DOCKET NO.: 1033300-00307US1
Filed on behalf of Apple Inc.
By: Monica Grewal, Reg. No. 40,056 (Lead Counsel)
Ben Fernandez Reg. No. 55,172 (Backup Counsel)
Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
Email: monica.grewal@wilmerhale.com
ben.fernandez@wilmerhale.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,

Patent Owner.

Case CBM2018-00026

U.S. Patent No. 8,577,813

DECLARATION OF DR. VICTOR SHOUP IN SUPPORT OF PETITION FOR COVERED BUSINESS METHOD REVIEW

TABLE OF CONTENTS

Page

I, Victor Shoup, Ph.D., declare as follows:

1. My name is Victor Shoup.

2. I have been retained by Apple to provide opinions in this proceeding relating to U.S. Patent No. 8,577,813 ("'813 patent").

I. BACKGROUND

3. I received a Bachelor of Science in Computer Science and Mathematics from the University of Wisconsin at Eau Claire in 1983. I received my Doctorate in Computer Science from the University of Wisconsin at Madison in 1989. I worked as a research scientist at Bellcore and at IBM Research Zurich. My work there included design of cryptographic protocols such as a new public key cryptosystem (now called the Cramer-Shoup cryptosystem) that achieved higher levels of security than were previously thought possible in a practical scheme.

4. I have been Professor of Computer Science at the Courant Institute of Mathematical Sciences at New York University since 2002 (initially as an Associate Professor, and as a Professor since 2007). I teach a variety of graduate and undergraduate courses on cryptography. Since 2012, I have also been a part-time visiting researcher at the IBM T. J. Watson Research Center in Yorktown, New York, where I collaborate with the Cryptography Research Group, which does work on a range of projects from the theoretical foundations of cryptography

to the design and implementation of cryptographic protocols, such as homomorphic encryption.

5. My areas of research include cryptography and number-theoretic algorithms, and I have published over 60 papers in these areas. In the area of cryptography, I have made substantial contributions in the sub-areas of digital signatures, public key encryption, hash functions, distributed computation, session key exchange, and secure anonymous credentials.

6. I was also an editor of the ISO18033-2 standard for public-key encryption, which was published in 2006.

7. I have been on the program committee of numerous international conferences on cryptography, and was the Program Chair at Crypto 2005 (Crypto is the premier international conference on cryptography). I have also acted as a consultant on cryptographic protocols for several companies.

8. In recognition of my contributions to the field of cryptography, I was named a Fellow of the International Association for Cryptographic Research (IACR) in 2016, for fundamental contributions to public-key cryptography and cryptographic security proofs, and for educational leadership.

9. I have given a number of invited lectures on my research in cryptographic protocol design. In 2005, I published a textbook on the mathematical underpinnings of cryptography titled *A Computational Introduction*

to Number Theory and Algebra, which I have made available online for free at http://www.shoup.net/ntb. I am also currently writing a textbook on applied cryptography. It is available in draft form at http://toc.cryptobook.us.

10. I am listed as an inventor on 6 United States patents, several related to authenticated key exchange, one related to secure multi-party computation, and one related to public-key encryption.

11. A copy of my curriculum vitae is attached as Appendix A.

12. I am being compensated at my normal consulting rate for my work. My compensation is not dependent on the outcome of this CBM proceeding or the related litigation, and does not affect the substance of my statements in this Declaration.

13. I have no financial interest in Petitioner. I have no financial interest in the '813 patent.

II. LEGAL PRINCIPLES

14. I am not an attorney. For purposes of this declaration, I have been informed about certain aspects of the law that are relevant to my analysis and opinions.

15. I have been informed that the claim terms in a CBM review should be given their broadest reasonable construction in light of the specification as commonly understood by a person of ordinary skill in the art.

16. I have been informed that laws of nature, abstract ideas, and natural phenomena are not patent eligible.

17. I have been informed that an application of an abstract idea, such as a mathematical formula, may be patent eligible if the patent claims add significantly more than routine, conventional activity to the underlying concept.

18. I have been informed that an important and useful clue to patent eligibility is whether a claim is tied to a particular machine or apparatus or transforms a particular article into a different state or thing, according to the so called "machine-or-transformation test." I have been informed that the machine-or-transformation test is not the only test for patent eligibility.

