicate that IPR2024-00212 (U.S. Patent No. 11,178,116), IPR2024-00213 (U.S. Patent No. 9,338,140); and IPR2024-00215 (U.S. Patent No. 10,452,854) are related administrative matters. Paper 7, 1; Paper 4, 1. Petitioner advises the Board that, on January 22, 2024, the Eastern District of Virginia entered an Order (ECF No. 313) staying the District Court Case pending resolution of this case and the above-listed *inter partes* reviews. Paper 7, 1.

Petitioner also identifies all of the related applications listed on the face of the ’609 patent as related matters, along with U.S. Patent Application No. 17/347,268, filed June 14, 2021. Pet. ix–x; see Ex. 1001, codes (60), (63).

C. *The ’609 Patent*

The ’609 patent is titled “Secure Data Parser Method and System,” and issued on July 20, 2021, from U.S. Application No. 16/658,506, filed

October 21, 2019. Ex. 1001, codes (10), (21), (22), (45), (54). The '609 patent claims priority through a series of continuation applications to U.S. Provisional Application No. 60/738,231, filed November 18, 2005. Ex. 1001, codes (60), (63). We note that the immediate parent of the '609 patent, namely Application No. 16/127,077, filed September 10, 2018, now U.S. Patent No. 10,452,854 B2, is the subject of IPR2024-00215, in which the Board has instituted *inter partes* review.

The '609 patent relates generally to securing data from unauthorized access or use. Ex. 1001, 1:26–27. The data to be secured is parsed, split, or separated into two or more parts or portions. *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 may be repeated for one or more portions of the data. *Id.* at 2:52–54.

In one embodiment, the '609 patent describes a fault-tolerant scheme for “disaster recovery.” Ex. 1001, 70:12–25. This scheme allows the original data to be regenerated from “fewer than all portions of the separated data generated by the secure data parser.” *Id.* at 70:14–16. For example, the data may be divided into four portions and stored in four different locations. *Id.* at 70:20–22. To successfully recreate the original data, the fault-tolerant scheme may only need two of the four portions. *Id.* at 70:20–26. This is beneficial if the data at two locations is corrupted, lost, or otherwise compromised. *Id.* Also, the fault-tolerant feature may 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 70:27–34.

D. Illustrative Claim

The '609 patent includes 10 claims, all of which are challenged.¹ Claim 1 is the sole independent claim, and is reproduced below with labels, such as “[1A],” added to limitations in the same manner as used by the parties.

1. [PRE] A method for securing data, the method comprising:
[1A] executing code by a processor to perform:
[1B] receiving a first key from a storage system;
[1C1] generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and [1C2] wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks;
[1D] encrypting each respective data chunk of the plurality of data chunks with a respective second key, wherein each of the respective second keys are distinct from each other;
[1E] performing a cryptographic operation based on the first key to further secure the plurality of data chunks; and
[1F] storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device.

Ex. 1001, 83:12–30.

¹ A Certificate of Correction issued on November 22, 2022, concerning dependent claims 6–10 of the '609 patent. Ex. 1002, 11–16. In particular, the Certificate replaced the term “external” key in each of claims 6–10 with the term “first” key as recited in independent claim 1 (limitation [1B]). *Id.*

E. Evidence of Record

Petitioner relies on the following published patent application evidence.

Name	Patent Document	Exhibit
Orsini	U.S. Patent Appl. Pub. No. 2004/0049687 A1, published March 11, 2004	1005
Foster	U.S. Patent Appl. Pub. No. 2003/0200176 A1, published October 23, 2003	1006

Pet. 3.

Petitioner also relies upon the Declaration of Samrat Bhattacharjee, Ph.D. (Ex. 1003).

Patent Owner relies upon the Declaration of Aviel D. Rubin, Ph.D. (Ex. 2003).

F. Asserted Challenges to Patentability

Petitioner challenges the patentability of claims 1–10 of the '609 patent on the following bases. Pet. 3.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–10	102 ²	Orsini
1–10	103	Orsini
1–3, 7, 8	102	Foster
1–10	103	Foster

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the '609 patent was filed before March 16, 2013, the effective date of the relevant amendment, the pre-AIA versions of §§ 102/103 apply.

III. PATENTABILITY

A. *Applicable Law*

Petitioner challenges the patentability of claims 1–10 of the '609 patent on grounds that the claims are anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 in light of two separate references, namely Orsini and Foster. “In an [*inter partes* review], the petitioner has the burden from the onset to show *with particularity* why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)) (emphasis added). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

1. *Anticipation*

To serve as an anticipatory reference under 35 U.S.C. § 102, “the reference must disclose each and every element of the claimed invention, whether it does so explicitly or inherently.” *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009). “The identical invention must be shown in as complete detail *as is contained in the . . . claim.*” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989) (emphasis added). The elements must be arranged as required by the claim, “but this is not an ‘*ipsissimis verbis*’ test,” i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 832–33 (Fed. Cir. 1990) (citing *Akzo N.V. v. United States Int’l Trade Comm’n*, 808 F.2d 1471, 1479 & n.11 (Fed. Cir. 1986)).

2. Obviousness

A claim is unpatentable under 35 U.S.C. § 103 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.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when of record, objective evidence of obviousness or non-obviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Secondary considerations may include the following: “commercial success, long felt but unsolved needs, failure of others, etc.”³ *Id.* The totality of the evidence submitted may show that the challenged claims would not have been obvious to one of ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The Supreme Court has made clear that we apply “an expansive and flexible approach” to the question of obviousness. *Id.* at 415. Whether a patent claiming a combination of prior art elements would have been obvious is determined by whether the improvement is more than the

³ At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

predictable use of prior art elements according to their established functions. *Id.* at 417. To reach this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.* “To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

B. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art, at the time of the invention of the ’609 patent, “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,” and that “[a] higher level of education may substitute for less experience.” Pet. 5 (citing Ex. 1003 ¶¶ 37–38).

Patent Owner does not present an alternative definition at this stage of the proceeding. *See generally* Prelim. Resp.

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art;

prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citation omitted). The level of ordinary skill in the art also may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Neither party argues, at least at this stage of the proceeding, that the outcome of this case would differ based on our adoption of any particular definition of the level of ordinary skill in the art. Considering the subject matter of the ’609 patent, the background technical field, the prior art, and Petitioner’s proposed and unopposed definition of the skilled artisan, we apply the level of skill set forth above, which is consistent with the testimony of Dr. Bhattacharjee (Ex. 1003 ¶¶ 37–38).

C. Claim Construction

We construe claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips*, 415 F.3d at 1312–13; *see CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (There is “a ‘heavy presumption’ that a claim term carries its ordinary

and customary meaning.”). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317.

Only those claim terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (stating that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

1. *Compliance 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 the related District Court Case, the parties proffered 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 mappings” of asserted prior art based on each construction in each pair. Pet. 8–9.

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. 53. Patent Owner argues that in challenging the claims here

(specifically, in addressing the limitation “generating a plurality of data chunks based on a data set . . . wherein 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 Case or “acquiesce” to Patent Owner’s construction. *See id.* at 53–54. Because Petitioner does neither, Patent Owner encourages the Board to deny the Petition. *See id.* (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 of its proffered constructions. *Hologic*, Paper 21 at 6. Patent Owner cites another case in which the Board came to a similar conclusion. Prelim. Resp. 53 (citing *CareFusion Corp. v. Baxter Int’l, Inc.*, IPR2016-01456, Paper 9 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)).

Here, however, Petitioner does not insist any construction is incorrect. Rather, Petitioner presents *alternative rationales* for why the claims are unpatentable, stating that the Petition demonstrates “unpatentability regardless of which proposed construction is correct.” Pet. 9. Even though some stated rationales are based on Patent Owner’s constructions in the District Court Case, 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., Inc.*, 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.⁴ *Samsung*, Paper 6 at 6–7. Petitioner expressly noted that the claims could not be properly construed. *Id.* The Board explained that Petitioner essentially requested the Board to 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. 53 (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.

⁴ “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).

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

2. *Order of Steps*

In the District Court Case, the parties disagree about whether the steps of the claims, particularly in independent claim 1, must be performed in the order written: Petitioner argues that the steps must be performed in order. Pet. 78 (citing Ex. 1064, 16). Patent Owner states that it “has not adopted this position.” Prelim. Resp. 62 n.2.

In claim 1, the step of “receiving a first key” appears before the step of “generating a plurality of data chunks,” which itself appears before the step of “performing a cryptographic operation based on the first key to further secure the plurality of data chunks.” Ex. 1001, 83:14–26. “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 first key received in the first step. Instead, those steps recite the “distinct” “second [encryption] keys” for encrypting the shares:

generating a plurality of data chunks based on a data set, wherein each data chunk of the plurality of data chunks comprises less than an entirety of data of the data set, and wherein the data set can be reconstructed using at least a minimum number of the plurality of chunks;

encrypting each respective data chunk of the plurality of data chunks with a *respective second key*, wherein each of the respective *second keys are distinct from each other*;

Ex. 1001, 83:15–24 (emphases added). The first key received in the first step is used to perform the encryption on the generated data chunks:

performing a cryptographic operation *based on the first key* to further secure the plurality of data chunks; and

storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one storage device

Id. at 83:25–30 (emphasis added). Because the claim recites that the first key is not used until the encryption operation on the data chunks, the claim’s logic and grammar do not indicate that the first 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 may provide an “external key” (the claimed “first key”) for encrypting the data chunks. Ex. 1001, 77:51–53, 79:8–12. In one embodiment, the data chunks are encrypted with the first key after the data set has been first encrypted by another key and split into shares. *See id.* at 78:59–79:12. But the “order of processes used may depend on the particular application or use,” among other factors. *Id.* at 79:33–39. 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 53:50–51. Thus, we determine that the Specification does not directly or implicitly require an order between receiving the first key and generating the data chunks.

