UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Dolby Laboratories, Inc.

Petitioner,

v.

Intertrust Technologies Corporation,

Patent Owner.

Case IPR2020-00660
Patent No. 6,785,815

PATENT OWNER'S EXHIBIT 2027
DECLARATION OF DR. MARKUS JAKOBSSON
IN SUPPORT OF PATENT OWNER'S RESPONSE

1. I have been retained on behalf of Intertrust Technologies Corporation ("Patent Owner" or "Intertrust") in connection with the above-captioned *inter partes* review (IPR). I have been retained to provide my opinions in support of Intertrust's Patent Owner Response. I am being compensated for my time at the rate of $650 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this declaration, I have reviewed and am familiar with the Petition for IPR2020-00660, U.S. Patent No. 6,785,815, ("the '815 patent") and its file history, and all other materials cited and discussed in the Petition (including the declaration and deposition transcript of Vijay Madisetti, Ph.D) and cited and discussed in this Declaration.

3. I understand the Petition proffers two invalidity grounds for claims 42 and 43 (the "Challenged Claims") of the '815 patent (Ex. 1001): (1) obviousness over PCT Publication WO 99/40702 ("Hanna") in view of U.S. Patent No. 5,629,980 ("Stefik") (Petition at 19-41); and (2) obviousness over U.S. Patent No. 6,009,176 ("Gennaro") (Petition at 42-59).

4. The statements made herein are based upon my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

I. QUALIFICATIONS

5. My qualifications can be found in my Curriculum Vitae (Appendix A), which includes my detailed employment background, professional experience, and list of technical publications and patents.

6. I am currently Principal Scientist at ByteDance and the CTO at ZapFraud, a cybersecurity company that develops techniques to detect deceptive emails, such as Business Email Compromise emails. At ByteDance and at ZapFraud, my research studies and addresses abuse, including social engineering, malware and privacy intrusions. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches.

7. I received a Master of Science degree in Computer Engineering from the Lund Institute of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

8. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract

exchange, digital commerce including crypto payments, and fraud detection and prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. During that time, I predicted the rise of what later became known as phishing. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

9. From 2004 to 2016, I held a faculty position at the Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books.

10. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, Chief Scientist at Agari from 2016 to

2018, and Chief of Security and Data Analytics at Amber Solutions from 2018 to 2020.

11. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

12. Amber Solutions is a cybersecurity company that develops home and office automation technologies. At Amber Solutions, my research addressed privacy, user interfaces and authentication techniques in the context of ubiquitous and wearable computing.

13. I have founded or co-founded several successful computer security companies. In 2005 I co-founded RavenWhite Security, a provider of authentication solutions, and I am currently its Chief Technical Officer. In 2007 I co-founded Extricatus, one of the first companies to address consumer security education. In 2009 I founded FatSkunk, a provider of mobile malware detection software; I served

as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. In 2013 I founded ZapFraud, a provider of anti-scam technology addressing Business Email Compromise, and I am currently its Chief Technical Officer. In 2014 I co-founded RightQuestion, a security consulting company.

14. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Stealth Security (an anti-fraud company). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

15. I have authored seven books and over 100 peer-reviewed publications, and have been a named inventor on over 100 patents and patent applications.

16. My work has included research in the area of applied security, privacy, cryptographic protocols, authentication, malware, social engineering, usability and fraud.

17. I have been engaged as a technical expert in over 40 computer-related cases, including numerous cases involving Internet security.

II. LEGAL UNDERSTANDING

A. Legal Principles

18. I am not a lawyer and will not provide any legal opinions. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

1. Priority

19. I am informed and understand that for a patent to claim the benefit of an earlier provisional application, the provisional must comply with the written description requirement of 35 U.S.C. § 112. To satisfy the written description requirement, the specification of the provisional must contain a written description of the claimed invention and the manner and process of making and using it, in such full, clear, concise, and exact terms to enable an ordinarily skilled artisan to practice the invention. Moreover, the provisional application must describe the later claimed invention in sufficient detail that a person of ordinary skill in the art can clearly conclude that the inventor had possession of the claimed invention as of the provisional filing date.

2. Obviousness

20. I understand that to obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of prior art in the field. I understand

that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.

21. I understand that to prove that prior art, or a combination of prior art, renders a patent obvious, it is necessary to: (1) identify the particular references that singly, or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined to create the inventions claimed in the asserted claim.

22. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art, and that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention.

23. I also 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, or would be led in a direction divergent from the path that was taken by the applicant. Even if a reference is not found to teach away, I understand its statements regarding preferences are relevant to a

finding regarding whether a skilled artisan would be motivated to combine that reference with another reference.

24. I understand that analogous art is that which is relevant to a consideration of obviousness. I also understand that 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.

25. I understand it its Petitioner's burden to prove that the Challenged Claims would have been obvious. I understand that for *inter partes* reviews, obviousness must be shown by a Petitioner under a preponderance of the evidence standard, which means that Petitioner need needs to prove it is more likely true than not true.

3. Claim Construction

26. I understand that claim interpretation is from the perspective of a person of ordinary skill in the art at the time of the invention.

27. I understand that in this *inter partes* review the claims must be given their broadest reasonable interpretation, but that interpretation must be consistent with the patent specification. In this Declaration, I have used the broadest reasonable interpretation ("BRI") standard when interpreting the claim terms.

B. The Person of Ordinary Skill in the Art

28. I understand that a person of ordinary skill in the relevant art (also referred to herein as "POSITA") is presumed to be aware of all analogous art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

29. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

30. A person of ordinary skill in the art ("POSITA") relevant to the ’815 patent at the time of the invention would have a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the field of digital piracy protection and/or digital rights management ("DRM"), or a Master’s degree in electrical engineering and/or computer science and two years of work or research experience in digital piracy protection and/or digital rights management.

31. I am well-qualified to determine the level of ordinary skill in the art and am personally familiar with the technology of the ’815 Patent. I was a person of at least ordinary skill in the art at the time of the priority date of the Asserted Claims of the ’815 patent.

32. I have reviewed the declaration and deposition transcript of Dr. Madisetti, including his opinions regarding the Person of Ordinary Skill in the Art ("{POSITA"). For the reasons stated below, I disagree with these opinions because Dr. Madisetti has incorrectly described the field of the Challenged Claims of the '815 patent. Otherwise, my description of the level of ordinary skill in the art is essentially the same as that of the Dr. Madisetti, except that his description requires four years of work or research experience (as compared to three years). My ultimate opinions regarding the validity of the Challenged Claims set forth in this Declaration would be the same under either my or Dr. Madisetti’s proposal.

33. I understand that Intertrust has asserted that the Asserted Claims of the '815 patent are entitled to a filing priority date of no later than June 8, 1999, the filing date of provisional application No. 60/138,171 ("'171 Application"). I further understand that Dr. Madisetti opines that the Asserted Claims are entitled to a filing priority date of no later than June 7, 2000, the filing date of U.S. Application No. 09/588,652 ("’652 Application").

34. For the reasons stated below, I disagree with Dr. Madisetti's opinion that the "relevant timeframe" for analyzing the alleged obviousness of claims 42 and 43 is "on or before June 7, 2000." *See* Ex. 1002, ¶ 47. Rather, it is my opinion that the "relevant timeframe" is on or before June 8, 1999, the filing date of the '171 Application.

35. If I do not explicitly state that my statements below are based on a specific timeframe, all of my statements are to be understood as a POSITA would have understood something as of the filing date of the '171 Application, unless stated otherwise. To the extent that I apply Dr. Madisetti's timeframe in forming my opinions, or that my opinions would change if the Board finds that Dr. Madisetti's timeframe is correct, I explicitly state that below.

36. The '171 Application's "Field of the Invention" section describes that the "present invention relates generally to systems and methods for protecting content that is stored or distributed using electronic media. More specifically, the present invention relates to systems and methods for controlling access to electronically stored information through the use of watermarking and digital signature techniques." Ex. 1004 at 1.

37. The '815 specification provides that the "Field of the Invention" is essentially the same as described in the '171 Application: The present invention relates generally to systems and methods for protecting data from unauthorized use

or modification. More specifically, the present invention relates to systems and methods for using digital signature and watermarking techniques to control access to, and use of, digital or electronic data. Ex. 1001 at 1:23-28.

38. The use of watermarking and digital signature techniques for controlling access to electronical content is within the field of digital piracy protection and/or digital rights management.

39. In his declaration, Dr. Madisetti opines that "I believe that the relevant general fields for the purposes of the '815 patent are electronic data protection and distribution." Ex. 1002, ¶ 46. I disagree, and note that Dr. Madisetti does not provide any evidence to support his description of the field of invention, nor does he define the scope of the fields of "electronic data protection and distribution."

40. First of all, "electronic data protection" is so broad as to make it irrelevant. For example, as a POSITA would understand that term, it would encompass encryption functions such as the Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Researchers studying how to create these types of encryption functions, for example, are concerned with creating block ciphers for the purpose of encrypting electronic data. Encrypting electronic data protects the electronic data from being known. At the same time, "electronic data protection" would also cover research into how long passwords should be to avoid people using passwords that can easily be brute forced. In another example, it would

also cover software such as the Kerberos software tool from the 1980s that was used to control who could access what data on a server. Almost any effort related to cryptography and Internet security involves some form of electronic data protection.

41. Similarly, "electronic data distribution" is also much too broad, as this would entail anything from satellite broadcast methods to email transmission standards to the file transfer protocol (FTP). Combining these fields as "electronic data protection and distribution", results in single field that would cover the transmission of any electronic data if such data has been protected in some way. This is very much like answering "Planet Earth" if somebody asks you for your address.

42. Dr. Madisetti testified that in this context, the field of "electronic data protection and distribution" "is "very similar" to the field of "digital file security," and was unable to identify any differences between them. Ex. 2026 at 171:16-172:1.

43. I disagree. In my opinion, the field of "electronic data protection and distribution" is not very similar to the field of "digital file security."

44. First of all, "digital file security" is not a term of the art, so there is no agreed-upon meaning of the term, whether in the context of the '815 patent or not. That said, a POSITA would have understood, for example, that one way of securing digital files would be to back them up, e.g., by copying them onto an archival unit. This would not have been called "electronic data protection", though, and has nothing to do with any distribution of the associated data. As a second example, a

POSITA would have understood that protection against computer viruses would be a form of "digital file security" since computer viruses infect software, which are files. While there are also files that comprise data, these are not the targets of computer viruses, since data files are not executable and computer viruses must infect executable files to be successful. Thus, anti-virus technology would not provide "electronic data protection and distribution". Conversely, not all data is in the format of files. For example, the output of a biometric sensor is data (describing, for example, a fingerprint) but is not a file. Therefore, data can be protected – and distributed – without the provision of any file security.

45. Whereas there are overlaps between "electronic data protection and distribution" and "digital file security," the most notable similarity in this context may be that they both describe very broad technological areas; as such, they are not very meaningful for the purposes of the describing the field of endeavor of the ’815 patent (including the Challenged Claims) or the asserted prior art.

46. I note that in a co-pending *inter partes* review, IPR20202-00663, Dr. Madisetti has opined that the field of the claims at issue in that IPR is "data protection, electronic content protection, and/or digital rights management." Ex. 2024 at 0022-00223. This indicates that Dr. Madisetti believes that "data protection" is a separate field from "electronic content protection" and "digital rights management."

47. In considering whether any of these descriptions would be an appropriate description of the field of the Challenged Claims, I note that "data protection" is even broader than "electronic data protection." In addition, "electronic content protection" is not a term of the art, thereby introducing uncertainty about the breadth of its scope. "Electronic content protection" could be understood to be at least as broad as "data protection" because one form of "electronic content" is "data". A person who distinguishes between "data" and "executable instructions," however, would understand "electronic content protection" to be broader than "data protection". Yet another person that believes "executable instructions" are just one special form of data would concluded that "electronic content protection" is narrower than "data protection." Nevertheless, with respect to the Challenged Claims, both "data protection" and ""electronic content protection," are overbroad, as they capture a wide swath of knowledge and efforts that are unrelated to the Challenged Claims, and for which there would be no overlaps in the skills needed to master these separate fields.

48. As Dr. Madisetti's declaration in IPR2020-00663 demonstrates, he recognizes that "digital rights management" is its own field, but he apparently does not believe it is an appropriate field for the Challenged Claims of the '815 patent. Ex. 2024 at 0022-0023. I disagree. The DRM field (also referred to as "Electronic Rights Protection") is a specialized field of security that is concerned with how to

control what information can be accessed and used by what parties, and under what conditions. This is determined by the "rights" that an entity has with respect to a particular digital work. Example of rights addressed by a DRM scheme include the rights to view a given satellite TV program; view an issue of a subscription-only magazine, or watch a movie a specified number of times within a given time period. DRM is particularly focused on the management of rights in the presence of a potential adversary with physical and logical access to a device comprising the content to be controlled by the rights. For example, a satellite decoder can receive the signal from any selected channel, but will only decrypt and enable the playing of programming that the user operating the decoder has paid for. As is well known by a POSITA, unscrupulous individuals would sell "pirate decoders" that would enable cheating users to access programming they had not paid for. This, of course, is not an example of a well-designed DRM system, but rather, of one that can be broken. However, this highlights the need for specialization within the area of security; accordingly, a person asked to design a DRM system would preferably have a good understanding of the risks that are caused by an adversary with physical and logical access to devices with access to proprietary content.

49. DRM technology addresses, among other things, how to curb copyright infringement and other types of acts of piracy. For example, DRM technology commonly is used to provide digital piracy protection by controlling the conditions

under which a file can be copied. However, DRM systems can also be used to control files in ways that are not protection against digital piracy, as the rights associated with content can specify any types of limitations of use, whether related to protecting against digital piracy or not. Similarly, whereas many digital piracy protection methods use DRM technologies to achieve their goals, not all do. For example, a vendor may place a hologram on a unit with digital content (such as a DVD movie) in order to protect against piracy of the digital content of the DVD; however, that does not have to utilize DRM technologies.

50. Dr. Madisetti also recognized the distinct field of DRM when he states that he has "nearly thirty issued or pending applications for US Patents in the past twenty years" in fields that include "content management and digital rights management." Ex. 1002 at ¶ 28 .

51. Therefore, I disagree with Dr. Madisetti's definition of the field of the inventions of claim 42 and 43.

III. TECHNICAL BACKGROUND AND STATE OF THE ART

A. The Adversarial Model

52. In a DRM system, an entity that owns and/or has access to a piece of proprietary content determines whether to allow the use of that content by another entity.

53. A POSITA would understand the adversarial model (sometimes referred to as the "threat model" or, even more simply, as the "model") is important to take into consideration when designing an electronic data system.

54. The adversarial model may be applied to a system that uses digital piracy protection or DRM techniques. In such a system, the potential adversary of the content owner is the user of the device that contains the content.

55. Adversarial models have been a prominent part of security research since at least the 1980s. One early example is the model introduced by Dolev and Yao in their paper, "On the Security of Public Key Protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198-208 (1983). *See* Ex. 2037. A more recent example is the work of D'Orazio and Choo, who proposed "[a]n adversary model to evaluate DRM protection of video contents on iOS devices" in the case of a physical attack." *See* "An Adversary Model to Evaluate DRM protection of video contents on iOS devices," Computers & Security, vol. 56, pp. 94-110 (2016); *see also* Do et al., "The Role of the Adversary Model in Applied Security Research," Computers & Security, vol. 81 (2018). Over the last 30 years, the notion of an adversarial model has been a critical tool in fields related to cryptography and security, enabling researchers to describe and compare threat scenarios.

56. An example publication from just before the relevant time period that discusses an application of the adversarial model is "Tamper Resistant Software: An

Implementation", by David Aucsmith, published in the Proceedings of the First International Workshop on Information Hiding, pages 317–333, in May 1996. *See* Ex. 2038. Aucsmith states "One of the principal characteristics of the PC is that it is an open, accessible architecture. Both hardware and software can be accessed for observation and modification. Arguably, this openness has led to the PC's market success. This same openness means that the PC is a fundamentally insecure platform. Observation or modification can be performed by either a malevolent user or a malicious program." Ex. 2038 at p. 317. In describing what the author refers to as the "Threat Model," Aucsmith states that "Malicious observation and manipulation of the PC can be classified into three categories, based on the origin of the threat. The origin of the threat is expressed in terms of the security perimeter that has been breached in order to effect the malicious act. This translates generally to who the perpetrator is, outsider or insider." *Id*. at 318.

57. I did work applying the adversarial model in the field of digital piracy protection and digital rights management in the relevant time period of the Challenged Claims. For example, in 2001 (and again in 2002), an article I co-authored, titled "Discouraging Software Piracy Using Software Aging", was published as part of the ACM Workshop on Digital Rights Management. *See* Ex. 2039. This publication described a DRM solution to the problem of software piracy. I began working on this general topic in the 1999-2000 timeframe.

58. Section 2 (titled "Model and Requirements", Ex. 2039 at 3) of the article describes the participants in the DRM adversarial model we considered:

- "Distributor. The distributor sells software, keeps a list of registered users, and maintains a service for software updates for legitimate users. The goal of the distributor is to maximize his profit, and to discourage pirate versions of his software from being used.
- "Legitimate users. Legitimate users purchase software from the distributor, and obtain updates from the same. The legitimate users want the piracy protection to be transparent as far as possible, in the sense that it should cause a minimum of negative side effects (such as delays and increases of file sizes). In other words, in terms of the features offered to the users, the legitimate users want their software to be as close as possible to the ideal of the software (where we use the word "ideal" as done by Plato)."
- "Pirate. The pirate obtains the software sold by the distributor, and redistributes (potentially altered) copies of the software for a charge. We make the pessimistic assumption that the pirate has access to the source code of the software he wants to redistribute, and that he is capable of altering (and compiling) this in order to remove any

protection mechanisms. The pirate wants to maximize his profit and minimize the risks of discovery/prosecution."

- "Illegitimate users. Illegitimate users obtain software from the pirate. Just like the legitimate user, the illegitimate user wants the software he uses to be as close as possible to the ideal of the software - again in terms of the functionality offered to the user. Additionally, illegitimate users want to maximize their profit (by buying software at "piracy discount") and minimize the risks of failure. We assume that illegitimate users generally do not cooperate with one another, but rather interact only with the pirate for the purposes of obtaining software."

59. The adversarial model may also be applied to systems that detect corruption during data transmission. In such a system, the potential adversary is not the receiver of the data transmission because both the sender and receiver are aligned in that they both do not want any of the transmitted data to be corrupted. Rather, one potential adversary during data transmission is any of countless, unknown third parties on the network that may corrupt data. Another potential adversary is the network itself, which can cause errors during transmission.

