

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case IPR2024-00215
Patent 10,452,854

EXHIBIT 2033

SECOND DECLARATION OF AVIEL D. RUBIN, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS	1
III. BASES OF OPINIONS	7
IV. APPLICABLE LEGAL STANDARDS.....	10
A. Level Of Ordinary Skill In The Art.....	10
B. My Understanding Of Legal Standards	12
V. CLAIMS-AT-ISSUE (CLAIMS 1-10)	16
VI. OPINIONS.....	16
A. Petitioner’s Orsini Ground Fails (All Claims, Ground 1).....	16
1. Prior Opinions Offered	16
a. The ’854 And Orsini.....	16
b. “Performing An Encryption Operation Based On The External Key To Further Secure The Plurality Of Data Chunks” (Limitation 1[c]).	22
2. Additional Opinions.....	44
B. Petitioner’s Foster-Hayhurst Ground Fails (All Claims, Ground 2).....	59
1. Hayhurst Is Not Analogous Art (All Claims).	59
a. The ’854 And Hayhurst Do Not Share The Same Field Of Endeavor.....	59
b. Hayhurst Is Not Reasonably Pertinent To The ’854’s Problem.....	62
2. Motivation To Combine Foster And Hayhurst (All Claims)...	64

a.	Foster’s System.....	65
b.	Hayhurst’s System.	71
c.	Petitioner And Dr. Bhattacharjee’s Proposed Combination.	73
d.	A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.	75
3.	“Generating A Plurality Of Data Chunks Based On A Data Set” (Limitations 1[b], 1[b1]).	83
VII.	CONCLUSION	89

I. INTRODUCTION

1. My name is Aviel D. Rubin. I have been retained as an expert witness to provide my independent opinion in regard to the matters at issue in *inter partes* review of U.S. Patent No. 11,068,609 (“the ’609 patent”) in IPR2024-00214 and of U.S. Patent No. 10,452,854 (“the ’854 patent”) in IPR2024-00215. I have been retained by Security First Innovations, LLC (“SFI”), the Patent Owner in the above proceedings. Petitioner is Google LLC. (“Google” or “Petitioner”).

2. I am being compensated \$925 per hour for my time spent working in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this report.

3. I am not a legal expert and offer no opinions on the law. However, I have been informed by counsel of the various legal standards that apply, and I have applied those standards in arriving at my conclusions.

II. QUALIFICATIONS

4. I have more than 30 years of experience in the fields of computer science and applied cryptography. My professional career has been dedicated to issues relating to software, networks, and computer systems more generally.

5. I received a Bachelor of Science in Computer Science with Honors from the University of Michigan in 1989, a Master of Science in Computer Science

and Engineering from the University of Michigan in 1991, and a Ph.D. in Computer Science and Engineering from the University of Michigan in 1994. My Ph.D. dissertation was titled “Nonmonotonic Cryptographic Protocols” and concerned authentication in long-running network operations.

6. I am a Professor Emeritus in Computer Science at Johns Hopkins University (the “University”). I joined the Computer Science faculty at the University in 2003 and was promoted to full professor with tenure in April 2004. As a member of the faculty, I perform research, teach graduate and undergraduate courses in computer science and related subjects, advise undergraduate and master’s students, and supervise the research of Ph.D. candidates and other students. I have taught courses including Networking, Security and Privacy in Computing, Cryptography, and Advanced Topics in Computer Security. In September 2023, I was appointed Professor Emeritus.

7. I also served as the Technical Director of the University’s Information Security Institute (“ISI”). The ISI is the University’s focal point for research and education in information security, assurance, and privacy. The University, through the ISI’s leadership, has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field.

8. I also have significant industry experience. Since 2011, I have served as the founder and chief scientist of Harbor Labs, a software and networking consulting firm specializing in data security and privacy. Previously, from 2005 to 2011, I served as the founder and President of Independent Security Evaluators (“ISE”), a computer security consulting firm. In that capacity, I guided ISE through the qualification process to become an independent testing laboratory for Consumer Union, which produces the Consumer Reports magazine. ISE provided consulting services to various companies on potential security flaws and weaknesses in products and systems. These companies included Fortify Software, Verdasys, and Security First Corp. As an independent testing laboratory for Consumer Union, I managed an annual project where we tested popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

9. In addition, I came to the University from AT&T Labs, Secure Systems Research Department, where I spent six years focused on Internet and computer security. Prior to AT&T Labs, I spent two years at Bellcore in its Cryptography and Network Security Research group, also focusing on Internet and computer security issues. I also interned at IBM in 1989. During my time there, I worked on the IBM System/360 family of mainframe computer systems.

10. I am the author or co-author of five books regarding information security issues: *Brave New Ballot*, Random House, 2006; *Firewalls and Internet Security* (second edition), Addison Wesley, 2003; *White-Hat Security Arsenal*, Addison Wesley, 2001; *Peer-to-Peer*, O'Reilly, 2001; and *Web Security Sourcebook*, John Wiley & Sons, 1997.

11. I have received numerous awards for my work and research in the field of computer security, including:

- In 2020, I received the Distinguished Service Award from the Institute of Electrical and Electronics Engineers (“IEEE”) Computer Society Technical Committee on Security and Privacy;
- In 2010, I received a Fulbright Scholarship to serve as a Visiting Professor at Tel Aviv University in Israel;
- In 2009, I received a Google Research Award for my work on securing medical records on smartphones;
- In 2007, I received the Privacy Enhancing Technologies Award for Outstanding Research for my work on a security analysis of a cryptographically enabled RFID device;
- In 2004, I was named Baltimorean of the Year by Baltimore Magazine for my work in safeguarding the election process;

- In 2004, I received the Electronic Frontiers Foundation Pioneer Award; and
- In 2000, I received the Best Paper Award at the 9th USENIX Security Symposium.

12. I serve, or have served, on several technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. In addition, I have been Associate Editor of the IEEE Security and Privacy Magazine and served as Associate Editor of the Association for Computing Machinery's ("ACM") Transactions on Internet Technology. I also served as Associate Editor of the journal Communications of the ACM, and I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of the Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors

of the USENIX Association (the leading academic computing systems society), and a member of the editorial board of the Bellcore Security Update Newsletter.

13. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics “Security of Electronic Voting” to Computer Security 2004 Mexico in Mexico City, Mexico, in May 2004; “Electronic Voting” to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington, D.C., in December 2003; “Security Problems on the Web” to the AT&T EUA Customer Conference in March 2000; and “Security on the Internet” to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and another TEDx talk on the same topic in September 2015.

14. I am a named inventor on 10 United States patents, including U.S. Patent Nos. 5,638,446 (“Method for the Secure Distribution of Electronic Files in a Distributed Environment”) and 5,809,140 (“Session Key Distribution Using Smart Cards”).

15. A detailed record of my professional qualifications is set forth in the attached Exhibit A, which is my *curriculum vitae*, including a list of publications, awards, research grants, and professional activities. My *curriculum vitae* also lists the matters in which I have served as an expert.

III. BASES OF OPINIONS

16. In the course of conducting my analysis and forming my opinions, I have reviewed materials including those listed below:

- i. U.S. Patent No. 10,452,854 (Ex. 1001) (“the ’854 patent” or “’854”);
- ii. The prosecution history of the ’854 Patent (Ex. 1002)
- iii. The Declaration signed by Samrat Bhattacharjee, Ph.D. in IPR2024-00215 (Ex. 1003) (the “Bhattacharjee Declaration”);
- iv. The Curriculum Vitae of Samrat Bhattacharjee, Ph.D. (Ex. 1004)
- v. The Petition by Google in IPR2024-00215;
- vi. U.S. Patent Application Publication 2004/0049687A1 (“Orsini”) (Ex. 1005);
- vii. U.S. Patent Application Publication 2003/0200176A1 (“Foster”) (Ex. 1006);
- viii. U.S. Patent Application Publication 2004/0216164A1 (“Hayhurst”) (Ex. 1007);
- ix. Security First Innovation’s 2023-08-14 Infringement Contentions, Chart A (Ex. 1009);
- x. Redline Comparison of U.S. Patent Application Publication 2004/0049687A1 to U.S. Patent No. 10,452,854 (Ex. 1010);
- xi. U.S. Patent No. 5,991,414 (Ex. 1011);

- xii. U.S. Patent Application Publication No. 2002/0169842 (Ex. 1012);
- xiii. U.S. Patent No. 6,393,568 (Ex. 1013);
- xiv. U.S. Patent No. 6,868,160 (Ex. 1014);
- xv. U.S. Patent Application Publication No. 2006/0053112 (Ex. 1015);
- xvi. U.S. Patent Application Publication No. 2004/0005061 (Ex. 1016);
- xvii. U.S. Patent No. 5,412,722 (Ex. 1017);
- xviii. U.S. Patent No. 7,689,829 (Ex. 1018);
- xix. U.S. Patent Application Publication No. 2003/0081784 (Ex. 1019);
- xx. U.S. Patent No. 7,634,650 (Ex. 1020);
- xxi. U.S. Patent Application Publication No. 2004/0143733 (Ex. 1021);
- xxii. U.S. Patent Application Publication No. 2002/0126850 (Ex. 1022);
- xxiii. U.S. Patent No. 5,812,671 (Ex. 1023);
- xxiv. U.S. Patent Application Publication No. 2003/0012386 (Ex. 1024);
- xxv. U.S. Patent No. 5,963,646 (Ex. 1025);
- xxvi. U.S. Patent No. 5,416,841 (Ex. 1026);
- xxvii. U.S. Patent No. 7,251,828 (Ex. 1027);
- xxviii. U.S. Patent Application Publication No. 2003/0167314 (Ex.
1028);
- xxix. U.S. Patent No. 6,598,161 (Ex. 1029);
- xxx. U.S. Patent Application Publication No. 2005/0198490 (Ex. 1030);

- xxxi. U.S. Patent Application Publication No. 2002/0169808 (Ex. 1031);
- xxxii. U.S. Patent No. 6,345,101 (Ex. 1032);
- xxxiii. U.S. Patent No. 8,707,034 (Ex. 1033);
- xxxiv. U.S. Patent Application Publication No. 2003/0105719 (Ex. 1034);
- xxxv. U.S. Patent No. 4,238,853 (Ex. 1035);
- xxxvi. U.S. Patent No. 6,819,766 (Ex. 1036);
- xxxvii. U.S. Patent Application Publication No. 2004/0172476 (Ex. 1037);
- xxxviii. U.S. Patent Application Publication No. 2004/0177257 (Ex. 1038);
- xxxix. U.S. Patent No. 7,885,405 (Ex. 1039);
- xl. U.S. Patent Application Publication No. 2005/0210269 (Ex. 1040);
- xli. U.S. Patent Application Publication No. 2005/0120065 (Ex. 1041);
- xlii. U.S. Patent Application Publication No. 2001/0037474 (Ex. 1043);
- xliii. U.S. Patent Application Publication No. 2003/0191938 (Ex. 1044);
- xliv. U.S. Patent Application Publication No. 2003/0028493 (Ex. 1045);
- xlv. U.S. Patent Application Publication No. 2003/0016820 (Ex. 1046);
- xlvi. U.S. Patent Application Publication No. 2002/0042859 (Ex. 1047);
- xlvii. U.S. Patent Application Publication No. 2003/0188153 (Ex. 1048);
- xlviii. PCT Application Publication No. WO 2004/057461 (Ex. 1049);

- xlix. U.S. Patent No. 7,529,834 (Ex. 1050);
- l. U.S. Patent Application Publication No. 2006/0034457 (Ex. 1051);
- li. U.S. Patent Application Publication No. 2005/0256972 (Ex. 1052);
- lii. U.S. Patent Application Publication No. 2004/0049700 (Ex. 1053);
- liii. U.S. Patent No. 5,675,653 (Ex. 1054);
- liv. U.S. Patent Application Publication No. 2006/0062384 (Ex. 1055);
- lv. U.S. Patent No. 6,490,353 (Ex. 1056);
- lvi. U.S. Patent Application Publication No. 2006/0059347 (Ex. 1061);
- lvii. U.S. Patent Application Publication No. 2006/0064386 (Ex. 1062);
- lviii. Google LLC's Proposed Claim Terms for Construction (Ex. 1064);
- lix. Letter from A. Mayron to D. Perlson re Preliminary Proposed
Constructions (Ex. 1065);
- lx. U.S. Patent Application Publication No. 2004/0228479 (Ex. 1066);
- lxi. U.S. Patent Application Publication No. 2004/0039925 (Ex. 1067);
- lxii. The Institution Decision in IPR2024-00215;
- lxiii. The exhibits and other documents cited herein.

IV. APPLICABLE LEGAL STANDARDS

A. Level Of Ordinary Skill In The Art

17. My opinions in this declaration are based on the understandings of a person of ordinary skill in the art, which I understand is sometimes referred to as

an “ordinary artisan” or by the acronyms “POSITA” or “PHOSITA,” as of the time of the invention, which I understand is here assumed to be the effective filing date (November 18, 2005) of the provisional application from which the ’854 patent issued. I understand that the person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. By “relevant,” I mean relevant to the challenged claims of the ’854 patent.

18. I understand that factual indicators of the level of ordinary skill in the art include the various prior art approaches employed, the types of problems encountered in the art, the rapidity with which innovations are made, the sophistication of the technology involved, and the educational background of those actively working in the field. I understand that, in assessing the level of skill of a person of ordinary skill in the art, one should consider the type of problems encountered in the art, the prior solutions to those problems found in the prior art references, the rapidity with which innovations are made, the sophistication of the technology, the level of education of active workers in the field, and my own experience working with those of skill in the art at the time of the invention.

19. In this case, Dr. Bhattacharjee has asserted in his declaration that a person of ordinary skill in the art as of the time of the ’854 patent would have had:
at least a bachelor’s degree in computer science, computer engineering,
or a related field, with three (3) years of experience in the area of

securing data from unauthorized access or use. A higher level of education may substitute for less experience.

Ex. 1003 [Bhattacharjee-Decl.] ¶ 40.

20. For the purposes of this declaration, I accept Dr. Bhattacharjee's proposed qualifications of a POSITA.

21. As further discussed below, my opinions as stated in this declaration are valid even if the Board adopts a slightly different level of ordinary skill in the art. For example, as will be discussed throughout my report, even a person with the level of knowledge or experience described by Dr. Bhattacharjee or adopted by the Board would not have a reasonable expectation of success in implementing certain aspects of the proposed combination as of the priority date of the '854 patent.

B. My Understanding Of Legal Standards

22. When considering the '854 patent and stating my opinions, I rely on the following legal standards as described to me by the attorneys for SFI.

23. I understand that a patent claim is unpatentable if the claimed invention was anticipated by a prior art reference or would have been obvious to a person of ordinary skill in the art at the time of the purported invention.

24. I understand that anticipation requires that every limitation of the claim at issue be disclosed, either expressly or under principles of inherency, in a single prior art reference.

25. I understand that inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. Instead, it must be proved that the claim limitation not expressly found in the reference necessarily follows from what is found there.

26. I understand that an obviousness analysis involves comparing a claim to the prior art to determine whether the claimed invention would have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art and in light of the general knowledge in the art as a whole. I also understand that obviousness is ultimately a legal conclusion based on underlying facts of four general types, all of which must be considered: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective indicia of non-obviousness, including any praise of the invention.

27. I also understand that obviousness may be established under certain circumstances by combining or modifying the teachings of the prior art. Specific teachings, suggestions, or motivations to combine any first prior art reference with a second prior art reference can be explicit or implicit, but must have existed

before the date of purported invention. I understand that prior art references themselves may be one source of a specific teaching or suggestion to combine features of the prior art, but that such suggestions or motivations to combine art may come from the knowledge that a person of ordinary skill in the art would have had.

28. I understand that a reference may be relied upon for all that it teaches, including uses beyond its primary purpose, but also including teachings that lead away from the invention. I understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, although the mere disclosure of alternative designs does not teach away.

29. I further understand that whether there is a reasonable expectation of success in combining references in a particular way is also relevant to the analysis.

30. I understand that it is improper to use hindsight to combine references or elements of references to reconstruct the invention using the claims as a guide. My analysis of the prior art is made from the perspective of a person of ordinary skill in the art at the time of the invention.

31. I understand that in order to be eligible as prior art and therefore form a reference in one of the instituted grounds, a reference must be analogous art to the '854 patent. I also understand that it is Petitioner's burden to prove that their

asserted references are analogous art to the '854 patent. I am informed that in order to determine whether a reference is analogous art to the '854 patent, a two-part test is applied as follows:

Two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

In re Bigio, 381 F.3d 1320, 1325 (Fed. Cir. 2004); *see also In re Clay*, 966 F.2d 656, 658 (Fed. Cir. 1992). I have been informed and understand that to discern the field of endeavor, courts have looked to the specifications of the patent and the alleged prior art reference and particularly to the respective “background of Invention” and/or “field of the invention” sections. *See, e.g., In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979) (determining field of endeavor based on “Background of Invention”); *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1237-38 (Fed. Cir. 2010) (finding reference concerning padlocks to be in the same field of endeavor where the “patent itself refers to ‘the prior art padlock’ in the background of the invention”); *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1381 n. 8 (Fed. Cir. 2019) (“[T]he specification of each reference includes a ‘Field of the Invention’ section that distinctly describes each applicable field of endeavor.”).

32. I am not offering any legal opinions in this declaration nor am I qualified to do so. I only consider such legal standards in framing my opinions and conclusions as well as placing assertions made by Petitioner in the Petition into the proper context. Additionally, from a subject matter perspective, I understand that the petitioner always has the burden of persuasion regarding a challenge of patentability of an invention under an inter partes review.

V. CLAIMS-AT-ISSUE (CLAIMS 1-10)

33. I understand that Petitioner has challenged independent claim 1 and its dependents based on anticipation and/or obviousness over Orsini (Ground 1) and obviousness over Foster combined with Hayhurst (Ground 2).