At this stage of the proceeding and based on the record before us, we construe claim 1 such that the first key may be received before or after the data chunks are generated.

3. *Limitation [1C2]: “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 chunks.” Ex. 1001, 83:18–20 (emphasis added).

Petitioner proffers two alternative rationales for addressing this limitation. See Pet. 9, 67–68. One rationale is based on Petitioner’s proposed construction for a “minimum number of . . . chunks”: “a predefined number of the lowest amount of the plurality of data chunks.” Ex. 1064, 13; Pet. 67–68; Prelim. Resp. 45. The other rationale 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. 67.⁵ 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. 67 (giving the example of “90 of 100 data chunks”); Prelim. Resp. 46–47 (discussing “redundant data”).

At this stage of the proceeding, we disagree that the claims are limited to reconstructing the data set from fewer than all data chunks. This feature is found in the ’609 patent’s fault-tolerant scheme. See, e.g., Ex. 1001, 70:12–26, 75:12–27 (describing optional “fault tolerance feature of the

⁵ In the District Court Case, Patent Owner also argues that “minimum number of the plurality of [data] chunks” does not need to be construed. Ex. 1065, 9.

secure data parser” as being “where fewer than all portions are necessary to restore the original data”), 77:44–47, 77:62–65, 78:50–55. The fault-tolerant scheme permits “disaster recovery.” *Id.* at 70:12–26. 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 may 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.* Under this scheme, the data may be recovered even if two portions are destroyed or otherwise compromised. *Id.*

“Any suitable value for n or m may be used.” Ex. 1001, 70:25–26. In fact, n could be equal to m . *See id.* at 70:12–26 (describing “ $n \leq m$ ”). In this case, restoring the original data set requires all shares. *See, e.g., id.* at 61:59–61. The embodiment in Figures 33 and 34, for example, stores four shares and reconstructs the original data using all four. *Id.* at 73:38–62, Figs. 33, 34.

Claim 1 does not expressly recite that a fault-tolerant scheme must be used. Ex. 1001, 83:12–30. Rather, the claim recites “*at least* a minimum number,” which encompasses quantities larger than some minimum. *Id.* at 83:19–20 (emphasis added). Thus, claim 1 covers embodiments in which *all* data shares are used to restore the original data, not just the fault-tolerant scheme. *See, e.g., id.* at 70:12–26, 61:59–61, 73:38–62, Figs. 33, 34.

One of the Petition’s alternative constructions is based on the fault-tolerant scheme. *See* Pet. 67. In particular, Petitioner’s first alternative construction calls for “a predefined number.” Ex. 1064, 13; Pet. 67. But that term or feature is not found in the claims. Ex. 1001, 83:12–30 (claim 1). According to the ’609 patent, “[i]n *some* embodiments, the data may be split

into a predefined number of shares.” *Id.* at 78:28–29 (emphasis added). The ’609 patent mentions the “predefined number of shares” only in connection with the embodiments that use the fault-tolerant scheme. *See, e.g., id.* at 77:42–43 (“split to the predefined number of shares with fault tolerance”), 77:61–62 (same), 78:9–12 (same), 78:18–19 (same). Because the claim is not limited to the fault-tolerant embodiments for the reasons discussed above, we determine that claim 1 does not require “a predefined number.”

At this stage of the proceeding and based on the record before us, we construe “the data set can be reconstructed using at least a minimum number of the plurality of chunks,” as recited in claim 1, 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 chunks.

4. *Limitation [1F]: “storage device”*

Claim 1 recites “storing, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys on at least one *storage device*.” Ex. 1001, 83:27–30 (emphasis added).

Patent Owner argues that the recited “storage device” is for long-term storage:

[The skilled artisan] reviewing the ’609 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 ’609—“magnetic or optical disk, USB key drive, etc.”—are each devices primarily dedicated to long-term storage.

Prelim. Resp. 57–58.

We note that claim 1 does not use the term “long-term.” Nonetheless, we need not resolve whether the claim requires long-term storage at this stage of the proceeding because we disagree with Patent Owner that this feature distinguishes Foster. *See infra* § III.D.2.a.

D. Alleged Anticipation or Obviousness of Claims 1–3, 7, and 8 by or over Foster

Petitioner contends claims 1–3, 7, and 8 would have been unpatentable under 35 U.S.C. § 102 as anticipated by Foster (Ex. 1006), or, alternatively, under 35 U.S.C. § 103 as obvious over Foster. Pet. 3, 56–79, 83–84. Patent Owner opposes Petitioner’s contentions. Prelim. Resp. 36–66. Based on our review of the record before us, we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1–3, 7, and 8 are unpatentable under 35 U.S.C. § 102 as anticipated by Foster, as discussed below.

A fortiori, we also determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1–3, 7, and 8 would have been unpatentable under 35 U.S.C. § 103 as obvious over Foster. *See Cohesive Techs., Inc. v. Waters Corp.*, 543 F.3d 1351, 1364 (Fed. Cir. 2008) (“[I]t is commonly understood that prior art references that anticipate a claim will usually render that claim obvious.”); *Game & Tech. Co. v. Activision Blizzard Inc.*, 926 F.3d 1370, 1381 (Fed. Cir. 2019) (“[Appellant’s] assertion that ‘a single reference . . . cannot support obviousness’ is wrong as a matter of law.” (internal citation omitted)); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016) (“[A] patent can be obvious in light of a single prior art reference if it would have been obvious to modify that reference to arrive at the patented

invention.”); *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1336–37 (Fed. Cir. 2010) (affirming an invalidity judgment where claims were held obvious over a single reference).

We turn first to an overview of Foster.

1. Overview of Foster (Ex. 1006)

Foster generally is directed to “a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient,” where “a title key used to encrypt content is itself encrypted, and attached to the encrypted content so that both can be synchronously transmitted to a recipient.” Ex. 1006 ¶ 2.

Foster’s Figure 8, as annotated by Petitioner, is reproduced below. Pet. 57 (citing Ex. 1003 ¶ 167).

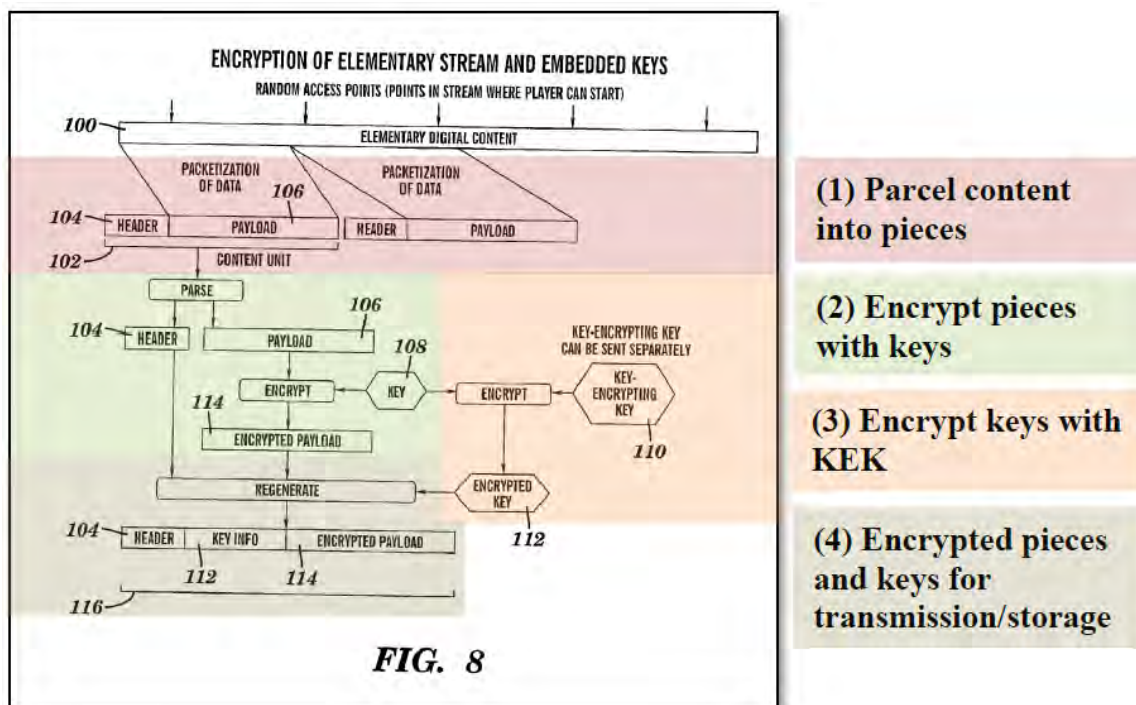


Figure 8, shown annotated by Petitioner, depicts a flow diagram of an elementary content stream being processed according to Foster’s invention.

Ex. 1006 ¶ 22, Fig. 8; Pet. 57.