60. Thus, the adversarial model distinguishes DRM systems from most systems that would be within the broad scope of "electronic data protection and

distribution. For example, in a system like those disclosed by the Hanna or Gennaro prior art references that detect transmission-related data errors (but do not *protect* against such), the adversary corresponds to a flawed or sometimes malicious communication network that does not deliver the same content that it was entrusted to transmit. This is a problem that is traditionally solved by adding message authentication codes or digital signatures to the transmitted data, as Hanna and Gennaro do. But neither Hanna nor Gennaro protect data against transmission errors; they simply detect when such errors take place. Moreover, neither Hanna nor Gennaro detect or protect against an adversary that attempts to interfere with the execution on the device receiving transmitted content. This sets both Hanna and Gennaro apart from DRM systems, since in DRM systems, the adversary includes the user (and software run by the user) of a device receiving content. Such a user may, for example, wish to use content in violation of the rights associated with the content (e.g., play a piece of content more times than the terms permit).

61. The adversarial model is a specification of the threat being addressed by a system. The difference of the adversarial models associated with Hanna and of the '815 patent, and of Gennaro and of the '815 patent, signifies that the different approaches address entirely different problems.

62. It is telling to look at how the different inventors characterize the goals of their inventions. Hanna and Gennaro both speak about detecting corruption. *See,*

e.g., Ex. 1006 at 2:6-7 ("If the data is communicated in discrete packets signed with a bulk signature, detecting corruption or invalid packets inserted by a hacker also carries a high cost"); Ex. 1008 at 2:35-40 ("With this invention, the receiver authenticates the stream without receiving the entire stream. Further the receiver detects corruption of the stream almost immediately after tampering of a portion of the stream."). In contrast, the '815 patent speaks of "preventing" piracy. *See; e.g.,* Ex. 1001 at 21:65-67 ("Content that the owner wishes to prevent from being copied is marked with a strong watermark."), 9:27-29 ("As described above, it is desirable to prevent attackers from copying a digital file from a storage medium such as a compact disc and distributing unauthorized copies to others."). Hanna does not speak at all about "preventing" corruption, and Gennaro uses the word only in the unrelated use describing the action of avoiding unnecessary actions. Ex. 1008 at 7:58-59 ("This prevents the MPEG software consuming unauthenticated data"). This difference in the choice of words is illustrative of the difference in goals: Hanna and Gennaro both *detect* transmission errors, whereas the principal goal of the '815 patent is to *prevent* unauthorized use.

B. Response to Dr. Madisetti's Discussion of the Technical Background and State of the Art

63. Dr. Madisetti's "Technical Background and State of the Art" section of his declaration (Ex. 1002, ¶¶49-60) reads like a Frankenstein creature of separate

and unrelated building blocks. It is difficult to tell whether the failure to recognize this is intentional or not, but it remains a glaring fact that Dr. Madisetti speaks of the existence of a set of known ingredients in order to argue that anything you cook with these ingredients is already a known dish. To begin with, it is worth noting both what technical components Dr. Madisetti identifies from the background prior art references (corresponding to ingredients), and the context in which they are used (the dishes made from the ingredients).

64. The Asserted Claims of the '815 patent are a textbook example of the whole being greater than the sum of its parts; therefore, a piecemeal approach to claiming that it was already known by reciting parts from different references in different fields that address different problems is not meaningful. This is made even less so by the fact that Dr. Madisetti does not identify all of the parts in each reference (such as the notion of "granting a request to use a file in a pre-defined manner", which is directly related to the fact that one computer system can have aspects controlled by two separate entities, whose interests are not always aligned). Moreover, Dr. Madisetti's analysis falls flat not only by arguing that a recipe was known since (some of) its ingredients were known, but also by failing to recognize the purpose of the cited reference. None of the prior art background references that Dr. Madisetti cites in the Technical Background section of his declaration addresses

the problems commonly addressed by digital piracy prevention or DRM systems and methods.

65. Dr. Madisetti cites Exhibit 1009 (Gennaro et al., "How to Sign Digital Streams"). *See, e.g.,* Ex. 1002 at ¶50. This article discusses using signatures and hashing in order to address corruption that occurs during the transmission of data. This is not a digital piracy protection or DRM application, and there is no notion of protecting received content from being inappropriately used. As such, there also is no concept of "granting a request to use a file in a pre-defined manner" disclosed in this article.

66. Dr. Madisetti cites Exhibit 1011 (Squilla). *See, e.g.,* Ex. 1002 at ¶50. Squilla uses signatures as hashing but solves a completely different problem from the Challenged Claims. Squilla is not concerned with transmission errors, nor is it concerned with controlling use (as is an objective of the '815 patent); rather, it addresses the problem of being able to identify/claim authorship of a document. There is no notion of "granting a request to use a file in a pre-defined manner" in Squilla, since there is no attempt to limit who can access data.

67. Dr. Madisetti cites exhibit 1012 (Renaud). *See, e.g.,* Ex. 1002 at ¶50. Renaud (like, for example, Gennaro (Ex. 1008)), addresses corruptions of transmitted data, but (like Gennaro) is not concerned with abuse (unpermitted use) by entities that are sent the data. To the extent that there is abuse, this takes the form

of corruption of data in transmission, as opposed to attempts to access data in violation of controls. In other words, Renaud is not a digital piracy protection or DRM system. Accordingly, the notion of "granting a request to use a file in a pre-defined manner" is absent from Renaud.

68. Dr. Madisetti cites "signature algorithms, such as Message Digest, RSA and DSA." *See* Ex. 1002 at ¶51. To begin with, "Message Digest" is not a signature algorithm, nor is it any other type of algorithm. Message Digest refers to the output of a hash function (as opposed to the hash function itself). Whereas hash functions are commonly used as components of digital signature algorithms, they are not digital signature algorithms; even if they were (which they are not), their outputs would be data (or hashed data, based on one's perspective) as opposed to algorithms. RSA and DSA are signature algorithms that can be used in DRM systems (as demonstrated by the '815 patent); however, a signature algorithm is not a digital piracy protection or DRM system, nor are its uses limited to such systems. A signature algorithm, like an encryption algorithm, is a basic building block that is used in many applications, to address a variety of threats.

69. Furthermore, Dr. Madisetti cites Exhibit 1013 (Dolan). *See, e.g.,* Ex. 1002 at ¶52. Dolan describes a method to encrypt data and transmit the encrypted data to other entities. Whereas Renaud and Squilla seek to detect manipulations of data, Dolan wishes to limit the ability of an adversary to access the plaintext data.

This is a very traditional problem, and one of the original raison d'etre of cryptography, with roots in warfare in ancient Greece. It is not the same as digital piracy protection or DRM. For example, there are no controls associated with the transmitted data, and likewise, the problem addressed is not the problem of controlling how data is accessed and used in a potentially untrusted computational environment, but by what entities the data can be accessed and used. Thus, Dolan wishes to limit an adversary (other than the intended recipient) from being able to decrypt the transmitted data. The intended recipient of the data is not considered a potential adversary, and is provided with the capability of decrypting the data, after which this entity can use the decrypted data in any way it wishes.

70. Dr. Madisetti cites Exhibit 1018 (Ransom), which discloses an application where signals controlling power usage are communicated securely between mutually trusted entities. *See, e.g.,* Ex. 1002 at ¶52. Ransom discusses controlling entities not in the sense of managing their use of content (such as a movie), but rather, in a physical sense. For example, these entities may be controlled in the sense of how electricity or produced or routed. While this is an important and interesting infrastructure problem, it has nothing to do with digital piracy protection or DRM, other than potentially using some of the same building blocks to create the system. This is like arguing that a curry is the same as a cake since they both use salt as an ingredient.

71. Dr. Madisetti further cites Exhibit 1017 (Schneier), which is a publication describing the innards of one particular hash function. *See, e.g.,* Ex. 1002 at ¶53. The Patent Owner is not arguing to have invented hash functions, and the argument Dr. Madisetti appears to make has no merit.

72. Dr. Madisetti uses the phrase "including a hash value in a digital signature" in a vague manner. *See, e.g.,* Ex. 1002 at ¶54. For a typical digital signature (such as DSA, which Dr. Madisetti cites), a hash function is applied to a message, creating a message digest. This message digest is then an input to the signature generation function. However, that is not the same as "including" it in the digital signature.

73. Dr. Madisetti also discusses the generation of multiple hash values for a file. *See, e.g.,* Ex. 1002 at ¶55. As before, he focuses single-mindedly on (some of) the ingredients, and not what is achieved using a particular combination of ingredients. For example, Sprunk (Ex. 1014) is concerned with how to generate digital signatures, and Davis (Ex. 1015) describes how to compress and digitally sign images. Neither of these are in the same field of endeavor as the '815 patent (namely digital piracy prevention and/or digital rights management) nor do they address the same problem as the '815 patent does (namely, how to manage authorized use of content in a potentially hostile computational environment). Thus, neither of these references (nor any of the other prior art cited) disclose (whether inherently or

explicitly) the notion of one entity granting a co-located entity's request to use a file in a predefined manner. The co-location at issue in the '815 patent is a typical complication associated with digital rights management, where a device receiving data has allegiances to both the data owner and the device user (who may attempt to interfere with the operation of usage controls). Therefore, the simple existence of one or more hash values associated with a digital signature, when solving a problem that does not address this computational environment, is not meaningful to the validity of the Challenged Claims.

74. Dr. Madisetti cites Rabin (Ex. 1016) for the proposition that it discloses "making a request, receiving the request, and granting the request to use an electronic file" Ex. 1002 at ¶58. First, "making a request, receiving the request, and granting the request to use an electronic file" does not include a recitation of any of the limitations of the Challenged Claims. Moreover, Dr. Madisetti does not explain how the cited portion from Rabin discloses a request (or granting of such a request) to "use the file in a predetermined manner." Rabin, like the other prior art background references cited by Dr. Madisetti that I've discussed above, has no apparent relevance to the issues in this matter.

75. For these reasons, among others, I disagree with Dr. Madisetti's characterization of the background prior art, and the conclusions he draws from those references regarding the state of the art in the relevant time period.

IV. OVERVIEW OF THE ’815 PATENT

A. The ’815 Patent

76. The ’815 patent describes novel systems and methods for using digital signatures and watermarking techniques to control access to, and use of, data. Ex. 1001 at 1:23-27. The use of "control" in the '815 patent is in the context of an adversary that may attempt to interfere with the computation being performed on a device receiving content. In other words, the goal of the adversary is to defy this control. The objective of the '815 patent, therefore, is to prevent an adversary from using content in a way that he has not established the rights to.

77. The '815 patent seeks to address two problems facing digital content creators. First, it observes that "[t]raditional content-distribution techniques offer little protection from piracy" and that "the threat of piracy has kept the market for digital goods from reaching its full potential." *Id*. at 1:41-43, 1:55-56. Second, and relatedly, it recognizes that "[a]nother problem faced by content owners and producers is that of protecting the integrity of their electronic content from unauthorized modification or corruption" *Id*., 2:6-10.

78. The '815 patent recognizes that that there is "a need for systems and methods for protecting electronic content and/or detecting unauthorized use or modification thereof." Ex. 1001, 2:32-34. "Unauthorized use," as used in this part of the '815 patent, is referring to the use of proprietary content by an entity that does

not have permission to use the electronic content. *See* Ex. 1001, 1:39-48. "Modification thereof," as used in this part of the '815 patent, is referring to modification of the content by the unauthorized entity to circumvent the use restrictions. See Ex. 1001 at 2:6-14.

79. Furthermore, the '815 patent speaks not only of detecting abuse, but also of *preventing* it, setting it apart from both Hanna and Gennaro. The '815 patent seeks to prevent attackers from distributing and playing unauthorized copies of a digital work and to "preserve the security of digital files by detecting unauthorized modifications." Ex. 1001 at 9:27-29 ("As described above, it is desirable to prevent attackers from copying a digital file from a storage medium such as a compact disc and distributing unauthorized copies to others."); 9:65-10:9 ("Some tracks or features may be encoded with a protection scheme (as described in more detail below) that prevents unauthorized copies and/or modified versions of the content from being played on supported devices, but does not otherwise modify the content, thus allowing it to be played on pre-existing or other devices that do not support the protection mechanism. Other tracks on the CD can be encoded in such a manner that they can only be played on devices or systems that include appropriate decoding software or hardware, thus encouraging users to purchase devices and/or software that supports the preferred content protection mechanism.").

80. But the '815 patent is not concerned with preventing modifications to the content that is played (*e.g.*, a music track) because a pirate would not be incentivized to corrupt such data. *See* Ex. 1001 at 1:43-44 (digital technology "enables information to be perfectly reproduced at little cost"). Rather, the patent is concerned with preventing removal of anti-piracy data (*e.g.*, special codes or signed hash files) that the content creator may store with the related content for the purpose of, for example, preventing use of the content on unauthorized devices. *Id*. at 9:52:57; 24:7-9 ("These signed hash files 1400 can be stored on CDs or other media along with the content to which the they relate."); 24:32-34 ("content management module 1534 checks for a signed hash file 1514 corresponding to content 1530"); 24:58-62 ("a user 1524 who downloads a track 1510 from a server 1508 may obtain the corresponding file of signed hashes as part of the same transaction (or by separately connecting to server 1506).") (emphases added). The '815 patent describes that the "content management module uses the signed hash file 1514 to control access to the file as shown in FIG. 13," reproduced below. *Id*. at 24:43-45.

81. Referring to FIG. 13 of the ’815 patent below, the ’815 patent discloses a content management scheme where content is first encoded with a "strong watermark," and then hashes of that content are signed by the content owner and provided to the user. Ex. 1001 at 22:63-13:4.

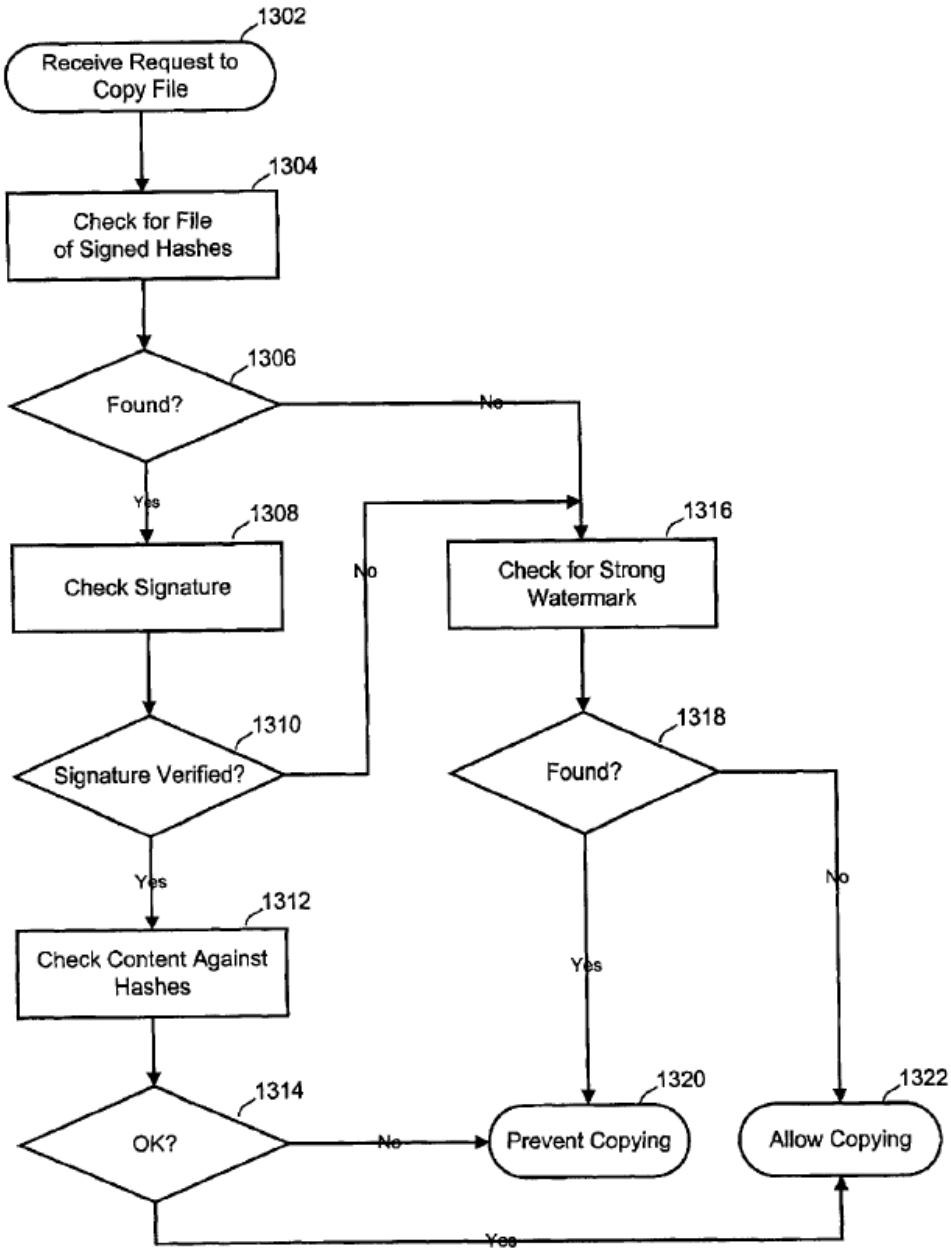

FIG. 13

82. The '815 patent also seeks to prevent attackers from adding special codes to an unprotected piece of content in order to, for example, "use the content on a device that checks for the presence of these codes as a precondition for granting

access to the content or for performing certain actions (*e.g.*, accessing the content more than a certain number of times, printing a copy of the content, saving the content to a memory device, etc.)." *Id*. at 9:57-63. Claims 42 and 43 of the '815 patent are two patented methods that may be used to detect unauthorized attempts to remove or add such encoding and prevent the circumvention of anti-piracy measures.

83. The '815 patent also incorporates by reference U.S. Pat. No. 5,892,900, entitled "Systems and Methods for Secure Transaction Management and Electronic Rights Protection," issued Apr. 6,1999 ("the '900 patent") and assigned to Intertrust. Ex. 1001 at 8:11-18; *see also* Ex. 2025.

84. Although the '900 patent does not describe the inventions disclosed in claims 42 or 43, it provides evidence of how a POSITA would have understood the meaning of the term "granting", as it appears in claims 42 and 43 of the '815 patent.

85. The act of granting is discussed in several places in the '815 patent. One example can be found in Ex. 1001 at 9:57-63: "Similarly, an attacker may attempt to add special codes to an unprotected piece of content in order to use the content on a device that checks for the presence of these codes as a precondition for ***granting*** access to the content or for performing certain actions (e.g., accessing the content more than a certain number of times, printing a copy of the content, saving the content to a memory device, etc.)" (emphasis added).