VI. OPINIONS

A. Petitioner's Orsini Ground Fails (All Claims, Ground 1).

1. Prior Opinions Offered

34. I have previously submitted a preliminary declaration in this case. For convenience, I include the testimony from my preliminary declaration with regard to the Orsini Ground.

a. The '854 And Orsini

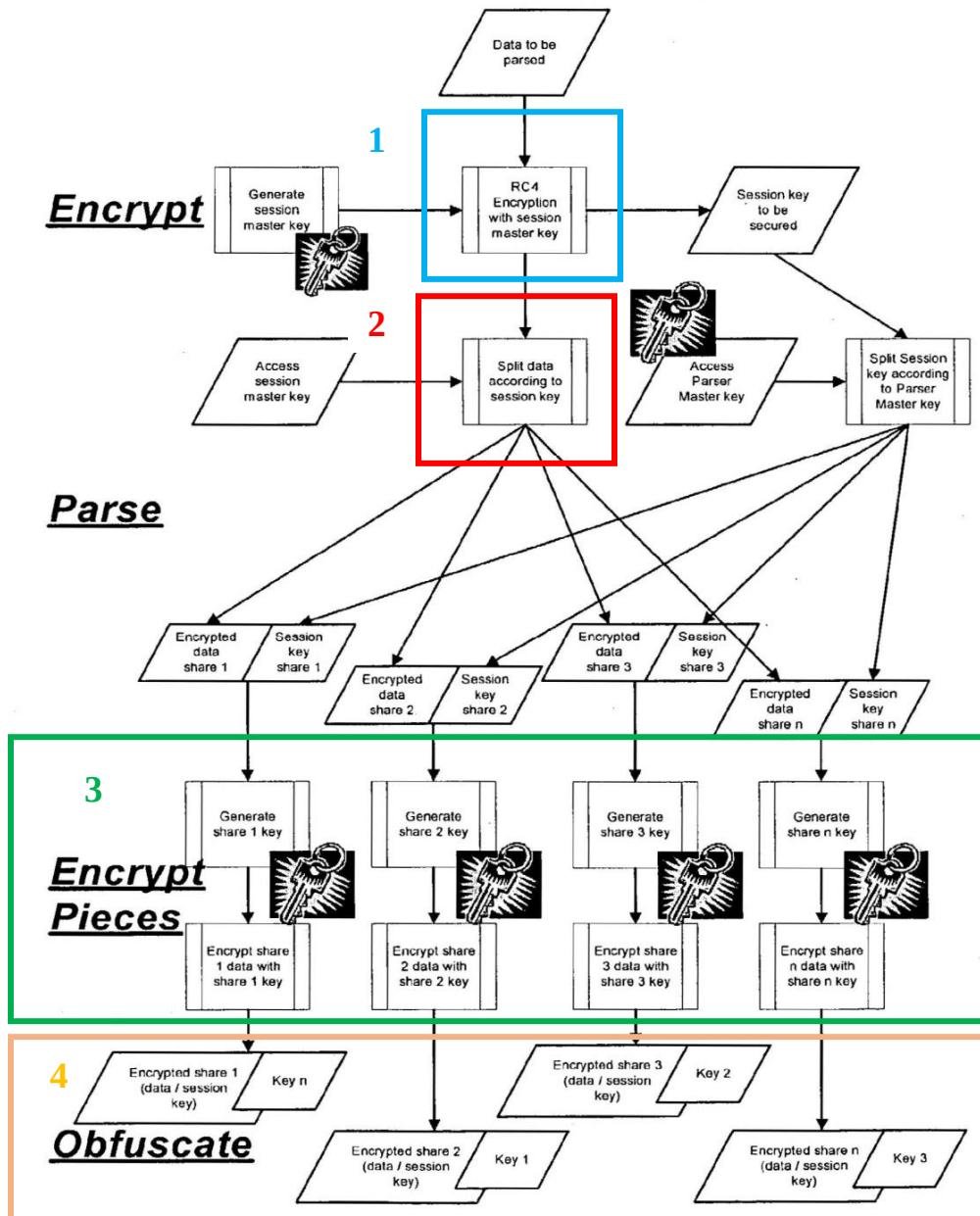
35. I have been informed and understand that Orsini Patent Owner's patent application with three out of four named inventors in common. I also understand that Orsini was disclosed to the Examiner in an IDS. Ex. 1002 ['854-FH] 66. While Orsini's Figures 1-25 and paragraphs 1-423 are largely included in

the '854's specification, the '854 includes **17 new figures and over eighteen columns of additional material** (~10,500 words) which contain significant improvements over Orsini's methods. See Ex. 1001 ['854] Figs. 26-41, 6:44-6:62, 8:10-8:61, 66:4-83:10.

36. Petitioner's Ground 1 almost entirely relies upon the dataset-securing method disclosed in Figure 21 of Orsini. *E.g.*, Pet., 8-15, 17, 29-30, 31, 45-46. Orsini's Figure 21 and the '854's claim 1 are each directed to methods for securing a "dataset." Both methods rely, in part, on dividing the dataset into pieces (called "chunks" or "shares" in the '854) and encrypting the chunks. But the methods diverge from here. Figure 21's method of securing data is centered around encrypting a dataset with a "session master key," parsing the dataset and the session master key into shares, applying a share key to each of the shares, and then storing the share keys with a share it was not used to encrypt.

37. As can be seen below, Figure 21 teaches **(1) encrypting the entire data set with the session master key**, **(2) parsing the data set and session master key into shares**, then **(3) encrypting those shares and split session master key with a set of share keys** followed by a **(4) non-cryptographic** step:

Figure 21



Ex. 1005 [Orsini] Fig. 21 (annotated), [0293].

38. Figure 21's attendant description discloses the steps of "[g]enerating a session master key, encrypt[ing] the [dataset]" with the session master key using RC4 encryption, splitting the encrypted data set into a number of shares or chunks,

breaking the session master key into the same number of pieces, and combining the pieces with the shares. Ex. 1005 [Orsini] [0294]-[0297]. Subsequently, “share keys” are generated for each of the shares, and used to encrypt each share/session master key-piece combination. *Id.*, [0298]. Finally, the share keys are hidden by “stor[ing] the [share] keys in different locations from the . . . shares” they encrypt such that “Share 1 gets Key 4, Share 2 gets Key 1, Share 3 gets Key 2, Share 4 gets Key 3.” *Id.*, [0299].

39. The end result of Orsini’s Figure 21’s method is that a piece of the “session master key” used to encrypt the original, undivided dataset is stored in each of the shares, and all of the shares (including a piece of the session master key) are themselves encrypted with a “share key.” Each share key is then hidden by storing it with a share that the key cannot decrypt. Thus, to reconstruct a dataset secured by Figure 21’s method, one can: (a) collect each of the shares together, (b) use the unencrypted share keys to decrypt the pieces of the encrypted dataset and session master key in the shares, (c) reconstruct the encrypted data set and the session master key, and (d) use the reconstructed session master key to decrypt the dataset.

40. The inventors of the ’854 appear to have realized that Orsini’s Figure 21 method potentially allows an attacker to reconstruct the dataset if the attacker

has access to each of the shares. In accord, the '854's claimed inventions eliminate that potential vulnerability.

41. Orsini's Figure 21 merely hides the keys used to encrypt the data chunks by storing each key with a chunk it was not used to encrypt. Ex. 1005 [Orsini] [0299]. Orsini's non-cryptographic approach, however, cannot protect a dataset if an attacker has access to all of the shares (and thus access to all of the share keys) and can therefore reveal the share keys and use them to decrypt the corresponding shares. In that case, reconstruction of the original dataset becomes straight-forward. Orsini's Figure 21 does not teach any method of "further securing" the dataset after the data shares have been encrypted with the share keys other than by hiding the share keys with different shares.

42. The '854 teaches further securing the share keys with an encryption operation "with a workgroup key," explaining that "[t]he workgroup key concept allows for enhanced protection of information assets by encrypting information stored within the shares." Ex. 1001 ['854] 79:66-80:1. Beneficially, "[o]nce this operation is performed, even if all required shares and external keys are discovered, an attacker has no hope of recreating the information without access to the workgroup key." *Id.*, 80:1-4. Thus, the '854 introduces an "external key" (*i.e.*, the workgroup key) used in an encryption operation to further secure data, and teaches the benefits of this approach. *See also id.*, Fig. 39, 80:30-33.

43. Consequently, the '854 discloses and claims a materially different and improved method for securing a dataset from that disclosed in Orsini that addresses a potential weakness in Figure 21's method. Among other differences, claim 1 of the '854 uses key-based cryptography to further secure the encrypted shares after they are created, a step that is not disclosed in Orsini (which merely hides the keys used to encrypt the shares among the shares themselves). Thus, Orsini does not disclose the new step of "performing an encryption operation based on the external key" after the data set has been split into shares/chunks and those shares have been individually encrypted with an encryption key.

44. Moreover, as I further discuss below, according to Petitioner's mapping, Figure 21's method is simply incompatible with claim 1 and cannot render it obvious. Petitioner equates the claimed "external key" (*i.e.*, the workgroup key) with the "session master key" of Orsini's Figure 21. In other words, under Petitioner's interpretation, the operation to "further secure" the dataset after encrypting the shares is based on the session master key. But, as I previously discussed, in Figure 21, the session master key is divided into pieces, the pieces are integrated into the shares, and then the session master/share combinations are encrypted with the share keys. Thus, 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. If the session master key is used in an "encryption operation" to "further secure the plurality of data chunks" as Petitioner suggests, a priori knowledge of the session master key would be needed to unpack the encrypted shares. This 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.

b. *"Performing An Encryption Operation Based On The External Key To Further Secure The Plurality Of Data Chunks" (Limitation 1[c]).*

45. Claim 1 requires:

Limitation 1[b] "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,"

Limitation 1[b][3] "encrypting each of the shares with a respective one of the plurality of distinct encryption keys,"

Limitation 1[c] "performing an encryption operation based on the external key to further secure the plurality of data chunks."

46. I note that the parties appear to agree that claim 1 requires the generation of data chunks from a data set, and that the data chunks must first be encrypted with a distinct encryption key before the plurality of data chunks is "**further** secur[ed]" with "an **encryption** operation based on the external key."

Pet., 14 (“claim 1 recites an encryption step with an encryption key (specifically, an ‘external key’) that occurs after a step corresponding to the ‘encrypt pieces’ stage”), 33-39. This is consistent with Petitioner’s proposed claim construction in District Court. Ex. 1064 [Petitioner-Proposed-Claim-Construction] 16 (claim 1 steps “must be performed in order”). In my opinion, without being already “encrypt[ed] ... with a distinct encryption key,” the plurality of data chunks could not be “*further* secure[d]” with an “encryption operation based on the external key.”

47. I do not believe Petitioner and Dr. Bhattacharjee have demonstrated that Orsini anticipates or render obvious “performing an encryption operation based on the external key to further secure the plurality of data chunks.”

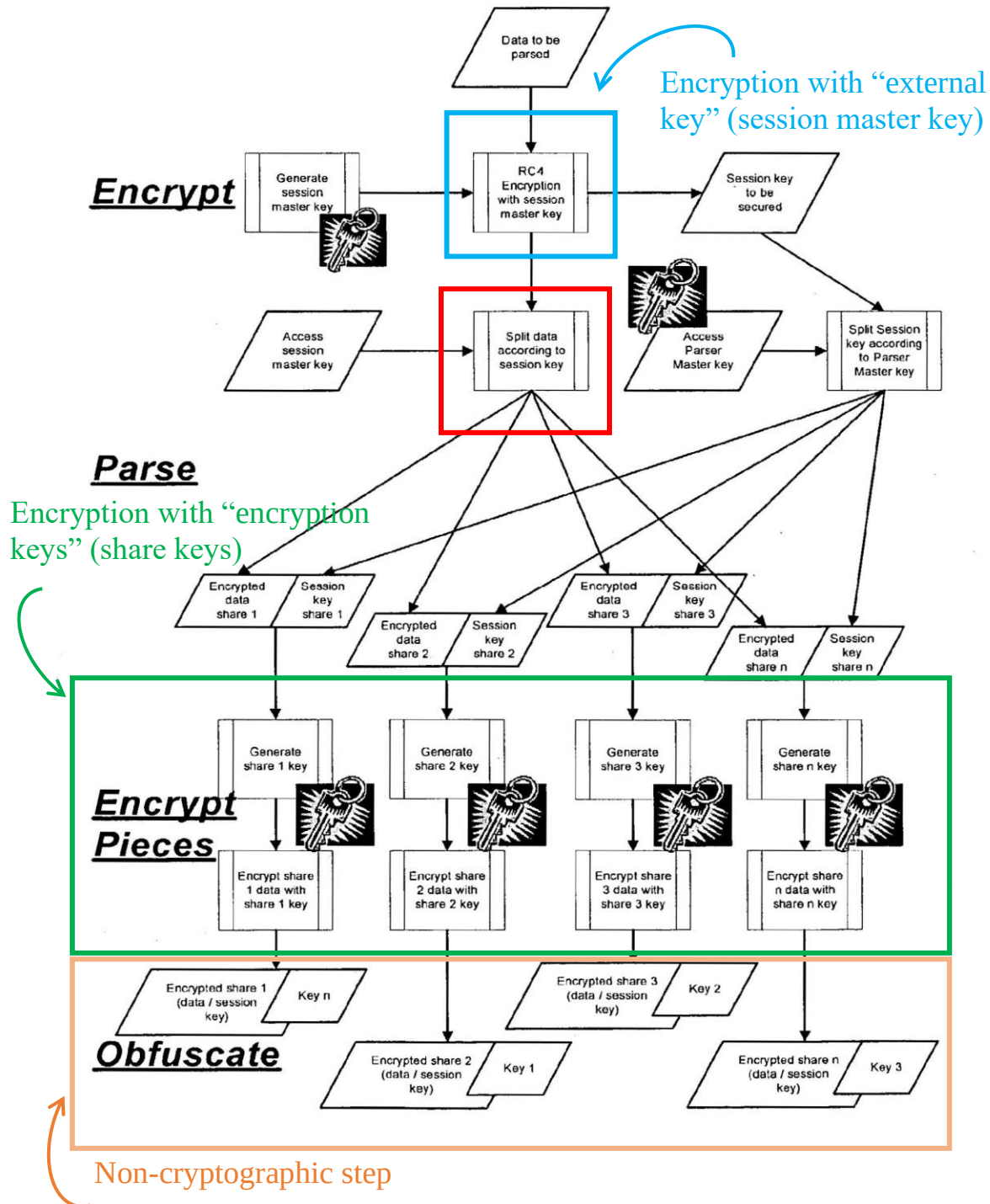
i. Orsini Does Not Anticipate Claim 1.

48. To reiterate, Petitioner and Dr. Bhattacharjee allege that Orsini’s Figure 21 anticipates claim 1. Pet., 8-15; Ex. 1003 [Bhattacharjee-Decl.] ¶¶ 50-59. In my opinion, however, Figure 21 does not disclose, either expressly or inherently, “performing an encryption operation ***based on the external key*** to ***further secure the plurality of data chunks***” after generating chunks from a data set and encrypting the chunks.

49. Assuming, as Petitioner does (*e.g.*, Pet., 10, 17, 33-38) that Orsini’s “session master key” corresponds to the claimed “external key,” Figure 21

undisputedly teaches **an encryption operation performed on the entire data set** **with the session master key** (an “external key”) ***before* parsing the data set and session master key into shares** and **encrypting those shares and split session master key with a set of share keys**. And any additional protection of the data chunks is achieved through a **non-cryptographic step**:

Figure 21

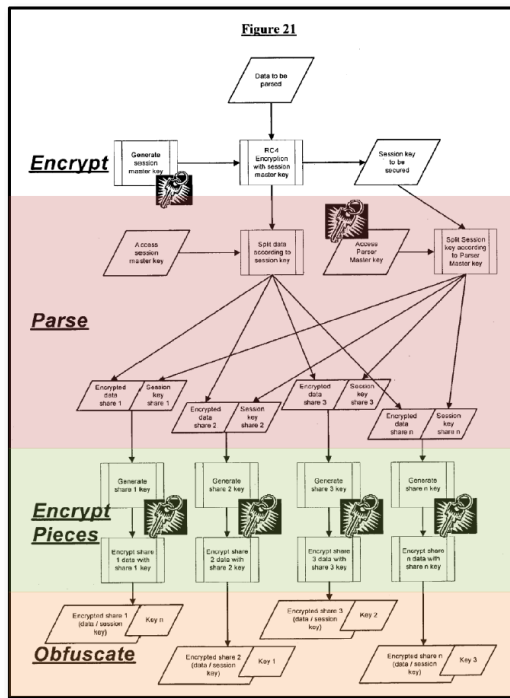


Ex. 1006 [Foster] Fig. 21 (annotated).

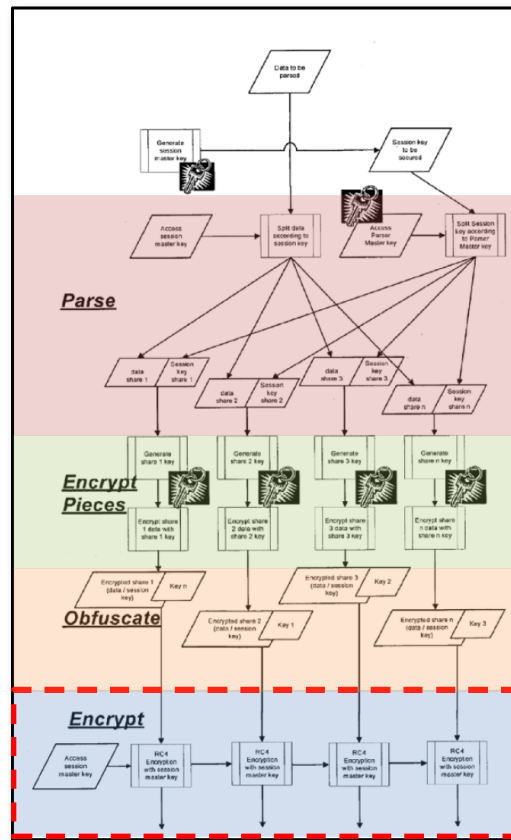
50. Orsini, however, does not disclose performing any “encryption operation . . . to further secure the plurality of data chunks” “based on the external [session master] key.” Indeed, Orsini ***cannot disclose this***, because in Figure 21, after the session master key/external key is used to encrypt the dataset as a whole, it is “separat[ed]” along with the data set and those “portions of the session master key” are “contain[ed]” in the chunks/shares of data which are then encrypted. Ex. 1005 [Orsini] [0293], [0297]-[0299]; *compare id. with* Ex. 1001 [’854] 80:30-33 (using workgroup key instead of session master key). Consequently, by the time the data set has been parsed into shares and those shares have been encrypted, the session master key (*i.e.*, the alleged “external key”) cannot be used for an encryption operation without removing the benefits provided from Orsini’s splitting and encrypting of that key.