19. I have been informed that the Supreme Court's decision in *Alice Corp. Pty. v. CLS Bank Int'l*, 137 S. Ct. 2347 (2014), articulates a two-step framework for distinguishing patents that claim ineligible abstract ideas from those that claim eligible applications of those ideas. In step one, the court must determine whether the claims at issue are directed to a patent-ineligible abstract concept. If the claim is directed to an abstract idea, the analysis proceeds to step two. In step two, the elements of the claim must be searched, both individually and as an "ordered combination," for an "inventive concept"—i.e., "an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id*. at 2355

(alteration in original). I am informed that a patentee cannot circumvent the prohibition on patenting abstract ideas by limiting the idea to "a particular technological environment," nor by adding "insignificant postsolution activity," or "well-understood, routine, conventional" features.

III. DESCRIPTION OF THE RELEVANT FIELD AND THE RELEVANT TIMEFRAME

20. I have reviewed and understand the specification, claims, and file history of the '813 patent. I have also reviewed the list of exhibits attached hereto as Appendix B. Based on my review of these materials, I believe that the relevant field for purposes of my analysis is computer science, including the areas of data security, encryption, and security algorithms. As described above, I have extensive experience in the relevant technology.

21. The '813 patent issued on November 5, 2013 from an application filed on September 20, 2011. *Id.* The '813 patent is a continuation and a continuation-in-part of numerous U.S. Applications, the earliest of which, App. No. 11/677,490 (now U.S. Patent No. 8,001,055 (Ex-1004)), was filed on February 21, 2007. The patent also claims priority to four provisional applications: Application Nos. 60/775,046 (Ex-1121), 60/812,279 (Ex-1122), 60/859,235 (Ex-1123) and 61/031,529, (Ex-1124). The earliest of which was filed on February 21, 2006; the

latest of which was filed February 26, 2008, and is the first application to disclose Figure 31 and the description of the embodiments claimed in the '813 patent.

IV. The '813 Patent

A. Specification and Claims

22. The '813 patent describes a secure database called a "Universal Secure Registry" ("USR"), which is "a universal identification system … used to selectively provide personal, financial or other information about a person to authorized users." Ex-1001, '813 patent at 3:66-4:1. The patent states that the USR database is designed to "take the place of [] conventional forms of identification" when conducting financial transactions to minimize the incidence of fraud. *E.g.*, *id.* at 4:12-15. The patent states that various forms of information can be stored in the database to verify a user's identity and prevent fraud: (1) algorithmically generated codes, such as a time-varying multicharacter code or an "uncounterfeitable token," (2) "secret information" like a PIN or password, and/or (3) a user's "biometric information," such as fingerprints, voice prints, an iris or facial scan, DNA analysis, or a photograph. *See id.* at 42:29-36, 12:19-31, Fig. 3. The patent does not, however, describe any new technology for generating, capturing, or combining such information.

23. Instead, the patent emphasizes that the USR database can be implemented in "a general-purpose computer system" using "a commercially

available microprocessor" running "any … commercially available operating system." *Id.* at 10:9-15. The alleged invention is also "not limited to a particular computer platform, particular processor, or particular high-level programming language." *Id.* at 10:58-60. The USR database itself "may be any kind of database" and communication with the database may take place over "any [network] protocol." *Id.* at 10:24-26, 11:24-28, Fig. 1. Transactions to and from the database are encrypted using known methods, and access restrictions for users are implemented using known cryptographic methods. *Id.* at 4:1-11.

24. In its complaint against Apple, USR identified '813 patent claim 1 as "exemplary" of the other claims of the patent. Claim 1, which is described by, for example, Figure 31 (shown below), claims "an electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction." *Id.* at 51:65-67. The claimed electronic ID device contains several generic components: (1) a biometric sensor that receives a biometric input from the user (367); (2) a user interface whereby a user can input secret information (such as a PIN code) and select the account he or she wants to access (364); (3) a communication interface that can communicate with the secure registry (366) and with a point of sale device (354) capable of communicating with the secure registry; and (4) a processor (not shown) that can grant access to the electronic ID device via authentication by biometric and/or secret information and

generate encrypted authentication information from some combination of a nonpredictable value and the biometric and/or secret information to send to the secure registry. *Id.* at 12:19-54.