86. This clarifies that "granting" in the context of DRM depends on information that is not related to whether the content has been corrupted, but rather, the circumstances under which it may be used (*e.g.*, depending on the number of times the file has been accessed exceeds a limit; whether a given party has the right to print a document). This understanding is consistent with how the term would be understood by a POSITA in the field of the '815 patent (*i.e.*, "digital piracy protection and/or digital rights management."). Moreover, how to determine the conditions for when one entity (*e.g.*, the content owner) may grant a request by another entity (e.g., the content user) to use a piece of content in a predefined manner, when both entities may reside on the same computational device, is consistent with the types of problem facing a POSITA that works in the field of digital piracy protection and/or digital rights management. It is also consistent with the application of the adversarial model to such DRM systems; namely the existence of two entities in potential conflict, on the same computational device.

87. The '900 patent provides additional support for this understanding of what "granting" means. *See* Ex. 2025 at 55:53-56 ("A 'permissioning agent' 200*f* may distribute 'rules and controls' granting usage or distribution permissions based on a profile of a consumer's credit worthiness, for example"); 57:1-4 ("For example, the 'rules and controls' shown in FIG. 2 may grant specific individuals or classes of content users 112 'permission' to use certain content."); 156:61-157:12 ("Each rights

record 906 defines a different 'right' corresponding to an object. A 'right" record 906 is the highest level of organization present in PERC 808. There can be several different rights in a PERC 808. A 'right' represents a major functional partitioning desired by a participant of the basic architecture of VDE 100. For example, the right to use an object and the right to distribute rights to use an object are major functional groupings within VDE 100. Some examples of possible rights include access to content, permission to distribute rights to access content, the ability to read and process audit trails related to content and/or control structures, the right to perform transactions that may or may not be related to content and/or related control structures (such as banking transactions, catalog purchases, the collection of taxes, EDI transactions, and such), and the ability to change some or all of the internal structure of PERCs created for distribution to other users. PERC 808 contains a rights record 906 for each type of right to object access/use the PERC grants."); 157:13-20 ("Normally, for VDE end users, the most frequently granted right is a usage right. Other types of rights include the 'extraction right,' the 'audit right' for accessing audit trail information of end users, and a 'distribution right' to distribute an object. Each of these different types of rights may be embodied in a different rights record 906 (or alternatively, different PERCs 808 corresponding to an object may be used to grant different rights)"); 163:55-164:5 ("As described above, secure database 610 stores at least one PERC 808 corresponding to each registered VDE

object 300. PERCS 808 specify a set of rights that may be exercised to use or access the corresponding VDE object 300. The preferred embodiment allows user to 'customize' their access rights by selecting a subset of rights authorized by a corresponding PERC 808 and/or by specifying parameters or choices that correspond to some or all of the rights granted by PERC 808. These user choices are set forth in a user rights table 464 in the preferred embodiment. User rights table (URT) 464 includes URT records, each of which corresponds to a user (or group of users). Each of these URT records specifies user choices for a corresponding VDE object 300. These user choices may, either independently or in combination with a PERC 808, reference one or more methods 1000 for exercising the rights granted to the user by the PERC 808 in a way specified by the choices contained within the URT record."); 186:6-13 ("Such information may include, for example, one or more replacement PERC (s) 808, methods, UDE(s), etc. (block 2482). This enables, for example, a distributor to distribute limited right permissions giving users only enough information to register an object, and then later, upon registration, replacing the limited right permissions with wider permissioning scope granting the user more complete access to the objects.")

88. Thus, a POSITA reading the '815 patent and the '900 patent would have understood that the meaning of "granting" in the context of the '815 patent (which incorporates the '900 patent by reference) requires a context in which the presence

of two or more entities in potential conflict with each other is possible, and in fact, expected. "Granting" means that one of the entities (that is trusted with access to some file) determines that the other entity (that is not *a priori* trusted with the access to the file) has indeed satisfied the requirements to gain access to use the file. However, the use is not arbitrary; according to claim 42, it is a "use … in a predefined manner".

89. If there is not a situation in which there are two or more entities in potential conflict with each other, then the notion of "granting" is not pertinent because (1) an entity would not "grant" itself access to use a file in a predefined manner of it already has access to the file, and (2) it would not grant access to an entity to use a file that it is, by default, already permitted to use.

B. <u>The Provisional Application</u>

90. The ’652 Application that led to the '815 patent claims priority to provisional application No. 60/138,171 ("'171 Application"), filed on June 8, 1999, which is also incorporated by reference into the ’815 patent. *See* Ex. 1001 at 1:6-11.

91. The '171 Application describes that the "present invention relates to systems and methods for controlling access to electronically stored information through the use of watermarking and digital signature techniques." Ex. 1004 at 1.

92. The '171 Application recognizes that "[a]s the electronic storage and

transmission of music, movies, documents, and other forms of proprietary content becomes more prevalent, owners of proprietary content have grown increasingly concerned with protecting that content from unauthorized use." Ex. 1004 at 1. The '171 Application describes that standards and encoding schemes "generally seek to protect proprietary content by preventing unauthorized users of being able to access or otherwise deliver benefit from the content." *Id*.

93. For example, the '171 Application states that "a music player that is compliant with such a standard might be unable to play unauthorized music, the unauthorized character of the music being derived from the encoding of the music itself." Ex. 1004 at 1. That is, the music player (which is in the possession of the user) determines whether or not to grant a request by the user to play the content. The fact that the music player may refuse a request to use the music, and yet is under the control of the user, means that the player is subject to at least two "masters": the user and the provider of the proprietary content. The music player, operating with a goal of protecting the content against the user of the device it is running on, determines, based on evaluating one or more rules or controls that are encoded in the file, whether to grant the user's request to play the music. *See also id*. at 8 ("Decoding system 104 is operable to decode the signal encoded by system 102, to apply security transformations to the signal, and to output the decoded signal to a user, if appropriate."); 9 ("In a preferred embodiment, a device is designed to play

or use digital content that embodies a new standard or encoding technology and to resist attempts to play or use unauthorized content"). This is an example of the use of digital rights management.

94. Annotated FIG. 6 of the provisional application below depicts a process for controlling access and use of data using signatures and watermarking techniques:

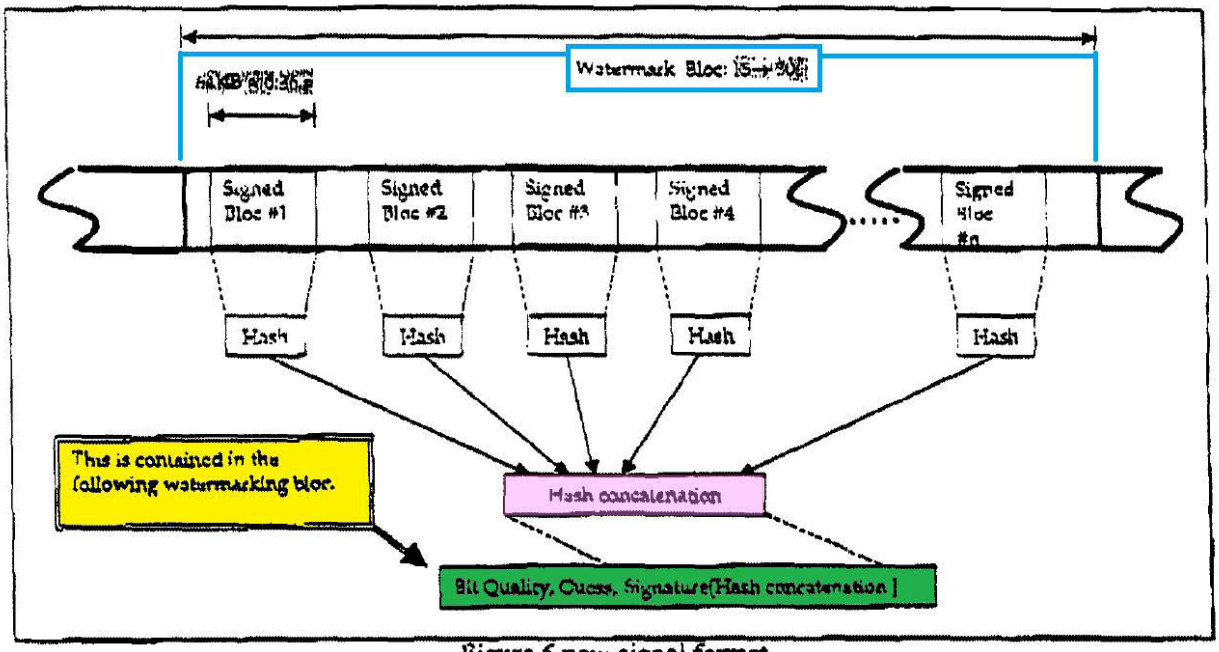

Figure 6 new signal format.

95. The '171 Application describes that in one embodiment, a signed data stream is first partitioned and then the partitions are hashed. Ex. 1004 at 20. The resulting hashes are concatenated, and the hash concatenation is signed. *Id*.

96. FIG. 6 explains that the signed hash concatenation (green) "is contained in the following watermarking bloc[k]." Ex. 1004 at FIG. 6 (quoted text in yellow box, and the hash concatenation shown in pink). That is, a signed hash concatenation

associated with a first data block is embedded in the watermark of the following data block in the transmission. In the "error-recoverable shared signature scheme" disclosed, "[i]f an error appears on the data, the signature will verify for all partitions except for the one that is affected." Ex. 1004 at 20. Thus, the signed hash concatenation received in the watermark of the following data block is used to verify the preceding data block.

97. A POSITA would understand that the signed hash concatenation would first be extracted from the watermark of the successive data block received to proceed with verification of the signed hash concatenation. The signature would then be, for example, processed (*e.g.,* "decrypted" according to RSA protocols, using the terminology of the '815 patent) to reveal the underlying hash concatenation. As part of the verification process, the actual data block received is partitioned and hashed to obtain a hash concatenation so that a comparison can be made between the hash concatenation retrieved from the data block and the hash concatenation retrieved from the digital signature. *See* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); *see also id.* at FIG. 2C (illustrating signature verification by comparing a hash of the data block received (*i.e.*, " X ") and a hash of the unsigned signature (*i.e.* " X' ")).

98. Moreover, since a signature is incorporated in the block that follows the block to which the signature corresponds (Ex. 1004 at 10-16), the hash values

extracted from block "n" have to be stored until block "n+1" (where block "n" and "n+1" are referred to as block "A" and "A+1" in Ex. 1004) is received and the associated signature is extracted. A POSITA would understand that an analogous storage operation would be performed on the receiver. Thus, when the signature is extracted, a POSITA would understand that the stored hash values will be loaded from the cache or other memory (such as "delay element 312") and compared to the "decrypted" signature.

99. When the hash concatenation from the digital signature is compared to the concatenation of the hash values retrieved from the received data block, a match between the two verifies the authenticity concatenation of the hash values obtained from the received data block. The individual hashes that make up the concatenation of hash values can then be used, one by one, to verify the authenticity of corresponding partitions of the data block received. *See* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); FIG. 6.

100. The '171 Application also provides for the detection of unregistered content that an attacker is attempting to appear as though it had never been registered. *See* Ex. 1004 at 21. This "involves detecting an attackers attempt to make previously-registered content appear as if it were pre-existing content, so as to

hide the fact that the previously registered content is being used without authorization." *Id*.

101. In one embodiment, depicted in Figures 7A and 7B, a technique for using a strong watermark is combined with techniques for using digital signatures described in the '171 Application. *See* Ex. 1004 at 22. A policy is applied to each block of the incoming signal to determine whether the block may be played. Each block is checked for the presence of a weak watermark. *Id*. If a weak watermark is found, this indicates that the content is proprietary and protected, and the signature is extracted from the watermark and determined to be authentic or not. *Id.* at 23. If the signature is found to be valid, then the block can be played. *Id*. If the signature is found to be invalid or no weak watermark is detected, the signal is checked for the presence of a strong watermark. *Id*. If one is found, this indicates that the content was registered at one point, but now has been corrupted or otherwise modified. *Id*. Thus, defensive action is taken, such as inhibiting further use of the signal.

102. It is noteworthy that the policy is not just a matter of looking for the presence of something, and, if it is there, to grant use of the block. Instead, there are rules that identify when the right to use the block is granted. In fact, if a weak and strong watermark are both not found, then use of the block is granted.

C. The ’815 Patent Claims

103. While the ’815 patent includes 46 claims, I understand that Petitioner only challenges independent claim 42 and dependent claim 43:

> 42. A method for managing at least one use of a file of electronic data, the method including:
>
> receiving a request to use the file in a predefined manner;
>
> retrieving at least one digital signature and at least one check value associated with the file;
>
> verifying the authenticity of the at least one check value using the digital signature;
>
> verifying the authenticity of at least a portion of the file using the at least one check value; and
>
> granting the request to use the file in the predefined manner.
>
> 43. A method as in claim 42, in which the at least one check value comprises one or more hash values, and in which verifying the authenticity of at least a portion of the file using the at least one check value includes:
>
> hashing at least a portion of the file to obtain a first hash value; and
>
> comparing the first hash value to at least one of the one or more hash values.

104. All of the claims recite methods for managing at least one use of a file of electronic data.

D. Prosecution History of the ’815 Patent

105. The ’815 patent issued on August 31, 2004 from U.S. Application No. 09/588,652 ("’652 Application"), filed on June 7, 2000. The ’652 Application claims priority to provisional application No. 60/138,171 ("'171 Application") filed on June 8, 1999, which is incorporated by reference into the ’815 patent. *See* Ex. 1001 at 1:6-11. The Examiner’s "Reasons For Allowance" stated that claim 42 (along with the other claims) included "uniquely distinct features" that were "not found in the prior art, either singularly or in combination." *See* Ex. 1003 at 145, 153.

E. The Priority Dates of the Claims

106. I understand that neither Petitioner nor Dr. Madisetti contends that limitations other than 42[b] and 42[c] found in Claim 42 (or any limitations of Claim 43) allegedly lack adequate written description support in the provisional application.

107. Petitioner incorrectly summarizes the relevant disclosures found in the '171 Application, by cursorily concluding that "[l]ike the other embodiments disclosed, the 'shared signature’ technique [of FIG. 6] does not involve retrieving a check/hash value associated with a file, or verifying the authenticity of the check/hash value using the digital signature." Petition at 17. Yet, FIG. 6 and the corresponding text, along with other portions of the specification and figures, reasonably convey to a POSITA "retrieving at least one digital signature and at least

one check value associated with the file" (Limitation 42[b]) and "verifying the authenticity of the at least one check value using the digital signature" (Limitation 42[c]).

108. Annotated FIG. 2D (below) of the provisional application illustrates "an embodiment of the present invention that solves [the] problems [of the conventional signature encoding techniques shown in FIGS. 2A-2C] by embedding a block's signature in the watermark of the block that follows the block to which the signature corresponds." Ex. 1004 at 10-12, FIGS. 2A-2D (emphasis added).

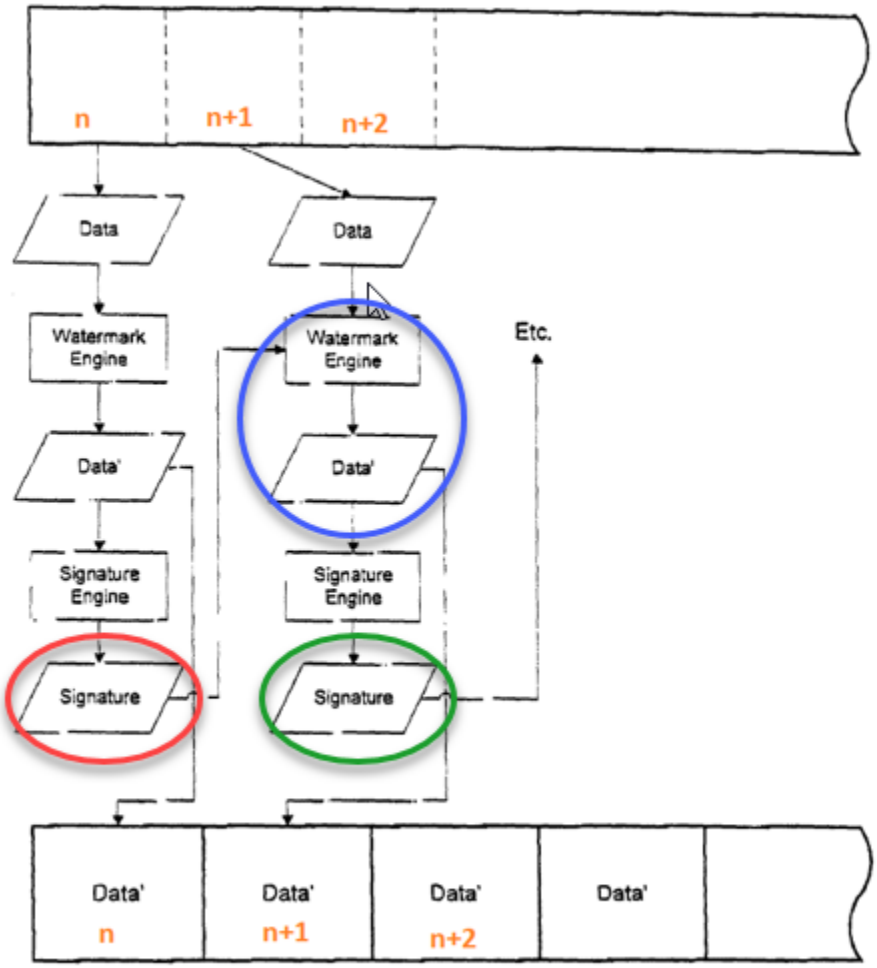

FIG. 2D

109. Thus, given a stream of data (*e.g.*, data blocks "n," "n+1," "n+2," etc. in FIG. 2D), a signature of data block "n" (circled in red) can be embedded into the watermark of data block "n+1" (circled in blue). Similarly, a signature of data block "n+1" (circled in green) can be embedded into the watermark of the following block in the transmission, data block "n+2," and so on. *See* Ex. 1004 at 12-13, FIGS. 2D, 3.

110. The '171 Application explains that a "technological constraint…is that watermarking algorithm[s] typically cannot transport relatively large amounts of data," and that some of the embodiments described in the '171 Application (*e.g.*, with respect to FIG. 5B and associated text) may use a watermark that "contains almost 261 bytes, which with current technology is a relatively large amount of data for a watermarking algorithm." Ex. 1004 at 20; *see also id.* at 17-19, FIG. 5B.