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 a 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 as processed content unit 116, which can be transmitted to and stored by a recipient. Pet. 57–58; see Ex. 1006 ¶ 64.

We further discuss below the disclosures of Foster in connection with the parties’ arguments.

2. *Independent Claim 1*

a) *Receiving the First Key and Generating the Data Chunks*

Claim 1 recites, in part, “receiving a first key from a storage system” and “generating a plurality of data chunks based on a data set.” Ex. 1001, 83:12–16.

As for the “receiving” step, Petitioner refers to Figures 8 and 16 and contends that Foster’s Key-Encrypting Key (KEK) 110 corresponds to the recited “first key” and database 426 corresponds to the recited “storage system.” Pet. 63–65 (citing Ex. 1003 ¶¶ 178–183; Ex. 1006 ¶¶ 46, 77–79, Figs. 8, 16). Petitioner argues that Foster discloses “receiving a first key from a storage system,” as claimed, because “[Foster’s] computer system 400 receives the KEK . . . from database 426” and database 426 “includes ‘storage devices.’” Pet. 64–65 (citing Ex. 1003 ¶¶ 181–183; Ex. 1006 ¶¶ 46, 77).

As for the data-chunk “generating” step, Petitioner contends that Foster’s system generates a “plurality of data chunks based on a data set,” as claimed, because it generates payloads (the claimed “data chunks”) of digital content (the claimed “data set”). Pet. 65–66. Petitioner annotates Foster’s Figure 8, reproduced below, to illustrate this argument. *Id.*

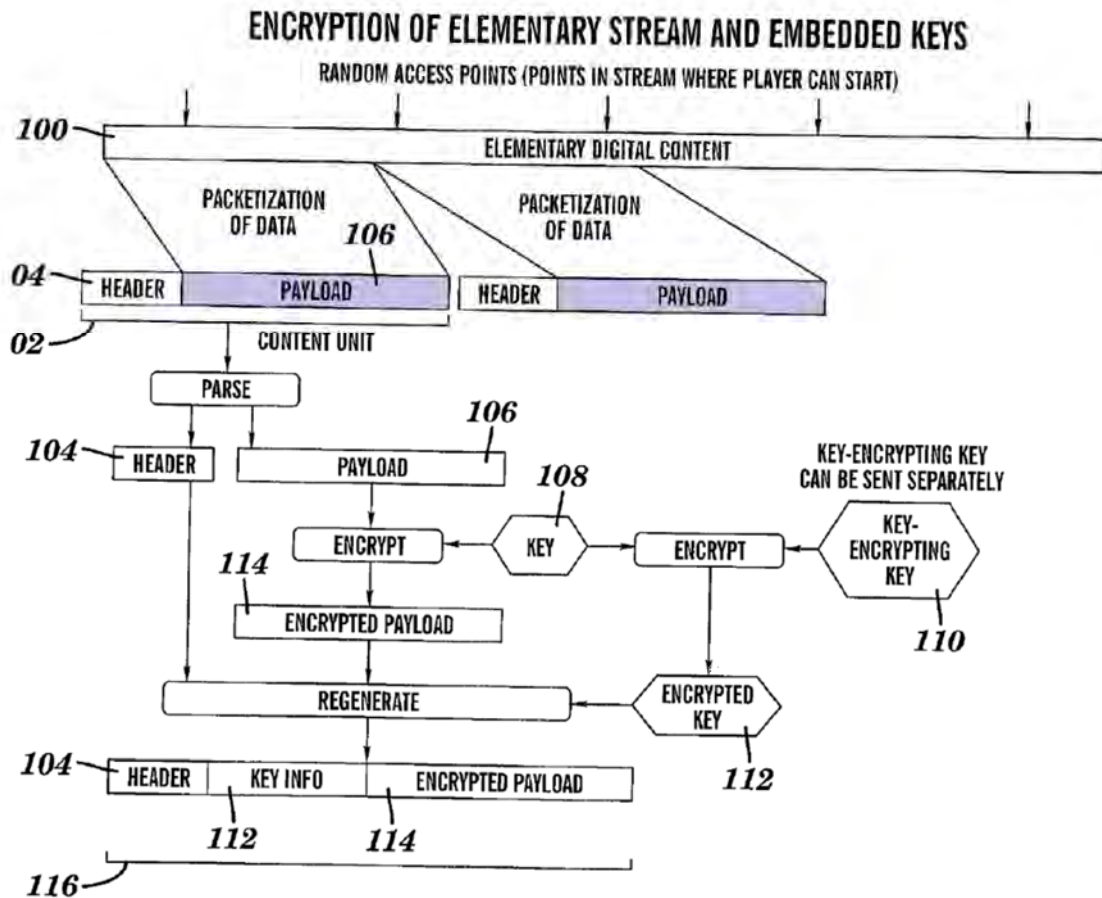


FIG. 8

Figure 8, shown annotated by Petitioner, depicts a flow diagram of an elementary content stream being processed according to Foster’s invention.

Ex. 1006 ¶ 22, Fig. 8; Pet. 66.

Petitioner highlights (in purple) payloads 106, which are shown as parceled from elementary digital content 100 using data packetization.

Pet. 65–66; Ex. 1001, Fig. 8. According to the Petition, elementary digital content stream 100 corresponds to the claimed “data set.” Pet. 65–66 (citing Ex. 1003 ¶¶ 183–186). Elementary digital content 100 is packetized to create content unit 102 (“102” is shown as “02” in annotated Fig. 8).

Ex. 1006 ¶ 64. Content unit 102 contains header 104 and payload 106 (“104” also is shown as “04” in annotated Fig. 8). *Id.* After parsing, the system encrypts payload 106 using tile key 108 to create encrypted payload 114. *Id.* Petitioner argues payloads 106 correspond to the claimed “data chunks,” and encrypted payload 114 corresponds to “an encrypted ‘data chunk.’” Pet. 67, 73.

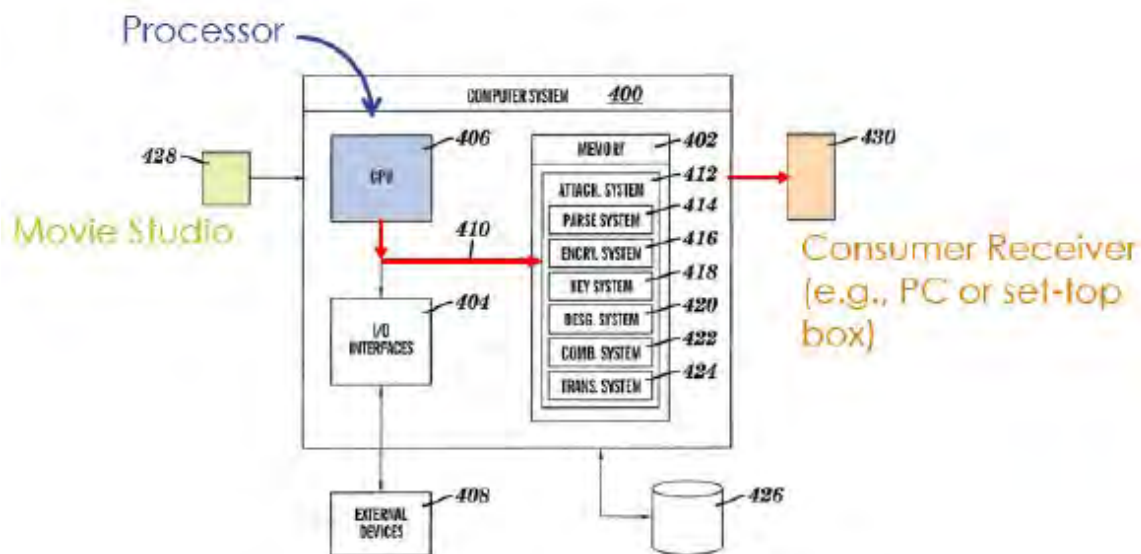
Patent Owner argues Petitioner has not shown that Foster’s digital content is a “data set,” as claimed. Prelim. Resp. 39 (“[Petitioner] fails to show that Foster’s ‘content’ is a ‘data set’ or that its ‘content units’ are ‘data chunks.’”); *see id.* at 36–45. According to Patent Owner, both parties agree that a “data set” must be “for storage.” *Id.* at 39 (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 ¶ 37⁶).

Patent Owner makes a similar argument with respect to the claimed data chunks. Prelim. Resp. 40–45. In particular, claim 1 recites “*storing*, in a memory coupled to the processor, at least one data chunk of the plurality of data chunks with data indicative of at least one of the distinct encryption keys *on at least one storage device.*” Ex. 1001, 83:27–30 (emphases added).

⁶ Patent Owner quotes this sentence from paragraph 37 but cites paragraph 8.

According to Patent Owner, Foster does not store its data packets on storage devices, as required by this limitation. *See* Prelim. Resp. 54–62. Patent Owner argues that Foster streams data to a receiver for immediate decoding and playback, not to a “storage device,” which Patent Owner contends means “secure long-term storage.” *Id.* at 55. In Patent Owner’s view, this is the “fundamental difference” between Foster and the claimed invention. *Id.* at 36–39, 55 (citing Ex. 2003 ¶¶ 78–80). Patent Owner argues Foster’s receiver is not a storage device because it is not dedicated to long-term storage. *Id.* at 55–58 (citing Ex. 2003 ¶¶ 104–105).