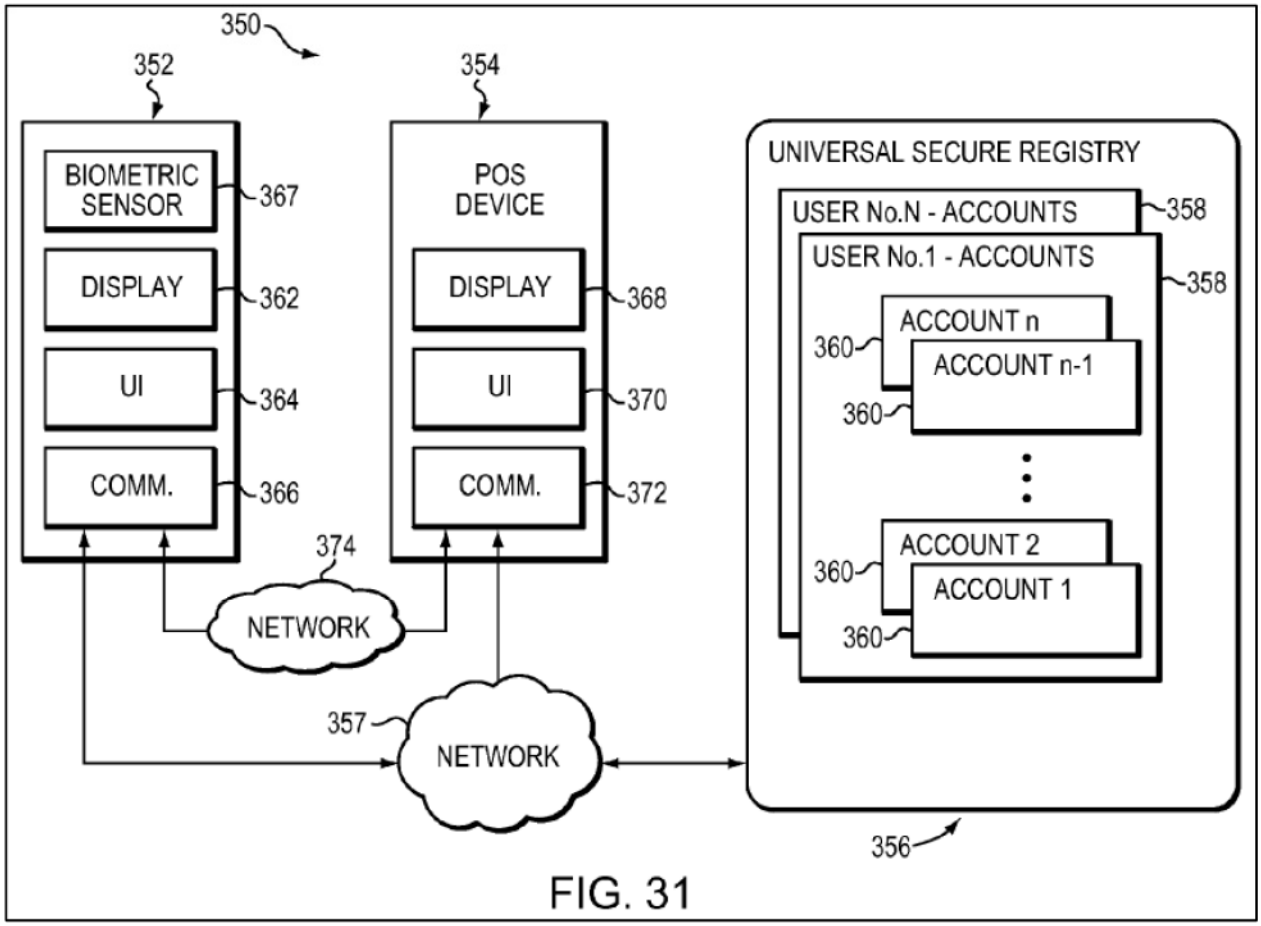

FIG. 31

Ex-1001, '813 patent, Fig. 31.