111. This problem is addressed "through the use of an error-recoverable shared signature scheme" that "is resistant to errors in the signed data," shown and described in the '171 Application with respect to FIG. 6. Ex. 1004 at 20, FIG. 6.

112. Annotated FIG. 6 (below) illustrates a process of generating a signed hash concatenation by "first partition[ing]" "a signed data stream 602" (the "Watermark Bloc" shown in blue), and then "hashing apart those partitions and concatenating the resulting hashes." Ex. 1004 at 20, FIG. 6.

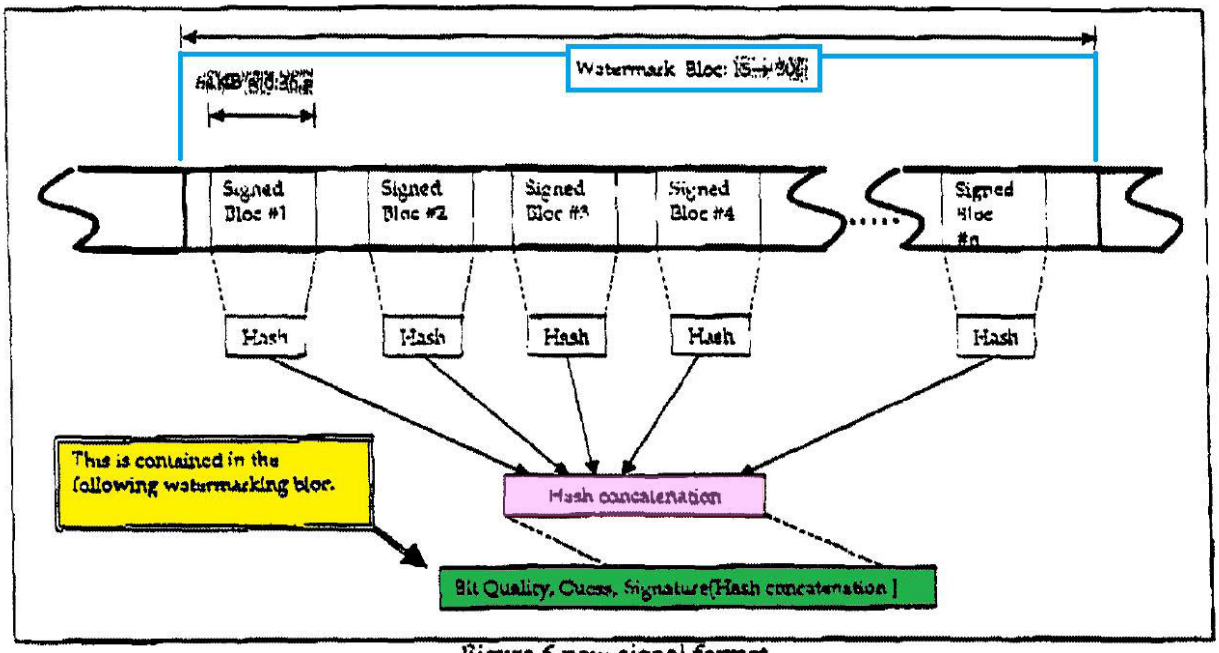

Figure 6 new signal format.

113. The hash concatenation (pink) is next signed. *Id.* FIG. 6 discloses that the signed hash concatenation (colored green) "is contained in the *following* watermarking bloc[k]." Ex. 1004 at FIG. 6 (quoted text in yellow, emphasis added). That is, consistent with the invention described with respect to FIGS. 2D and 3, FIG. 6 teaches that a signature (signed hash concatenation) associated with a first data block (*e.g.*, data block "n" in annotated FIG. 2D above) is embedded in the watermark of the following data block (*e.g.*, data block "n+1") in the transmission.

114. In the "error-recoverable shared signature scheme" disclosed, "[i]f an error appears on the data, the signature will verify for all partitions except for the one that is affected." Ex. 1004 at 20. In this fashion, the '171 Application teaches that such errors "can be readily detected and recovered from." *Id.*; *see also id.* at 6

("The data signal is divided into a sequence of blocks, and digital signatures of the blocks are embedded in the blocks using watermarks. When a user plays or uses the data sequence, the sequence is checked for the presence of the watermark containing the digital signature. If this watermark is found, then the digital signature is used to verify the authenticity of the content."). Thus, the digital signature received in the watermark of the following data block (*e.g.*, data block "n+1") is used to verify the preceding data block (*e.g.*, data block "n").

115. The disclosure of the entire '171 Application would reasonably convey to a POSITA that the claimed "digital signature" would first be extracted from the watermark of the successive data block (*e.g.*, data block "n+1") to proceed with verification of the "current" data block (*e.g.*, data block "n") (*e.g.*, teaching, in part, Limitation 42[b]: "retrieving at least one digital signature…associated with the file"). The signature would then be, for example, "decrypted" using the public key of the signer to reveal the "unencrypted" hash concatenation to be used for the matching with the hash concatenation of the "current" data block. Although digital signature verification does not necessarily entail "decryption," since the '171 Application expressly discloses the use of the RSA algorithm (*see* Ex. 1004 at 19), a POSITA would understand that decryption" may be used as part of the verification process.

116. As part of the verification process, a POSITA would further understand that the hash concatenation of the current data block would be retrieved (*e.g.*, from received data block "n") by partitioning and hashing the current data block (*e.g.*, disclosing, in part, Limitation 42[b]: "retrieving…at least one check value associated with the file").

117. A comparison can then be made between the hash concatenation retrieved from the current data block and the hash concatenation extracted from the digital signature in the watermark of the successive data block (*e.g.*, data block "n+1"). *See* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); *see also id.* at FIG. 2C (illustrating signature verification by comparing a hash of the data block received (*i.e.*, " X ") and a hash of the unsigned signature (*i.e.* " X' ")).

118. When the hash concatenation extracted from the digital signature is compared to the concatenation of hash values retrieved from the received data block, a match between the two (or parts thereof) verifies the authenticity of the hash concatenation retrieved from the received data block (*e.g.*, claimed "check value") (*e.g.*, disclosing Limitation 42[c]: "verifying the authenticity of the at least one check value using the digital signature"). The entire hash concatenation values do not need to match in their entirety to authenticate the check value since the ’171 Application explains that a statistical analysis can be used to determine the "appropriate number

of correct blocks" needed "to decide that the signature is correct." Ex. 1004 at 20. Thus, a comparison is made between a series of stored hash values (retrieved from block "n") and a corresponding series of hash values (extracted from the signature associated with block "n+1") and if the "appropriate number" match, the signature is determined to be correct.

119. The individual hashes that make up the concatenation of hash values can then be used, one by one, to verify the authenticity of corresponding partitions of the data block received (*e.g.*, disclosing Limitation 42[d]: "verifying the authenticity of at least a portion of the file using the at least one check value").

120. As part of the verification process, a POSITA would further understand that the watermark of the current data block "n" could be another form of "check value" that would also be retrieved. The watermark is a value that may be used to check the file, among other reasons.

121. In a given stream of data (*e.g.*, data blocks "n," "n+1," "n+2," etc. in annotated FIG. 2D), a signature of data block "n" is embedded into the watermark of data block "n+1". *See* Ex. 1004 at 12-13, FIGS. 2D, 3. A signature is therefore retrieved from data block "n+1", as is the watermark (*i.e.*, check value) of block "n", therefore providing additional written support for limitation 42[b] ("retrieving at least one digital signature and at least one check value associated with the file"). *See* Ex. 1004 at 12 ("Signature engine 308 is operable to create a signature 310 that

corresponds to watermarked PCM data 306. Signature 310 is then input to a delay element 312. Delay element 312 is operable to delay signature 310 until the next block of input PCM data 301 is ready to be input to watermarking engine 304 (Ex. 1004, page 12).”; 15 ("Since the signature for a given block, A, is embedded in the watermark for the following block, A+1, incoming blocks are held until the next block has been received and the signature has been extracted from it. The signature, and the block to which it corresponds, are then processed by signature verification engine 510, which verifies the integrity of the block using the signature.”)

122. Next, the authenticity of block "n" (including the watermark contained in block "n", which comprises the "check value") is verified using the digital signature retrieved from block "n+1". *See*, *e.g.*, FIG 4A. This provides additional written support for limitation 42[c] ("verifying the authenticity of the at least one check value using the digital signature.") Just like the watermark in block "n+1", comprising a signature, is used to verify the contents of block n, including the watermark in block n. The watermark in block "n" (*i.e.*, the "at least one check value") is used to verify the contents of block "n-1" (*i.e.*, at least a portion of the file).

123. Based on these disclosures, I disagree with Petitioner and Dr. Madisetti that limitations 42[b] and 42[c] of Claim 42 lack adequate written description support in the provisional application. The '171 Application describes the inventions

in sufficient detail that a person of ordinary skill in the art can clearly conclude that the inventors had possession of claims 42 and 43 as of the provisional filing date, and that the skilled artisan is enabled to make and use those claimed inventions.

124. For these reasons, I also disagree with Dr. Madisetti's opinion that the "relevant timeframe" for analyzing the alleged obviousness of claims 42 and 43 is "on or before June 7, 2000." *See* Ex. 1002, ¶ 47. Rather, it is my opinion that the "relevant timeframe" is on or before June 8, 1999, the filing date of the '171 Application.

V. OVERVIEW OF CITED ART

A. Hanna (Ex. 1006)

125. Hanna's "Field of the Invention" section describes that "[t]his invention generally relates to transmission-related data corruption detection and, more particularly, to a method and apparatus for efficient authentication and integrity checking in data processing using hierarchical hashing." Ex. 1006 at 3:1-4. This description of the field of invention as "data corruption detection" is consistent with the disclosures of Hanna, which describes "[c]reating a hierarchy of hash values that start with packet hashes of an arbitrary data set and culminate in a single signed block allows a single digital signature to protect the data set from both data corruption and malicious acts that cause errors in data processing. Receiving this hierarchy of hashes before the data also allows the data packets to be quickly verified

as they are received. The hierarchical structure used in the method cryptographically protects individual portions of the data and makes it easier to recognize corruption. Systems consistent with the present invention verify portions of the data even if other portions of the data are corrupt or have not yet been received." *Id*. at 3:6-14.

126. However, while "data corruption detection" is consistent with the disclosures in Hanna, it is too broad to be meaningful. Hanna describes a technology that allows a party receiving data to detect whether the data arrived corrupted. This is distinct from, for example, anti-virus technology, which aims at detecting whether data at rest has been corrupted, where such data may encode a software program. Whereas corruption of transmitted data can be detected by verifying a digital signature (as disclosed by Hanna and by Gennaro (discussed below)), anti-virus technology do not (and cannot) use digital signatures to detect corruption of software. One common anti-virus technique is so-called "behavioral detection", which is based on observing sequences of computer operations taking place on a device. Seen from another perspective, the threat of corruption of transmitted data can be modelled by an external adversary (that modifies what is being transmitted) whereas anti-virus technology faces the threat of an internal adversary: software that attempts to corrupt not only the same device that the anti-virus software is running on, but potentially also the anti-virus software itself.

127. In Hanna, the device sending data and the device receiving data are aligned: success for one of the devices is success for the other one. Here, success means verification that data was not corrupted in transmission, whether this is used in the context of a videoconferencing application or a backup application. These two applications, similarly, are applications where there is a natural alignment of incentives. In a backup application, the entity with the data to be backed up wishes to perform a backup in order later to retrieve data from a backup. The entity responsible for storing backed up data, similarly, is designed for the singular goal of enabling such a recovery. The backup device does not embody two (or more) conflicting goals. The problem solved in Hanna is simply that of enabling a verification that received data was not corrupted in transmission; this applies also for the teleconferencing application disclosed in Hanna. The adversarial model of Hanna is therefore very different from that of the '815 patent, as Hanna is not addressing malicious interference on the device that receives the data. Such interference, which can be thought of as the receiving device not being aligned with the sending device in terms of its goals, corresponds to a different field of endeavor, namely that of digital piracy protection and/or DRM.

128. Hanna contends that "[d]igital signatures are often used in a bulk signature format in which a digital signature is applied to a complete data set," but that this is approach has "several drawbacks," including the problem of high

computational overhead associated with verifying "bulk signature[s]" applied to a complete data set. *See* Ex. 1006 at 2:1-3:4. It alleges that there is "no system that allows a single digital signature to apply to an arbitrary amount of data and allows the data to be verified as it is received." *Id*. at 2:27-28.

129. Hanna purports to address "a need for a system that protects against unintentional data corruption and malicious acts that cause errors in data processing," Ex. 1006 at 3:1-4. Dr. Madisetti acknowledges that the "objective of Hanna is to protect against unintentional corruption and malicious acts that cause errors in data processing." Ex. 1002 at ¶ 75.

130. To address this problem, Hanna "create[s] a hierarchy of hash values that start with packet hashes of an arbitrary data set and culminate in a single signed block allow[ing] a single digital signature protect the data set from both data corruption and malicious acts" during transmission ." *Id*. at 3:6-8. "Receiving this hierarchy of hashes before the data also allows the data packets to be quickly verified as they are received." *Id.* at 3:8-10; *see also* 3:11-13 ("Systems consistent with the present invention verify portions of the data even if other portions of the data are corrupt have not yet been received.).

131. Referring to FIG. 4 of Hanna below, Hanna's hierarchical hashing scheme includes dividing a sequence of data values 401 into groups of data packets 402a-f. Ex. 1006 at 10:26-27.

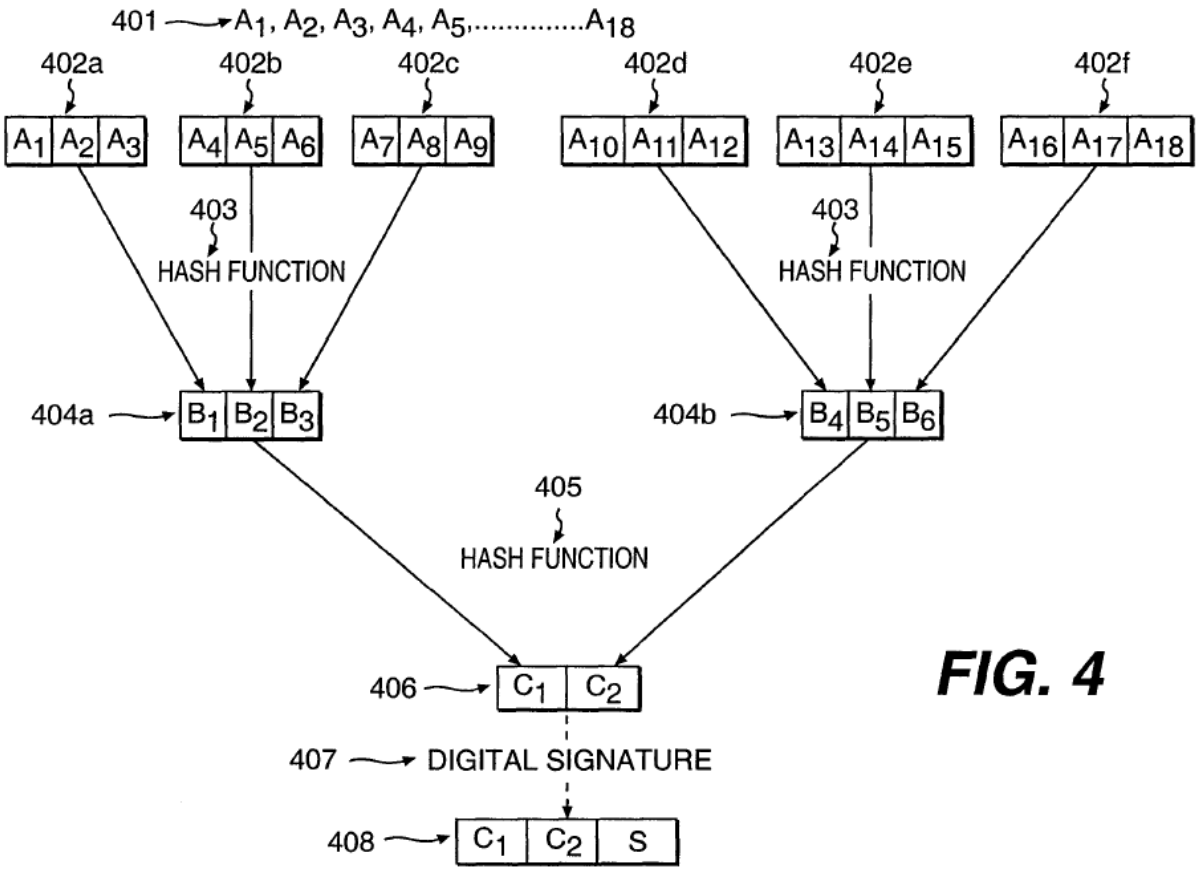

FIG. 4

132. A hash function is applied to each data packet group 402a-f to generate a hash block 404 consisting of hash values B_1-B_6. *Id.* at 10:28-11:1. The resulting hash values are grouped themselves (404a, 404b) and hashed again to generate a higher level hash block 406. *See id.* at 11:2-8. The process continues until the resulting hash block (and associated signature) is small enough to fit within a single packet. *Id.* The highest level hash block 406 is then signed. *Id.* at 11:8-10. The hash blocks are all transmitted. *Id.* at 9:11-13.

133. Referring to FIG. 5 of Hanna below, data verification "begins with checking the digital signature on the top level hash block 502." Ex. 1006 (Hanna)

at 11:12-13. If the top level hash block 502 passes the check, the next level hash 501 is verified by hashing the grouping of B_1-B_6 and comparing it to the higher level hash C_1. *Id.* at 11:13-19. The data packets A_1-A_{18} are verified by comparing their hashes with the lowest level hash blocks. *See id.* at 11:24-29.