We disagree that Petitioner has not sufficiently shown, at this stage of the proceeding, that Foster’s digital content is for storage or that its receiver is a “storage device.” Petitioner argues that Foster’s receiver 430 stores the data chunks in its storage device. Pet. 73–74 (citing, *inter alia* Ex. 1003 ¶ 201); *see id.* at 75–76 (citing, *inter alia*, Ex. 1003 ¶¶ 202–205). Foster’s Figure 16, with the annotations of Patent Owner’s declarant, Aviel D. Rubin, Ph.D., is reproduced below. Ex. 2003 ¶ 79.



Foster’s Figure 16 as annotated by Dr. Rubin.

Annotated Figure 16 shows that the content is sent from movie studio 428 to computer system 400 to receiver 430. Ex. 2003 ¶ 79.

The record at this stage of the proceeding sufficiently supports Petitioner's argument that Foster's receiver 430 stores content that it receives. Pet. 73–76 (citing, *inter alia*, Ex. 1006 ¶¶ 40, 52, 58, 78–79, Figs. 8, 16). According to Dr. Rubin's annotations, receiver 430 can be a personal computer (PC) or set-top box. Ex. 2003 ¶ 79 (labeling the receiver in Figure 16 as such). This is consistent with Foster. Ex. 1006 ¶¶ 49, 52 (describing PC 18 and a set-top box). Foster describes how the receiver stores encrypted content. *See id.* ¶¶ 8, 79. For example, Foster explains, “[o]nce received, recipient 430 can then synchronously store the encrypted content.” *Id.* ¶ 79 (*cited in* Pet. 75–76). 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. 60). 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 of the proceeding that Foster's data set is “for storage.” *See* Pet. 72–76.

At this stage of the proceeding, we find Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 175, 201, 205) more persuasive than Dr. Rubin's (Ex. 2003 ¶¶ 102–105) 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 '609 patent's storage devices. *See* Ex. 2003 ¶¶ 104–105. For instance, we see little difference between the magnetic or optical disk, USB key drive, or other devices that Dr. Rubin claims are long-term storage devices and Foster's PC 18.

Ex. 1001, 67:1–4 (*cited in* Ex. 2003 ¶ 104). 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 (“storage by a receiver”). In view of at least these parts of Foster, we find Dr. Bhattacharjee’s testimony that Foster’s receiver has data storage (Ex. 1003 ¶¶ 175, 201, 205) more persuasive than Dr. Rubin’s testimony that Foster’s devices are unlike those described in the ’609 patent (Ex. 2003 ¶¶ 102–105), at this stage of the proceeding.

Based on the record before us, Petitioner sufficiently shows that Foster discloses the recited “data set,” the step of “generating a plurality of data chunks based on a 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 “first key” appears before the step of “generating” the “data chunks.” See Ex. 1001, 83:14–15. Petitioner argues that “Foster does not limit when it receives a KEK.” Pet. 78. As shown in Figure 8 (reproduced above), Foster uses key 108 to create encrypted payload 114 (the “data chunks”) and encrypts key 108 using KEK 110 (the “first key”) to create the encrypted key 112. Ex. 1006, Fig. 8.

Patent Owner argues that, under Petitioner’s proposed claim construction in the District Court Case, the steps must be performed in order. Prelim. Resp. 62 (citing Ex. 1064, 16; Pet. 78). 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 62 n.2.

For the reasons discussed above in Section III.C.2, we disagree that the step of receiving the first key must be performed before the step of generating the data chunks. At this stage of the proceeding, Petitioner sufficiently shows that the Foster discloses the recited “receiving” and “generating” steps for the reasons discussed above in Section III.D.2.a.

c) *Data Chunks*

Claim 1 recites, in part, “generating a plurality of *data chunks* based on a data set . . . and storing . . . at least one *data chunk* of the plurality of *data chunks* with data indicative of at least one of the distinct encryption keys on at least one storage device.” Ex. 1001, 83:15–16, 26–30 (emphases added).

As discussed above, Petitioner asserts that Foster’s payloads are the claimed “data chunks.” See Pet. 65–66. Patent Owner argues at length that Petitioner has not explained why Foster’s payloads are data chunks. Prelim. Resp. 39–45 (citing, *inter alia*, Pet. 65–66). In Patent Owner’s view, Petitioner’s reasoning is conclusory. See, e.g., *id.* at 40. 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 41. Patent Owner argues that packets are parsed into chunks but are not chunks themselves. *Id.* at 41–45. Patent Owner argues that the purpose of generating the data chunks is to secure the data. *Id.* at 43–44. We find Patent Owner’s arguments unavailing on the record before us.

We turn to the plain language of claim 1, and are mindful of Judge Rich’s guidance from over thirty years ago: in all aspects of claim construction, “the name of the game is the claim.” *In re Hiniker Co.*,

150 F.3d 1362, 1369 (Fed. Cir. 1998) (quoting Giles Sutherland Rich, *Extent of Protection and Interpretation of Claims—American Perspectives*, 21 Int’l Rev. Indus. Prop. & Copyright L. 497, 499 (1990)). Here, claim 1 requires, in part, “generating a plurality of data chunks based on a data set,” and does so in the context of an 83-column Specification that never mentions the term “data chunk.” Ex. 1001, 83:15–16; *see generally id.* On its face, this limitation plainly requires nothing more or less than generating chunks of data out of a data set. Based on the record before us, this is what Petitioner sufficiently evidences—Foster’s elementary digital content stream 100 is the “data set” or set of data, and Foster breaks up (or parcels) that data set into chunks of data called payloads (or “data chunks”). *See* Pet. 65–66. We find persuasive Petitioner’s application of Foster to this limitation, as it stays true to the plain meaning of the claim limitation at issue (including the broad nature of the claimed term “data” in “data set” and “data chunk”). To the contrary, at least on the record before us, we find Patent Owner’s arguments (Prelim. Resp. 39–45) and its declarant’s testimony (Ex. 2003 ¶¶ 83–88) to be divorced from that plain meaning.

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*,” citing *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022) (precedential). Prelim. Resp. 40. 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. 65–66), as well as Dr. Bhattacharjee’s testimony

(Ex. 1003 ¶¶ 184–187), are adequately supported by Foster for all the reasons discussed above.

Patent Owner further argues that Foster’s payloads do not correspond to the claimed data chunks because Foster does not store them on storage devices. Prelim. Resp. 39, 54–58. As discussed above in Section III.D.2.a, we disagree with Patent Owner’s argument that Foster does not teach storing the encrypted payloads.

Based on the record before us, Petitioner sufficiently shows that Foster discloses “generating” and “storing” “data chunks” as recited in claim 1.

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 chunks.” Ex. 1001, 83:18–20. Petitioner shows that Foster teaches the claimed data set under Patent Owner’s proposed construction in the District Court Case: “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. 67 (citing Ex. 1065, 9).⁷ Under this construction, Petitioner argues that Foster’s system needs all encrypted content packets to access the entire elementary content stream. Pet. 67. Petitioner argues that this disclosure 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.” Pet. 67 (quoting Ex. 1006 ¶ 71) (emphasis omitted). According to the Petition, the content packets correspond to the recited data

⁷ In the District Court Case, Patent Owner alternatively argues that the claim limitation need not be construed. See Ex. 1065, 9.

chunks, and accessing the entire stream corresponds to reconstructing the data set, as recited. Pet. 67.

Patent Owner does not present arguments specific to this rationale. *See* Prelim. Resp. 53–54; *see generally id.* Based on the record before us, Petitioner sufficiently 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. 67; *see supra* §§ III.C.1, C.3. We credit Dr. Bhattacharjee’s testimony that Foster uses all encrypted content packets to reconstruct, or access, the original content stream. Ex. 1003 ¶¶ 188–189. This testimony is consistent with Foster’s explanation that the title keys are attached and transmitted with the content 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 remainder of independent claim 1. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. The Petition provides a detailed assessment of these remaining limitations, with references to disclosures in Foster and the declaration testimony of Dr. Bhattacharjee. Pet. 56–78. We have reviewed Petitioner’s arguments and evidence in this regard (Pet. 56–78), and are persuaded that Petitioner sufficiently shows that Foster discloses these remaining limitations.

f) Conclusion

For the foregoing reasons, and the reasons stated in the Petition (Pet. 56–78), we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that independent claim 1 is unpatentable as anticipated by Foster.

3. Dependent Claims 2, 3, 7, and 8

Claims 2, 3, 7, and 8 depend directly or indirectly from independent claim 1. Ex. 1001, 84:1–8, 20–25. The Petition provides a detailed assessment of these claims, with references to the Petition’s analysis of claim 1, disclosures in Foster, and the declaration testimony of Dr. Bhattacharjee. Pet. 78–79, 83–84. At this stage of the proceeding, Patent Owner does not present any separate arguments that are distinct to these claims. Rather, Patent Owner generally is of the view its alleged deficiencies in the Petition with respect to claim 1 are also applicable to these dependent claims. *See generally* Prelim. Resp. As discussed above, on the present record and at this stage of the proceeding, we are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that independent claim 1 is unpatentable as anticipated by Foster. For the reasons set forth in the Petition (Pet. 78–79, 83–84), we also are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that dependent claims 2, 3, 7, and 8 are unpatentable as anticipated by Foster, for purposes of institution.