B. Prosecution History

25. I have been informed that the '813 patent was filed as U.S. Application No. 13/237,184 ("'813 application") on September 20, 2011. (Ex-1001.) The '813 application claimed priority back to the four provisional applications, No. 60/812,279, filed on June 9, 2006, Provisional Application No.

60/859,235, filed on Nov. 15, 2006, Provisional Application No. 60/775,046, filed on February 21, 2006, and Provisional Application No. 61/031,529, filed on February 26, 2008.

26. I have been informed that with the filing, Patent Owner included International Search Reports from three PCT applications with the filing documentation of the '813 application as part of the Information Disclosure Statement. *See* Ex-1005, '813 Patent File History, 09/20/2011 Documents Submitted With 371 Applications at 1, 8, 25.

27. I have been informed that on September 26, 2011, Patent Owner filed a Petition to Make Special Based on Age for Advancement of Examination under 37 C.F.R. § 1.102(c)(1). *See* Ex-1006, '813 Patent File History, 09/26/2011 Petition Automatically Granted by EFS. The petition was automatically granted. *Id.*

28. I have been informed that the examiner issued a Non-Final Rejection on August 15, 2012. *See* Ex-1007, '813 Patent File History, 08/15/2012 Non-Final Rejection. The examiner rejected application claims 1-2, 4-6, and 13-20 (issued claims 1, 2-4, and 11-18) under 35 U.S.C. § 102 as anticipated by U.S. Patent App. Publication 20020178364 ("Weiss"). *Id.* at 3. The examiner also rejected application claim 3 under 35 U.S.C. § 103 as obvious over Weiss in view of U.S. Patent App. Publication 20040117302 ("Weichart") (explaining that although

Weiss does not explicitly teach a POS system with a magnetic strip reader and a converter device to emulate the output, Weichart includes the missing limitations). *Id.* at 8.

29. I have been informed that the examiner rejected application claim 7 (issued claim 5) under § 103 as obvious over Weiss in view of U.S. Patent No. 6,819,219 ("Bolle"), explaining that Bolle "teaches a memory stor[ing] information employed by the device to authenticate the biometric received by the biometric sensor." *Id.* at 9.

30. I have been informed that the examiner rejected application claims 8-12 (issued claims 6-10) under § 103 as obvious over Weiss in view of Bolle and further in view of an Official Notice. *Id.* at 10. The reasoning of the Official Notice is included below.

> The Examiner takes Official Notice it is well known in the art a mismatch or non-matched biometric reading not belonging to the rightful user provides a negative result which prevents access. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the devices as disclosed by Weiss/Bolle Combination by incorporating a measure which prevents access when biometric readings do not match as taught by Official Notice in order to increase security to personal equipment and information.

31. I have been informed that the examiner also rejected claims under the non-statutory doctrine of double patenting. *Id.* at 13.

32. I have been informed that Patent Owner responded to the Non-Final Office Action on December 17, 2012. *See* Ex-1008, '813 Patent File History, 12/17/2012 Amendment/Req. Reconsideration After Non-Final Rejection. Patent Owner amended the specification to properly reference the newly issued '220 patent. *Id.* at 2.

33. I have been informed that Patent Owner canceled application claim 3 "without prejudice or disclaimer." *Id.* at 9. Patent Owner also amended application claims 1-2, 4-5, 9, 12-16, and 20 (issued claims 1, 2-3, 7, 10-14, and 18). *Id.* at 3. Claim 1 (also issued claim 1) was amended as follows:

> 1. (Currently Amended) An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> a biometric sensor configured to receive a biometric input provided by the user;
>
> a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;
>
> a communication interface ~~link~~ configured to communicate with a secure registry; and
>
> a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface ~~link~~, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, ~~the identifying information, and at least one of~~ information derived from at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface ~~link~~ to the secure registry.

34. I have been informed that Patent Owner argued that the amendment traversed Weiss because the prior art does not "teach or suggest the generation of authentication information from the non-predictable value, information derived from at least a portion of the biometric input, and the secret information." *Id.* at 9.

35. I have been informed that the examiner issued a Final Office Action on January 17, 2013. *See* Ex-1009, '813 Patent File History, 01/17/2013 Final Rejection. In addition to reiterating the previous rejections, the examiner rejected all claims under 35 U.S.C. § 112 for indefiniteness, citing a lack of antecedent basis for the phrase "the device" in all claims. *Id.* at 3-7.