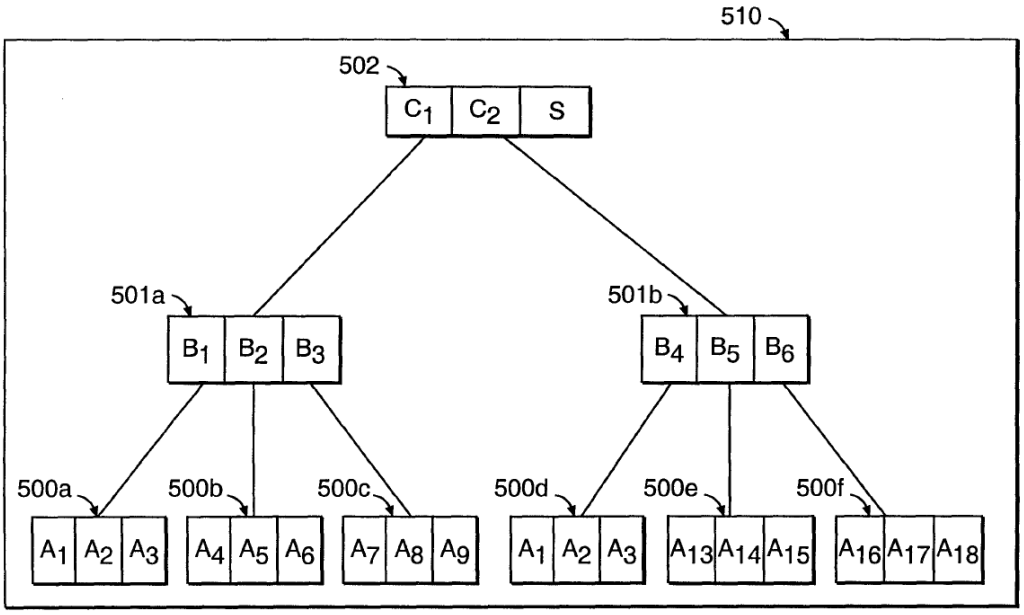

FIG. 5

134. Hanna describes methods that seek to detect data corruption by an adversary that is on the network, rather than one on the device that is configured to use the data, such as the intended user. Ex. 1006 at 9:24-26 ("If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335)." Repairing or recovering data addresses network corruption, but does nothing against an adversary on the same device.

B. Stefik (Ex. 1007)

135. Stefik's "Field of the Invention" section describes that "[t]he present invention relates to the field of distribution and usage rights enforcement for digitally encoded works. Ex. 1007 at 1:6-7. I agree with this description of the field and further note that it is within the same field of endeavor as the '815 patent (*i.e.*, digital rights management).

136. Dr. Madisetti, on the other hand, opines that Stefik is in the much broader field of "digital file security" because it allegedly "address[es] the problem of unauthorized manipulation of digital files." Ex. 1002 at ¶ 90. But he also acknowledges that Stefik explicitly states that it addresses a different problem, namely "the problem of unauthorized distribution and usage of digital works." *Id*. at ¶ 79.

137. Rather than being concerned with the unauthorized "manipulation" of digital files, Stefik says that a "major concern" is preventing an unauthorized user from being able to "'perfectly' reproduce[] and distribute[]" the digital work, not preventing an unauthorized modification of the work by the unauthorized user. Ex. 1007 at 1:24:26.

138. Indeed, Stefik describes that it is directed generally at the problem of preventing the unauthorized and unaccounted distribution or usage of electronically published materials, and, in particular, to the problem posed to such accounting

systems when "the means for billing runs with the media rather than the underlying work." *Id.* at Abstract, 1:10-23, 3:40-47, 3:50-52. In response, Stefik provides a system where the "owner of a digital work [] attach[es] usage rights to the work" that "define how it may be used and distributed." *Id.* at 3:50-58.

139. Stefik describes that a "key feature of the present invention is that 'usage rights' are permanently attached to the digital work" because it ensures that copies of a digital work also have usage rights attached, and that those rights "will always remain with a digital work." Ex. 1007 at 6:51-56.

140. Referring to FIG. 1 of Stefik below, a creator of a digital work determines the appropriate usage rights and fees, attaches them to the digital work, and stores the work in a first repository. Ex. 1007 at 7:6-11.

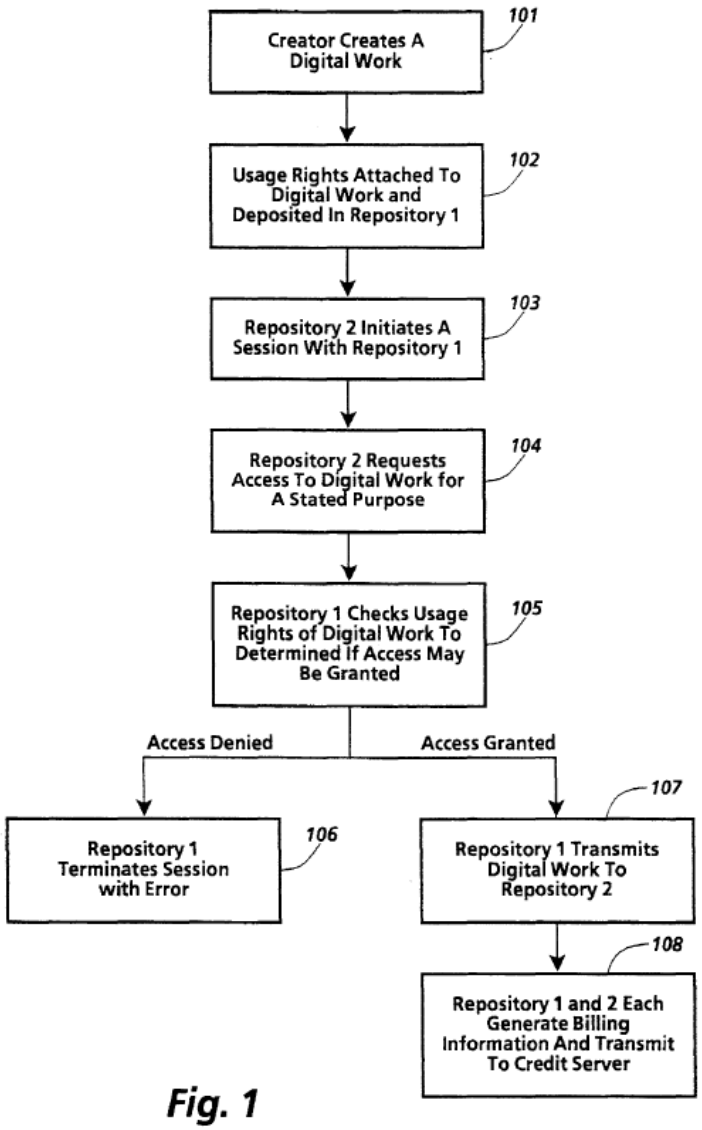

Fig. 1

141. The second repository may request access to the digital work for a stated purpose, for example, to print or to obtain a copy of the digital work. Ex. 1007 at 7:19-22. That purpose will correspond to a specific usage right. *Id.* at 7:22-23. The first repository checks the usage rights associated with the digital work to determine if the access to the digital work may be granted. *Id.* at 7:24-26. The check involves a determination of whether a right associated with the access request has

been attached to the digital work and if all conditions associated with the right are satisfied. *Id.* at 7:26-29. If access is denied, the first repository terminates the session with an error message; otherwise, the repository transmits the digital work. *Id.* at 7:29-32.

C. Gennaro (Ex. 1008)

142. Gennaro describes its Technical Field as a "method of signing and authenticating a stream of data using a reduced number of digital signatures." Ex. 1008 at 1:4-6; Abstract ("A method of signing digital streams so that a receiver of the stream can authenticate and consume the stream at the same rate which the stream is being sent to the receiver."). This, like Hanna (but unlike the '815 patent), addresses the problem of detecting corruption of data in transmission. Gennaro is not concerned with defending content against a user intent on accessing content in a manner that is in breach with the terms specified by the content owner. This is consistent with the fact that Gennaro is not a DRM system; that Gennaro does not address a problem related to an adversary with potential presence on the device receiving content; and the fact that Gennaro is not concerned with how content will be used by the recipient. Thus, the adversarial model of Genarro, like Hanna, is very different from that of the '815 patent. *See* ¶¶ 126-127. Accordingly, the notion of "granting the request to use the file in the predefined manner" as disclosed by the '815 patent is not applicable to Gennaro, among other things.

143. Gennaro asserts that it is "an object of this invention to reduce computation time necessary to sign and authenticate a stream of data by reducing the number of digital signatures required for one to authenticate the data stream." *Id*. at 2:29-32. It purports to address problems presented by prior art stream signing methods that "resort to storing large portions of the data stream" and "maintaining excessively large authentication tables." Ex. 1008 at 2:32-35. Gennaro states that its solution achieves the objective of "reduc[ing] computation time" because "only one expensive digital signature is ever computed, there are no big tables to store, and the size of the authentication information associated with each block does not depend on the size of the stream." *Id*. at 1:59-62, 2:29-33.

144. Gennaro emphasizes that one benefit of its invention is that the "receiver authenticates the stream without receiving the entire stream." *Id*. at 2:35-37; 14:13-16 (when "[u]sing our solution [to transmit log files,] the receiver can interrupt the transmission as soon as tampering is detected thus saving precious communication resources.") Another benefit is that the "receiver detects corruption almost immediately after tampering of a portion of the stream." *Id*. at 2:37-39. Even if it is possible to receive a whole file, Gennaro teaches it is not a satisfactory solution to wait until after transmission for "the user" to detect tampering. Instead, Gennaro's "solution" allows the "receiver" to "interrupt transmission as soon as tampering is detected thus saving precious communication resources." Accordingly, it is the

receiver (*i.e.*, potential user) of the data, not the sender (*i.e.*, the content owner/distributor), that performs the steps of authenticating data and detecting corruption.

145. Gennaro describes how a data stream is divided up into a series of data blocks that each include a hash of the successive block in the stream. *See id.* at 4:14-58, FIG. 1A. The first block in the stream, which includes the hash of the second block in the stream, is then hashed and signed to generate authentication data consisting of a signature, hash, and size. *Id.* at 4:59-65, FIG. 1B. The authentication data is then sent to the receiver before the data stream is sent. *Id.* at 4:66-5:2.

146. Upon receipt of the authentication data, the receiver verifies the signature in the authentication data, and, if authentic, extracts the hash and size values in order to begin authenticating the received data stream. Ex. 1008 (Gennaro) at 5:23-34. The data stream is split into blocks according to the size information received, and each block (after the first block) is authenticated using the hash found in the preceding block. *See id.* at 5:35-67.

VI. CLAIM CONSTRUCTION

147. I understand that neither party has identified any terms that they allege require construction.

VII. PETITION'S ARGUMENTS: HANNA, STEFIK & GENNARO

A. Ground 1

148. I understand that the Petition alleges the Challenged Claims are obvious over Hanna in view of Stefik. I disagree. The relevant time period for my opinions below is on or before June 8, 2000, the filing date of the '815 patent's non-provisional application. I understand that Hanna is only prior art if the Board finds that the Challenged Claims are not entitled to a priority date established by the filing date of the '171 Application.

1. The Petition Has Failed To Prove Hanna Discloses Limitation 42[a]

149. Limitation 42[a] recites "receiving a request to use [a] file in a predefined manner." Ex. 1001, '815 patent, Cl. 42.

150. I understand that the Petition alleges Hanna discloses Limitation 42[a]. However, to a POSITA, none of the three disclosures from Hanna identified by Petitioner disclose Limitation 42[a].

151. First, Petitioner misleadingly implies that Hanna's discussion concerning an "application program" (Ex. 1006 at 7:15-26) involves receiving an application program that is cryptographically verified according to Hanna's data processing protocols (*e.g.*, hierarchical hashing scheme). *See* Petition at 26-27 (citing Ex. at 7:15-23), 31 (citing Ex. 1006 at 7:16-18, 7:24-26). Hanna makes no such disclosure.

152. Instead, this portion of Hanna is discussing the initial transmission of the software that will be installed at computer 100 to implement Hanna's hashing scheme. Hanna explains that the "requested [application] code" is transmitted from the remote server 130 (*see* FIG. 1 below) to computer system 100 over the network 122, 126, 128 to "provide[] the data processing operations described herein." Ex. 1006 at 7:16-20; 5:22-28, 6:3-25.

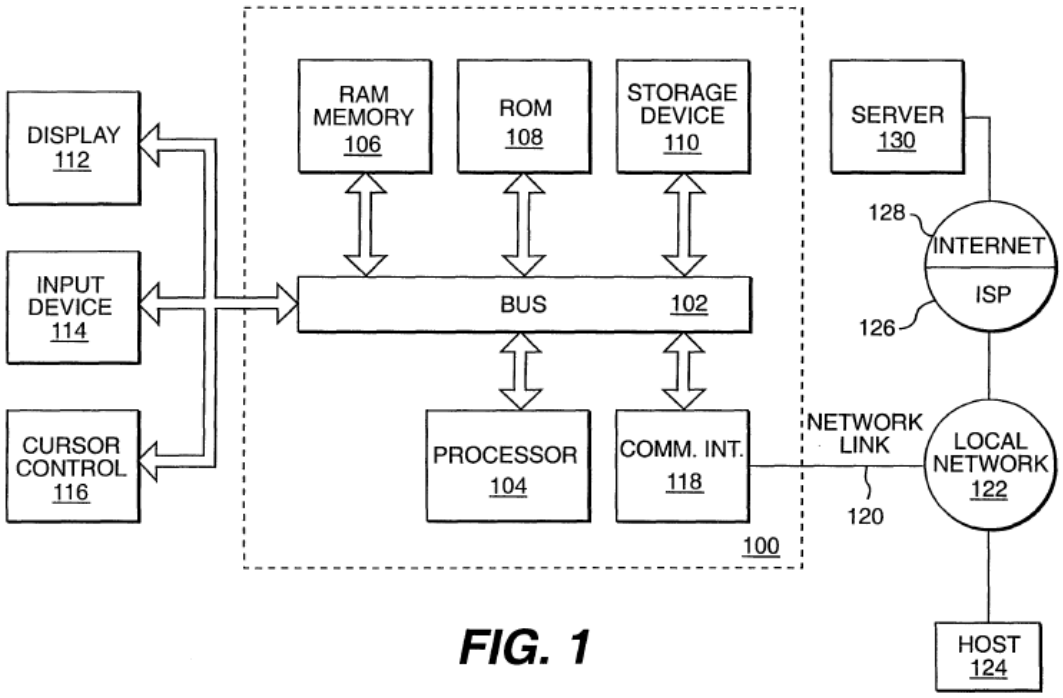

FIG. 1

153. Hanna does not teach that this software transfer is performed using Hanna's hashing scheme (described in Hanna with respect to FIGS. 2-5), nor could it, since there would be no prior software residing on computer system 100 capable

of carrying out Hanna's data processing protocols as computer system 100 receives this software.

154. Thus, any "request" for Hanna's hashing scheme application program is irrelevant to the Challenged Claims, which require that the "file" requested be the subject of the digital signature(s) and check value(s) retrieved and verified. Ex. 1001 at 32:13-29.

155. Second, Petitioner argues that a POSITA would inherently understand that requests for both computer file back-ups and video conferencing would "necessarily" be present in Hanna. *See* Petition at 28; *see also id.* at 31 ("A POSITA would recognize that in each case a request to transmit, copy and/or store files of electronic data is made.")

156. Petitioner contends that Hanna's lone sentence concerning a bank backing up files to a remote central server would be understood by a POSITA as a "request to transmit, copy and/or store files of electronic data is made." Petition at 31. But Hanna never discloses that this "backup" is performed in response to a request, let alone that it is performed using Hanna's hashing scheme. *See* Ex. 1006 (Hanna) at 1:10-13.

157. Petitioner does not provide any basis in Hanna for why a bank would send a request that needs to be granted before it can "transmit, copy and/or store" its own data. Indeed, Hanna teaches that any transmission, copying and/or storing of

such data would begin before the entire file is received. *See* Ex. 1006 (Hanna) at 8:10-11 ("Systems consistent with the present invention generally begin the hashing process by dividing the data set into small packets (step 210)"); 12:4-5 ("Systems consistent with the present invention need not wait for all of the packets to be delivered to verify a data packet.")

158. The '815 patent is concerned with "attackers" transmitting perfect, but unauthorized, copies of content to others, or removing data related to the content placed there to restrict the attacker's use. *See* Ex. 1001 at 9:27-29 ("it is desirable to prevent ***attackers*** from copying a digital file from a storage medium such as a compact disc and ***distributing unauthorized copies to others***."); 9:32-36 ("***attackers*** often employ compression techniques to reduce content files to a fraction of their original size, thus ***enabling copies to be transmitted*** over networks such as the Internet with relative ease"); 9:52-57 (if a content file contains special codes indicating…that the content cannot be compressed, copied, or transmitted, ***an attacker may attempt to remove those codes*** in order to make unauthorized use of the content.") (emphases added). Because a bank is not at risk of "attacking" its own data, the requesting (and granting) steps recited in the Challenged Claims are not practiced in this backup example.

159. By Petitioner's reasoning, any action taken on a content file, including verifying whether it was received in an uncorrupted state, would constitute a "use".

This makes no sense, and would not have been how a POSITA would understand the meaning of "use," as recited in the Challenged Claims, For example, a POSITA would not have understood that a request by a content owner, such as a bank, to back up its own files as a request to a remote central server to "use [its own files] in a predefined manner." First, backing up data is not a "use" of data in any manner; at most, it is enabling potential use. Second, although the '815 patent discloses example uses such as "accessing the content more than a certain number of times, printing a copy of the content, saving the content to a memory device," (Ex. 1001 at 9:61-63), it does so in the context of potential use by an "attacker" that makes "unauthorized modifications" to circumvent controls on such use. Id. at 9:58-61 ("an attacker may attempt to add special codes to an unprotected piece of content in order to use the content on a device that checks for the presence of these codes as a precondition for granting access to the content or for performing certain actions"); *see id*. at 22:54-62 (providing examples operations that the "control management mechanisms" can be used to "control or manage."). This context is notably absent from the back up scenario presented in the "Description of Related Art" in Hanna.

160. It also would not make sense for the central remote backup server to be the entity making a request to "use [the bank's files] in a predefined manner." Because the backup server would be the computer performing the "receiving" and the wo "verifying" steps of claim 42 to ensure "that these files were

successfully copied to the remote database without having been changed or corrupted during the [backup] process," (Ex. 1006 at 1:11-13), it would also need to perform the "receiving" and "granting" steps. Therefore, it is not possible that the backup server sends the request.

161. Third, no disclosure is made that Hanna's "video conferencing" involves the receipt of a request to a use a file in a predefined manner (including providing no information about which of the video conferencing participants would receive such a request, what "file" would be used, and in what predefined manner), or how its hashing scheme would apply (if at all) to this application. Ex. 1006 at 1:13-15.

162. A POSITA would understand that a video conference involves a *real time* transmission of a data stream, and does not implicate a "request to use [a] file in a predefined manner." For example, when one party initiates the video conference, there is no "file" to request (or even in existence) to use in "a predefined manner." Moreover, none of the participants are potential "attackers" who would need to make a request to use a file in a predefined manner to participate in the video conference.

163. The word "request" appears nowhere in Hanna except in relation to the "requested code for an application program." As discussed above, receipt of the

application program requested is accomplished without using Hanna's data processing protocols.

164. Because Petitioner fails to show that the "receiving a request to use a file in a predefined manner" step is necessarily present in Hanna, Hanna does not inherently teach or disclose Limitation 42[a].