51. Indeed, I note that rather than point to any actual disclosure in Orsini, Petitioner and Dr. Bhattacharjee must ***alter*** Figure 21 to add another, undisclosed, chunk encryption step, this time using the session master key, after the data chunks are generated and encrypted a first time with distinct encryption keys. For example, Petitioner and Dr. Bhattacharjee illustrate a “different order” version of Figure 21:

Original

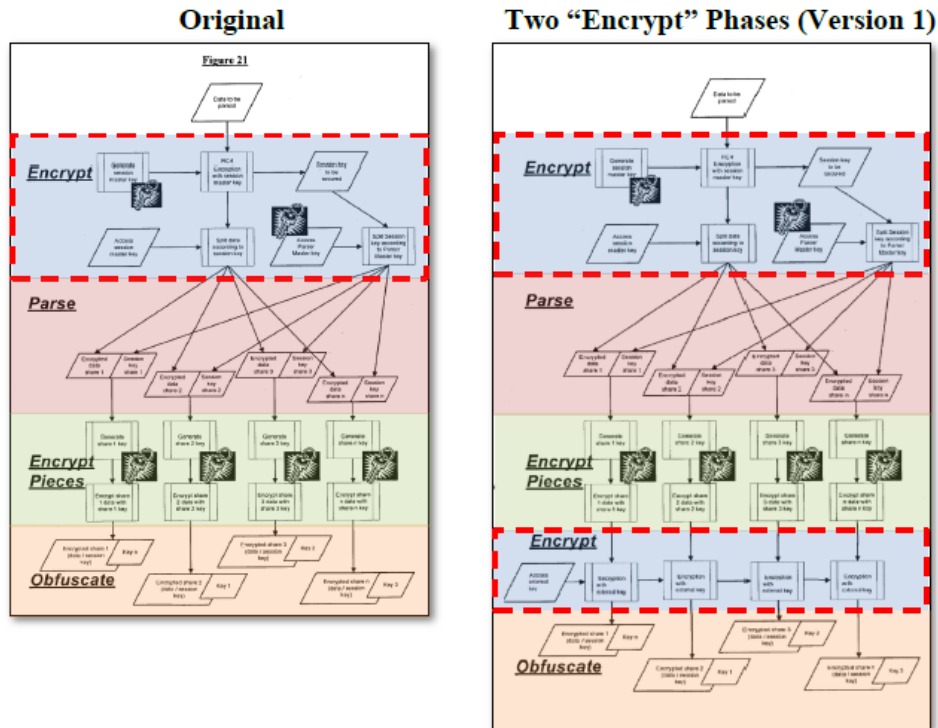


Different Order (Version 1)



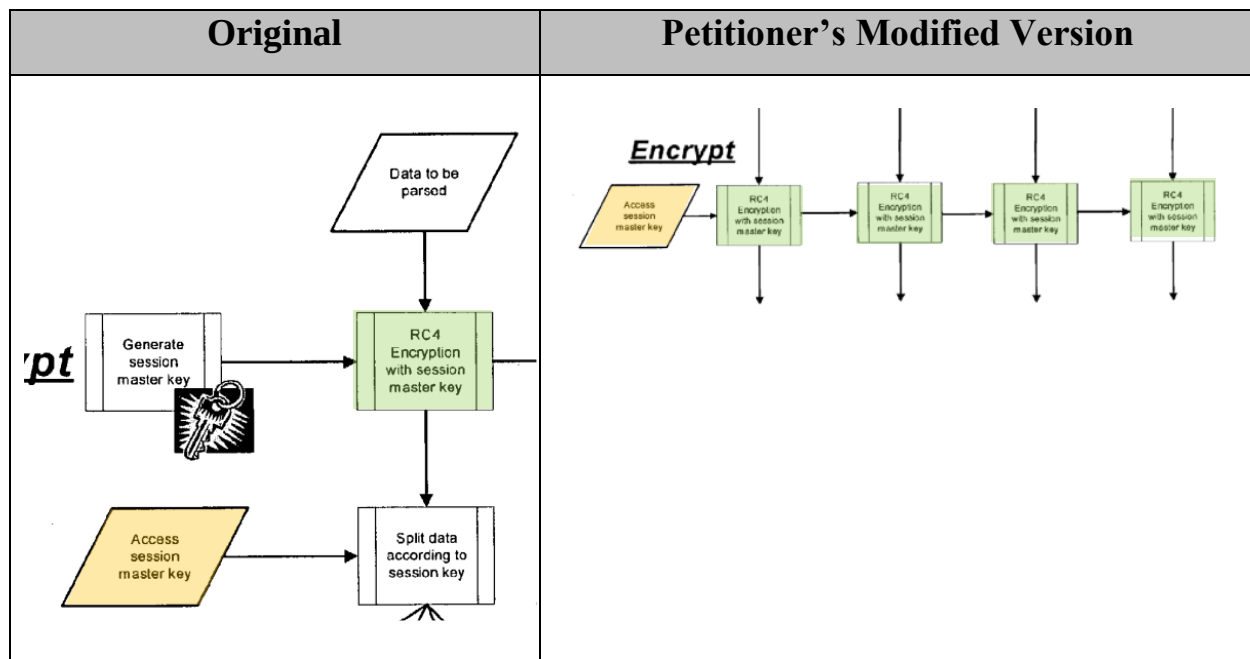
Pet., 34-35; Ex. 1003 [Bhattacharjee-Decl.] ¶¶ 112-113. Petitioner and Dr.

Bhattacharjee also illustrate “two ‘encrypt’ phases” versions of Figure 21:



Pet., 37-38; Ex. 1003 [Bhattacharjee-Decl.] ¶ 117.

52. As shown below, not only does Petitioner and Dr. Bhattacharjee move (or copy and move) the dataset encryption step from the beginning of Figure 21 to the end, but they also then re-write the step **to apply to each of the chunks rather than to the dataset as a whole**. Thus, Petitioner and Dr. Bhattacharjee not merely reorder Figure 21, they fundamentally alter what is being encrypted (the dataset versus the shares). Petitioner and Dr. Bhattacharjee additionally move the step **wherein the session master key is accessed from prior to the data being parsed to after the non-cryptographic step**.



53. The claims require generating data chunks from the data set (1[b]), then encrypting those data chunks with distinct encryption keys (1[b3]), and only then “performing an encryption operation based on the external key to further secure the plurality of data chunks” (1[c]). Thus, Orsini cannot satisfy claim 1 merely by reordering an encryption step from before splitting the data set to after. Indeed, Orsini’s Figure 21 already teaches encrypting data chunks after the data set is split with distinct encryption keys. Ex. 1005 [Orsini] [0299] (Step “5. Encrypting each share”). Rather, the claims require another encryption operation based on the external key to “*further* secure” the data chunks *after* those data chunks are already encrypted.

54. Petitioner and Dr. Bhattacharjee rely upon Orsini’s statement that “certain steps of the methods described herein may be performed in different order, or repeated multiple times, as desired.” Pet., 33 (citing Ex. 1005 [Orsini] [0301]). This statement, however, does not necessarily disclose that the parsed data would be further encrypted using the encryption/session master key as Petitioner argues it does. Indeed, neither parsed data nor the session master key is even mentioned in this statement.

55. Orsini, moreover, only specifies that “**certain** steps” “may be performed in different order.” Ex. 1005 [Orsini] [0301]. Orsini does not teach that the encryption of the data set step is one such step. Rather, Orsini discloses that “[f]or example, multiple parsing steps may be performed on only one portion of the parsed data,” and that “[e]ach portion of parsed data may uniquely secured.” *Id.* Orsini, therefore, only identifies the parsing and encryption with the plurality of distinct encryption keys as steps which may be repeated or reordered, and on “only one portion of the parsed data” at a time at that. There is simply no disclosure that would necessitate that the data chunks, after already being individually encrypted with the alleged plurality of distinct encryption keys, would be encrypted again, let alone with the alleged external key, or that the “plurality of data chunks” rather than an individual data chunk would be encrypted based on the external key. Indeed, a POSITA 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.

56. I note that, moreover, Petitioner does not, and cannot, point to any step in Orsini that could be “performed in a different order” or “repeated” to achieve the limitations of claim 1. No matter how many times one repeats the step of encrypting ***the original data set*** using the session master key, and regardless of the order in which that step is carried out, it cannot disclose encrypting ***the chunks***, as Petitioner contends is a way of meeting the “further securing” step of claim 1.

57. Additionally, I understand that Petitioner points to certain dependent claims in Orsini that claim encrypting shares/chunks a second time using “a different encryption algorithm.” Pet., 35 (citing Ex. 1001 [’854] cls. 12, 29, 39).

58. Dependent claims 12, 29, and 39, directed to repeating encryption of shares with a “different encryption algorithm,” do not disclose claim 1, which requires that the encrypted data shares undergo an “encryption operation ***based on the external key*** to further secure the plurality of data chunks.” Simply repeating encryption using a “different algorithm” does not even suggest, much less necessarily disclose, that the “different algorithm” would be based on the session

master key. *See* Ex. 1005 [Orsini] [0071] (explaining “a wide number of algorithms [are] available”).

59. None of the claims that Petitioner cites claim Orsini’s Figure 21 embodiment. Again, Orsini’s Figure 21 describes encrypting a data set with a session master key, splitting the data set and session master key into shares, encrypting those shares with respective share keys, and then storing the shares with a share key not used to encrypt it. Ex. 1005 [Orsini] Fig. 21, [0295]-[0299]. The claims Petitioner cites, however, are each far afield of Figure 21. For example, claim 10, from which claim 12 depends, does not even involve a master key or another set of keys with which to encrypt the data or a step hiding the share keys with different shares. *Compare id.* [0294] (embodiment for “stor[ing] the session master key with the parsed data”), [0295]-[0299] (describing “[g]enerating a session master key and encrypt[ing] the data,” “generat[ing] a stream cipher key for each of the four data shares,” and “[e]ncrypting each share”) *with* cl. 10. Similarly, claims 20 and 30 (from which claims 29 and 39 depend) do not require generating a key for each of the data portions and are also missing the step hiding the share keys. Thus, the dependent claims Petitioner cites are not even relevant to what Figure 21 may or may not disclose.

60. Finally, Petitioner and Dr. Bhattacharjee also argue that Orsini’s public keys are the claimed “external key.” I disagree.

61. Petitioner and Dr. Bhattacharjee argue that Orsini discloses “public encryption keys” used “to further encrypt already-encrypted ‘data chunks.’” Pet., 38-39 (citing Ex. 1005 [Orsini] [0095], [0097], [0107], [0119], [0172]). Orsini’s discussion of “public encryption keys” arise in separate embodiments, unrelated to Orsini’s Figure 21 embodiment. Indeed, Petitioner relies upon descriptions of Figures 4- 6, 8, and 12. Pet., 38-39. These are all unrelated to Figure 21, which discloses “a process for parsing, splitting or separating data with encryption and storage of the encryption master key with the data.” *Id.*, [0054]. None of Petitioner’s cited figures describe encrypting a dataset with a session master key, parsing the dataset and session master key into shares, encrypting those shares with share keys, and storing the shares with a share key not used to encrypt it. *Compare id.*, [0095], [0097], [0107], [0119], [0172] *with* [0293]-[0299].

62. Orsini’s depository or data storage facility teachings (Ex. 1005 [Orsini] [0095], [0097], [0119]) are of no help as Petitioner does not allege that the claimed data chunks are stored there. Indeed, Petitioner maps the “plurality of storage devices” to Orsini’s “storage devices” rather than Orsini’s “data depositories” and never argues that Orsini’s storage devices can perform public-key encryption. See Pet., 46; Ex. 1005 [Orsini] [0095] (“**depository** 210” can “encrypt[] with public key encryption” “incoming and outgoing communications.”); [0097] (“data from the transaction engine 205 or the

depository 210, which was encrypted with a corresponding public key”); [0119] (“public key encryption may be used to further secure the data **at the data storage facilities.**”). Therefore, Petitioner has not identified any entity in Figure 21 that performs public-key encryption. The claim, moreover, requires “performing **an** encryption operation based on the external key to further secure the **plurality of data chunks.**” Assuming for the sake of argument that the encrypted chunks are eventually distributed and stored on the depository or data storage facilities, an encryption step performed at a depository or data storage facility would only secure a single chunk rather than “the plurality of data chunks.”

63. Petitioner also cites Ex. 1005 [Orsini] [0097] and [0172], but these do not disclose public-key encryption of already-encrypted chunks/shares. *See id.*, [0097] (“**data** from the transaction engine 205 or the depository 210, which was encrypted with a corresponding public key”); [0172] (“the requesting application or vendor uses the public key of the user, for example, to encrypt the session key that will be used to encrypt the **document or message**”). Indeed, these embodiments never parse data into chunks or shares, let alone encrypt chunks with distinct encryption keys and then perform an encryption operation based on an external key to further secure the plurality of chunks. *Id.*, [0097], [0168]-[0172].

ii. Orsini Does Not Render Claim 1 Obvious.

64. I understand that Petitioner and Dr. Bhattacharjee “alternatively” contend that Orsini renders claim 1 obvious. Pet., 39-44; Ex. 1003 [Bhattacharjee-Decl.] ¶¶ 120-134. In my opinion, they have failed to demonstrate so.

65. I have been informed and understand that in single-reference obviousness, when a missing limitation goes to the heart of an invention, review of any purported reasoned basis for resort to common sense must be especially searching. Moreover, common sense used to supply a missing limitation can be used only when the missing limitation is unusually simple and the technology particularly straightforward.

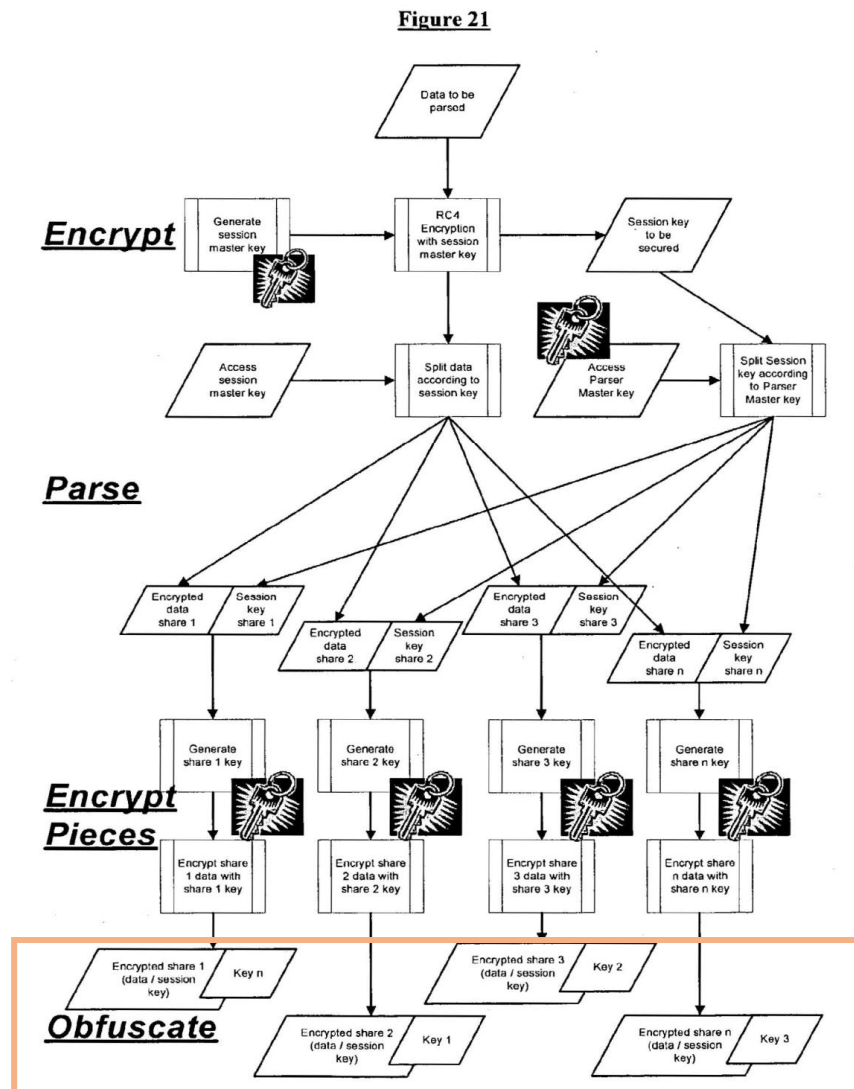
66. The inventions-at-issue concern cryptography, which is a technologically-involved and complex field involving incredibly high stakes and safeguarding against a wide variety of highly sophisticated and ever-evolving cybersecurity attacks. As internationally-renowned cryptologist Bruce Schneier (Ex. 2005 [Schneier-CV]) has observed “[f]ew can do the science [of cryptography] properly” and “[g]ood cryptographers know that nothing substitutes for extensive peer review and years of analysis.” Ex. 2006 [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks] 3.

67. And, as previously discussed, the ’854’s new teachings and the claimed inventions arose from the inventor’s insight regarding a potential

vulnerability in Orsini’s Figure 21 approach wherein if an attacker obtains each of the shares, the dataset can be reconstructed. The ’854 eliminates this vulnerability by encrypting the encryption keys using a workgroup key—corresponding to the “external key” of claim 1—a technique not disclosed in Orsini. The workgroup key provides “enhanced protection of information assets by encrypting key information stored within the shares” (Ex. 1001 [’854] 79:66-80:1) adding “an extra level of security to a secured data set” (*id.*, 77:22-23). As the ’854 explains “even if all required shares and external keys are discovered, an attacker has no hope of recreating the information without access to the workgroup key.” *Id.*, 80:1-4. Thus, this limitation goes to the heart of the invention. Moreover, given the benefits associated with the “workgroup key” delineated in the ’854, it further seems clear that the inventors of the ’854 (and Orsini) considered the “workgroup key” concept to be a fundamentally different approach that solved a problem that Orsini did not recognize or address.

68. Petitioner argues that “POSAs would have been motivated” by Orsini’s disclosures to add “performing an encryption operation based on the external key to further secure the plurality of data chunks” because they “would have understood that doing so would provide additional security and efficiency benefits.” Pet., 39-40. In my opinion, Petitioner and Dr. Bhattacharjee have failed to prove so.

69. Orsini already teaches hiding the encryption key used to encrypt each data chunk with a different chunk through a **non-cryptographic process**, illustrated in Figure 21 below.



Ex. 1005 [Orsini] Fig. 21. As can be seen in Figure 21, in this step, the system “store[s] the encryption keys in different locations from the encrypted data portions or shares ...” *Id.*, [0299]; see also [0353] (“it may not be desired to have any one depository contain enough information to decrypt the information held there, so the

key required to decrypt the share is stored in a different data depository.”); [0396]; cl. 26.

70. As Petitioner does not dispute, the step taught in Orsini’s Figure 21 is not an encryption operation (much less one involving the external key). *See generally* Pet.; Ex. 1003 [Bhattacharjee-Decl.]. As there is no encryption scheme or “scrambling” or altering of the data or the alleged distinct encryption keys (Ex. 2007 [Katz] 4), it cannot be an encryption operation.

71. I do not see any explanation from Petitioner or Dr. Bhattacharjee of why a POSITA would be motivated to modify Orsini using other allegedly “known” methods, particularly when it non-cryptographically hides each share key with a share it did not encrypt. Indeed, I note that Orsini teaches that its method provides a “comprehensive package for data security.” Ex. 1005 [Orsini] [0380] (“The data shares are then encrypted individually and the keys are stored safely with different encrypted shares. When combined, the entire process for securing data according to the methods disclosed herein becomes a comprehensive package for data security.”).

72. I note that Petitioner appears to indirectly criticize Orsini’s non-cryptographic approach by arguing that POSITAs “knew” that “cryptographic keys should never occur in clear form outside the cryptographic device” and that “when ‘encryption keys are included with the encrypted message’ ‘[s]ecurity’ comes from

‘encrypt[ing] the encryption keys themselves’ with ‘a key encryption key.’” Pet., 43 (citing Exs. 1035, 1036). In my opinion, however, these concerns are addressed by Orsini’s non-cryptographic step, by storing the keys, not with the encrypted message but rather “in different locations from the encrypted data portions or shares.” Ex. 1005 [Orsini] [0299]. Orsini teaches that this is sufficient because an attacker would not have “enough information to decrypt the” data chunk stored in each data depository. *Id.*, [0353]. Notably, in Figure 21’s data-securing method, the session master key, data chunks, and session keys are all either encrypted, parsed, and/or hidden, and thus each potentially vulnerable part of the encryption method is secured.

73. Thus, in my opinion, a POSITA would recognize that Orsini already employs a non-cryptographic method rather than an “encryption operation based on the external key to further secure the plurality of data chunks” as required by claim 1.

74. Simply concluding that adding an encryption layer would “benefit” Orsini’s method oversimplifies the myriad considerations a POSITA must make in cryptography, even for what may seem to be a “simple” or “small” change. For example, a POSITA would recognize that when fully considering the costs and benefits, an additional layer of encryption may not in reality benefit an encryption scheme or “further secure the plurality of the data chunks” as the claims require.

Rather, an additional encryption step may in fact introduce a weakness that an attacker can exploit. *See, e.g.*, Ex. 2007 [Katz] 22 (“As an example, an encryption scheme that has been proven secure ... might be implemented on a smart-card. It may then be possible for an adversary to monitor the power usage of the smartcard (e.g. how this power usage fluctuates over time) and use this information to determine the key.”); Ex. 2008 [Schneier-Security-Pitfalls-In-Cryptography] (“And just as it’s possible to build a weak structure using strong materials, it’s possible to build a weak cryptographic system using strong algorithms and protocols.”); Ex. 2009 [Anderson] (new computer “security systems have a nasty habit of backfiring”). One such weakness is in the critical area of key management, as it is where systems tend to be most vulnerable. *See* Ex. 2010 [Schneier-Applied-Cryptography] 169 (“In the real world, key management is the hardest part of cryptography. Designing secure cryptographic algorithms and protocols isn’t easy, but you can rely on a large body of academic research. Keeping the keys secret is much harder.”).

75. Thus, while adding an additional round of encryption with the same or additional keys may appear to provide improved security, doing so may, on balance, compromise security.