4. Summary of Anticipation by or Obviousness over Foster

At this stage of the proceeding and based on the record before us, we are persuaded that Petitioner’s cited evidence sufficiently supports Petitioner’s contentions that claims 1–3, 7, and 8 are unpatentable as

anticipated by Foster, or, alternatively, as obvious over Foster. Pet. 3, 56–79, 83–84. Accordingly, we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that claims 1–3, 7, and 8 are unpatentable as anticipated by Foster, or, alternatively, as obvious over Foster.

E. Alleged Obviousness of Claims 4–6, 9, and 10 over Foster

Petitioner contends claims 4–6, 9, and 10 would have been unpatentable under 35 U.S.C. § 103 as obvious over Foster. Pet. 80–83, 85. Claims 4–6, 9, and 10 each depend directly from independent claim 1. Ex. 1001, 84:9–19, 26–29. The Petition provides a detailed assessment of these claims, with references to the Petition’s analysis of claim 1, disclosures in Foster, and the declaration testimony of Dr. Bhattacharjee. Pet. 80–83, 85. At this stage of the proceeding, Patent Owner does not present any separate arguments that are distinct to these claims. Rather, Patent Owner generally is of the view its alleged deficiencies in the Petition with respect to claim 1 are also applicable to these dependent claims. *See generally* Prelim. Resp. As discussed above, on the present record and at this stage of the proceeding, we are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that independent claim 1 is unpatentable as anticipated by Foster. For the reasons set forth in the Petition (Pet. 80–83, 85), we also are persuaded that the cited evidence sufficiently supports Petitioner’s contentions that dependent claims 4–6, 9, and 10 are unpatentable as anticipated by Foster, for purposes of institution.

F. Alleged Anticipation or Obviousness of Claims 1–10 by or over Orsini

Petitioner contends claims 1–10 would have been unpatentable under 35 U.S.C. § 102 as anticipated by Orsini (Ex. 1005), or, alternatively, under 35 U.S.C. § 103 as obvious over Orsini. Pet. 3, 9–55. Patent Owner opposes Petitioner’s contentions. Prelim. Resp. 1–36. Based on our review of the record before us, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that any of claims 1–10 is unpatentable as anticipated by or obvious over Foster, as discussed below. We turn first to an overview of Orsini.

1. Orsini

Orsini and the ’609 patent share three named inventors and contain overlapping disclosures and figures. Pet. 9 (citing Exs. 1001, 1005) (noting that paragraphs 1–423 and figures 1–25 of Orsini are found in the ’609 patent); Prelim. Resp. 1 (same). Like the ’609 patent, Orsini is directed to a system for securing sensitive data from unauthorized access and use. Ex. 1005, code (57). According to Patent Owner, the ’609 patent “includes 17 new figures and over eighteen columns of additional material (~10,500 words) which contain significantly different technology than that disclosed in Orsini.” Prelim. Resp. 1 (citing Ex. 1001, Figs. 26–41, 6:44–6:62, 8:10–8:61, 65:56–83:3) (emphasis omitted).

We further discuss below the disclosures of Orsini in connection with the parties’ arguments.

2. Independent 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. 15. Petitioner argues that this encryption step would occur after Orsini’s “encrypt pieces” step, as shown in Figure 21 (annotated by Petitioner), reproduced below. Pet. 11, 15–16.

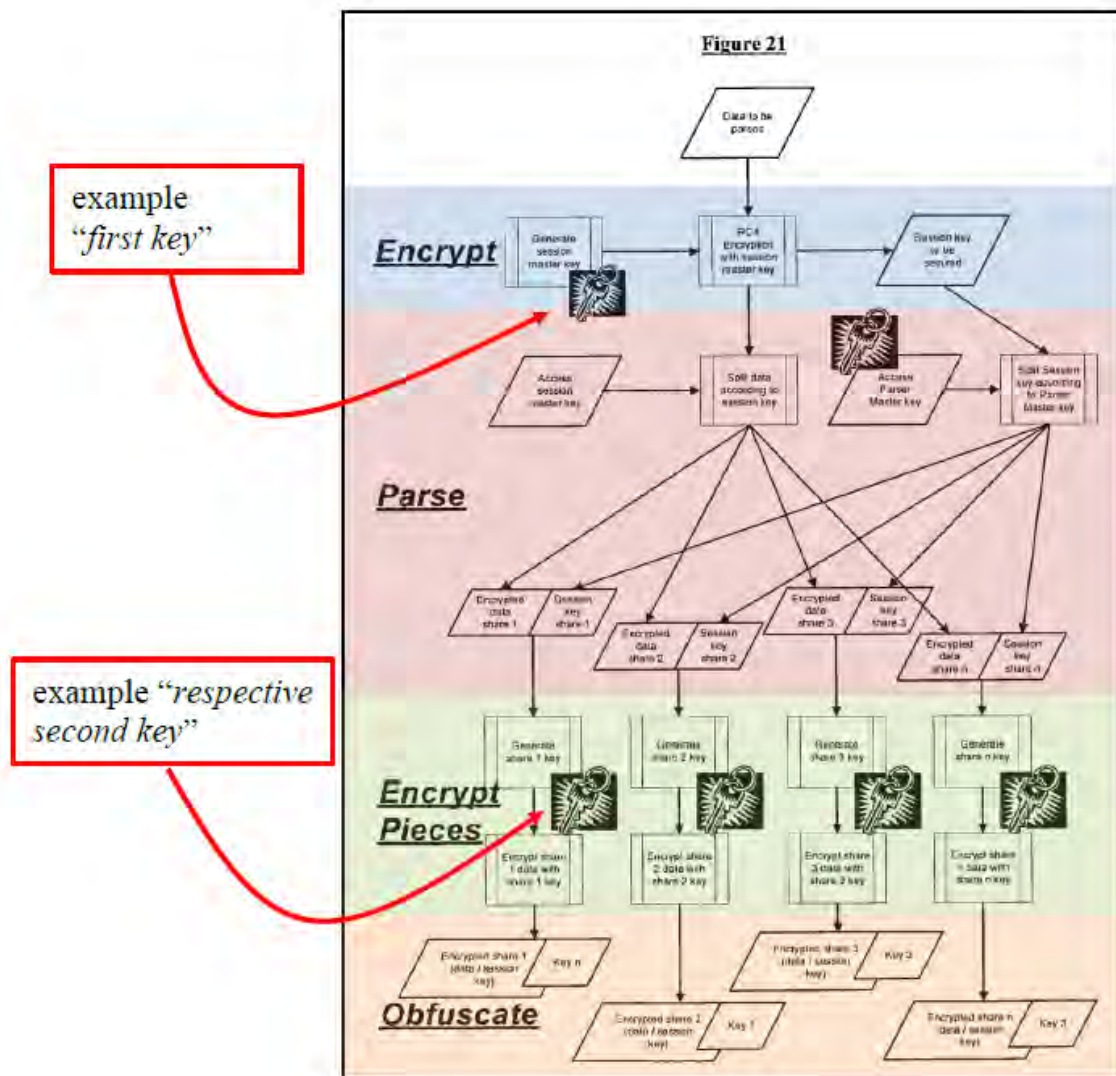


Figure 21, annotated by Petitioner, depicts a process for parsing, splitting, or separating data with encryption and storage of the encryption master key with the data.

Ex. 1005 ¶ 54, Fig. 21. Petitioner argues that Orsini’s Figure 21 has four steps: encrypt, parse, encrypt pieces, and obfuscate. Pet. 11. This method uses a session master key and multiple share keys. Pet. 11. Petitioner argues that the session master key corresponds to the claimed first key, and the multiple share keys correspond to distinct encryption keys, as labeled above (see red boxes with arrows). Pet. 11.