2. The Petition Has Failed To Prove Hanna Discloses Limitation 42[e]

165. Limitation 42[e] recites "granting the request to use the file in the predefined manner."

166. I understand that the Petition does not allege that Hanna expressly teaches or discloses "granting the request to use the file in the predefined manner." Petitioner nevertheless suggests that the "granting" step is inherently taught by Hanna because it discloses that data portions that are not verified "should be repaired, recovered, or discarded." Petition at 38. According to Petitioner, "[a] POSITA would have recognized that corrupted data, or data not properly signed with a recognized/authenticated signature, would be undesirable to be used. *Id*.

167. Hanna's hierarchical hashing scheme requires that each file is divided into a set of portions, and teaches that portions of the data may be verified even if "if other portions of the data are corrupt or have not yet been received." Ex. 1006 at 3:10-17. Thus, Petitioner's contention that "it would have been obvious to allow or

prevent a requested use of a file depending on whether it passes the authentication process" makes no sense because portions of the file may be verified while others are not. *See* Petition at 38.

168. In fact, in the backup application of Hanna, a POSITA would not have wanted to accept a partially corrupted file. *See* Ex. 1006, 1:11-13 (banks "need to know that these files were successfully copied to the remote database without having been changed or corrupted during the process"). In other words, the decision of whether to "grant the request" is not part of the transport layer, which is the focus of Hanna. Indeed, this example shows that any potential "granting" is part of the processing on the application layer. Hanna describes two possible applications of the disclosed technology, neither describes processing on the application layer. Hanna is agnostic when it comes to how data is eventually consumed.

169. Petitioner concedes that a POSITA would understand that Hanna is intended to benefit the user, rather than to prevent the user's unauthorized use of the data, as is intended by claims 42 and 43. *See* Petition at 9 ("A POSITA would have recognized that corrupted data…would be undesirable to be used.") Indeed, repairing or recovering data addresses network corruption, but does nothing to protect against an adversarial user that is on the same device as the content.

170. Because Petitioner fails to show that the "granting a request to use a file in a predefined manner" step is necessarily present in Hanna, Hanna inherently does not teach or disclose Limitation 42[e].

3. A Person of Ordinary Skill in the Art Would Not Not Be Motivated to Combine Hanna and Stefik to Achieve a Combination That Discloses Limitations 42[a] and 42[e]

171. Petitioner fails to show that a POSITA would be motivated to combine or modify Hanna with the teachings of Stefik to achieve a combination having the claimed features, and that such combination would have a reasonable expectation of success.

172. I understand that prior art can only be combined to invalidate a claim if there is, in fact, a reason for a POSITA to have done so at the time of the invention.

173. Petitioner proffers a number of reasons why Hanna and Stefik are allegedly similar. *See* Petition at 28-29.

174. Hanna and Stefik are not directed to the same field of endeavor. As discussed above, Hanna discloses that it is directed to the field of transmission-related data corruption detection. By contrast, Stefik's field of endeavor is not data corruption detection, but piracy protection and/or DRM. *See* Ex. 1007 at 1:5-8 ("relates to the field of distribution and usage rights enforcement for digitally encoded works"); Petition at 23 (acknowledging that Stefik is "directed to a method

and system for controlling usage and distribution of digital works, such as software.")

175. Hanna and Stefik also do not address the same problems. Although Hanna expressly states that it addresses the problem of "unintentional data corruption and malicious acts that cause errors in data processing" (Ex. 1006 at 3:1-4), Stefik addresses a very different problem. Petitioner concedes that Stefik "recognizes the problem of unauthorized distribution and usage of digital work," and provides no evidence from the patent to support its contention that it also deals with the problem of unauthorized manipulation of digital files. Petition at 23. Stefik says that a "major concern" is preventing an unauthorized user from being able to "'perfectly' reproduce[] and distribute[]" the digital work, not preventing an unauthorized modification of the work during transmission. Ex. 1007 at 1:24-25.

176. Hanna and Stefik's also propose significantly different solutions to their respective problems. Hanna divides a data set into portions, and then "create[s] a hierarchy of hash values" that "allows a single digital signature to protect the data set from both data corruption and malicious acts that cause errors in data processing." Ex. 1006 at 3:6-8. "Receiving this hierarchy of hashes before the data also allows the data packets to be quickly verified as they are received." *Id.* at 3:8-10. Conversely, Stefik does not teach dividing a work into small portions, and applying a hash function to each of them. Rather, Stefik teaches permanently attaching usage

rights to the entire work, not splitting it up. Ex. 1007 at 3:50-58 (providing a system where the "owner of a digital work [] attach[es] usage rights to the work" that "define how it may be used and distributed.") Stefik explains that "'usage rights'…is a term which refers to rights granted to a recipient of a digital work." *Id*. at 6:43-45. "[T]hese rights define how a digital work can be used and if it can be further distributed," and each "may have one or more specified conditions which must be satisfied before the right may be exercised." *Id*. at 6:45-50. A POSITA would not look to Stefik's digital works distribution and usage rights system that leverages a "means for billing [that] is always transported with the work," (*id*. at 3:46-48), to modify Hanna's transmission-related data corruption detection system, including its hierarchical hashing scheme because Hanna has nothing to do with the enforcement of usage rights. Accordingly, because Hanna and Stefik are in different fields and address different problems in significantly different ways, a POSITA would not have been motivated to look to Stefik to modify Hanna's teachings.

177. Petitioner argues that a POSITA would be motivated to modify Hanna in view of Stefik because "it would facilitate timely detection of data corruption in a file of electronic data, *i.e.*, when data that could be corrupted or hacked during transmission is about to be used." Petition at 29. I disagree. Hanna's system already provides for timely detection of data corruption through its hierarchical hashing scheme that "allows [] data packets to be quickly verified as they are received." Ex.

1006 at 3:8-10; *see also id.* at 3:2-3, 12:3-10, 12:17-21. Moreover, Hanna already ensures that corrupted data is not delivered to the intended recipient, let alone used, because any corrupt packet "must be repaired or replaced before any packets that depend on this hash block can be verified." Ex. 1006 at 10:9-11. Since Hanna's system detects data corruption concurrently with its transmission, modifying Hanna's data corruption detection scheme as Petitioner proposes to include "receiving a request…" and "granting the request…" would not provide any meaningful improvement in Hanna's detection time. A POSITA would not have been motivated to modify Hanna's transmission-related data corruption detection scheme that uses hierarchical hashing with Stefik's digital works usage rights system to achieve a combination that includes the "receiving a request to use [a] file in a predefined manner" and "granting the request…." steps of the Challenged Claims.

B. Ground 2

1. The Petition Has Failed To Prove Gennaro Discloses Limitation 42[a]

178. I understand that the Petition alleges the Challenged Claims are obvious over Gennaro by itself. I disagree.

179. Limitation 42[a] recites "receiving a request to use [a] file in a predefined manner." Ex. 1001, ’815 patent, Cl. 42.

180. I understand that the Petition alleges Gennaro discloses Limitation 42[a]. However, to a POSITA, none of the three disclosures from Gennaro identified by Petitioner disclose Limitation 42[a].

181. First, Petitioner contends, without support, that Gennaro "discloses" that a "sender receives [a] 'request' from the receiver." Petition at 48. Gennaro makes no such disclosure. Indeed, the word "request" is used one time in Gennaro, and in a very different context related to accommodating classes and data resources. *See* Ex. 1008 at 13:35-46.

182. Second, Petitioner asserts that "Gennaro discloses a user requesting to use a file in a predefined manner (e.g., playing 'internet applications (digital movies, digital sounds, applets)')." Petition at 49 (citing Ex. 1008 at 2:64-67). What the cited section of Gennaro actually discloses is that finite streams of data commonly related to internet applications, such as "digital movies, digital sounds, [and] applets," can be processed according to Gennaro's method of signing and authenticating a data stream (*e.g.*, as described with respect to FIGS. 2 and 3 of Gennaro). Ex. 1008 (Gennaro) at 2:64-3:4. Gennaro does not teach or disclose that a "user request[]" is received to use these "digital movies, digital sounds, [and] applets."

183. These streams are divided into blocks, and Gennaro asserts "a single hash computation will suffice to authenticate the [] blocks." Ex. 1008 at 2:55-57,

2:67-3:2. Gennaro does not teach or disclose anything in this section regarding how the recipient may use the authenticated stream, including any suggestion that this process is initiated by receiving a request to use these "digital movies, digital sounds, [and] applets" in a predefined manner. Some or all of the blocks of the stream may not be usable by the intended recipient because if a block is determined to be corrupted, "then tampering has been detected and processing halted." Ex. 1008 at 5:57-58. Moreover, the MPEG software on the receiving device is not even made aware of this corrupted data block. Ex. 1008 at 5:36-38.

184. Contrary to Dr. Madisetti's opinion, Gennaro also does not disclose "rendering or playing" these internet applications. *See* Ex. 1002 at ¶140. Thus, Dr. Madisetti's conclusion that a "POSITA would have understood such [rendering or playing] as a user requesting to use a file in a predefined manner (*e.g.*, play)" is unfounded and unsupported by the evidence.

185. Third, Petitioner misleadingly argues that Gennaro at 1:28-29 "discloses that, when a user requests to play a file, a receiver requests transmission of the digital stream comprising the video for that purpose." Petition at 49. But Gennaro makes no such disclosure. Rather, Gennaro describes a prior art system where a "receiver asks for [an] authenticated stream." Ex. 1008 at 1:23-33. The cited portion (Gennaro at 1:28-29) relates to the description of a prior art system—one that Gennaro identifies as having a "problem." *See* Ex. 1008 at 1:7, 1:23-36.

Thus, the "receiver" that "asks for the authenticated stream" at issue there is unrelated to Gennaro's system (*e.g.*, described in Ex. 1008 at 3:46-5:67).

186. Moreover, asking for an authenticated stream of data is not the same thing as "receiving a request to use [a] file in a predefined way" because asking for and receiving data is not a request to use that data in any particular way. Accordingly, does not matter whether "a POSITA would make similar requests for all file transmissions" (Petition at 49) because the end result would simply be an ask for different types of authenticated data streams (*e.g.*, video, audio, etc.), not a request to actually "use" those file types "in a predefined manner."

187. Fourth, Petitioner contends that it would have been obvious to a POSITA "to configure" the receiver in Gennaro "so that, when it passes the data to the authentication software, it is in the context of a request for the MPEG software to convert the data into video for playback." Petition at 49. But Gennaro explains that its system "requires additional authentication software to be added to any existing MPEG software or hardware." Ex. 1008 (Gennaro) at 5:4-6. The authentication software authenticates the incoming data blocks before passing them on to the MPEG software that converts the received blocks back into video. *Id.* at 5:7-11. This authentication software is tasked with informing the MPEG software of incoming data that has been authenticated. *Id.* at 5:15-20, 5:35-39.

188. Petitioner fails to explain what specifically about the addition of the authentication software to the front-end of a standard MPEG receiver would motivate a POSITA to "configure" the receiving system to operate in the context of receiving a request to use a file in a predefined manner. In place of providing a cogent explanation, Petitioner puts forth a conclusory argument: because the authentication software passes data to the MPEG software, it would be in response to a request to use a file in a predefined way. *See* Petition at 49. There is no evidence to support this contention.

2. The Petition Has Failed To Prove Gennaro Discloses Limitation 42[e]

189. Limitation 42[e] recites "granting the request to use the file in the predefined manner."

190. Gennaro does not expressly teach or disclose "granting the request to use the file in the predefined manner."

191. I understand that the Petition alleges Gennaro discloses Limitation 42[e]. However, to a POSITA, none of the three disclosures from Gennaro identified by Petitioner disclose Limitation 42[e].

192. First, Petitioner contends that Gennaro at 2:54, 2:65-67 "disclose[] that the receiver plays a stream, thus granting the user's request to play an internet application." Petition at 56. As discussed above with respect to Limitation 42[a],

the cited portion of Gennaro does *not* disclose that a receiver "plays" a stream, but instead explains that finite streams of data, such as "digital movies, digital sounds, [and] applets," can be processed according to Gennaro's system. *See* Ex. 1008 at 2:64-3:4.

193. Furthermore, even if the cited portion described the playback of a data stream, there is no disclosure that the system takes an affirmative step to *grant* any request to use a file in a predefined way. This is evidenced by Gennaro itself, which, as explained below, merely allows the conversion of the data stream into video by the MPEG software to continue if no errors are detected. *See* Ex. 1008 (Gennaro) at 5:54-63 (if an error is detected the process is "halted," "[o]therwise" the processing of incoming data blocks continues.)

194. Gennaro describes an iterative process that divides the stream into blocks, and authenticates each block individually. Hence, like Hanna discussed above, Gennaro describes that some portions of the stream may be verified, while other are not. If verified, the MPEG software is informed of the block and "it can proceed to process the incoming original block that was authenticated." Ex. 1008 ar 5:61-63. This processing of authenticated blocks by the MPEG software (not further described in Gennaro) may include performing methods, such as those disclosed in the '815 patent, that process requests by the recipient to use the block in a predefined

manner, but there is no such suggestion or motivation in Gennaro regarding managing the use of the block, nor is a block a "file."

195. Conversely, the MPEG software is not informed of any blocks that cannot be authenticated, and those corrupted portions of the stream are not further processed. In such a system as Gennaro that verifies the stream in a block-by-block manner, it is unclear what it would even mean "to *grant* a request to use a file in a predefined way," as all of the file may not be further processed by the MPEG software for use. Moreover, that Gennaro's processing of a block can be halted at any time tampering is detected shows that there is no single step performed that "grants" the use of the file in a predefined manner.

196. Second, Petitioner contends that Limitation 42[e] is disclosed because a prior art receiver "asks for the authenticated stream" (Petition at 56 (citing Ex. 1008 (Gennaro) at 1:28-29)). However, Gennaro teaches away from this method of using the prior art device, which Gennaro criticizes as having a "problem." Moreover, simply asking for a data stream is also not the same thing as receiving a request to "*use* the file *in a predefined manner*." No explicit or implicit disclosure is made that Gennaro's receiver *grants* a request to use a file in a predefined manner simply because a receiver asks for a data stream.

197. Third, Petitioner contends that Limitation 42[e] is disclosed because, if tampering is detected, Gennaro's authentication software "halt[s]" the MPEG

software/hardware's processing of the data stream by not informing the MPEG software/hardware of the receipt of incoming data. *See* Petition at 56-57 (citing Ex. 1008 at 5:8-12, 5:35-39, 5:54-63). Gennaro expressly discloses that if no tampering is detected then the authentication software simply continues informing the MPEG software/hardware of incoming data. Thus, no affirmative *granting* step is performed in Gennaro.

C. Petitioner Fails to Show Claim 43 is Obvious

198. Claim 43 depends from independent claim 42 and, therefore, includes all of the features and limitations of claim 42. Accordingly, Petitioner fails to show that claim 43 is unpatentable in Grounds 1 and 2 for at least the same reasons provided above with respect to claim 42, and for its own unique features and limitations.

VIII. CONCLUSION

199. 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 of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

200. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were 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.

Executed: January 21, 2021

Markus Jakobsson, Ph.D.

APPENDIX A

CV and Research Statement

Markus Jakobsson
www.linkedin.com/in/markusjakobsson
www.markus-jakobsson.com

1 At a Glance

- **Focus.** *Identification of security problems, trends and solution along four axes* – computational, structural, physical *and* social*; quantitative and qualitative fraud analysis; development of disruptive security technologies.*
- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1994).
- **Large research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); PayPal (Principal Scientist of Consumer Security, Director, 2010-2013); Qualcomm (Senior Director, 2013-2015); Agari (Chief Scientist, 2016–2018); Amber Solutions Inc (Chief of Security and Data Analytics, 2018 – 2019); ByteDance (Principal Scientist, 2020-current)
- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2016).
- **Entrepreneurial activity.** *ZapFraud* (Anti-scam technology; CTO and founder, 2012-current); *RavenWhite Security* (Authentication solutions; CTO and founder, 2005-); *RightQuestion* (Consulting; Founder, 2007-current); *FatSkunk* (Malware detection; CTO and founder, 2009-2013 – FatSkunk was acquired by Qualcomm); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2013); *CellFony* (Mobile security; Member of technical advisory board, 2009-2013); *PopGiro* (User Reputation; Member of technical advisory board, 2012-2013); *MobiSocial* (Social networking, Member of technical advisory board, 2013); *Cequence Security* (Anti-fraud, Member of technical advisory board, 2013–current)
- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2011); *Boku* (2009-2010); *Western Union* (2009-2010).

- **Intellectual Property, Testifying Expert Witness.** *Inventor of 100+ patents; expert witness in 25+ patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale; Hunton & Williams; Quinn Emanuel Urquhart & Sullivan; Freed & Weiss; Berry & Domer; Fish & Richardson; DLA Piper; Cipher Law Group; Keker & Van Nest). Details and references upon request.

- **Publications**. Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crimeware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *Towards Trustworthy Elections: New Directions in Electronic Voting* (Springer Verlag, 2010); *Mobile Authentication: Problems and Solutions*)Springer Verlag, 2012); *The Death of the Internet* (Wiley, 2012); *Understanding Social Engineering* (Springer Verlag, 2016); *Security, Privacy and User Interaction* (Springer Verlag, 2020); *100+ peer-reviewed publications*

2 Summary

I am one of the more prominent computer scientists studying fraud and fraud prevention. I have performed and published novel research on fraud and authentication since 1993, with a focus on the payments industry since 1995. In 1999, I posited that what later became known as phishing would become a big problem. As a Principal Scientist at RSA Laboratories in 2001, my mandate was to determine the impact of future fraud scenarios on commerce and authentication, and developing intellectual property to address such problems. In 2004, I built a research group around online fraud and countermeasures, resulting in more than 50 publications and two books ("Phishing and Countermeasures", Wiley; "Crimeware", Symantec Press.) I co-founded the first company to address consumer security education, and am a pioneer in that area. I also co-founded an RSA Security spinoff (RavenWhite Security), and a company to address mobile malware (FatSkunk), and have overseen their intellectual property creation. FatSkunk was acquired by Qualcomm in 2013. I also founded ZapFraud, a company addressing Business Email Compromise. I am currently the Chief Scientist at Agari, a company addressing email-based fraud.

I have recruited and supervised junior colleagues, developers and PhD/Masters students for twenty years. I have been in charge with building research groups at Bell Laboratories, RSA Laboratories and Indiana University. I was the most senior security researcher at Indiana University, and was hired to Xerox PARC to provide thought leadership to their security group. My former advisees have prominent roles at RSA Laboratories, Mozilla, Google, and top universities such as MIT and ETH Zurich MIT. I played a prominent role in defining the intellectual property efforts at PayPal/eBay, and contributed significantly to their portfolio. I founded and built FatSkunk, bringing a new security paradigm to the marketplace. I am the most senior researcher at ByteDance.