76. Petitioner’s proposal to “re-encrypt data chunks with an external encryption key” (Pet., 36-37) has significant security flaws. Ex. 2010 [Schneier-

Applied-Cryptography] 357 (“Encrypting a plaintext block twice with the same key, whether with the same algorithm or a different one, is not smart.”). If Orsini were modified such that the session master key (the alleged “external key”) were either reapplied or otherwise utilized after the data has been split, that would undermine Orsini’s method which protects the alleged external key by splitting it amongst the data shares. And it would entail further complications. By involving the session master key after the splitting process, Petitioner’s proposal would necessitate the key management and transport of the session master key, effectively making the division and inclusion of the session master key within the encrypted shares pointless. Under Orsini’s existing method, the master session key has already been parsed among the data shares and encrypted. Consequently, the session master key which was previously secured in Figure 21 would be unnecessarily exposed in this proposed modification. “Encrypting already-encrypted data chunks with the same encryption key,” thus, presents security vulnerabilities and complications that Petitioner and Dr. Bhattacharjee fail to account for.

77. Petitioner and Dr. Bhattacharjee also argue that a POSITA would modify Orsini’s Figure 21 to use a “group key,” “encryption key,” or “key-encryption key.” Pet., 40-44; Ex. 1003 [Bhattacharjee-Decl.] ¶¶ 124-133.

Petitioner and Dr. Bhattacharjee, however, fail to address the drawbacks associated with managing and securing such keys against discovery by an attacker.

78. Petitioner and Dr. Bhattacharjee argue that “Orsini provides ‘external **session** key management’” and discloses a “single point of...key management” that could be modified to “centrally generat[e] Orsini’s session master keys (***and any of the conventional encryption keys [used in Petitioner’s obviousness argument]***).” Pet., 25-26 (citing Ex. 1005 [Orsini] [0176]-[0179], [0293], [0381]-[0386], [0412]). But **session** key management is very different than key management for longer-lived keys such as the other “conventional encryption keys” Petitioner relies upon, especially as Figure 21’s session keys (the session master key and share keys) are stored alongside the encrypted data. For example, “session keys should be changed at least daily” if not for each “particular communications session” while “key-encryption keys don’t have to be replaced as frequently,” perhaps “once a year.” Ex. 2010 [Schneier-Applied-Cryptography] 184, 47; *see also id.*, 184 (“Encryption keys used to encrypt data files for storage cannot be changed often.”).

79. This longer lifespan, however, makes potential compromise of a key-encryption key all the more consequential. *Id.* (“However, if a key-encryption key is compromised, the potential loss is extreme: all communications encrypted with every key encrypted with the key-encryption key.”). Consequently, a POSITA

would recognize that a key management solution for session keys would not be appropriate for the “group key,” “encryption key,” or “key-encryption key” used in Petitioner’s alternative proposed modifications. *See* Ex. 1001 [’854] 62:28-29 (parser master, session master, and share encryption “keys may have individual key storage, retrieval, security and recovery options.”).

80. Moreover, key management for a “group key,” “encryption key,” or “key-encryption key” would necessarily be different than for key management for the “session” keys in Figure 21. In Figure 21, the session master key used to encrypt the dataset is parsed within the data shares (Ex. 1005 [Orsini] [0297]) and the session share keys are stored along with the data shares (*id.*, [0299]).

Therefore, so long as the party reconstructing the dataset possesses the shares, he or she also possesses the session keys necessary to decrypt the data. By contrast, the “group key,” “encryption key,” or “key-encryption key” would not be stored alongside the data but would rather need to be distributed out-of-band to the decrypting party. Consequently, those keys would need to be maintained and stored on both ends and in transit such that no adversary gets access to them.

Thus, the threat model for the “group key,” “encryption key,” or “key-encryption key” is very different than for a “session key.” Petitioner and Dr. Bhattacharjee have not mentioned, let alone adequately addressed, these different threat models.

Their superficial consideration of key management, an incredibly important aspect of cryptography, is thus insufficient and flawed.

81. Petitioner’s proffered modifications do not seem to create any advantage for Orsini’s system and, instead, would seem to undermine Orsini’s approach. At the very least, Petitioner’s proffered modifications are inadequately developed. Instead, Petitioner’s modifications ultimately seem to be driven by hindsight. To reiterate, in each instance, Petitioner begins with Orsini’s Figure 21 which sets out a fully functional system (Ex. 1005 [Orsini] [0380]) that Petitioner has not improved upon. Adopting the solution of “performing an encryption operation based on the external key to further secure the plurality of data chunks” seems driven by hindsight, not any technological need or benefit that would improve upon Orsini. It seems the claim limitation itself is being used as a roadmap driving the modification.

82. Consequently, in my opinion, Petitioner and Dr. Bhattacharjee have failed to demonstrate that a POSITA would be motivated to modify Orsini as proposed.

2. Additional Opinions

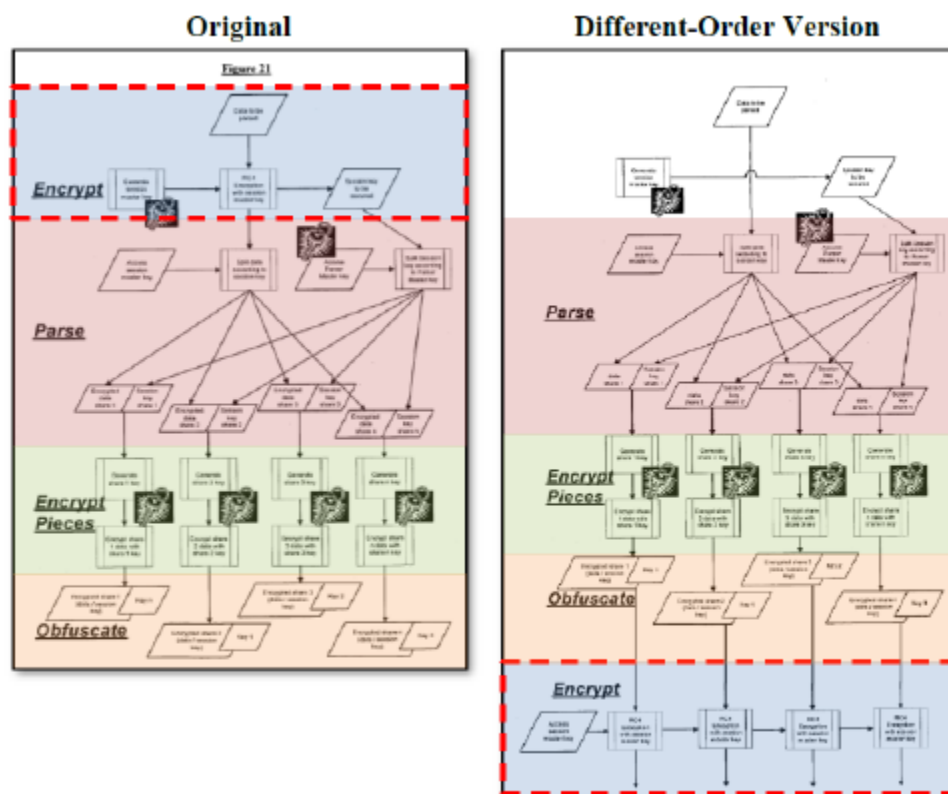
83. I understand that the Board in its Institution Decision (“ID”) found that Petitioner and Dr. Bhattacharjee have “not shown a reasonable likelihood of

prevailing as to the unpatentability of claim 1 under its challenge based on Orsini.”

ID, 25-39. I agree with the Board’s findings.

84. More specifically, the Board found with regard to Petitioner’s “Different-Order” anticipation argument:

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:

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.*

ID, 27-29.

85. In my opinion, the Board is correct. I agree with its findings for at least the reasons further explained in my first declaration in at least paragraphs 47-48 and 50-54, which are replicated in the instant declaration in paragraphs 49-50 and 52-56.

86. With regard to the “repeated steps” anticipation argument, the Board found the following:

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:

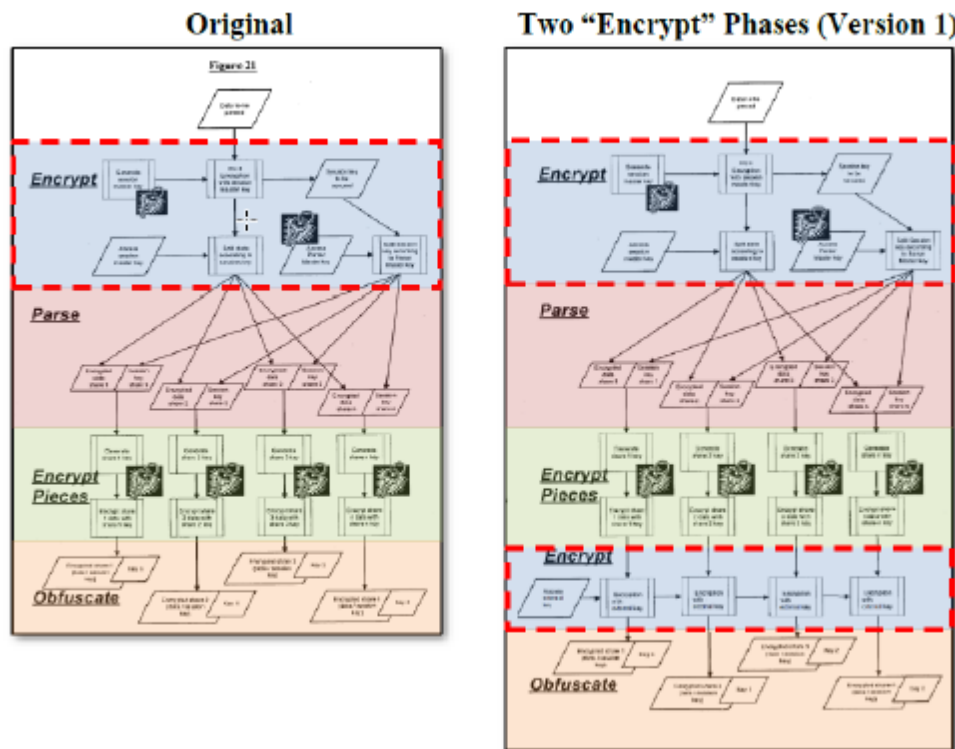
One different algorithm performed after encrypting the ‘shares’ (thus, after generating ‘data chunks’) that would have been obvious to [skilled artisans] includes using a single encryption key to further encrypt all data chunks with that key, similar to using the session master key to encrypt the entire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

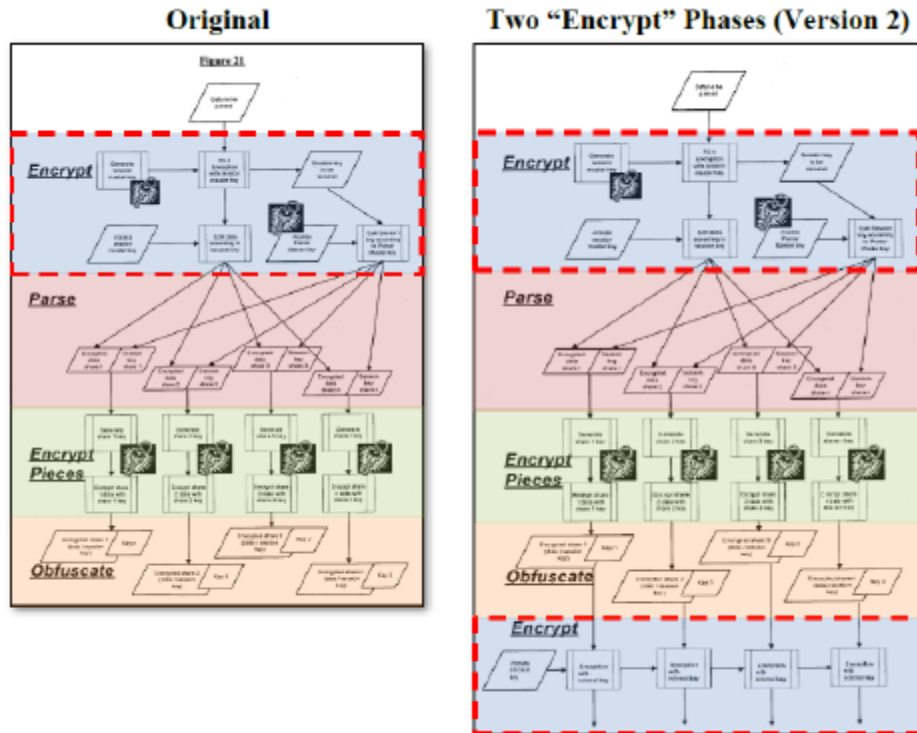
Id. (emphases in original).

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.





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, 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 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.

ID, 29-34.

87. In my opinion, the Board is correct. I agree with these findings for the reasons further explained in my first declaration in at least paragraphs 42, 47-48, 50-54, and 56-57, which are replicated in the instant declaration in paragraphs 44, 49-50, 52-56, and 58-59.

88. For Petitioner’s “encrypting with a public key” anticipation argument, the Board found the following:

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.

ID, 34.

89. In my opinion, the Board is correct. I agree with its findings for the reasons further explained in at least paragraphs 58-61 of my first declaration, which are replicated in the instant declaration in paragraphs 60-63.

90. With regard to Petitioner’s argument that it would be obvious to modify Orsini to re-encrypt with the external key, the Board found the following:

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.

ID, 35-36.

91. The Board is correct, in my opinion, and I agree with its findings for the reasons further explained in at least paragraphs 62-80 of my first declaration, which are replicated in the instant declaration in paragraphs 64-82.

92. For Petitioner’s “re-encrypting with externally received group key” obviousness argument, the Board found the following:

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.

ID, 36-37.

93. The Board is correct, in my opinion, and I agree with its findings for the reasons further explained in at least paragraphs 62-80 of my first declaration, which are replicated in the instant declaration in paragraphs 64-82.

94. The Board found as follows with regard to Petitioner’s “reordering data” obviousness argument:

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.

ID, 37-38.

95. The Board is correct, in my opinion, and I agree with its findings for the reasons further explained in at least paragraphs 62-80 of my first declaration, which are replicated in the instant declaration in paragraphs 64-82.

96. With regard to Petitioner’s “encrypting the distinct encryption keys with externally-stored KEK” obviousness argument, the Board found:

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*.

ID, 38-39.

97. The Board is correct, in my opinion, and I agree with its findings for the reasons further explained in at least paragraphs 62-80 of my first declaration, which are replicated in the instant declaration in paragraphs 64-82.

B. Petitioner’s Foster-Hayhurst Ground Fails (All Claims, Ground 2).

1. Hayhurst Is Not Analogous Art (All Claims).

98. Petitioner’s second ground relies upon the Hayhurst reference. Pet., 3. Based on the law regarding analogous art as explained to me by SFI’s attorneys and as summarized in Section IV above, it is my opinion that Petitioner and Dr. Bhattacharjee have not shown Hayhurst to be analogous art to the ’854 patent.

99. I note that neither Petitioner nor Dr. Bhattacharjee argue that Hayhurst is analogous art to the ’854 patent. *See generally* Pet.; Ex. 1003 [Bhattacharjee-Decl.].

a. The ’854 And Hayhurst Do Not Share The Same Field Of Endeavor.

100. As an initial matter, I note that Petitioner and Dr. Bhattacharjee admit that ’854 and Hayhurst have different fields. According to Petitioner and Dr. Bhattacharjee, the ’854’s field is securing data while Hayhurst’s is decentralized electronic media delivery. Pet., 4 (“[t]he ’854 patent relates to techniques for securing electronic data from unauthorized access.”); Ex. 1003 [Bhattacharjee-Decl.] ¶ 33 (same); Pet., 59 (“Hayhurst concerns ‘**electronic media delivery, such**

as video-on-demand”); Ex. 1003 [Bhattacharjee-Decl.] ¶ 178 (same); Ex. 2034 [Bhattacharjee-Depo.] 101:19-25. I agree that the ’854 and Hayhurst have different fields.

101. I have been informed by counsel and understand that to discern the field of endeavor, it is appropriate to look to several traditional sources such as a patent’s title, claim preamble, abstract, “background of invention” and “field of the invention,” and the function and structure of the claimed inventions.

102. Each of these traditional sources for identifying a field of endeavor uniformly confirms that the ’854’s field is securing data.

The ’854’s Field Is “Securing Data”	
Title	“ secure data parser and network”
Abstract	“ secure data parser for “ securely storing and communicating data ”
Field of Invention	“ securing data from unauthorized access or use.” Ex. 1001 [’854] 1:25-26.
Background of the Invention	focuses on the need “for ensuring data stored and transmitted ... cannot be read or otherwise compromised ” and seeks “to provide a cryptographic system whose security is user-independent ...” <i>Id.</i> , 1:35-37, 2:42-44.
Summary of the Invention	“one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use.” <i>Id.</i> , 2:45-47.
Claims	each claim concerns “ securely storing a data set ” or “ securing a data set ”

103. Hayhurst’s field, per these same traditional sources, is “decentralized media delivery.”

Hayhurst’s Field Is “Decentralized Media Delivery”	
Title	“Decentralized Media Delivery”
Abstract	“A decentralized approach to delivering a media file ...”
Technical Field	“This application relates to the field of electronic media delivery ...” <i>Id.</i>, [0002].
Background of the Invention	Focuses entirely upon delivering movie files. <i>Id.</i> , [0003]-[0004].
Summary of the Invention	“The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in <i>delivering video-on-demand or other large media files.</i> ” <i>Id.</i> , [0005].
Specification/Figures	“FIG. 1 is a block diagram of a system adapted for carrying out the <i>decentralized media delivery</i> of the present invention.” <i>Id.</i> , [0012] “FIG. 4 is a flow diagram showing how the <i>decentralized media file delivery</i> of the present invention is carried out.” [0015]
Claims	each claim concerns “securely storing a data set” or “securing a data set”

104. I note that Petitioner argues that “Hayhurst concerns ‘electronic media delivery, such as video-on-demand’ and how the data is ‘secure[ly] handl[ed] and stor[ed].” Pet., 59 (citing Ex. 1007 [Hayhurst] [0002]). While Hayhurst does include disclosures about the security of the electronic media files it delivers, in my opinion, that is not Hayhurst’s field of endeavor as established by the traditional sources I discussed above. Rather, security only tangentially relates to

Hayhurst's field of decentralized electronic media delivery. Hayhurst does not teach, for example, that prior art systems did not adequately secure media files, or that its invention addresses a need for more security. Ex. 1007 [Hayhurst] [0003]-[0005]. The mere mention of "secure handling and storage" of the media files does not change or expand Hayhurst's field from decentralized electronic media delivery to also somehow encompass the '854's field.

b. Hayhurst Is Not Reasonably Pertinent To The '854's Problem.

105. In my opinion, Hayhurst is not reasonably pertinent to the problem that the inventors of the '854 were concerned with.

106. The '854 is directed towards creating a cryptographic system whose security is user independent, while still supporting mobile users. Ex. 1001 ['854] 2:42-44. The '854 notes the "ever-increasing need ... for ensuring data stored and transmitted" to not "be read or otherwise compromised." *Id.*, 1:30-37. The '854 discusses certain prior art methods of securing data and the ways in which those methods may be compromised because they rely upon users. *Id.*, 1:38-44 (deficiencies in login/password systems); 1:46-2:14 (deficiencies in public-key systems that are "highly reliant on the user for security"); 2:15-38 (deficiencies in biometric systems that "suffer[] from a variety of drawbacks" from user losing/breaking smartcard). Consequently, the '854 addresses the need "to provide

a cryptographic system whose security is user-independent while still supporting mobile users.” *Id.*, 1:35-37, 2:42-44.