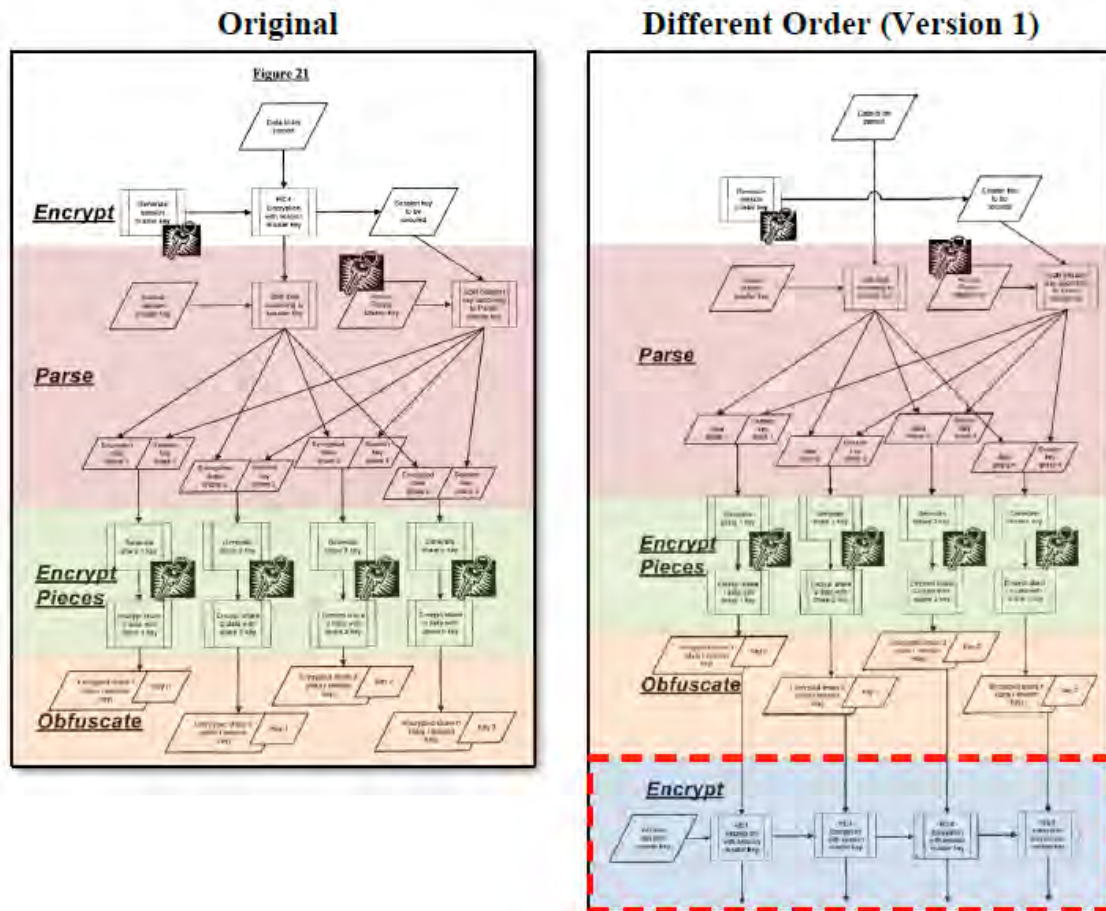
Petitioner gives the label “[1E]” to the claimed step of “performing a cryptographic operation based on the first key to further secure the plurality of data chunks.” Pet. 30. Petitioner argues that Orsini discloses, teaches, or suggests limitation [1E]. See Pet. 30–42.

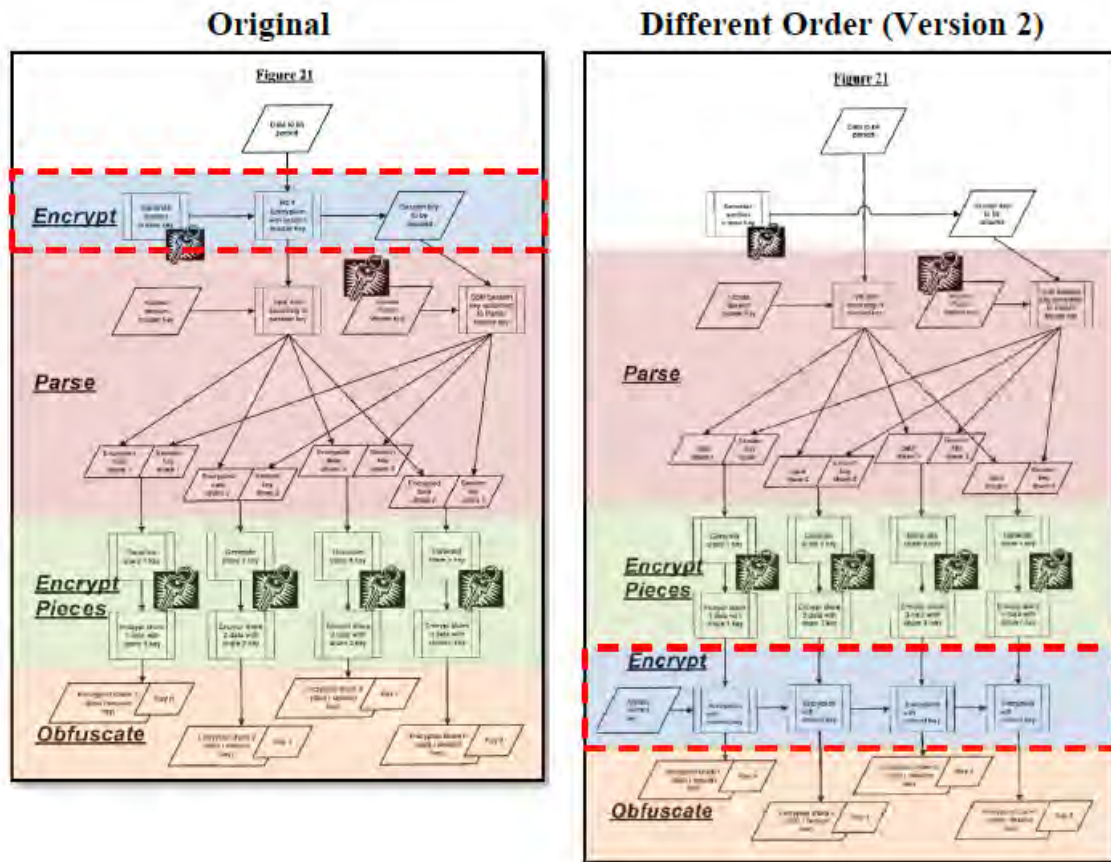
a) Anticipation by Orsini

Petitioner argues that, “in discussing Figure 21’s encryption method, Orsini teaches that ‘[i]t is readily apparent’ to [the skilled artisan] ‘that certain steps of the method[] described herein may be performed **in different order.**’” Pet. 30 (citing Ex. 1005 ¶ 301). Petitioner argues that one “certain step” could be the first “encrypt” step with the session master key. Pet. 30–31 (citing Ex. 1003 ¶¶ 102–103). Petitioner argues “Orsini also teaches that Figure 21’s steps can be ‘**repeated multiple times.**’” Pet. 33 (citing Ex. 1005 ¶ 301). Petitioner argues “Orsini discloses embodiments that encrypt encryption keys with other encryption keys, the latter of which are known in the art as key-encrypting keys (‘KEKs’).” Pet. 40 (citing Ex. 1005 ¶ 172 (discussing “public keys”). Thus, Petitioner presents three different rationales for how Orsini allegedly discloses limitation 1[E]: one based on the different order, another based on repeating the steps, and a third based on encrypting with a public key. Pet. 30, 33, 40.

(1) *Different Order*

Petitioner illustrates its “different-order Orsini embodiment that [allegedly] meets claim 1” (Ex. 1003 ¶ 59) using the two sets of annotated versions of Figure 21 reproduced below. Pet. 31–33.





The above illustrations depict two sets of Petitioner’s annotated versions of Figure 21 allegedly revealing different-order Orsini embodiments that satisfy limitation 1[E].

Pet. 31–33 (citing Ex. 1003 ¶¶ 104–105).

In the Different-Order Versions 1 and 2 (right), the second encryption further secures the data chunks using Orsini’s session master key, which Petitioner argues is the claimed “first key.” Pet. 31. Unlike Orsini’s Original Figure 21 (left), Petitioner’s Different-Order Versions lack an initial encrypt step. Pet. 31. Instead, there is an encryption step after either the “obfuscate” step or the “encrypt pieces” step. Pet. 31, 35. We find Petitioner’s arguments unpersuasive.

Rather, we preliminarily agree with Patent Owner that Petitioner has not shown that Orsini anticipates claim 1 based on the Different-Order Versions. Prelim. Resp. 7–19. “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., Inc. 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 Versions. See Pet. 30–33. Instead, Petitioner argues that Orsini “teaches” or suggests reordering some steps. Pet. 30–33. For example, Petitioner argues that Orsini teaches that “certain steps” can be reordered, and Orsini’s parsing processes design “reinforces” reordering the steps. See Pet. 30 (citing Ex. 1005 ¶ 301; Ex. 1005 ¶ 279). For at least this reason, Petitioner has not shown that Orsini discloses the Different-Order Versions.

Moreover, Petitioner’s Different-Order Versions go beyond mere reordering. Pet. 30–33. Rather, Petitioner’s Different-Order Versions change what is being encrypted compared to Orsini’s Figure 21. Pet. 30–33. Specifically, by moving the data set encryption steps from the beginning of Figure 21 to after the “obfuscating” or “encrypt pieces” steps, the “encrypt” step is applied to the individual chunks instead of the entire data set. See Prelim. Resp. 12 (“[N]ot only does Petitioner move (or copy and move) the dataset encryption step from the beginning of Figure 21 to the end, but it also then re-writes the step to apply to each of the chunks rather than to the dataset as a whole. Thus, Petitioner does not merely reorder Figure 21, it fundamentally alters what is being encrypted (the dataset versus the shares).” (text coloration omitted) (citing Ex. 2003 ¶ 50)).

We also 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 cryptographic operation Petitioner contends would be reordered/repeated).” Prelim. Resp. 16. Dr. Rubin explains why reordering the steps in the way that Petitioner proposes would have been “pointless:”

Indeed, [the skilled artisan] would recognize that encryption with the alleged first 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 first key (*i.e.*, the session master key) would render the splitting and encryption of the alleged first 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 ¶¶ 101–105. Thus, we find Dr. Rubin’s testimony (Ex. 2003 ¶¶ 52–53) more persuasive than Dr. Bhattacharjee’s (Ex. 1003 ¶¶ 101–105) on this issue. For this additional reason, Petitioner has not shown that Orsini discloses the Different-Order Versions.

Thus, based on the record before us, we determine that Petitioner has not shown that Orsini discloses limitation [1E] by performing the steps in a different order.