3 Work History (Highlights)

1. **Member of Technical Staff, Bell Labs (1997-2001).** Markus was part of the security research group at Bell Labs. He formalized the notion of *proof of work*, later an integral part of BitCoin.

2. **Principal Scientist, RSA Labs (2001-2005).** Markus posited that phishing would become a mainstream problem, and developed ethical techniques for identifying likely trends based on human subject experiments.

3. **Associate Professor, Indiana University (2005-2008).** Markus was hired to lead the newly formed security group at Indiana University, and created a research group comprising approximately 10 professors and 30 students, studying social engineering and fraud.

4. **Principal Scientist, Xerox PARC (2008-2010).** Markus was hired to lead the research efforts of the Xerox PARC security group, and developed the notion of *implicit authentication*, a technology that is now ubiquitous.

5. **Principal Scientist, PayPal (2010-2013).** Markus did research on security and user interfaces, and developed techniques to reduce the losses associated with *liar buyer fraud*.

6. **Senior Director, Qualcomm (2013-2016).** Qualcomm acquires FatSkunk, a company founded by Markus. At FatSkunk, Markus developed *retroactive* malware detection with provable security guarantees. A simplified version of this is now deployed with almost all Qualcomm chipsets.

7. **Chief Scientist, Agari (2016-2018).** Markus developed a technique to acquire fraudster intelligence by compromising scammer email accounts – *while staying within the law* – resulting in the extradition of several African scam lords to the U.S.

8. **Chief of Security and Data Analytics, Amber Solutions (2018-2020).** Markus developed usable configuration methods supporting improved security and privacy for IoT installations.

4 Recent Focus

My work primarily involves identifying trends in fraud and computing before they affect the market, and to develop and test countermeasures – whether technical, or based on user interaction or education. I am the inventor of more than 100 patents. At PayPal, I developed and tested a technology that allows the automatic creation of PINs from passwords [57], with direct applications to improved mobile security and simplified user experience. I also studied liar buyer fraud [50] and developed improved authentication and fraud detection methods. At FatSkunk, I developed a new Anti-Virus paradigm (see, e.g., [53]); protected the intellectual property; built a team to build the technology; and worked towards commercializing the technology. After the acquisition of FatSkunk, this work was continued at Qualcomm, where I also worked on IoT, wearable authentication methods [52], anti-theft technology and privacy technology aimed at automatically detecting and block attempts to track users. My work at ZapFraud focused on understanding and blocking email scams [51], with a focus on business email compromise, and building a foundational patent portfolio. My work at Agari addressed enterprise-facing scams such as Business Email Compromise, Ransomware, and other abuse based on social engineering and identity deception. My work at Amber Solutions has involved protocol design for defending against attacks on consumer and enterprise sensor networks. My work at ByteDance relates to anticipating future abuse and proactively addressing it.

My PhD is in theoretical computer science, but my later emphasis has been on applied security, including authentication, click-fraud [40], mobile malware detection [53], detection of business email compromise, and the development of metrics to detect new types of fraud.

5 Publication List

Books (1-8); book chapters, journals, conference publications and other scientific publications (9-147), issued /published U.S. patents (148-234). For an updated list, and for international patents, please see `www.markus-jakobsson.com/publications` and appropriate patent search engines.

References

[1] M. Jakobsson, *Security, Privacy and User Interaction*, ISBN 978-3-030-43753-4, 110 pages, 2020.

[2] M. Jakobsson, *Understanding Social Engineering Based Scams*, ISBN 978-1-4939-6457-4, 130 pages, Springer, 2016.

[3] M. Jakobsson, *Mobile Authentication: Problems and Solutions*, ISBN 1461448778, 125 pages, Springer, 2013.

[4] M. Jakobsson, (editor) *The Death of the Internet*, ASIN B009CN2JVE, 359 pages, IEEE Computer Society Press, 2012.

[5] D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. Ryan, J. Benaloh, and M. Kutylowski, (editors), *Towards Trustworthy Elections: New Directions in Electronic Voting*, 411 pages, (Vol. 6000), Springer, 2010.

[6] M. Jakobsson and Z. Ramzan (editors), *Crimeware: Trends in Attacks and Countermeasures*, ISBN 0321501950, Hardcover, 582 pages, Symantec Press / Addison Wesley, 2008.

[7] M. Jakobsson and S. A. Myers (editors), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, ISBN 0-471-78245-9, Hardcover, 739 pages, Wiley, 2006.

[8] M. Jakobsson, M. Yung, J. Zhou, *Applied Cryptography and Network Security: Second International Conference , Yellow Mountain, China, 2004*, 511 pages, Lecture Notes in Computer Science (Book 3089), 2004.

[9] M. Jakobsson, "Permissions and Privacy," in IEEE Security & Privacy, vol. 18, no. 2, pp. 46-55, March-April 2020

[10] M. Jakobsson, "The Rising Threat of Launchpad Attacks," in IEEE Security & Privacy, vol. 17, no. 5, pp. 68-72, Sept.-Oct. 2019

[11] J Koven, C Felix, H Siadati, M Jakobsson, E Bertini, "Lessons learned developing a visual analytics solution for investigative analysis of scamming activities," IEEE transactions on visualization and computer graphics 25 (1), 225-234

[12] M Jakobsson, "Two-factor inauthentication?the rise in SMS phishing attacks" Computer Fraud & Security 2018 (6), 6-8

[13] M. Dhiman, M. Jakobsson, T.-F. Yen, "Breaking and fixing content-based filtering," 2017 APWG Symposium on Electronic Crime Research (eCrime), 52-56

[14] M. Jakobsson, "Addressing sophisticated email attacks," 2017 International Conference on Financial Cryptography and Data Security, 310-317

[15] M. Jakobsson, "User trust assessment: a new approach to combat deception," Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 2016, pages 73-78

[16] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, "Mind your SMSes: Mitigating social engineering in second factor authentication," Computers and Security, 2016

[17] M. Jakobsson, W. Leddy, "Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters," IEEE Spectrum 53 (5), 2016, 40-55

[18] N. Sae-Bae, M. Jakobsson, *Hand Authentication on Multi-Touch Tablets*, HotMobile 2014

[19] Y. Park, J. Jones, D. McCoy, E. Shi, M. Jakobsson, *Scambaiter: Understanding Targeted Nigerian Scams on Craigslist*, NDSS 2014

[20] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, and P. van Oorschot, "The future of authentication," Security & Privacy, IEEE, 10(1), 22-27, 2012.

[21] M. Jakobsson, and H. Siadati, *Improved Visual Preference Authentication: Socio-Technical Aspects in Security and Trust*, (STAST), 2012 Workshop on IEEE, 27–34, 2012.

[22] M. Jakobsson, R. I. Chow, and J. Molina, "Authentication-Are We Doing Well Enough?[Guest Editors' Introduction]" Security & Privacy, IEEE, 10(1), 19-21, 2012.

[23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," Information Security, 99-113, Springer Berlin Heidelberg, 2011.

[24] M. Jakobsson and K. Johansson, "Practical and Secure Software-Based Attestation," Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 1–9, 2011.

[25] A. Juels, D. Catalano, and M.Jakobsson, *Coercion-resistant electronic elections: Towards Trustworthy Elections*, 37–63, Springer Berlin Heidelberg, 2010.

[26] M. Jakobsson and F. Menczer, "Web Forms and Untraceable DDoS Attacks," in Network Security, Huang, S., MacCallum, D., and Du, D. Z., Eds.,77–95, Springer, 2010.

[27] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the Clouds: A Framework and its Application to Mobile Users," 2010.

[28] X. Wang, P. Golle, M. Jakobsson, and A. Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur., 13(2), 1-24, 2010.

[29] X. Wang, P. Golle, M. Jakobsson, A.Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur. 13(2): (2010)

[30] M. Jakobsson, and C. Soghoian, "Social Engineering in Phishing," Information Assurance, Security and Privacy Services, 4, 2009.

[31] M. Jakobsson, C. Soghoian and S. Stamm, "Phishing," Handbook of Financial Cryptography (CRC press, 2008)

[32] M. Jakobsson and A. Tsow, "Identity Theft," In John R. Vacca, Editor, "Computer And Information Security Handbook" (Morgan Kaufmann, 2008)

[33] S. Srikwan and M. Jakobsson, "Using Cartoons to Teach Internet Security," Cryptologia, vol. 32, no. 2, 2008

[34] M. Jakobsson, N. Johnson and P. Finn, "Why and How to Perform Fraud Experiments," IEEE Security and Privacy, March/April 2008 (Vol. 6, No. 2) pp. 66-68

[35] M. Jakobsson and S. Myers, "Delayed Password Disclosure," International Journal of Applied Cryptography, 2008, pp. 47-59.

[36] M. Jakobsson and S. Stamm, "Web Camouflage: Protecting Your Clients from Browser Sniffing Attacks," IEEE Security & Privacy Magazine. November/December 2007

[37] P. Finn and M. Jakobsson, "Designing and Conducting Phishing Experiments," IEEE Technology and Society Magazine, Special Issue on Usability and Security

[38] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer. "Social Phishing," The Communications of the ACM, October 2007

[39] A. Tsow, M. Jakobsson, L. Yang and S. Wetzel, "Warkitting: the Drive-by Subversion of Wireless Home Routers," Anti-Phishing and Online Fraud, Part II Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006

[40] M. Gandhi, M. Jakobsson and J. Ratkiewicz, "Badvertisements: Stealthy Click-Fraud with Unwitting Accessories," Anti-Phishing and Online Fraud, Part I Journal of Digital Forensic Practice, Volume 1, Special Issue 2, November 2006

[41] N. Ben Salem, J.-P. Hubaux and M. Jakobsson. "Reputation-based Wi-Fi Deployment," Mobile Computing and Communications Review, Volume 9, Number 3 (Best papers of WMASH 2004)

[42] N. Ben Salem, J. P. Hubaux, and M. Jakobsson. "Node Cooperation in Hybrid Ad hoc Networks," IEEE Transactions on Mobile Computing, Vol. 5, No. 4, April 2006.

[43] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," Journal of Cryptology, 2005

[44] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. "How To Turn Loaded Dice Into Fair Coins." IEEE Transactions on Information Theory, vol. 46(3). May 2000. pp. 911–921.

[45] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," Journal of Computer Networks, vol. 31, issue 11–16, Elsevier North-Holland, Inc., 1999. pp. 1101–1109.

[46] M. Jakobsson, "Cryptographic Protocols," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[47] M. Jakobsson, "Cryptographic Privacy Protection Techniques," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[48] M. Jakobsson, E. Shi, P. Golle, R. Chow, "Implicit authentication for mobile devices," 4th USENIX Workshop on Hot Topics in Security (HotSec '09); 2009 August 11; Montreal, Canada.

[49] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); 2009 November 13; Chicago, IL. NY: ACM; 2009; pp. 85–90.

[50] M. Jakobsson, H. Siadati, M. Dhiman, "Liar Buyer Fraud, and How to Curb It," NDSS, 2015

[51] M. Jakobsson, T.-F. Yen, "How Vulnerable Are We To Scams?," BlackHat, 2015

[52] M. Jakobsson, "How to Wear Your Password," BlackHat, 2014

[53] M. Jakobsson and G. Stewart, "Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines," in BlackHat, 2013.

[54] M. Jakobsson, and H. Siadati,"SpoofKiller: You Can Teach People How to Pay, but Not How to Pay Attention" in Socio-Technical Aspects in Security and Trust (STAST), 2012 Workshop on, 3-10, 2012.

[55] M. Jakobsson, and M. Dhiman,"The benefits of understanding passwords," in Proceedings of the 7th USENIX conference on Hot Topics in Security, Berkeley, CA, USA, 2012.

[56] M. Jakobsson, and S. Taveau, "The Case for Replacing Passwords with Biometrics," Mobile Security Technologies, 2012.

[57] M. Jakobsson and D. Liu, "Bootstrapping mobile PINs using passwords," W2SP, 2011.

[58] M. Jakobsson and R. Akavipat, "Rethinking passwords to adapt to constrained keyboards," 2011.

[59] Y. Niu, E. Shi, R. Chow, P. Golle, and M. Jakobsson, "One Experience Collecting Sensitive Mobile Data," In USER Workshop of SOUPS, 2010.

[60] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit Authentication through Learning User Behavior," 2010.

[61] M. Jakobsson and K. Johansson, Assured Detection of Malware With Applications to Mobile Platforms, 2010.

[62] M. Jakobsson and K. Johansson, "Retroactive Detection of Malware With Applications to Mobile Platforms," in HotSec 2010, Washington, DC, 2010.

[63] M. Jakobsson, A Central Nervous System for Automatically Detecting Malware, 2009.

[64] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, and J. Staddon, "Controlling data in the cloud: outsourcing computation without outsourcing control," ACM workshop on Cloud computing security (CCSW), 2009.

[65] M. Jakobsson and A. Juels, "Server-Side Detection of Malware Infection," in New Security Paradigms Workshop (NSPW), Oxford, UK, 2009.

[66] M. Jakobsson, "Captcha-free throttling," Proceedings of the 2nd ACM workshop on Security and artificial intelligence, 15–22, 2009.

[67] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," Proceedings of the 4th USENIX conference on Hot topics in security, 9–9, 2009.

[68] C. Soghoian, O. Friedrichs and M. Jakobsson, "The Threat of Political Phishing," International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)

[69] R. Chow, P. Golle, M. Jakobsson, L. Wang and X. Wang, "Making CAPTCHAs Clickable," In proc. of HotMobile 2008.

[70] M. Jakobsson, A. Juels, and J. Ratkiewicz, "Privacy-Preserving History Mining for Web Browsers," Web 2.0 Security and Privacy, 2008.

[71] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang, "Love and Authentication," (Notes) ACM Computer/Human Interaction Conference (CHI), 2008. Also see `www.I-forgot-my-password.com`

[72] M. Jakobsson and S. Myers, "Delayed Password Disclosure," Proceedings of the 2007 ACM workshop on Digital Identity Management

[73] M. Jakobsson, S. Stamm, Z. Ramzan, "JavaScript Breaks Free," W2SP '07

[74] A. Juels, S. Stamm, M. Jakobsson, "Combatting Click Fraud via Premium Clicks," USENIX Security 2007

[75] R. Chow, P. Golle, M. Jakobsson, X. Wang, "Clickable CAPTCHAs," Ad-Fraud '07 Workshop; 2007 September 14; Stanford, CA, USA

[76] S. Stamm, Z. Ramzan, and M. Jakobsson, "Drive-by Pharming," In Proceedings of Information and Communications Security, 9th International Conference, ICICS 2007

[77] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, "What Instills Trust? A Qualitative Study of Phishing," USEC '07.

[78] R. Akavipat, V. Anandpara, A. Dingman, C. Liu, D. Liu, K. Pongsanon, H. Roinestad and M. Jakobsson, "Phishing IQ Tests Measure Fear, not Ability," USEC '07.

[79] M. Jakobsson, "The Human Factor in Phishing," American Conference Institute's Forum on Privacy & Security of Consumer Information, 2007

[80] S. Srikwan, M. Jakobsson, A. Albrecht and M. Dalkilic, "Trust Establishment in Data Sharing: An Incentive Model for Biodiversity Information Systems," TrustCol 2006

[81] J.Y. Choi, P. Golle, M. Jakobsson, "Tamper-Evident Digital Signatures: Protecting Certification Authorities Against Malware," DACS '06

[82] L. Yang, M. Jakobsson, S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," SECURECOMM '06

[83] P. Golle, X. Wang, M. Jakobsson, A. Tsow, "Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks." IEEE S&P '06

[84] M. Jakobsson, A. Juels, T. Jagatic, "Cache Cookies for Browser Authentication (Extended Abstract)," IEEE S&P '06

[85] M. Jakobsson and J. Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features.", WWW '06

[86] M. Jakobsson and S. Stamm. "Invasive Browser Sniffing and Countermeasures," WWW '06

[87] J.Y. Choi, P. Golle and M. Jakobsson. "Auditable Privacy: On Tamper-Evident Mix Networks," Financial Crypto '06

[88] A. Juels, D. Catalano and M. Jakobsson. "Coercion-Resistant Electronic Elections," WPES '05

[89] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," ACNS '05, 2005.

[90] M. Jakobsson and L. Yang. "Quantifying Security in Hybrid Cellular Networks," ACNS '05, 2005

[91] Y.-C. Hu, M. Jakobsson, and A. Perrig. "Efficient Constructions for One-way Hash Chains," ACNS '05, 2005

[92] M. Jakobsson. "Modeling and Preventing Phishing Attacks," Phishing Panel in Financial Cryptography '05. 2005, abstract in proceedings.

[93] N. Ben Salem, J.-P. Hubaux, and M. Jakobsson. "Reputation-based Wi-Fi Deployment Protocols and Security Analysis," In WMASH '04. ACM Press, 2004. pp. 29–40.

[94] M. Jakobsson and S. Wetzel. "Efficient Attribute Authentication with Applications to Ad Hoc Networks," In VANET '04. ACM Press, 2004. pp. 38–46.

[95] M. Jakobsson, X. Wang, and S. Wetzel. "Stealth Attacks in Vehicular Technologies," Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004 Fall (VTC-Fall 2004). IEEE, 2004.

[96] A. Ambainis, H. Lipmaa, and M. Jakobsson. "Cryptographic Randomized Response Technique," In PKC '04. LNCS 2947. Springer-Verlag, 2004. pp. 425–438.

[97] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. "Universal Re-encryption for Mixnets," In CT-RSA '04. LNCS 2964. Springer-Verlag, 2004. pp. 163–178.

[98] P. Golle and M. Jakobsson. "Reusable Anonymous Return Channels," In WPES '03. ACM Press, 2003. pp. 94–100.

[99] M. Jakobsson, S. Wetzel, B. Yener. "Stealth Attacks on Ad-Hoc Wireless Networks," In IEEE VTC '03, 2003.

[100] N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks," In ACM MobiHoc '03. ACM Press, 2003. pp. 13–24.

[101] M. Jakobsson, J.-P.Hubaux and L. Buttyan. "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks," In FC '03. LNCS 2742. Springer-Verlag, 2003. pp. 15–33.

[102] M. Jakobsson, T. Leighton, S. Micali and M. Szydlo. "Fractal Merkle Tree Representation and Traversal," In RSA-CT '03 2003.

[103] A. Boldyreva and M Jakobsson. "Theft protected proprietary certificates," In DRM '02. LNCS 2696, 2002. pp. 208–220.