107. By contrast, Hayhurst is directed towards “address[ing] the prohibitive bandwidth requirements for a content provider associated with delivering video-on-demand other large media files.” Ex. 1007 [Hayhurst] [0005].

More specifically, Hayhurst explains:

It is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers ***because such a system requires a extensive amount of bandwidth between the content provider and each of the subscriber units*** (televisions or other display devices) of the network.

Id., [0004]. Thus, to solve this problem of “prohibitive bandwidth requirements” in the video-on-demand context, Hayhurst teaches “a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units” by utilizing the network of subscribers to distribute the electronic media files in a decentralized fashion. I note that Dr. Bhattacharjee agrees that Hayhurst is directed towards the “problem” of extensive bandwidth associated with providing “delivery-on-demand” media content. Ex. 1003 [Bhattacharjee-Decl.] ¶ 178; Ex. 2034 [Bhattacharjee-Depo.] 87:7-13; 92:1-11.

108. The '854, again, addresses eliminating user vulnerabilities in storing sensitive information. Hayhurst, by contrast, addresses the prohibitive bandwidth requirements for video-on-demand from the perspective of the content provider. Ex. 1007 [Hayhurst] [0003]-[0005].

109. Security from piracy is merely an ancillary benefit to Hayhurst's solution of decentralizing content delivery. And, what little Hayhurst has to say about encryption does not suggest that it is directed towards securing data in a manner that is "user-independent." Rather, in Hayhurst's system, a subscriber requests both an encrypted movie and an encryption key. Ex. 1007 [Hayhurst] [0028], [0030]. While the movie is originally dispersed amongst thousands of subscribers, it is reassembled, along with the key, by a single user. Thus, the security of the data (the movie) is user-dependent.

110. A POSITA looking to solve a problem with securing data sets in a user-independent fashion would not have looked to a reference directed to reducing the bandwidth required to transmit video-on-demand. Thus, in my opinion, Hayhurst is not reasonably pertinent to the '854 because they are directed to different problems, and Petitioner and Dr. Bhattacharjee fail to demonstrate that Hayhurst is analogous art to the '854 patent.

2. Motivation To Combine Foster And Hayhurst (All Claims).

111. Claim 1 requires:

Limitation 1[d] “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.”

112. As Foster does not teach “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,” Petitioner relies upon Hayhurst’s teachings for this limitation. Petitioner argues that “POSAs had reason to store Foster’s encrypted content units on multiple storage devices (*e.g.*, consumer set-top boxes like Hayhurst’s subscriber units and Foster’s recipients 430) based on Hayhurst’s techniques for storing and distributing encrypted data segments.” Pet., 61.

113. Petitioner and Dr. Bhattacharjee, however, fail to demonstrate that a POSITA would have been motivated to combine Foster and Hayhurst as proposed. As I explain below, Foster and Hayhurst are incompatible and have conflicting goals. Any alleged benefit would be far outweighed by the drawbacks of the combination.

a. Foster’s System.

114. As can be seen throughout Foster’s disclosure, Foster’s fundamental goal is to synchronize the transmission of encrypted content packets with the keys used to encrypt those packets. Doing so allows each packet to be viewed as soon as it is received and from any point in the content stream. *E.g.*, Ex. 1006 [Foster] Title; Abstract, [0002], [0008].

115. Notably, Dr. Bhattacharjee agrees that Foster is directed toward synchronized transmission of encrypted content with corresponding encryption keys. Ex. 2034 [Bhattacharjee-Depo.] 16:8-12. At his deposition, Dr. Bhattacharjee testified that “synchronous transmission to a receiver [to] foster random access to content” was “sort of the whole invention in Foster.” *Id.*, 32:20-23.

116. More specifically, Foster’s synchronization is directed towards reducing delays in viewer access to content as it is transmitted by a provider.

117. Foster seeks to improve upon prior art systems that were susceptible to “loss of synchronization between the content and the keys.” *Id.*, [0006]. The lack of synchronization impacted user experience with “inherent latencies” and “delays,” particularly when “providing random access of protected content,” *e.g.*, when the user changes the channel and when the image the new image displays. *Id.*, [0006], [0052] (“because delivery of keys and protected content are non-synchronized in a CAS, certain latencies such as delays are inherent in attempting to gain random access to the content.”); [0056] (without synchronization, “a delay could be incurred between when encrypted content is received and when it [is] accessed (*e.g.*, between when a channel is changed and when an image is displayed).”); [0063] (similar); [0064] (“both DRMS and CAS have inherent latencies (*e.g.*, delays) in providing random access [to] content.”). Foster,

moreover, indicates that “synchronous transmission to ... a receiver fosters random access to the content.” *Id.*, [0007]; [0052].

118. In order to achieve synchronization (thereby avoiding delays), Foster processes content into “content unit[s]” consisting of an encrypted content packet and the “title key” used to encrypt the packet. The title key is itself encrypted with a “key-encrypting-key,” or “KEK,” before it is combined with the content packet in a single content unit. *Id.*, [0008]. As illustrated in Figure 16 below—which Petitioner consistently relies upon (Pet., 58, 64)—Foster’s system transmits content units **directly** to **recipient 430**:

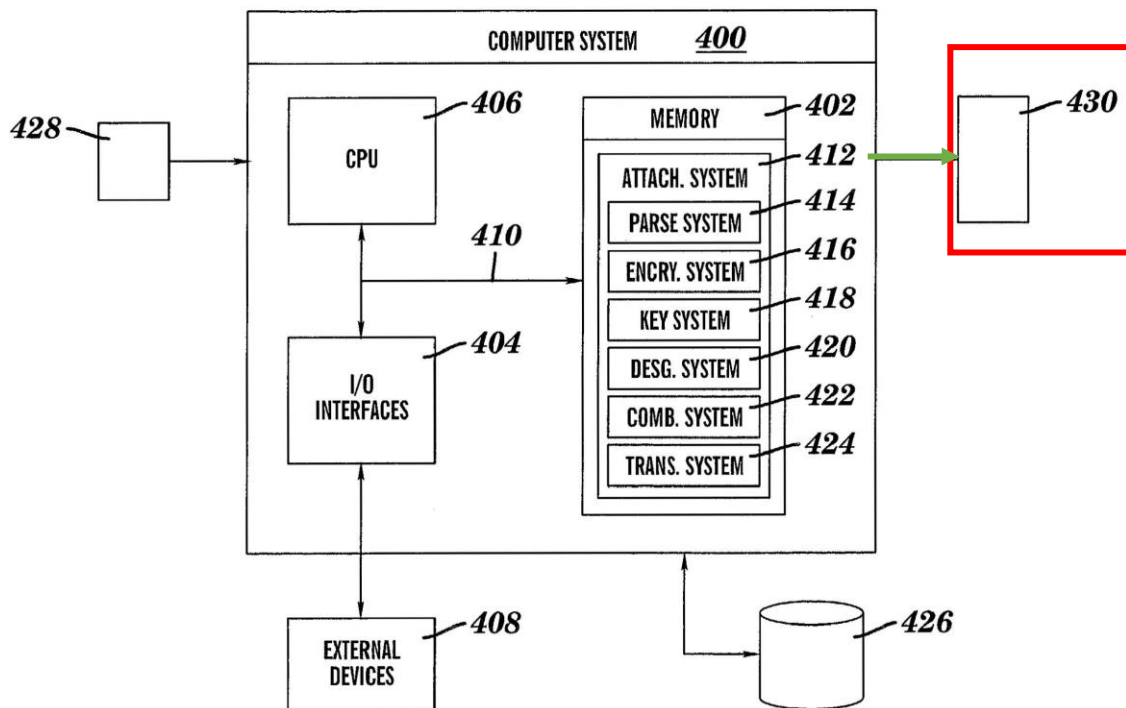


FIG. 16

Ex. 1006 [Foster] Fig. 16 (annotated); [0078] (“computer system 400 ... process[es] content units ... and transmit[s] the processed content units to a recipient 430.”). Because each content unit contains both the content and the key, each content unit may be encrypted and transmitted by the source as it is generated, and then decrypted and viewed without the delay found in prior art systems wherein the key had to be separately attained. *Id.*, [0064].

119. Importantly, Foster contemplates using its invention in the cable television context. Foster teaches that its system processes and transmits content

units between a “Content Service Provider” “such as a cable service provider” (*id.*, [0039]) and a “Receiver” “such as a set-top box” (*id.*, [0040]). *Id.*, Fig. 16, [0078]. It seeks to improve upon prior art cable systems providing real-time television. *Id.*, [0052] (Foster is directed towards “Conditional Access System[s] (CAS),” which are “cable or satellite television system[s]”); [0006].

120. Foster’s teachings of synchronized transmission to reduce delays/latencies are particularly significant in a streaming context contemplated by Foster’s Figure 8, which Petitioner relies upon (*e.g.*, Pet., 56, 65-66). “In streaming, multimedia data is transferred in a stream of packets that are interpreted and rendered in real time by a software application, as the packets arrive in the user’s terminal.” Ex. 2035 [Patrikakis] 220. Because packets are transmitted as a stream and rendered in real-time, any delays have an especially noticeable impact. When watching, *e.g.*, a live sporting event, any delay in receiving, decrypting and/or rendering each content unit in a stream would be a significant drawback. Figure 8 depicts the “Encryption of [an] Elementary Stream,” provided to a set-top box which has “random access points (points in stream where player can start [displaying the stream])”:

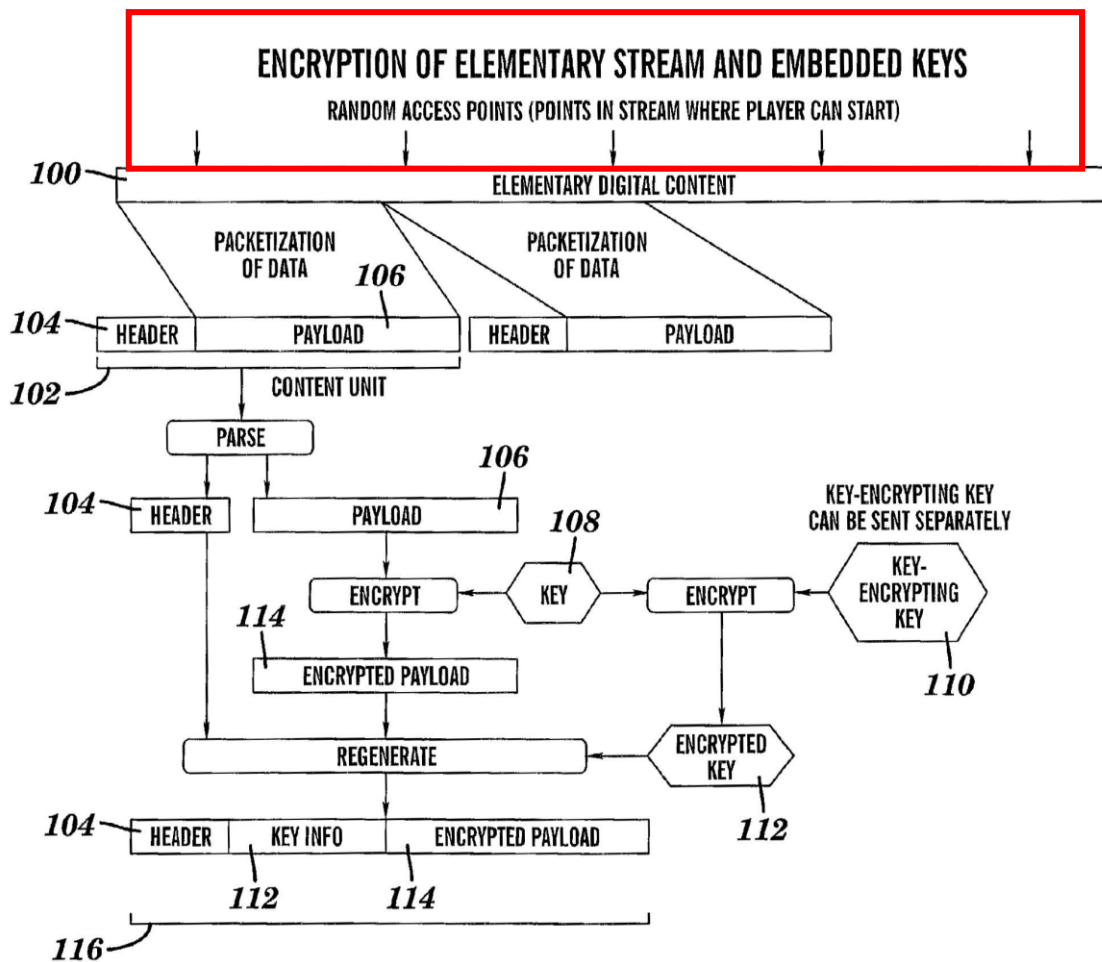


FIG. 8

Ex. 1006 [Foster] Fig. 8 (annotated); *see also* [0064]. Foster makes clear that when content and keys are not sent synchronously, the type of random access of content contemplated by Figure 8 “is not possible” in the streaming context. *Id.*, [0063]; *see also* [0064], [0071]. This is because without synchronization, the resulting delays would prevent streaming.

121. Although Foster discusses the DVD player context, this is not its main focus, as evidenced by the fact that multiple of Foster’s figures—including Figure 8 which Petitioner relies upon—refer to streaming content. *E.g.*, Ex. 1006 [Foster] Figs. 8, 14. Moreover, Foster teaches that its invention processes content units “for synchronized transmission to, or storage by a receiver.” *Id.*, [0008]. As a DVD player can neither receive transmitted content nor store content (*cf.* Ex. 2019 [Microsoft-Computer-Dictionary] 90 (defining CD player as “device that reads the information stored on a CD.”)), it is clear that the DVD player is not Foster’s focus.

b. Hayhurst’s System.

122. Unlike Foster, Hayhurst is not concerned with synchronous transmission, avoiding delays, or facilitating real-time streaming. Indeed, Hayhurst purports to facilitate the transmission and playback of content files rather than content streams. As I previously explained in Section VI.B.1(b), Hayhurst aims to overcome “prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files” to a subscriber network. Ex. 1007 [Hayhurst] [0005]. Hayhurst teaches that, in light of the size of these files and the bandwidth required to transmit them, it is “usually not economically feasible” for a content provider “to provide for delivery-on-demand [of] a large number of movie selections to subscribers.” *Id.*, [0004]. To address this problem,

Hayhurst “shifts the bandwidth requirements away from the content provider [] to the network of subscriber units.” *Id.*

123. Hayhurst divides a movie file into segments that are then stored across a network of subscriber units. When a movie is requested by one subscriber, the system directs other subscribers to send their respective segments of the file to the requesting subscriber. When all of the segments are received at the requester’s computer, they are then decrypted and the file is reassembled from the collection of segments for viewing. Ex. 1007 [Hayhurst] [0006]. Hayhurst’s system is a network of “thousands of subscribers.” *Id.*, [0016]; Ex. 2034 [Bhattacharjee-Depo.] 101:15-25.

124. Hayhurst’s methodology is not compatible with real-time streaming or random-access viewing of live television. Hayhurst requires that an entire movie file be segmented, and the segments transmitted to, and stored among, the members of a subscriber network before the movie can even be requested for viewing by any individual subscriber. Beyond that, because the segments are not stored in or received in any particular order, the movie cannot be viewed at all until (i) **all** segments are received from the subscriber network by the subscriber, (ii) the requesting unit obtains authorization, and (iii) the packets are descrambled and then reassembled into the complete movie file. Ex. 1007 [Hayhurst] [0029]; [0030]; Ex. 2034 [Bhattacharjee-Depo.] 101:19-25. Thus, Hayhurst’s system

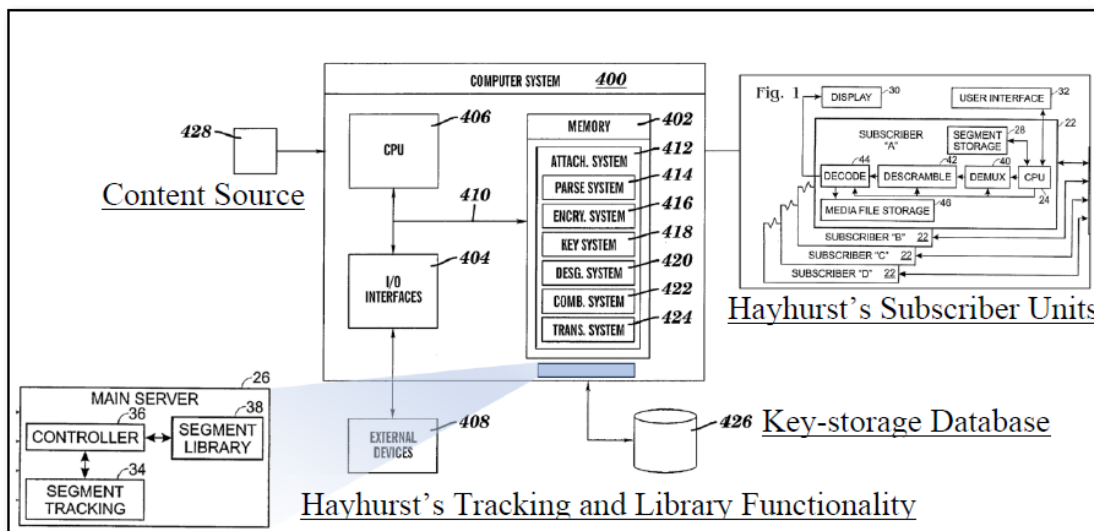
requires all segments to be received and for the entire file to be reassembled the system can play the movie, thus, “excluding the use for covering live events.” Ex. 2035 [Patrikakis] 219.

125. Indeed, in “download and play” systems such as Hayhurst, “the client has to download and store first **the whole media content** on his PC and only then he/she will be able to view and use it.” Ex. 2035 [Patrikakis] 219. This requirement “**exclud[es] the use [of such systems] for covering live events**, as the multimedia information that is to be transmitted cannot be ‘a-priori’ available.” *Id.*

c. Petitioner And Dr. Bhattacharjee’s Proposed Combination.

126. I understand that Petitioner and Dr. Bhattacharjee propose combining Foster and Hayhurst such that Foster’s media **content units** are distributed and stored in Hayhurst’s decentralized media **file** storage system. Specifically, “Foster’s encrypted content units” would be stored “on multiple storage devices ... based on Hayhurst’s techniques for storing and distributing encrypted data segments” of a media file. Pet., 61. In Petitioner and Dr. Bhattacharjee’s “exemplary implementation of Foster-Hayhurst,” illustrated below, “Foster’s ‘computer system 400’ is augmented to ... control distribution of and access to Foster’s encrypted content portions on [Hayhurst’s] ‘subscriber units.’” *Id.*, 64. Thus, in Petitioner and Dr. Bhattacharjee’s combination, Foster’s “content stream 100” “is parceled into content units 102” (*id.*, 56) and rather than sending content

units directly to the requesting subscriber, the content units would be distributed amongst Hayhurst's network of thousands of subscribers.



Foster-Hayhurst (exemplary implementation)

Id., 64; 61 (“POSAs would have recognized several benefits in storing Foster’s encrypted content units distributed on different storage devices as Hayhurst teaches.”); 62 (similar); 63 (similar). While this implementation is purportedly only “exemplary,” at his deposition, Dr. Bhattacharjee admitted that this is the only implementation of the combination that is described or relied on in his declaration. Ex. 2034 [Bhattacharjee-Depo.] 126:3-9.¹

¹ While Dr. Bhattacharjee was referring to the Foster-Hayhurst ground in IPR2024-00212, that ground is substantively identical to the ground presented here, including the sole “exemplary implementation.”

d. *A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed.*

i. Hayhurst's Delivery Method Would Result In Delays.