(2) Repeated Steps

Petitioner argues that Orsini discloses embodiments in which encrypted data shares (the claimed encrypted “data chunks”) are encrypted an additional time using a different algorithm. Pet. 34 (citing Ex. 1003 ¶ 107). Petitioner argues that Orsini’s dependent claims recite using “a different encryption algorithm.” Pet. 33 (citing Ex. 1005,

claims 12, 29, 39). According to Petitioner, Orsini's claimed embodiment that uses a "different encryption algorithm" performs encryption with the first key:

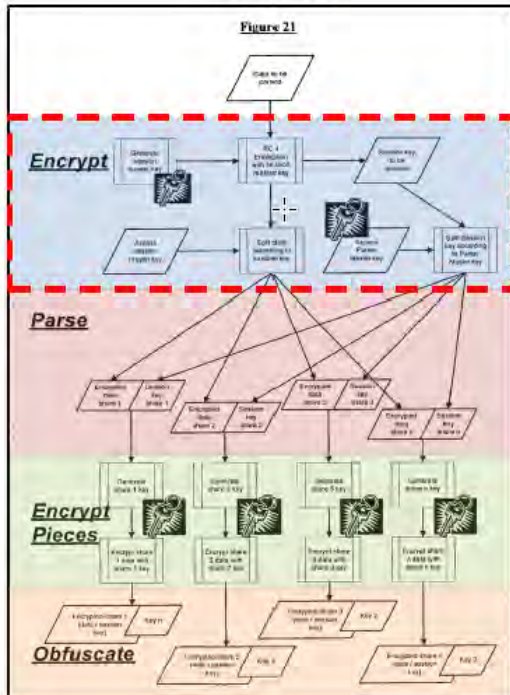
One different algorithm performed after encrypting shares (thus after generating the encrypted "*data chunks*") that would have been obvious to [the skilled artisan] includes using a single encryption key to further encrypt all encrypted shares with that encryption key similar to using the session master key to encrypt the entire data set before splitting it.

Pet. 34 (emphasis in original).

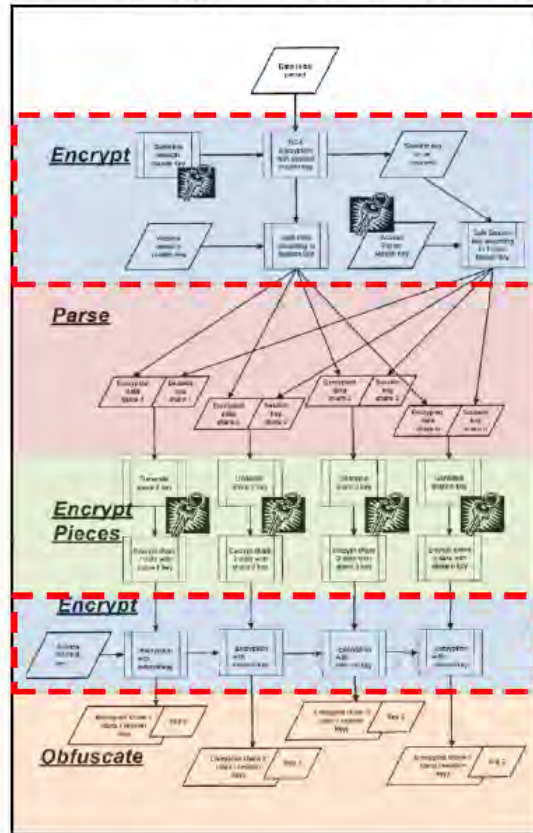
On the record before us, the only support for Petitioner's conclusions is Orsini's statement that "the methods described herein may be . . . repeated multiple times" (Ex. 1005 ¶ 301), Orsini's claims reciting "a different encryption algorithm" (*see id.*, claims 12, 29, 39), and Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 106–108). Petitioner does not identify anything from Orsini that explains how the algorithms are different. *See* Pet. 33–36. Dr. Bhattacharjee's testimony (Ex. 1003 ¶¶ 106–108) 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. 14–19.

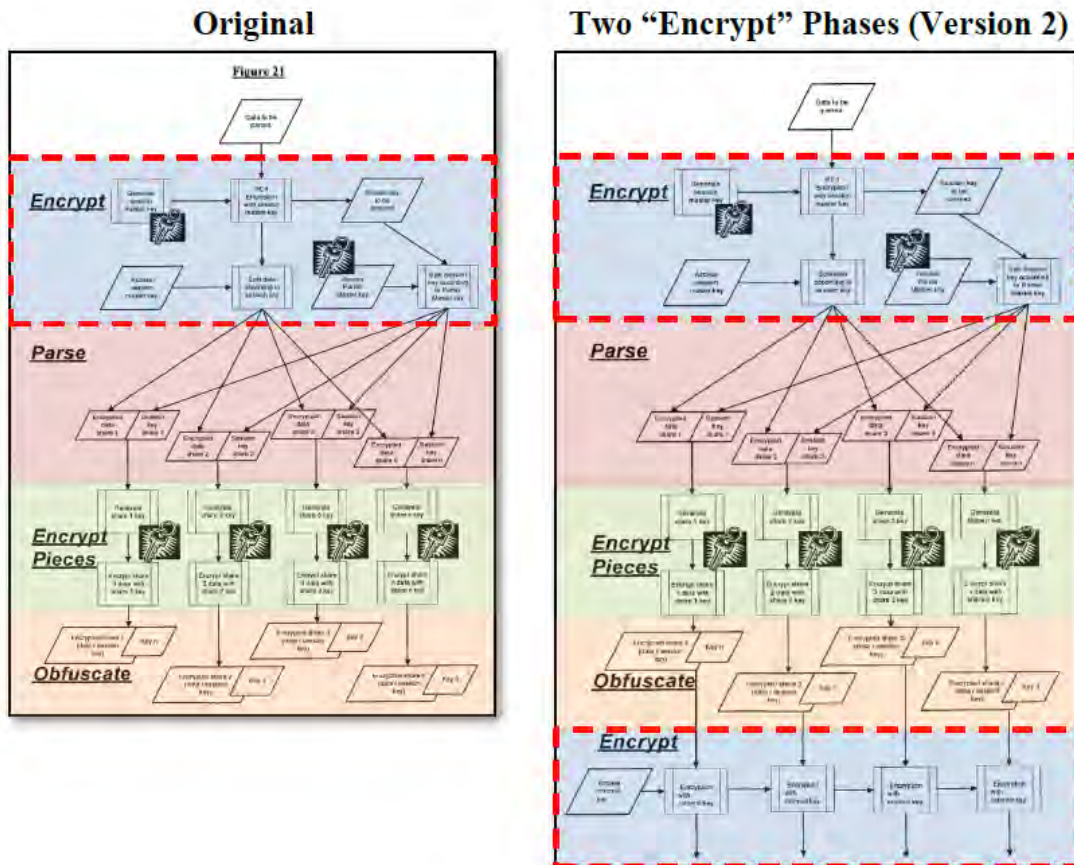
Petitioner's Two-Encrypt-Phases rationale also is deficient for reasons similar to those for the Different-Order rationale: Petitioner does not sufficiently explain or support its arguments about Orsini's session master key and common key. *See supra* § III.F.2.a.1. Petitioner illustrates its Two-Encrypt-Phases rationale using the two sets of annotated versions of Figure 21 reproduced below. Pet. 34–36.

Original



Two "Encrypt" Phases (Version 1)





The above illustrations depict two sets of Petitioner’s annotated versions of Figure 21 allegedly revealing Two-Encrypt-Phases Orsini embodiments that satisfy limitation 1[E].

Pet. 34–36 (citing Ex. 1003 ¶ 108).

In either version, Orsini’s method would have an additional encryption step. Pet. 34–36. That is, Version 1 would “(1) encrypt the original data set with a session master key, (2) split the data into shares (‘data chunks’), (3) encrypt the data shares with distinct share keys, (4) encrypt each encrypted share (‘data chunk’) with a common key (e.g., a

conventional encryption key),^[8] and (5) obfuscate the encrypted shares.” Pet. 34 (bold emphases omitted). Version 2 obfuscates before it encrypts. Pet. 34–36.

Petitioner argues that the common key used in step (4) “would have been, or had reason to be, received from a ‘*storage system*,’” and thus “meets ‘*the first key*,’” as recited in claim 1. Pet. 34–35. As noted above, the additional encryption uses an algorithm that is somehow different, according to Petitioner. Pet. 33. Thus, Petitioner contends that its Two-Encrypt-Phases rationale discloses limitation [1E]. Pet. 33–36.

The claim recites “performing a cryptographic operation *based on the first key* to further secure the plurality of data chunks.” Ex. 1001, 83:25–26. Yet Orsini divides the session master key into pieces that are integrated into the data chunks 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. 33–36. Further, 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. 33–36. For at least this reason, based on the record before us, we determine that Petitioner has not shown that Orsini discloses limitation [1E] by repeating encryption steps.

⁸ 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.

Also, even if Orsini repeats the method, both versions of Petitioner's Two-Encrypt-Phases rationale go beyond mere repetition. Pet. 33–36. 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 first 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 find Dr. Rubin's testimony (Ex. 2003 ¶ 42) more persuasive than Dr. Bhattacharjee's (Ex. 1003 ¶¶ 106–108) at least because it is better supported by Orsini's Figure 21. For this additional reason, based on the record before us, we determine that Petitioner has not shown that Orsini discloses limitation [1E] by repeating encryption steps.