[104] P. Golle, S. Zhong, M. Jakobsson, A. Juels, and D. Boneh. "Optimistic Mixing for Exit-Polls," In Asiacrypt '02. LNCS 2501. Springer-Verlag, 2002. pp. 451–465.

[105] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," In CRYPTO '02. LNCS 2442. Springer-Verlag, 2002. pp. 385–400.

[106] M. Jakobsson. "Fractal Hash Sequence Representation and Traversal," In Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT '02). 2002. pp. 437–444.

[107] M. Jakobsson, A. Juels, and R. Rivest. "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking," In Proceedings of the 11th USENIX Security Symposium. USENIX Association, 2002. pp. 339–353.

[108] D. Coppersmith and M. Jakobsson. "Almost Optimal Hash Sequence Traversal," In Financial Crypto '02. 2002.

[109] M. Jakobsson. "Financial Instruments in Recommendation Mechanisms," In Financial Crypto '02. 2002.

[110] J. Garay, and M. Jakobsson. "Timed Release of Standard Digital Signatures," In Financial Crypto '02. 2002.

[111] F. Menczer, N. Street, N. Vishwakarma, A. Monge, and M. Jakobsson. "Intellishopper: A Proactive, Personal, Private Shopping Assistant," In AAMAS '02. ACM Press, 2002. pp. 1001–1008.

[112] M. Jakobsson, A. Juels, and P. Nguyen. "Proprietary Certificates," In CT-RSA '02. LNCS 2271. Springer-Verlag, 2002. pp. 164–181.

[113] M. Jakobsson and A. Juels. "An Optimally Robust Hybrid Mix Network," In PODC '01. ACM Press. 2001. pp. 284–292.

[114] M. Jakobsson and M. Reiter. "Discouraging Software Piracy Using Software Aging," In DRM '01. LNCS 2320. Springer-Verlag, 2002. pp. 1–12.

[115] M. Jakobsson and S. Wetzel. "Security Weaknesses in Bluetooth," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 176–191.

[116] M. Jakobsson and D. Pointcheval. "Mutual Authentication for Low-Power Mobile Devices," In Financial Crypto '01. LNCS 2339. Springer-Verlag, 2001. pp. 178–195.

[117] M. Jakobsson, D. Pointcheval, and A. Young. "Secure Mobile Gambling," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 110–125.

[118] M. Jakobsson and S.Wetzel. "Secure Server-Aided Signature Generation," In PKC '01. LNCS 1992. Springer-Verlag, 2001. pp. 383–401.

[119] M. Jakobsson and A. Juels. "Addition of ElGamal Plaintexts," In T. Okamoto, ed., ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 346–358.

[120] M. Jakobsson, and A. Juels. "Mix and Match: Secure Function Evaluation via Ciphertexts," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 162–177.

[121] R. Arlein, B. Jai, M. Jakobsson, F. Monrose, and M. Reiter. "Privacy-Preserving Global Customization," In ACM E-Commerce '00. ACM Press, 2000. pp. 176–184.

[122] C.-P. Schnorr and M. Jakobsson. "Security of Signed ElGamal Encryption," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 73–89.

[123] P. Bohannon, M. Jakobsson, and S. Srikwan. "Cryptographic Approaches to Privacy in Forensic DNA Databases," In Public Key Cryptography '00. LNCS 1751. Springer-Verlag, 2000, pp. 373–390.

[124] J. Garay, M. Jakobsson, and P. MacKenzie. "Abuse-free Optimistic Contract Signing," In CRYPTO '99. LNCS 1666. Springer-Verlag, 1999. pp. 449–466.

[125] M. Jakobsson. "Flash Mixing," In PODC '99. ACM Press, 1999. pp. 83–89.

[126] G. Di Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. "How To Forget a Secret," In STACS '99. LNCS 1563. Springer-Verlag, 1999. pp. 500–509.

[127] M. Jakobsson, D. M'Raihi, Y. Tsiounis, and M. Yung. "Electronic Payments: Where Do We Go from Here?," In CQRE (Secure) '99. LNCS 1740. Springer-Verlag, 1999. pp. 43–63.

[128] C.P. Schnorr and M. Jakobsson. "Security Of Discrete Log Cryptosystems in the Random Oracle + Generic Model," In Conference on The Mathematics of Public-Key Cryptography. 1999.

[129] M. Jakobsson and A. Juels "Proofs of Work and Breadpudding Protocols," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 252 – 272.

[130] M. Jakobsson and C-P Schnorr. "Efficient Oblivious Proofs of Correct Exponentiation," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 71–86.

[131] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," In World Wide Web '99

[132] M. Jakobsson, J.P. Stern, and M. Yung. "Scramble All, Encrypt Small," In Fast Software Encryption '99. LNCS 1636. Springer-Verlag, 1999. pp. 95–111.

[133] M. Jakobsson and J. Mueller. "Improved Magic Ink Signatures Using Hints," In Financial Cryptography '99. LNCS 1648. Springer-Verlag, 1999. pp. 253–268.

[134] M. Jakobsson. "Mini-Cash: A Minimalistic Approach to E-Commerce," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 122–135.

[135] M. Jakobsson. "On Quorum Controlled Asymmetric Proxy Re-encryption," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 112–121.

[136] M. Jakobsson and A. Juels. "X-Cash: Executable Digital Cash," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 16–27.

[137] M. Jakobsson and D. M'Raihi. "Mix-based Electronic Payments," In Proceedings of the Selected Areas in Cryptography. LNCS 1556. Springer-Verlag, 1998. pp. 157173.

[138] M. Jakobsson, E. Shriver, B. Hillyer, and A. Juels. "A Practical Secure Physical Random Bit Generator," In CCS '98: Proceedings of the 5th ACM conference on Computer and communications security. ACM Press, 1998. pp. 103–111.

[139] M. Jakobsson. "A Practical Mix," In Advances in Cryptology – EuroCrypt '98. LNCS 1403. Springer-Verlag, 1998. pp. 448–461.

[140] M. Jakobsson and M. Yung. "On Assurance Structures for WWW Commerce," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 141–157.

[141] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. "Curbing Junk E-Mail via Secure Classification," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 198–213.

[142] M. Jakobsson and M. Yung. "Distributed 'Magic Ink' Signatures," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 450–464.

[143] M. Jakobsson and M. Yung. "Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System," In Financial Cryptography '97. LNCS 1318. Springer-Verlag, 1997. pp. 217–238.

[144] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. "Proactive public-key and signature schemes," In Proceedings of the 4th Annual Conference on Computer Communications Security. ACM Press, 1997. pp. 100–110.

[145] M. Bellare, M. Jakobsson, and M. Yung. "Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 280–305.

[146] M. Jakobsson and M. Yung. "Proving Without Knowing," In Crypto '96. LNCS 1109. Springer-Verlag, 1996. pp. 186–200.

[147] M. Jakobsson, K. Sako, and R. Impagliazzo. "Designated Verifier Proofs and Their Applications," In Advances in Cryptology – EuroCrypt '96. LNCS 1070. Springer-Verlag, 1996. pp. 143–154.

[148] M. Jakobsson and M. Yung. "Revokable and Versatile Electronic Money," In CCS '96: Proceedings of the 3rd ACM conference on Computer and communications security. ACM Press, 1996. pp. 76–87.

[149] M. Jakobsson. "Ripping Coins for a Fair Exchange," In Advances in Cryptology – EuroCrypt '95. LNCS 921. Springer-Verlag, 1995. pp. 220–230.

[150] M. Jakobsson. "Blackmailing using Undeniable Signatures," In Advances in Cryptology EuroCrypt '94. LNCS 950. Springer-Verlag, 1994. pp. 425–427.

[151] M. Jakobsson. "Reducing costs in identification protocols," Crypto '92, 1992.

[152] M. Jakobsson. "Machine-Generated Music with Themes," In International Conference on Artificial Neural Networks '92. Vol 2. Amsterdam: Elsevier, 1992. pp. 1645–1646

[153] M. Jakobsson, "Social Engineering 2.0: What's Next," McAfee Security Journal, Fall 2008

[154] M. Jakobsson and S. Myers, "Delayed Password Disclosure," ACM SIGACT News archive, Volume 38, Issue 3 (September 2007), pp. 56 - 75

[155] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," CryptoBytes, 2007.

[156] M. Jakobsson, A. Juels, J. Ratkiewicz, "Remote-Harm Detection," Beta-version available at `rhd.ravenwhitedevelopment.com/`

[157] S. Stamm, M. Jakobsson, "Social Malware," Experimental results available at `www.indiana.edu/ phishing/verybigad/`

[158] M. Jakobsson. "Privacy vs. Authenticity," Ph.D. Thesis, University of California at San Diego, 1997

[159] Markus Jakobsson, Automatic PIN creation using passwords, US20130125214 A1, 2012.

[160] Markus Jakobsson, Systems and methods for creating a user credential and authentication using the created user credential, US 20130111571 A1, 2012.

[161] Markus Jakobsson, Password check by decomposing password, US 20120284783 A1, 2012.

[162] Markus Jakobsson, William Leddy, System and methods for protecting users from malicious content, US 20120192277 A1, 2011.

[163] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8370935 B1, 2011.

[164] Markus Jakobsson, Methods and Apparatus for Efficient Computation of One-Way Chains in Cryptographic Applications, US20120303969 A1, 2011.

[165] Markus Jakobsson, Automatic PIN creation using password, US 20120110634 A1, 2011.

[166] Markus Jakobsson, Jim Roy Palmer, Gustavo Maldonado, Interactive CAPTCHA, US20130007875 A1, 2011.

[167] Markus Jakobsson, System access determination based on classification of stimuli, US 20110314559 A1, 2011.

[168] Markus Jakobsson, System access determination based on classification of stimuli, WO 2011159356 A1, 2011.

[169] Markus Jakobsson, Method, medium, and system for reducing fraud by increasing guilt during a purchase transaction, US8458041 B1, 2011.

[170] Markus Jakobsson, Visualization of Access Information, US 20120233314 A1, 2011.

[171] Markus Jakobsson, Richard Chow,Runting Shi, Implicit authentication, US20120137340 A1, 2010.

[172] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, EP2467793 A1, 2010.

[173] Markus Jakobsson, Event log authentication using secure components, US 20110314297 A1, 2010.

[174] Markus Jakobsson, Philippe J.P. Golle, Risk-based alerts, US 20110314426 A1, 2010.

[175] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041178 A1, 2010.

[176] M. Jakobsson, A. Juels, J. Kaliski Jr, S. Burton and others, Identity authentication system and method, US Patent 7,502,933, 2009.

[177] Markus Jakobsson, Method and system for facilitating throttling of interpolation-based authentication, US8219810 B2, 2009.

[178] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8375442 B2, 2009.

[179] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041180 A1, 2009.

[180] Markus Jakobsson, Pattern-based application classification, US 20110055925 A1, 2009.

[181] Markus Jakobsson, Method and apparatus for detecting cyber threats, US8286225 B2, 2009.

[182] Markus Jakobsson, Method and apparatus for detecting cyber threats, US20110035784 A1, 2009.

[183] Markus Jakobsson, CAPTCHA-free throttling, US8312073 B2, 2009.

[184] Markus Jakobsson, Captcha-free throttling, US 20110035505 A1, 2009.

[185] Markus Jakobsson, Christopher Soghoian, Method and apparatus for throttling access using small payments, US 20100153275 A1, 2008.

[186] Markus Jakobsson, Christopher Soghoian, Method and apparatus for mutual authentication using small payments, US 20100153274 A1, 2008.

[187] Philippe J.P. Golle, Markus Jakobsson,Richard Chow, Resetting a forgotten password using the password itself as authentication, US 20100125906 A1, 2008.

[188] Philippe J. P. Golle, Markus Jakobsson,Richard Chow, Authenticating users with memorable personal questions, US8161534 B2, 2008.

[189] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Authentication based on user behavior, US20100122329 A1, 2008.

[190] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Enterprise password reset, US 20100122340 A1, 2008.

[191] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US8086866 B2, 2008.

[192] Richard Chow, Philippe J. P. Golle, Markus Jakobsson, Selectable captchas, US8307407 B2, 2008.

[193] Markus Jakobsson, Ari Juels, Sidney Louis Stamm, Method and apparatus for combatting click fraud, US 20080162227 A1, 2007.

[194] Jakobsson, Method and apparatus for evaluating actions performed on a client device, US 20080037791 A1, 2007.

[195] Jakobsson, Ari Juels, Method and apparatus for storing information in a browser storage area of a client device, US 20070106748 A1, 2006.

[196] Markus Jakobsson, Steven Andrew Myers, Anti-phising logon authentication object oriented system and method, WO 2006062838 A1, 2005.

[197] Jakobsson, Jean-Pierre Hubaux,Levente Buttyan, Micro-payment scheme encouraging collaboration in multi-hop cellular networks, US 20050165696 A1, 2004.

[198] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , System and method providing disconnected authentication, WO2005029746 A3, 2004.

[199] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane Rice, Ronald Rivest, Less , System and method providing disconnected authentication, US 20050166263 A1, 2004.

[200] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , Systeme et procede d'authentification deconnectee, WO 2005029746 A2, 2004.

[201] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Identity authentication system and method, WO2004051585 A3, 2003.

[202] Markus Jakobsson, Ari Juels, Burton S. Kaliski, Jr., Identity authentication system and method, US 7502933 B2, 2003.

[203] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Systeme et procede de validation d'identite, WO 2004051585 A2, 2003.

[204] Markus Jakobsson, Burton S. Kaliski, Jr., Method and apparatus for graph-based partition of cryptographic functionality, US7730518 B2, 2003.

[205] Markus Jakobsson, Phong Q. Nguyen, Methods and apparatus for private certificates in public key cryptography, US7404078 B2, 2002.

[206] Jakobsson, Philip MacKenzie, Thomas Shrimpton, Method and apparatus for performing multi-server threshold password-authenticated key exchange, US20030221102 A1, 2002.

[207] Markus Jakobsson, Philip D MacKenzie, Method and apparatus for distributing shares of a password for use in multi-server password authentication, US 7073068 B2, 2002.

[208] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, EP 1389376 A1 (text from WO2002084944A1), 2002.

[209] Markus Jakobsson, Adam Lucas Young, Method and apparatus for identification tagging documents in a computer system, US 7356845 B2, 2002.

[210] Juan A. Garay, Markus Jakobsson, Methods and apparatus for computationally-efficient generation of secure digital signatures, US 7366911 B2, 2001.

[211] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US 7404080 B2, 2001.

[212] Markus Jakobsson, Susanne Gudrun Wetzel, Securing the identity of a bluetooth master device (bd addr) against eavesdropping by preventing the association of a detected channel access code (cac) with the identity of a particular bluetooth device, WO2002019641 A3, 2001.

[213] Markus Jakobsson, Susanne Gudrun Wetzel, Procede et appareil permettant d'assurer la securite d'utilisateurs de dispositifs a capacites bluetooth, WO 2002019641 A2, 2001.

[214] Robert M. Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose, Michael Kendrick Reiter, Less , Methods and apparatus for providing privacy-preserving global customization, US 7107269 B2, 2001.

[215] Markus Jakobsson, Susanne Gudrun Wetzel, Secure distributed computation in cryptographic applications, US6950937 B2, 2001.

[216] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of short range wireless enable devices, US6981157 B2, 2001.

[217] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of bluetooth TM-enabled devices, US 6574455 B2, 2001.

[218] Garay; Juan A. (West New York, NJ), Jakobsson; M. (Hoboken, NJ), Kristol; David M. (Summit, NJ), Mizikovsky; Semyon B.(Morganville, NJ), Cryptographic key processing and storage , 7023998, 2001.

[219] Markus Jakobsson, Method, apparatus, and article of manufacture for generating secure recommendations from market-based financial instrument prices, US 6970839 B2, 2001.

[220] Markus Jakobsson, Encryption method and apparatus with escrow guarantees, US7035403 B2, 2001.

[221] Jakobsson, Call originator access control through user-specified pricing mechanism in a communication network, US20020099670 A1, 2001.

[222] Markus Jakobsson, Claus Peter Schnorr, Tagged private information retrieval, US7013295 B2, 2000.

[223] Markus Jakobsson, Secure enclosure for key exchange, US 7065655 B1, 2000.

[224] Markus Jakobsson, Michael Kendrick Reiter, Software aging method and apparatus for discouraging software piracy, US 7003110 B1, 2000.

[225] Markus Jakobsson, Probabilistic theft deterrence, US6501380 B1, 2000.

[226] Markus Jakobsson, Michael Kendrick Reiter, Abraham Silberschatz, Anonymous and secure electronic commerce, EP 1150227 A1, 2000.

[227] Markus Jakobsson, Ari Juels, Proofs of work and bread pudding protocols, US 7356696 B1, 2000.

[228] Markus Jakobsson, Joy Colette Mueller, Methods of protecting against spam electronic mail, US7644274 B1, 2000.

[229] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, EP1043862 B1, 2000.

[230] Markus Jakobsson, Ari Juels, Mix and match: a new approach to secure multiparty computation, US6772339 B1, 2000.

[231] Markus Jakobsson, Ari Juels, Mixing in small batches, US6813354 B1, 2000.

[232] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, US 6901145 B1, 36566

[233] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US6931126 B1, 2000.

[234] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US 6931126 B1, 2000.

[235] Markus Jakobsson, Flash mixing apparatus and method, US 6598163 B1, 1999.

[236] Markus Jakobsson, Minimalistic electronic commerce system, US 6529884 B1, 1999.

[237] Markus Jakobsson, Method and system for providing translation certificates, US 6687822 B1, 1999.

[238] Markus Jakobsson, Verification of correct exponentiation or other operations in cryptographic applications, US6978372 B1, 1999.

[239] Markus Jakobsson, Non malleable encryption apparatus and method, US 6507656 B1, 1999.

[240] Markus Jakobsson, Method and system for quorum controlled asymmetric proxy encryption, US 6587946 B1, 1998.

[241] Markus Jakobsson, Practical mix-based election scheme, US 6317833 B1, 1998.

[242] Markus Jakobsson, Ari Juels, Method and apparatus for extracting unbiased random bits from a potentially biased source of randomness, US 6393447 B1, 1998.

[243] Markus Jakobsson, Ari Juels, Executable digital cash for electronic commerce, US6157920 A, 1998.

[244] Bruce Kenneth Hillyer, Markus Jakobsson, Elizabeth Shriver, Storage device random bit generator, US 6317499 B1, 1998.

[245] Markus Jakobsson, Method and apparatus for encrypting, decrypting, and providing privacy for data values, US 6049613 A, 1998.