127. Petitioner's Foster/Hayhurst combination would result in inevitable, significant, and crippling delays, the very thing Foster was intended to avoid. Petitioner's proposed combination of Foster and Hayhurst relies upon Hayhurst's methods of storing and delivering segments of media files. Pet., 61. In Petitioner's proposed combination, all of Foster's encrypted content units would, rather than be sent directly to the requestor as in Foster, instead be distributed across thousands of subscriber units before they are then, when requested, sent to a requesting unit, as taught in Hayhurst. Ex. 1007 [Hayhurst] [0016].

128. This introduces delay in a number of ways. First, in Hayhurst the content must exist as a discrete file before it can be divided into segments and distributed for storage among the subscriber network. (This is in stark contrast to Foster, where the content units can be created and transmitted as the stream of content is generated.) Then, in Hayhurst, the main server, upon receiving a request, must direct the thousands of subscribers to send segments to the requestor. *Id.*, [0028] ("after the main server receives a movie request 104 from a requesting subscriber ..., the server responds 106 by sending over the network instructions to the network subscriber units to direct all of the segments of the requested movie to the requesting subscriber."). Should there be one or more missing packets, which

there inevitably would be for subscribers whose systems are turned off, internet is down, are no longer subscribers, etc., the main server must either direct another subscriber with the same packet to resend it or redistribute the packet. *See id.*, [0025] (“Each segment [] is copied and distributed to a plurality of different subscribers to provide for redundant availability of each segment in the event a subscriber’s segment storage 28 becomes inaccessible. As noted, the main server’s segment-tracking module 34 can ...facilitate replacement or redistribution of segments when necessary.”); Ex. 2034 [Bhattacharjee-Depo.] 106:17-109:6. Accordingly, the requesting unit must wait until “**all** packets are received” before sending a request to the main server to decrypt the segments and reassemble the movie file. *Id.*, [0029] (“The subscriber unit CPU 24 and associated buffers (not shown) log the received packets and, once **all packets** are received, sends a notice to the main server 26 that **all packets** now reside in the unit of the requesting subscriber.”). Only once all packets are on the requesting unit does the main server “transmit[] authorization.” *Id.* After obtaining authorization, the receiving unit may descramble, process, and reassemble the entire media file for playback. *Id.*, [0029]-[0030]; Ex. 2034 [Bhattacharjee-Depo.] 109:8-111:1. Only after all of these steps are completed, the movie can be viewed.

129. Consequently, Hayhurst’s methods of storing and delivering content make playback delays—the underlying problem Foster seeks to address—

exponentially worse. Rather than immediately streaming content in packets that are synchronized with the encryption keys as Foster does, Petitioner would have Foster's system store and deliver content using Hayhurst's decentralized, time-consuming method. In other words, Petitioner proposes changing Foster's method which has been designed to reduce delays to one that prioritizes bandwidth at the expense of creating delays.

130. In my opinion, a POSITA would not be motivated to change Foster to implement methods which greatly exacerbate the underlying problem Foster seeks to address.

ii. Hayhurst's Method Of Delivery Is Incompatible With Foster's System.

131. Foster's system serves as an intermediary between "source 428" and "recipient 430," where the "source" includes "a cable service provider" (Ex. 1006, [0039], [0042]) and the "recipient" includes a "set-top box" (*id.*, [0040], [0041]).

As Dr. Bhattacharjee agrees, Foster specifically seeks to improve upon the "Conditional Access System (CAS)," "such as a cable or satellite television system." *See id.*, [0052]; Ex. 2034 [Bhattacharjee-Depo.] 41:10-15, 30:8-10. Consequently, Foster's principle of operation concerns delivering live cable television to a set-top box. Ex. 2039 [Marlin-DRM] 1 (CAS used for OTT digital video streaming service, "such as live sports"); Ex. 2040 [Verimatrix] 2 (CAS used for "content [transmitted] as a signal, which virtually anyone can pick up via

satellite, terrestrial, or cable network.”); *see* Ex. 1006 [Foster] [0056] (Foster seeks to avoid delays “when a channel is changed”); *see also* Ex. 2034 [Bhattacharjee-Depo.] 37:11-39:9.

132. Foster’s system is able to deliver live or real-time content as required for cable television because Foster’s methods do not require a user to have an entire media file before it can view content. Rather, Foster’s system allows viewers to receive and process packets in real-time as they are generated and sent by the content provider. Ex. 1006 [Foster] [0065] (“the teachings of the present invention can be applied to the scenario where the content is received as content units”); Ex. 2035 [Patrikakis] 220 (“In streaming, multimedia data is transferred in a stream of packets that are ***interpreted and rendered in real time*** by a software application, ***as the packets arrive in the user’s terminal.***” As a result, Foster avoids “delay[s]” “between when encrypted content is received and when it [is] accessed (e.g., between when a channel is changed and when an image is displayed).” *Id.*, [0056].

133. Hayhurst is directed toward delivering video-on-demand and not live television. In particular, Hayhurst’s focus is upon delivering movies—*i.e.*, an already defined media file—in a fashion that avoids bandwidth limitations. Ex. 1007 [Hayhurst] [0003]-[0004]. As such, Hayhurst utilizes a decentralized delivery system in which segments of a movie are stored on set-top boxes

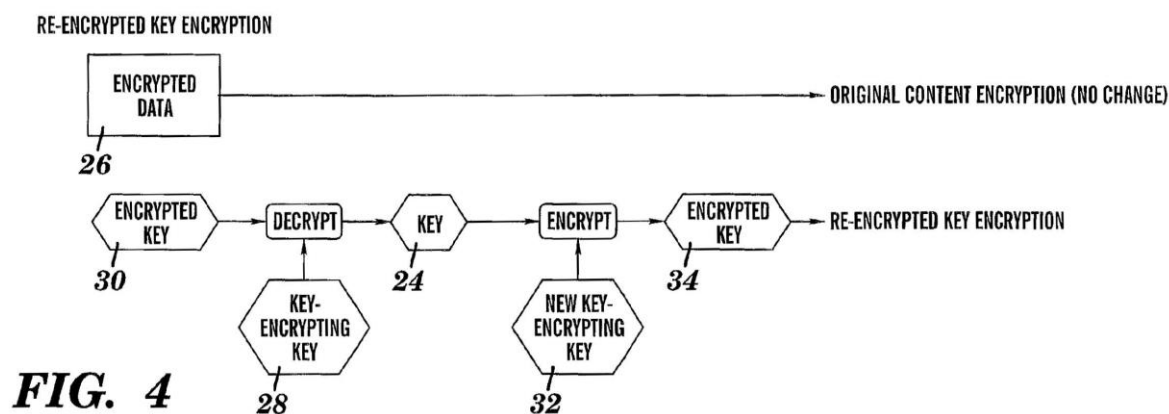
throughout Hayhurst's system until one set-top box requests the entire movie. *Id.*, Abstract, [0006], [0028]. When a requesting set top box requests a movie, it cannot be played immediately. Rather, viewing can only begin after all segments are received, because "the segments are separate in the sense that they represent discontinuous or non-sequential portions of the movie and must be soiled and integrated with the remaining segments (distributed elsewhere in the network) to provide the complete movie." *Id.*, [0021]; Ex. 2034 [Bhattacharjee-Depo.] 104:2-13. There is no indication in Hayhurst that the segments arrive in order to the requesting unit. Nor would it be feasible for Hayhurst's main server to facilitate such a thing, as there would be significant delays incurred as the main server would have to ensure successfully receipt of each segment before directing the next subscribing to send to following segment. Thus, only after all segments are received from the different members of the subscriber network can authorization to decode them be sought and obtained, and the segments are assembled and processed. *Id.*, [0028]-[0030].

134. In the Foster/Hayhurst combination, a set-top box requesting cable television content would have to wait to receive all of the packets sent from the set-top boxes of a multitude of other subscribers before seeking and obtaining authorization and before reassembling and processing the entire content file. This

wait-and-see approach would not work when trying to watch live television. Ex. 1006 [Foster] [0063].

iii. Petitioner's Proposed Combination Makes Foster Less Secure.

135. In Foster, should a key-encrypting-key be compromised or “protection on the content [need] to be varied,” “an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26.” Ex. 1006 [Foster] [0054].



Id., Fig. 4. Thus, Foster contemplates seamlessly switching the KEK for security purposes without re-encrypting the underlying content. Thus, if a key-encrypting-key is compromised, or a switch is otherwise desirable, a new KEK may be utilized going forward.

136. Moreover, Foster allows for a key-encrypting-key to be unique to each recipient. Foster teaches that “key encrypting key 28 is generally determined

based on a key management block (KMB), which is typically delivered to a recipient concurrently with or prior to the delivery of encrypted content 26.” *Id.*, [0054]. Because each recipient receives a KMB from which a key-encrypting-key can be determined, that key-encrypting-key can be unique to each recipient. This further increases the security of Foster’s content as the damage from any compromise of a recipient’s key-encrypting-key can be limited to that recipient and further prevented by simply changing that recipient’s key-encrypting-key.

137. Foster/Hayhurst uses Hayhurst’s method of storing and distributing content. Consequently, any subscriber (of thousands) is able to request content that has been divided into segments across thousands of subscribers. Because any one of Hayhurst’s subscribers can request the content, which has already been segmented and divided in advance, in any combination, Foster’s content units would all have to be secured using the same KEK(s), regardless of which subscriber will eventually request the content.

138. This, however, makes the combined system less secure for two reasons. First, it makes the KEKs more vulnerable. Because the KEK(s) is/are distributed amongst thousands of subscribers, there are thousands of potential points of failure. And, if one set-top-box (of thousands) with the KEK(s) gets compromised, all of the content is compromised because all of the content is encrypted using the same KEK(s) and title keys. Second, it would be more

complicated to switch KEKs than in Foster alone as all of the content units are distributed across the subscribers instead of streamed in real time as in Foster. Thus, adding Hayhurst's methods to Foster's system would make Foster's system less secure in contravention of Foster's aims. Ex. 1006 [Foster] [0004] ("In transmitting such content, however, the security thereof must be ensured.").

iv. The Purported Benefits Of The Proposed Combination Are Outweighed By The Drawbacks.

139. Petitioner argues that a POSITA would be motivated to combine Foster and Hayhurst as proposed because Hayhurst's methods would reduce bandwidth requirements, provide more security, and support redundancy. Pet., 61-62. Petitioner also argues that Hayhurst's methods result in aggregate speed and efficiency/intelligence. *Id.*, 62.

140. Foster's system, however, has no need for any of these alleged benefits. Foster's system simply processes content and transmits streamed content to a particular recipient. Ex. 1006 [Foster] Fig. 16; [0078]. Because Foster's system focuses upon streamed content (or content stored on a DVD) and provides a one-to-one transmission from Foster's system to a particular recipient, there is no indication that Foster's system suffers from the bandwidth constraints confronted by Hayhurst's video-on-demand system. Foster's system, moreover, has sufficient security at the source, security which would be undermined in the combination, as

discussed previously. Further, Foster's system has no need for redundancy as Foster's system can simply resend dropped packets, nor any need for efficiency/intelligence when sending on a one-to-one basis.

141. Moreover, any benefits are easily outweighed by the drawbacks. Again, Foster is directed towards reducing delays, particularly delays frustrating random access to content. The Foster/Hayhurst combination, however, would introduce enormous delays preventing random access to content and rendering Foster's system unsuitable for streaming live television. Further, the combination would also decrease Foster's security by exposing KEKs and hindering Foster's ability to replace a KEK when desirable.

142. Notably, I see no consideration, let alone weighing, of these drawbacks against the purported benefits from Petitioner or Dr. Bhattacharjee.

143. Thus, in my opinion, a POSITA would not be motivated to combine Foster and Hayhurst as Petitioner and Dr. Bhattacharjee propose.

3. “Generating A Plurality Of Data Chunks Based On A Data Set”
(Limitations 1[b], 1[b1]).

144. Claim 1 requires:

Limitation 1[b] “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:”

Ex. 1006 [Foster] Fig. 13, [0072] (“a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302 PES unit 302 includes packetized elementary stream (PES) packet payload 306” which “will be encrypted with a title key”). Foster’s PES packets are also referred to as “data packets.” See Ex. 2011 [Tsai] [0001], cl. 1. Consequently, Petitioner and Dr. Bhattacharjee map the claimed “data shares” to Foster’s packets (specifically, the payloads of those packets) which are then individually encrypted, resulting in “data chunks.” There is no teaching in Foster that these packet payloads are themselves sub-divided into shares or chunks.

146. I see no explanation from Petitioner or Dr. Bhattacharjee of what “data chunks” or “data shares” are or why packet “payloads” are “data shares” (or “data chunks” when encrypted). Certainly, Foster never refers to its packet payloads as “data chunks” or “shares.”

147. Petitioner and Dr. Bhattacharjee, again, rely upon Foster’s packet payloads as data shares and encrypted packet payloads as data chunks. Numerous technical articles, however, refer to a packet or packet payload being divided into chunks or shares. See, e.g., Ex. 2042 [Kumar] 9 (“each node sends out 3 shares in a single packet”); Ex. 2043 [Mao] 9532 (“We break [data packet] D into n shares according to the (t, n) -threshold secret sharing algorithm.”); Ex. 2036 [Hur] 1202 (“The new scheme uses a content-based chunking algorithm to consistently divide

both files and packet payloads into multiple byte sequences, called chunks.”); Ex. 2037 [Li-I] 1 (“These services allow breaking down packet payloads into smaller units (called chunks) ...”); *see also id.*, 2 (“It provides a packetization method that breaks down the payload into multiple chunks, each with a certain significance.”); Ex. 2012 [Pek] 3 (“[The d]ata packet is delivered as a sequence of chunks.”); Ex. 2013 [Groote] 3 (“the input is a large data packet ... which is delivered in small chunks.”); Ex. 2038 [McKeown] 4-5 (“A packet consists of multiple chunks...); Ex. 2041 [Li-II] 7(“the payload could be divided into multiple equal-sized chunks ...”).

148. Consistent with this usage in the literature, the ’854 identifies a data packet (or packet payload) as something that is divided into shares. Ex. 1001 [’854] 82:21-24 (“At step 4106, ***the data packet or data block may then be partitioned into two or more data shares ...***”), 81:36-37 (“***Packets of data (e.g., network packets) may also be efficiently split*** and restored”), 81:54-58 (“...simplified ***data partitioning process 4010 ... may be performed on network packets, ...***”). Therefore, the ’854 identifies data packets for streaming, such as those disclosed in Foster and in Hayhurst, as the unit to be parsed, not as “data chunks [generated] based on a data set” by “distributing the data set into a plurality of shares” and encrypting. In other words, by disclosing a method for secure transmission of MPEG data packets, neither Foster nor Hayhurst disclose

“generating a plurality of data chunks” by “distributing the data set into a plurality of shares” as a POSITA would understand the limitation based on the ’854’s specification. Notably, neither Petitioner nor Dr. Bhattacharjee identifies any teaching in the ’854 or in the technical literature suggesting that a data packet payload would qualify as a “data share” or a “data chunk” when encrypted.

149. Nor does the ’854’s discussion of shares suggest that a packet payload would be deemed a “data share” or a “data chunk” when encrypted. As the ’854 explains, partitioning the data set into chunks increases security because when “data ... remains whole and intact,” it is “subject to attack.” The ’854 addresses this concern, in part, by “performing a cryptographic parsing and splitting of the encrypted file.” Ex. 1001 [’854] 56:47-61. Thus, the ’854 teaches that splitting the data set into shares helps secure the data.

150. A packet payload (as in Foster as well as Hayhurst), however, does not exist to protect the data. Rather it exists by virtue of the MPEG packetized elementary stream standard. Ex. 1006 [Foster] [0072]-[0073]; Ex. 2014 [Overview-of-MPEG-2-Systems] (“An elementary stream is broken up into packets, forming a *packetized elementary stream* (PES).”). These packets allow for transmission of the content. See Ex. 2015 [Newton’s-Telecom-Dictionary] 626 (“**Packet** 1. Generic term for a bundle of data, usually in binary form, organized in a specific way *for transmission*.”); Ex. 2016 [Oxford-Dictionary-of-Computing]

257 (“a group of binary digits forming a message. The group is **transmitted** together”).

151. Thus, the ’854 splits a data set into shares or chunks as a means of protecting a dataset. This is why a packet in the ’854 is an example of a data set that is split into shares. See Ex. 1001 [’854] 82:21-24. By contrast, Foster’s packet payloads exist not to protect data but, rather, because it is just a by-product of a pre-existing standard. Consequently, a POSITA reading the ’854 patent would not consider a packet payload to be a data share (or a data chunk when encrypted) in view of the ’854’s disclosure.

152. I note that while Petitioner and Dr. Bhattacharjee do not rely upon Hayhurst teachings of segmenting data (see Pet., 74, 61-64), Hayhurst’s segments are also not “shares” or “chunks” when encrypted. Hayhurst’s segments are also data packets. Ex. 1007 [Hayhurst] [0020] (“**a segment is a digital packet** that includes data representing a small portion of the movie (video and audio)”). Thus, for the same reasons that Foster’s packet payloads are not shares and encrypted packet payloads are not chunks, Hayhurst’s segments are also not shares (or chunks when encrypted).

153. Thus, in my opinion, Petitioner and Dr. Bhattacharjee fail to demonstrate that Foster discloses or renders obvious “generating a plurality of data chunks based on the data set.”

VII. CONCLUSION

154. Although my complete opinions are set forth above, for convenience I summarize several points of my opinions in conclusion. For the foregoing reasons, based on my expertise and experience and the record of this case that I have reviewed, it is my opinion that:

- Claims 1-10 are not anticipated by or obvious over Orsini;
- Claims 1-10 are not obvious over Foster in combination with Hayhurst.

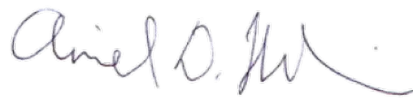
155. I understand that my opinions discussed above support a legal conclusion that claims 1-10 are nonobvious.

In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

I hereby declare that all statements made herein of my own knowledge are true and all statements made herein on information and belief were and are believed by me to be true, and that all statements herein were and are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code and that any such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Respectfully submitted,

Dated: September 12, 2024

A handwritten signature in blue ink, appearing to read "Aviel D. Rubin".

Aviel D. Rubin, Ph.D.

EXHIBIT A

Aviel D. Rubin, Ph.D.

Professor Emeritus, Johns Hopkins University
Chief Scientist & Founder, Harbor Labs

avirubin@gmail.com

<https://www.linkedin.com/in/avirubin/>



Overview

Avi Rubin is a Computer Scientist with almost a decade of industry experience followed by over 20 years in academia. After receiving his Ph.D. in Computer Science from the University of Michigan in 1994, Dr. Rubin worked as a researcher at Bellcore and then at AT&T Labs. In 2003, he joined the Computer Science faculty at Johns Hopkins University and was promoted to Full Professor with Tenure in 2004. During his over 20 years at Johns Hopkins, Dr. Rubin was Technical Director of the JHU Information Security Institute, along with his regular faculty position. In 2023, he was appointed Computer Science Professor Emeritus at Johns Hopkins and joined Harbor Labs, a company he founded in 2011, as Chief Scientist. Dr. Rubin is a frequent keynote speaker at industry and academic conferences and delivered widely viewed TED talks in 2011 and 2015. He has testified about information and network security before Congress on multiple occasions and frequently testifies as an expert witness in Federal court. His awards include Fulbright Scholar, Baltimorean of the Year, and the EFF Pioneer Award.