(3) Encrypting with a Public Key

Petitioner argues “Orsini discloses using a so-called ‘public key’ ‘to encrypt the session key that will be used to encrypt the document or message,’” and “[t]hus, Orsini discloses embodiments that encrypt encryption keys with other encryption keys, the latter of which are known in the art as key-encrypting keys (‘KEKs’).” Pet. 40 (citing Ex. 1005 ¶ 172; Ex. 1003 ¶ 120) (emphasis omitted).

As Patent Owner points out, the public key is not shown in Figure 21. Prelim. Resp. 18–19. Rather, Petitioner combines features from multiple embodiments to arrive at the claimed invention. See Pet. 33–36, 40. But

“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, based on the record before us, we determine that Petitioner has not shown that Orsini discloses limitation [1E] under its public-key rationale.

(4) Conclusion – Anticipation by Orsini

Based on our review of the record before us, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that independent claim 1 is unpatentable as anticipated by Foster.

b) Obviousness Over Orsini

Petitioner argues that the skilled artisan “had multiple reasons to implement Orsini to perform [limitation [1C]].” Pet. 36. Petitioner proffers four alternative obviousness rationales. Pet. 36–42. Petitioner argues that the skilled artisan had reason to (1) re-encrypt data chunks with a first encryption key, (2) re-encrypt data chunks with a group key, (3) reorder data within each chunk based on an encryption key, or (4) encrypt distinct encryption keys with a key-encryption key (KEK). Pet. 36–42.

(1) Re-encrypting with First Key

Petitioner argues that the skilled artisan “would have been motivated . . . to reorder and/or repeat certain specific steps by encrypting (‘*perform[] a cryptographic operation*’ on) already-encrypted data chunks with the same encryption key, and would have understood that doing so would have

provided additional security and efficiency benefits.” Pet. 36–37 (citing Ex. 1003 ¶¶ 109–111). According to Petitioner, “[r]e-encrypting data chunks with a common encryption key was also a known solution to the known problem of how to further secure data using encryption, and thus was obvious.” Pet. 37.

Here, Petitioner’s rationale is deficient for all the reasons discussed above in Sections III.F.2.a.1 and a.2. Petitioner’s additional reasoning that the proposed modification would “provide[] additional security and efficiency benefits” is unsupported and conclusory. *Id.* Indeed, providing additional security is recited in the claim limitation [1E] itself: “performing a cryptographic operation based on the first key *to further secure* the plurality of data chunks.” Ex. 1001, 83:25–26 (emphasis added). Petitioner’s obviousness rationale is circular and does nothing more than restate the claim language. Pet. 36–37 (citing Ex. 1003 ¶¶ 109–113). Petitioner also does not explain why repeating or reordering steps would be efficient. Pet. 36–37. Further, for the reasons discussed above in Sections III.F.2.a.1 and a.2, we disagree that reordering and repeating Orsini’s steps in the way that Petitioner describes was a “known solution.” Pet. 37.

The Bhattacharjee Declaration largely repeats the Petition’s conclusory assertions, adding scant supporting evidence and technical reasoning. *See* Ex. 1003 ¶¶ 110–113 (*cited in* Pet. 36–37). According to Dr. Bhattacharjee, the skilled artisan “would have understood that encrypting multiple smaller chunks of data with a common key would have been computationally easier than encrypting the single larger data set before splitting it into shares.” *Id.* ¶ 110. But Dr. Bhattacharjee provides no supporting citations or additional technical reasoning for this statement. *See*

id. According to Dr. Bhattacharjee, “[s]uch further encryption would have also provided greater security by re-encrypting the data chunks [a second time].” *Id.* As with the statement in the Petition, reciting 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, 83:25–26. Thus, based on the record before us, we do not credit Dr. Bhattacharjee’s testimony (Ex. 1003 ¶¶ 110–113) on this issue.

Based on the record before us, we also agree with Patent Owner that Petitioner’s reason to modify Orsini is based on impermissible hindsight. *See* Prelim. Resp. 33–36. The Board must “recognize that we cannot allow hindsight bias to be the thread that stitches together prior art patches into something that is the claimed invention.” *Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017) (“Without any explanation as to how or why the references would be combined to arrive at the claimed invention, we are left with only hindsight bias that *KSR* warns against.”); *see KSR*, 550 U.S. at 421 (2007) (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”). “Any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made and does not include knowledge gleaned only from applicant’s disclosure, such a reconstruction is proper.” *In re McLaughlin*, 443 F.2d 1392, 1313–14 (CCPA 1971). In this case, Petitioner relies on the very reason set forth in claim 1 (“to further secure”) as its rationale for re-encrypting data chunks with the first key.

Accordingly, based on the record before us, 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 the first key.

(2) *Re-encrypting with a Group Key*

Petitioner argues that the skilled artisan had reason to re-encrypt data chunks with a *group* key. Pet. 37–38. 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.’” Pet. 37–38 (quoting Ex. 1005 ¶ 412). According to Petitioner, the conventional implementation of these embodiments uses a group-level encryption key, citing several other references. Pet. 37 (citing Ex. 1003 ¶¶ 114–115; 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.” Pet. 38 (citing *KSR*, 550 U.S. at 417). Petitioner, though, provides no explanation why the additional cited references were “similar.” Pet. 38. Nor does Petitioner explain how the cited prior art would have been used to modify Orsini. Pet. 38. Thus, it is not apparent how Petitioner intends to rely on these references in its challenge. Generally, the challenge based on re-encrypting with a group key 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). Based

on the record before us, we agree with Patent Owner that Petitioner's reason to modify Orsini by re-encrypting with a group key is entirely based on impermissible hindsight (*see supra* § III.F.2.b.1 (discussing hindsight)).

Accordingly, based on the record before us, 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 a group key.

(3) *Reordering Data*

Petitioner argues that the skilled artisan “had reason to add additional security to Orsini’s encrypted shares (encrypted ‘data chunks’) by cryptographically reordering/shuffling the data within each ‘data chunk,’ which was a conventional cryptographic operation to secure data.” Pet. 38–39 (emphases omitted). Petitioner claims that this is a “conventional cryptographic operation to secure the data,” expressly taught by Orsini, or rendered obvious by Orsini. Pet. 39 (citing, *inter alia*, Ex. 1005 ¶ 281; Ex. 1030 ¶ 2).

For the reasons discussed above in Section III.F.2.a.1, 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.

As for whether this reordering would have been obvious, the Petition lacks an articulated rationale. *See* Pet. 38–39. So Petitioner’s obviousness rationale is deficient for the same reasons discussed above in Section III.F.2.b.2. For example, Petitioner states that the skilled artisan would have understood the benefits of reordering but fails to sufficiently identify or analyze any specific benefit. *See* Pet. 38–39. Based on the record before us, 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 (*see supra* § III.F.2.b.1 (discussing hindsight)).

Accordingly, based on the record before us, Petitioner has not shown a reasonable likelihood in demonstrating that claim 1 would have been obvious under its rationale based on cryptographically reordering or shuffling the data.

(4) *Encrypting the Distinct Encryption Keys with a Key-Encryption Key*

Petitioner argues that the skilled artisan had reason to encrypt the distinct encryption keys with a KEK. Pet. 40–42.

Petitioner argues that Orsini discloses or teaches encrypting session keys with a public-key encryption key. Pet. 40. For the reasons discussed above in Section III.F.2.a.3, 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. 18–19. Petitioner’s argument about the public-key encryption key is based on the features from multiple embodiments. *See* Pet. 33–36, 40. Yet Petitioner does not provide a sufficient rationale for combining these multiple embodiments. *See id.*

Petitioner’s analysis in § VI.B.7.b.iv of the Petition does not remedy the deficiencies in Petitioner’s analysis of the public-key encryption key. *See supra* § III.F.2.a.3. Rather, the reasoning in § VI.B.7.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. 40 (citing Ex. 1005 ¶ 172).

Accordingly, based on the record before us, 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 a KEK.

(5) Conclusion – Obviousness Over Orsini

Based on our review of the record before us, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that independent claim 1 is unpatentable as obvious over Foster.

3. Dependent Claims 2–10

Claims 2–10 depend directly or indirectly from independent claim 1. Ex. 1001, 84:1–29. At this stage of the proceeding and based on the record before us, we determine that Petitioner’s analysis for claims 2–10 does not remedy the deficiencies with respect to claim 1. *See* Pet. 45–55. 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.

4. Summary

Based on our review of the record before us, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that any of claims 1–10 is unpatentable as anticipated by or obvious over Foster.

IV. CONCLUSION

Based on the evidence before us, we determine that Petitioner has established a reasonable likelihood that at least one claim of the ’609 patent is unpatentable. Accordingly, we institute trial on all the challenges in the Petition.

We base our factual findings and conclusions at this stage of the proceeding on the evidentiary record developed so far. This is not a final

decision as to the construction of any claim term or the patentability of any claim. Any final decision shall be based on the full trial record, including any response timely filed by Patent Owner. Any arguments not raised by Patent Owner in a timely filed response may be deemed waived, even if they were presented in the Preliminary Response.

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–10 of the '609 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '609 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2024-00214
Patent 11,068,609 B2

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