Academic Degrees

- 1994, **Ph.D.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, **M.S.E.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, **B.S.**, Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

September, 2023 - present

Professor Emeritus, Johns Hopkins University

April, 2004 - August, 2023

Professor (with tenure), Johns Hopkins University

August, 2010 - July, 2011

Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

January, 2003 - April, 2004

Associate Professor, Johns Hopkins University

January, 2003 - August, 2023

Technical Director, Johns Hopkins University Information Security Institute

2006 - 2010

Director and Principal Investigator (PI), NSF ACCURATE Center

1995 - 1999

Adjunct Professor, New York University

Summer, 1999

Visiting Professor, École Normale Supérieure, Paris, France

1988 - 1993

Teaching Assistant, University of Michigan

Doctoral Committees

Doctoral Thesis Advisor: David Inyangson, JHU

Doctoral Thesis Advisor: Logan Kostick, JHU

Doctoral Thesis Advisor: Atheer Almogbil, JHU (May, 2024)

Doctoral Thesis Advisor: Tushar Jois, JHU (May, 2023)

Doctoral Thesis Advisor: Random Gwinn, JHU (May, 2022)

Doctoral Thesis Advisor: Karl Siil, JHU (May, 2022)

Doctoral Thesis Advisor: James Cervini, JHU (May, 2022)

Doctoral Thesis Advisor: Jeff Chavis, JHU (May, 2021)

Doctoral Thesis Advisor: Gabe Kaptchuk, JHU (May, 2020)

Dissertation Committee: Thomas Tantillo, JHU (September, 2018)

Doctoral Thesis Advisor: Paul Martin, JHU (February, 2016)

Doctoral Thesis Advisor: Michael Rushanan, JHU (May, 2016)

Doctoral Thesis Advisor: Ayo Akinyele, JHU (December, 2013)

Doctoral Thesis Advisor: Matthew Pagano, JHU (August, 2013)

Doctoral Thesis Advisor: Ryan Gardner, JHU (August, 2009)

Doctoral Thesis Advisor: Sam Small, JHU (May, 2009)

Doctoral Thesis Advisor: Sujata Doshi, JHU (May, 2009)

Doctoral Thesis Advisor: Joshua Mason, JHU (June, 2009).

Dissertation Committee: J. Alex Halderman, Princeton University (May, 2009).

Dissertation Committee: Sophie Qiu (May, 2007).

Doctoral Thesis Advisor: Adam Stubblefield (April, 2005).

Dissertation Committee: Kevin FU, MIT (February, 2005).

Dissertation Committee: Robert Fischer, Harvard University (June, 2003).

Dissertation Committee: Marc Waldman, New York University, (April, 2003).

Dissertation Committee: Patrick McDaniel, U. of Michigan (September, 2001).

Doctoral Thesis Advisor: Fabian Monrose, New York University (April, 1999).

Dissertation Committee: Mike Just, Carleton University (November, 1998).

Dissertation Committee: Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

2011 - present

Harbor Labs, Founder & Chief Scientist

2005 - 2011

Independent Security Evaluators, Founder & President

1997 - 2002

AT&T Labs -- Research, Secure Systems Research Department

1994 - 1996

Bellcore, Cryptography and Network Security Research Group

Summer, 1990

Great Lakes Software Co., Programmer, Howell, MI

Summer, 1989

IBM, Programmer, Meyers Corners Lab, Poughkeepsie, NY

Books

- Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
- William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
- **Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
- Aviel D. Rubin, *Whitehat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
- **Chapter 8**, Publius and **Chapter 14**, Trust in Distributed Systems, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *PeertoPeer*, O'Reilly & Associates, Inc., (February, 2001).
- Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc , (June, 1997).
- **Ph.D. dissertation**: *Nonmonotonic Cryptographic Protocols*, University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

- David Kotz, Kevin Fu, Carl Gunter, Avi Rubin, *Security for Mobile and Cloud Frontiers in Healthcare*, Communications of the ACM (July, 2015).
- Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems*, Journal of Cryptographic Engineering (JCEN), (January, 2013).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
- Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
- Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
- David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).
- Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* ACM Transactions on Information and System Security, May, 2004.

- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single-Signon Protocol*, Computer Networks, (July, 2000).
- Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
- Fabian Monroe and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, Future Generation Computer Systems, (March, 2000).
- Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds*, Communications of the ACM (February, 1999).
- Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security*, IEEE Internet Computing (November/December, 1998).
- Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
- Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions*, ACM Transactions on Information and System Security, (June, 1998).
- Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography*, Cryptologia (April, 1997).
- Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
- Aviel D. Rubin, *Independent One-Time Passwords*, USENIX Journal of Computer Systems (February, 1996).
- Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk, Aviel D. Rubin, *SocloTy: Practical Cryptography in Smart Home Contexts*, Privacy Enhancing Technologies Symposium 2024 (PETS '24), (July, 2024).
- Atheer Almogbil , Momo Steele , Sofia Belikovetsky , Adil Inam, Olivia Wu, Aviel Rubin, Adam Bates, *Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments*, NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec), (February, 2024).
- Samra Kasim, Nawal Valliani, Nelson Ka Ki Wong, Shahin Samadi, Lanier Watkins and Aviel Rubin, *Explainable Autonomic Cybersecurity for Industrial Control Systems*, IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), (March, 2023).
- Valeti Manoj, Shao Wenda, Niu Sihan, Christopher Rouff, Lanier Watkins, Aviel Rubin, *Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System*, IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM),(October, 2022).

- James Cervini & Aviel D. Rubin, *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack*, ICCWS 17th International Conference on Cyber Warfare and Security, (July, 2022).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Make Steganography Great Again — Before It's Too Late*, Real World Crypto 2022, (April, 2022).
- James Cervini, Daniel Muller, Alexander Beall, Joseph Maurio, Aviel Rubin & Lanier Watkins, *A Backfit Approach for Trusted Virtualization-Based Programmable Logic Controller Resilience*, Sixteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, (March, 2022).
- Hedin Beattie, Lanier Watkins, William H. Robinson, Aviel Rubin, Shari Watkins, *Measuring and Mitigating Bias in AI-Chatbots*, 2022 IEEE International Conference on Assured Autonomy (ICAA'22), (March, 2022).
- Random Gwinn, Mark Matties, Aviel D. Rubin, *Wavelet Selection and Employment for Side-Channel Disassembly*, IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), (December, 2021).
- Karl A Siil, Aviel D. Rubin, Matthew C. Elder, Anton T Dahbura, Matthew Green, Lanier Watkins, *Cost-Effective Mission Assurance Engineering Through Simulation*, The 2021 International Conference on Internet of Things and Intelligence Systems (IoTIS'21), (November, 2021).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Meteor: Cryptographically Secure Steganography for Realistic Distributions*, 28th ACM Conference on Computer and Communications Security (CCS '21), (November, 2021).
- James Schaffter, Aviel Rubin and Lanier Watkins, *A Containerization-Based Backfit Approach for Industrial Control System Resiliency*, SafeThings '21 Workshop, (May, 2021).
- Tushar Jois, Claudia Moncaliano, Khir Henderson, Aviel D. Rubin, *WDPKR: Wireless Device Profiling Kit and Reconnaissance*, 2021 Hot Topics in the Science of Security (HotSoS) Symposium (April, 2021).
- Lanier Watkins, ChangHao Cho, John Hurley, Aviel D. Rubin, *Collaborative Global Impact Cloud Computing Risk Assessment Framework*, International IoT, Electronics and Mechatronics Conference (IEMTRONICS '21), (April, 2021).
- Jeffrey S. Chavis, Malcom Doster, Michelle Feng, Syeda Zeeshan, Samantha Fu, Elizabeth Aguirre, Antonio Davila, Kofi Nyarko, Aaron Kunz, Tracy Herriotts, Daniel Syed, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Voice Assistant for IoT Cybersecurity*, Integrated STEM Education Conference (ISEC '21), (March, 2021).
- Lanier Watkins, Danzel Hamilton, Kevin Kornegay, Aviel Rubin, *Triaging Autonomous Drone Faults by Simultaneously Assuring Autonomy and Security in Autonomous Drones*, 55th Annual Conference on Information Sciences and Systems (CISS '21), (March, 2021).
- Lanier Watkins, James Ballard, Kevin Hamilton, William H. Robinson, Aviel Rubin, Cleon Davis, *Bio-Inspired, Host-based Firewall* (Refereed WIP paper), 23rd IEEE International Conference on Computational Science and Engineering (CSE), (December, 2020).
- Lanier Watkins, Yue Yu, Sifan Li, William H. Robinson, Aviel D. Rubin, *Using Deep Learning to Identify Security Risks of Personal Mobile Devices in Enterprise Networks*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).

- Lanier Watkins, Kevin D. Fairbanks, Chengyu Li, Mengdi Yang, William H. Robinson, Aviel D. Rubin, *A Black Box Approach to Inferring Characterizing, and Breaking Native Device Tracking Autonomy*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).
- Karl Siil, Aviel Rubin, Matthew Elder, Anton Dahbura, Matthew Green, Lanier Watkins, *Mission Assurance for Autonomous Undersea Vehicles*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Jeffrey Chavis, Aaron Kunz, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Capability for Autonomous IoT System Security: Pushing IoT Assurance to the Edge*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Lanier Watkins, Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, William H. Robinson, Aviel Rubin, *Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool*, ISOC Workshop on Decentralized IoT Systems and Security (DISS 2020), (February, 2020).
- Adrian Cartagena, Gerald Rimmer, Thomas Van Dalsen, Lanier Watkins, William H. Robinson, Aviel D. Rubin, *Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Jeffrey Chavis, Lanier Watkins, Anna Buczak, Aviel D. Rubin, *Connected Home Automated Security Monitor (CHASM): Protecting IoT Through Application of Machine Learning*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Lanier Watkins, Shreya Aggarwal, Omotola Akeredolu, William H. Robinson and Aviel D. Rubin, *Tattle Tail Security: An Intrusion Detection System for Medical Body Area Networks*, Workshop on Decentralized IoT Systems and Security (DISS '19), (February, 2019).
- Lanier Watkins, Juan Ramon, Gaetano Snow, Jessica Vallejo, William H. Robinson, Aviel D. Rubin, Joshua Ciocco, Felix Jedrzejewski, Jinglun Liu, Chengyu Li, *Exploiting Multi-Vendor Vulnerabilities as BackDoors to Counter the Threat of Rogue Small Unmanned Aerial Systems*, ACM Workshop on Mobile IoT Sensing, Security, and Privacy (Mobile IoT SSP '18), (June, 2018).
- Paul D. Martin, David Russel, Malek Ben Salem, Stephen Checkoway, Aviel D. Rubin, *Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems*, Proc. ACM/IEEE International Conference on Internet-of-Things Design and Implementation, (April, 2018).
- Gabriel Kaptchuk, Matthew D. Green and Aviel D. Rubin, *Outsourcing Medical Dataset Analysis: A Possible Solution*, Financial Cryptography Conference, (April, 2017).
- Michael Rushanan, David Russell and Aviel D. Rubin, *Mallory-Worker: Stealthy Computation and Covert Channels using Web Workers*, Proceedings of the 12th International Workshop on Security and Trust Management, (September, 2016).
- Paul Martin, Michael Rushanan, Thomas Tantillo, Christoph Lehmann and Aviel Rubin, *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics, (October, 2016).

- Gabriel Kaptchuk and Aviel D. Rubin, *A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker*, Proceedings of the 15th Annual Security Conference, (March, 2016).
- Aviel D. Rubin, *Taking Two-Factor to the Next Level: Protecting Online Poker, Banking, Healthcare and Other Applications*, Proceedings of the 2014 Annual Computer Security Applications Conference, Invited Keynote Essay, (December, 2014).
- Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy-SoK Track (May, 2014).
- Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, 1st Workshop on Bitcoin Research (March, 2014).
- Paul Martin, Aviel Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control*, Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).
- Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
- Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).
- Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
- Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report 4-page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January, 2010).
- Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones*, Workshop on Security and Privacy in Medical and Home-Care Systems, (November, 2009).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).
- Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
- Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM '07), (November, 2007).
- Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).

- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
- Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
- Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Aviel Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
- Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem*, Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
- Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device*, 14th USENIX Security Symposium, (August, 2005).
- Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
- Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks*, Proc. 11th International Workshop on Security Protocols (April, 2003).
- Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
- Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Workshop on Privacy in the Electronic Society (November, 2002).
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).
- Aviel D. Rubin and Rebecca N. Wright, *Offline generation of limited-use credit card numbers*, Financial Cryptography Conference, (February, 2001).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Sign-on Protocol*, 9th International World Wide Web Conference, (May, 2000).
- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, Financial Cryptography Conference, (February, 2000).

- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device*, 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monroe, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords*, 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monroe, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground*, Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread Email in an Untrusted Network*, Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monroe and Aviel D. Rubin, *Authentication via Keystroke Dynamics*, 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin, *PseudoRandom Functions for OneTime Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

- Aviel D. Rubin, "Broadband Certified Mail", **US Patent Numbers 6,990,581**, (January 24, 2006) and 9,876,769, (January 23, 2018).

- Aviel D. Rubin, Utilization of multiple devices to secure online transactions, **US Patent Number 9,064,376**, (June 23, 2015).
- Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Numbers 8,239,531**, (August 7, 2012) and **8,676,916** (March 18, 2014).
- Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
- Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).
- Frederick Douglass, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
- William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T. Marshall, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
- Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
- Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

Board of Directors

Director, Maryland Israel Development Center (MIDC), (2013-2018).

Director, USENIX Organization, elected by popular vote (2000-2004).

Editorial and Committees

Chair: IEEE Security & Privacy Symposium Test of Time Awards Committee for 2008-2010 Conferences, May, 2020.

Associate Editor: IEEE Transactions on Information Forensics and Security (2009 - 2011).

Associate Editor: Communications of the ACM (CACM), 2009 - 2017.

Guest Co-Editor: IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, December 1, 2009.

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting, October/November, 2007.

Associate Editor: IEEE Transactions on Software Engineering (2005-2006). Editorial and

Advisory Board: International Journal of Information and Computer Security (IJICS) (2004 - 2006).

Guest Co-Editor: IEEE Computer Networks, Special Issue on Web Security, January, 2005.

Editorial Board: Journal of Privacy Technology (2004-2006).

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting Security, January/February, 2004.

Member: Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003 - 2004.

Member: DARPA Information Science And Technology Study Group (2003 - 2006).

Associate Editor: IEEE Security & Privacy Magazine (2003 - 2011).

Guest Editor: Communications of the ACM, Special Issue on Wireless Networking Security, May, 2003.

Associate Editor: ACM Transactions on Internet Technology (2002-2005).

Executive Committee Member: DIMACS Workshop Series with Special Focus on Network Security (2002 - 2004).

Advisory Board Member: Information Security and Cryptography Book Series, Springer, 2001- 2006.

Member: Steering Group, ISOC Symposium on Network and Distributed System Security, 2001 - 2004.

Member: Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.

Member: AT&T Internet Intellectual Property Review Team, 1999 - 2001. Associate Editor: Electronic Commerce Research Journal, Baltzer Science Publishers, 1999 - 2002.

CoEditor: Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.

Editorial Board: Bellcore Security Update Newsletter, 1995 - 1996.

Conference Committees

- **Program Committee member:** NDSS Workshop: Innovative Secure IT Technologies Against COVID19, San Diego, CA, February, 2020.
- **Program Committee member:** Financial Cryptography '15 Barbados, February, 2015.
- **Program Committee member:** USENIX HealthTech Workshop on Health Information Technologies (HealthTech '15), August 11, 2015.
- **Program Co-chair:** (w/Eugene Vasserman) USENIX HealthTech Workshop on Health Information Technologies (HealthTech '14), August 19, 2014.
- **Program committee member:** 2nd USENIX Workshop on Health Security & Privacy (HealthSec '11), August 9, 2011.
- **Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- **Program Committee member:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
- **Invited Talks Co-Coordinator:** 17th USENIX Security Symposium, San Jose, CA, July 28 August 1, 2008.
- **Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 18-22, 2008.
- **Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
- **Program Committee member:** Financial Cryptography '04 Key West, Florida, February 9-12, 2004.

- **Program Committee member:** 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- **Program Committee member:** 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- **Program Committee member:** 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 2004, 2003.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 11-14, 2003.
- **Program Committee member:** Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- **Program Committee member:** 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRD), Singapore December 9-12, 2002.
- **Program Committee member:** ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- **Program Committee member:** 9th ACM Conference on Computer and Communications Security, Washington D.C., November 17-21, 2002.
- **Program Committee member:** 5th International Conference on Electronic Commerce Research (ICECR5), Montreal, Canada, October 23-27, 2002.
- **Program Committee member:** 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 14-15, 2002.
- **Program Committee member:** 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 14-16, 2002.
- **Program Committee member:** 11th USENIX Security Symposium, San Francisco, Ca, August 5-9, 2002.
- **Program Committee member:** International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 21-24, 2002.
- **Program Committee member:** 11th International World Wide Web Conference Honolulu, Hawaii, May 7-11, 2002.
- **Program Committee member:** 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 14-15, 2002.
- **Program Committee member:** The 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 7-8, 2002.
- **Program Committee member:** The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001. **Program Committee member:** 10th USENIX Security Symposium, Washington D.C., August 13-17, 2001.
- **Program Committee member:** Financial Cryptography '01 Grand Cayman, Cayman Islands, BVI, February, 2001.
- **Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 7-9, 2001.
- **Program Committee member:** The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 16-19, 2000. **Program Committee member:** 9th USENIX Security Symposium, Denver, Colorado, August 14-17, 2000.

- **Program Committee member:** Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 2526, 2000.
- **Program Committee member:** Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
- **Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 24, 2000.
- **Program Committee member:** 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 67, 1999.
- **Program Committee member:** 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 68, 1999.
- **Invited Talks coordinator:** 8th USENIX Security Symposium, Washington D.C., August, 1999.
- **Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 711, 1999.
- **Program Committee member:** 8th International World Wide Web Conference , Toronto, Canada, May 1114, 1999.
- **Program Committee member:** 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 September 3, 1998.
- **Program Committee member:** 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 35, 1998.
- **Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 2629, 1998.
- **Program Committee member:** 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 24, 1997.
- **Program Committee member:** 6th USENIX Security Symposium, San Jose, CA, July 2225, 1996.
- **Program Committee member:** ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2223, 1996.

Panels

- **Panelist:** CyberTech Global Conference: The Post-COVID Cyber Challenges in the Health Sector, UAE-Dubai (April 6, 2021).
- **Panel Organizer and Moderator:** USENIX Security Conference: The 2020 Election: Remote Voting, Disinformation, and Audit (August 12, 2020).
- **Panelist:** Cardozo Society Associated panel: Cybersecurity and Privacy Law in the Digital Era, Baltimore, MD (February 19, 2020).
- **Panelist:** Washington Post panel: Hacking Health, Washington DC (June 14, 2016).
- **Panelist:** Financial Cryptography Conference, Security & Privacy, Barbados (February 24, 2016).
- **Panelist:** RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
- **Panelist:** Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).
- **Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).

- **Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
- **Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
- **Panelist:** American Association for the Advancement of Science, Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel, Washington DC, (November 27, 2006).
- **Panelist:** California Secretary of State's Voting System Testing Summit, Security Panel, Sacramento, CA, (November 2829, 2005).
- **Panelist:** NIST Symposium on Voting System Threats, Configuration and Usability Threats, Gaithersburg, MD, (October 7, 2005).
- **Panelist:** Conference of State Supreme Court Chief Justices, Voting Technologies, Charleston, SC (August 1, 2005).
- **Panelist:** Workshop on observation of automated elections, The Carter Center, Atlanta, GA (March 18, 2005).
- **Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).
- **Panelist:** Workshop on Voting, Vote Capture and Vote Counting, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
- **Panelist:** Computer Science and Telecommunications Board of The National Academy of Science Workshop on Dependable Software Systems, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** Democracy Now, 2003, Voter-Verifiable Elections: How Do We Get There?, Washington D.C. (November 23, 2003).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** IEEE Infocom 2002, Securing Wireless and Mobile Networks, Is It Possible?, New York City (June 25, 2002).
- **Participant:** 2002 Security Visionary Roundtable: A Roadmap for a Safer Wireless World, Washington D.C., (May 5-7, 2002).
- **Panelist:** Computers Freedom and Privacy 2002, Who Goes There? Privacy in Identity and Location Services, San Francisco (April 18, 2002).
- **Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe Overview of On-Line Voting: Systems and Issues, New York, NY (March, 2001).
- **Panelist:** Financial Cryptography 2001, The Business of Electronic Voting, Grand Cayman (February, 2001).
- **Panelist:** National Science Foundation E-voting workshop, Washington, D.C., (October, 2000).
- **Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November, 1998).
- **Panelist:** Open Systems Security and ISSA Annual Conference, Securing the Web, Orlando, FL (March, 1998).

- **Panel organizer and moderator:** Implementation Issues for Electronic Commerce: What Every Developer Should Know. ISOC Symposium on Network and Distributed System Security, (March, 1998).
- **Panel organizer and moderator:** Downloadable Executable Content Past, Present and Future. ISOC Symposium on Network and Distributed System Security (February, 1997).
- **Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

Testimony

Before Government Bodies

- United States House Committee on Administration, Full Committee Hearing, Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House, Live via WebEx, (July 17, 2020).
- Maryland House, Expert Testimony, Hearing on HB 888, Consumer Protection, Security Features for Connected Devices, Economic Matters Committee, Annapolis, MD, (February 26, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 443 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 19, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 553/HB 1276 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 26, 2019). United States Pentagon, High Level Security Briefing on the Security of Embedded Devices (January 15, 2014).
- United States House Committee on Science, Space, and Technology, Full Committee Hearing Is My Data on Healthcare.gov Secure?, Washington, D.C., (November 19, 2013).
- United States House Committee on Oversight and Government Reform, hearing on electronic voting, Washington, D.C., (April 18, 2007).
- United States House Committee on Appropriations, hearing on ensuring the integrity of elections, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, Hearing on Senate Bill 392 for VoterVerified Records in Voting Systems, Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 18 for improving voting systems in Maryland, Annapolis, MD, (February 1, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, Hearing on Voluntary Voting Systems Guidelines, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
- Senate hearing: Voting in 2004: A Report to the Nation on America's Election Process, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, Public Hearings on Computer

Security and Transparency, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).

- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, Hearing on Electronic Voting, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, Hearing on Security of Electronic Voting, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, Hearing on Electronic Voting Security, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- Epic Games, Inc & Anor vs. **Apple Inc & Anor.**, Case # NSD 1236 of 2020, Gibson Dunn, Federal Court of Australia, District of New South Wales. (App Store Security & Privacy)
 - Expert Testimony at Trial, Melbourne, Australia (May 29, 2024).
- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent claim construction)
 - Expert Testimony at deposition, Key West, FL (December 18, 2023).
- **Softex LLC** vs Absolute Software Corporation, Dell Technologies Inc, and HP Inc, Case # 1:22-cv-01309-DAE; McKool Smith, United States District Court, Western District of Texas. (Patent Claim Construction)
 - Expert Testimony at deposition, Key West, FL (November 27, 2023).
- **Milliman, Inc** and Vigilytics LLC, vs. Gradient A.I. Corp., Case # 1:21-cv-10865-NMG; K&L Gates, United States District Court, District of Massachusetts. (Patent Claim Construction, Patent Infringement, Patent Validity, Trade Secret)
 - Expert Testimony at deposition, Annapolis, MD (November 27, 2023).
 - Expert Testimony at deposition, Annapolis, MD (November 17, 2022).
- Microsoft Corporation vs. **Mediapointe, Inc**, Case # 2:22-cv-01009-MCS-MRW; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2023).
- Akamai Technologies, Inc vs. **Mediapointe, Inc**, Case # 2:22-cv-06233-MCS-AFM; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 22, 2023).
- Lauri Valjakka vs. **Netflix Inc**, Case # 4:22-cv-01490-JST, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Annapolis, MD (September 8, 2023).
- **TecSec Inc** vs. Oracle, Case # 1:10CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (June 13, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 11, 2020).

- Global Eticket Exchange Ltd. vs. **TicketMaster LLC**, Case # 6:21-cv-00399-ADA, Fish & Richardson, United States District Court, Western District of Texas. (Patent Non-infringement and validity)
 - Expert Testimony at Trial, Waco, TX (May 3, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 31, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 16, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01306, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 20, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01307, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 19, 2023).
- **TecSec Inc** vs. Cisco, Case # 1:10-CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Washington DC (April 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 14, 2020).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
 - Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- Finjan vs. **Palo Alto Networks**, Case # 4:14-CV-04908-PJH, Morrison and Foerster, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Annapolis, MD (March 17, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Annapolis, MD (March 15, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Pikesville, MD (August 16, 2021). (*Claim Construction*)
- Centripetal Networks, Inc. vs. **Keysight Technologies, Inc.**, Investigation No. 337-TA-1314-MJM, Reed Smith LLP, United States International Trade Commission (ITC). (Patent Non-infringement & Domestic Industry Technical Prong)
 - Expert Testimony at Trial, Washington DC (March 6, 2023).
 - Expert Testimony at Deposition, Las Vegas, NV (December 2, 2022).
- **Proxense, LLC**, vs. Samsung Electronics Co., Case # 6:21-cv-00210ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (January 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 30, 2022).
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2022).
- **US Dominion, Inc.** vs. Fox News Network, Case # N21C-03-257-EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (January 10, 2022).
- **Rimini Street, Inc.** vs. Oracle International Corporation, et. al., Case # 2:14-CV-01699 LRHCWH, Gibson Dunn, United States District Court, District of Nevada. (Software security)

- Expert Testimony at trial, Las Vegas, NV (December 9, 2022).
- Expert Testimony at deposition, Baltimore, MD (August 30, 2018).
- **IOEngine, LLC**, vs. Ingenico Inc., Case # 1:18-cv-826 WCB; Dechert LLP, United States District Court, District of Delaware. (Patent Infringement & Patent Validity)
 - Expert Testimony at trial, Wilmington, DE (July 12 & 14, 2022).
 - Expert Testimony at deposition, Annapolis, MD (January 28, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 19, 2022).
- **WSOU Investments, LLC**, vs. Microsoft Corporation, Case # 6:20-cv-00464-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (May 15 & 16, 2022).
- **10Tales Inc.** vs. TikTok PTE. LTD., Case # 4:21-cv-3868-YGR; Cozen O'Connor, United States District Court, Northern District of California. (Patent Claim Construction)
 - Expert Testimony at deposition, Annapolis, MD (May 11, 2022).
- **IOEngine, LLC**, vs. PayPal Holdings, Inc., Case # 1:18-cv-452-WCB; Dechert LLP, United States District Court, District of Delaware. (Patent infringement)
 - Expert Testimony at deposition, Bonita Springs, FL (January 18, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 26, 2022).
- AGIS Software Development LLC vs. **Uber Technologies Inc.**, Case # 2:21-cv-00026-JRG-RSP, Gibson Dunn, United States District Court, Eastern District of Texas. (Non-infringement)
 - Expert Testimony at Deposition, Annapolis, MD (December 22, 2021).
- Sable Networks vs. **Splunk Inc.**, Case # 5:21-CV-00040-RWS, Morrison and Foerster, United States District Court, Eastern District of Texas. (Claim Construction)
 - Expert Testimony at Deposition, Annapolis, MD (December 13, 2021).
- Huawei Technologies Co. vs. **Verizon Communications Inc.**, Case # 6:20-CV-00090, Quinn Emanuel, United States District Court, Western District of Texas. (Patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Pikesville, MD (July 1, 2021).
- Epic Games, Inc. vs. **Apple Inc.**, Case # 4:20-cv-05640-YGR-TSH, Gibson Dunn, United States District Court, Northern District of California. (Sherman Act)
 - Expert Testimony at Trial, Oakland, CA (May 20-21, 2021).
 - Expert Testimony at Deposition, Pikesville, MD (March 26, 2021).
- Philips North America LLC ; Koninklijke Philips N.V. vs. **Summit Imaging Inc.**, Case # 2:19cv01745JLR, Seed IP, United States District Court, Western District of Washington at Seattle. (DMCA and Copyright)
 - Expert Testimony at deposition, Pikesville, MD (March 16, 2021).
- **California Physicians Service, Inc D/B/A Blue Shield of California** vs. Healthplan Services Inc, Case # 3:18-cv-3730 Latham & Watkins, United States District Court, Northern District of California. (Contract Dispute: Software Quality and Security)
 - Expert Testimony at Deposition, Pikesville, MD (March 9, 2021).
- Finjan vs. **Qualys Inc.**, Case # 4:18-cv-07229-YGR, Wilson Sonsini, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at Deposition, Pikesville, MD (March 4, 2021).

- Finjan vs. **Sonicwall Inc.**, Case # 5:17-cv-04467-BLF-HRL, Duane Morris, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Pikesville, MD (October 30, 2020).
 - Expert Testimony at deposition, Pikesville, MD (October 29, 2020).
- **Blackberry Limited** vs. Facebook, Inc, Case #2:18-cv-01844 (KSx), Quinn Emanuel Urquhart & Sullivan, LLP, United States District Court, Central District of California. Expert Testimony at Deposition, Baltimore, MD (December 20, 2019). (patent infringement & patent validity)
- **Netfuel, Inc.** vs. Cisco Systems, Inc, Case # 5:18-cv-2352-EJD, Susman Godfrey, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 16 & 17, 2019). (patent infringement & patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (June 11, 2019). (patent infringement)
 - Expert Testimony at Markman Hearing, San Jose, CA (February 28, 2019). (courtroom tutorial)
 - Expert Testimony at deposition, Baltimore, MD (December 20, 2018). (claim construction)
- **Symantec Corporation** vs. Zscaler, Inc., Case # 3:17-CV-04414-JST, Baker Botts, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 6, 2019). (patent infringement)
 - Expert Testimony at Deposition, Baltimore, MD (August 2, 2019). (Assignor Estoppel)
- Koninklijke Philips vs. **Microsoft Inc**, Case # 4:18-cv-01885-HSG, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Baltimore, MD (July 17, 2019).
- **Cypress Lake Software, Inc.** vs. Samsung Electronics & Dell Inc, Case # 6:18-cv-030-JKD and 6:18cv0138JDK, Garteiser Honea, United States District Court, Eastern District of Texas. (patent infringement and patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (July 1011, 2019).
- Finjan vs. **Juniper Networks**, Case # 3:17-cv-05659-WHA , Irell and Manella, United States District Court, Northern District of California.
 - Expert Testimony at deposition, Baltimore, MD (April 2, 2019). (patent Non-infringement)
 - Expert Testimony at deposition, San Francisco, CA (March 9, 2019). (patent Non-infringement)
 - Expert Testimony at trial, San Francisco, CA (December 13, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 9, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 6, 2018). (patent Non-infringement)

- Expert Testimony at deposition, Baltimore, MD (June 12, 2018). (patent Non-infringement)
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551LHK (NC), Durie Tangri, United States District Court, Northern District of California. (class action)
 - Expert Testimony at deposition, Towson, MD (September 26, 2018).
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551-LHK (NC), Kirkland & Ellis, United States District Court, Northern District of California. (class certification)
 - Expert Testimony at deposition, Pikesville, MD (July 3, 2018).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (January 24, 2018).
- **Amazon.com Inc., Hulu, LLC, and Netflix, Inc.** vs. Uniloc Luxembourg S.A., IPR 201700948, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (October 9, 2017).
- Phishme, Inc. vs. **Wombat Technologies, Inc.**, Case # 16403-LPS-CJB, K&L Gates, United States District Court, Delaware. (patent claim construction)
 - Expert Testimony at deposition, Washington DC, (October 5, 2017).
- Finjan vs. **Symantec Corporation.**, Case # 14-cv-02998-HSG, Quinn Emanuel, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Baltimore, MD (September 14-15, 2017).
- **Kudelski SA, Nagra USA, Inc., Nagravision SA, and OpenTV, Inc.** vs. Comcast Corporation, Case # 2:16-cv-1362-JRG, Covington, United States District Court, Eastern District of Texas. (patent claim construction).
 - Expert Testimony at deposition, Baltimore, MD (September 1, 2017).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 10, 2017).
- Intellectual Ventures vs. **JP Morgan Chase & Co.**, Case # 1:13-cv-03777, Kirkland & Ellis, United States District Court, Southern District of New York. (Patent Non-infringement).
 - Expert Testimony at deposition, Baltimore, MD (June 1, 2017).
- Nader AsghariKamrani and Kamran AsghariKamrani vs. **United Services Automobile Association.** Case # 2:15-CV-478, Fish & Richardson, United States District Court, Eastern District of Virginia. (Patent Written Description Support related to Inequitable Conduct).
 - Expert Testimony at trial, Norfolk, VA (April 21, 2017).
 - Expert Testimony at deposition, Baltimore, MD (March 21, 2017).
- **Sabre GBL Inc.** vs. HP Enterprise Services LLC. Case # 1310022761, JAMS Binding Arbitration Hearing, Dallas, TX (Contract dispute).
 - Expert Testimony at arbitration hearing, Dallas, TX (April 5, 2017).
- **Al Cioffi et. al.** vs. Google, Case # 2:13cv103JRGRSP, Vasquez, Benisek & Lindgren, United States District Court, Eastern District of Texas. (patent Infringement).
 - Expert Testimony at trial, Marshall, TX (February 7, 2016).
 - Expert Testimony at deposition, Baltimore, MD (September 26, 2016).

- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 14, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2016-00151, Morrison & Foerster, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 19, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01974, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 2, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-02001 & IPR 2016-00157, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 26 & 27, 2016).
- **Amazon.com, Inc** vs. Zitovault, LLC, IPR 2016-00021, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 22, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (May 20, 2016).
- **Vir2us Inc. v. Invincea, Inc. and Invincea Labs, LLC**, Case # 2:15-cv-l62; Cooley, United States District Court, Eastern District of Virginia. (Patent Non-infringement and Invalidity)
 - Expert Testimony at deposition, Reston, VA (April 20, 2016).
- **TVIIM. v. McAfee Inc.**, Case # 3:13-cv-04545-VC; Wilmer Hale, United States District Court, District of N. California. (Patent Non-infringement and Invalidity)
 - Expert Testimony **at trial**, San Francisco, CA (July, 2015).
 - Expert Testimony at deposition, Baltimore, MD (February, 2015).
- **Intellectual Ventures vs. Symantec**, Case # 1:10-cv-01067-LPS; Latham & Watkins, United States District Court, District of Delaware. (Patent Invalidity)
 - Expert Testimony **at trial**, Wilmington, DE (February, 2015).
 - Expert Testimony at deposition, Baltimore, MD (May, 2013).
- **Rovi Solutions & Veracode** vs. Appthority, Case # 1210487-DPW; Goodwin Procter, United States District Court, District of Massachusetts. (Patent Infringement and Validity)
 - Expert Testimony **at trial**, Boston, MA (August 11, 2014).
 - Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
- **Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR; Irell & Manella, United States District Court, District of Delaware. (Patent Infringement)
 - Expert Testimony **at trial**, Wilmington, DE (February, 2014).
 - Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).
 - Expert Testimony at deposition, Baltimore, MD (June, 2013).
- **Prism Technologies. v. Adobe Systems Inc.**, Case # 8:10-cv-00220-LEST-DT; DLA Piper, United States District Court, District of Nebraska. (Patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August, 2012).
- **Finjan Inc. vs. McAfee, Inc.**, Case # 10593 (GSM), Kirkland & Ellis, United States District Court, District of Delaware. (Patent Non-infringement)
 - Expert Testimony at deposition, Washington, DC (June, 2012).

- Avaya Inc. vs. **Telecom Labs Inc., TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB); K&L Gates, United States District Court, District of New Jersey. (Contract Dispute)
 - Expert Testimony at deposition, Newark, NJ (August, 2011).
- **Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461; Flachsbar & Greenspoon, United States District Court, Eastern District of Michigan. (Patent Infringement and Validity)
 - Expert Testimony **at trial**, Detroit, MI (February, 2011).
 - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- **TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV-115-LMB/TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement)
 - Expert Testimony at deposition, Newark, NJ (November, 2010).
- **Echostar Satellite Corporation** vs. NDS Group, Case # SA-CV-03950-DOC(JTL); T. Wade Welch & Associates, United States District Court, Central District of California. (Copyright and DMCA)
 - Expert Testimony **at trial**, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- **Web.com Inc** vs. The Go Daddy Group Inc., Case # CV-0701552-PHX-MHM; Graves Law Office, United States District Court, Arizona. (Patent Infringement)
 - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
 - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED; Fish & Richardson, United States District Court, Eastern District of Texas. (Patent Non-Infringement and Invalidity)
 - Expert Testimony **at trial**, Tyler, TX, (April, 2006).
 - Expert Testimony at deposition, Washington DC (January, 2006).
- **Linda Schade** vs. Linda Lamone et. al., Trial on the Legality of Paperless Voting Machines in Maryland. (Adequacy of Voting Equipment)
 - Expert Testimony **at trial**, Annapolis, MD (August 25, 2004).

Awards

- 2020, **Best Paper Award**, in the category of Mobile & Wireless Computing, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- 2020, **Best Paper Award**, in the category of Image Processing & Multimedia Technology, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- IEEE Computer Society Technical Committee on Security and Privacy, **Distinguished Service Award**, May, 2020.
- **Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.
- 2009, **Google Research Award**, Securing Medical Records on Smartphones.
- Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.

- 2007 **Award for Outstanding Research in Privacy Enhancing Technologies**, for Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2004 Electronic Frontiers Foundation **Pioneer Award**.
- **Baltimorean of the Year**, Baltimore Magazine, January, 2004.
- 2001 Index on Censorship **Freedom of Expression Award** for the Best Circumvention of Censorship for the Publius project.
- 2000 **Best Paper Award** at the 9th USENIX Security Symposium, A robust, tamper-evident and censorship-resistant web publishing system (with Marc Waldman and Lorrie Cranor).
- 1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, The Design and Analysis of Graphical Passwords (with Ian Jermyn, Alain Mayer, Fabian Monroe, and Michael K. Reiter).
- 1996 Coauthor of **Best Student Paper**, Building Systems that Flexibly Control Downloaded Executable Content, at the 6th USENIX UNIX Security Symposium. Student: Trent Jaeger.
- 1992 National Science Foundation **Fellowship Summer Institute in Japan**
- 1986 **Branstrom Prize**, University of Michigan

Technical Advisory Boards

Current Positions

Qualytics: Data Quality Assurance

RunSafe: Binary rewriting to protect software

MarinaLife: Online boat slip bookings

Past Technical Advisory Board Positions with Successful Exits

Arbor Networks: Acquired by Danaher, August, 2010.

Authentica: Acquired by EMC Corporation, March, 2006.

Fortify Software: Acquired by Hewlett Packard, September 2010.

Gilian Technologies: Acquired by Breach Security, Inc, July, 2004.

Hx Technologies: Acquired by MEDecision, May, 2009.

Indigo Security: Acquired by Tablus, February, 2005.

NeoPath Networks: Acquired by Cisco, April, 2007.

Netscaler: Acquired Citrix Systems, August, 2005.

SiteAdvisor: Acquired by McAfee, April, 2006.

Tablus: Acquired by EMC Corporation, August, 2007.

ZeroFox: Public Offering via SPAC, July, 2022.