36. I have been informed that Patent Owner conducted a telephone interview with the examiner on March 7, 2013, the summary of which follows. *See* Ex-1010, '813 Patent File History, 03/19/2013 Applicant Initiated Interview Summary at 5.

> *Main discussion objective was to provide greater clarification of invention as it relates to claim language. It was pointed out to the Examiner that the pending application contains an additional step that is not found in the prior art Weiss. After further discussion, review, and consideration; the Examiner agreed. To further clarify the invention as a whole, claim 2 will be rolled into claim 1 and subject matter related with claim 2 will be added to the other independent claims.*.

37. I have been informed that Patent Owner responded to the Final Office Action following the phone call on March 7, 2013. *See* Ex-1011, '813 Patent File History, 03/07/2013 Response After Final Action. Patent Owner canceled application claim 2 without prejudice or disclaimer. *Id.* at 8. Patent Owner

amended application claims 1, 4-18, and 20-24 (issued claims 1, 2-16, and 18-22). *Id.* Citing the examiner interview, Patent Owner explained that the parties "agreed that incorporation of dependent claim 2 into independent claim 1 results in allowable subject matter." *Id.*

> 1. (Currently Amended) An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> a biometric sensor configured to receive a biometric input provided by the user;
>
> a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;
>
> a communication interface configured to communicate with a secure registry; ~~and~~
>
> a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with ~~derived from~~ at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and
>
> wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

38. I have been informed that Patent Owner also amended application claims 4-14 (issued claims 2-12), adding the limitation of the "electronic ID" device that corresponds with claim 1. *Id.* A similar amendment was made in

application claim 15 (issued claim 13). Patent Owner amended application claims 16-18 (issued claims 14-16) to include the limitation of the "electronic ID" device that corresponds with the amendments to claims 1 and 15 (issued claims 1 and 13). *Id.* at 5.

39. I have been informed that Patent Owner also amended application claims 22-24 (issued claims 20-22) to include the limitation of the "electronic ID" device that corresponds to the amendments to claims 1 and 20 (issued claims 1 and 18). *Id.* at 5.

40. I have been informed that the examiner issued a Notice of Allowance on March 19, 2013. *See* Ex-1012, '813 Patent File History, 03/19/2013 Notice of Allowance and Fees Due.

41. The '813 patent subsequently issued on November 5, 2013.

C. Rejection of Patent Family Members Under §101

42. I have been informed that after the application that led to the '813 patent was granted, Patent Owner filed four subsequent continuation applications. The applications are U.S. Appl. Nos. 14/071,126, 15/045,408, 15/661,943, and 15/661,955. All four patent applications currently stand rejected, *inter alia*, for failing to claim patentable subject matter under §101. *See e.g.* Exs-1014-1017. The rejected continuation patent applications contain claims that are substantially similar to those in the '813 patent. For example, the chart below provides the

language of a currently-rejected claim of U.S. Patent Application No. 14/071,126 ("'126 application") and claim 1 of the '813 patent:[1]

'126 Patent Application, Claim 21	**'813 Patent, Claim 1**
An electronic ID device configured to encrypt information to enable execution of a secure operation, comprising:	An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
a biometric sensor configured to receive a biometric input provided by a user;	a biometric sensor configured to receive a biometric input provided by the user;
a user interface configured to receive a user input including secret authentication information known to the user and information indicative of a secure operation to be executed;	a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;
a communication interface configured to communicate with a system configured to execute the secure operation;	a communication interface configured to communicate with a secure registry;
a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed such that after the electronic ID device receives at least one of the biometric input and the secret authentication information, the processor is configured to generate a non-predictable value and to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived	a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-

[1] The claims of the other pending patents are similarly continuations of the '813 patent and claim substantially the same subject matter as those in the chart and in the '813 patent. The examiner similarly rejected the claims under § 101, as documented in the § 101 rejections provided for the three applications.

from at least a portion of the secret authentication information to generate encrypted authentication information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation.	predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

43. The patent examiner reasoned that the rejected pending claims of the '126 application are directed toward "automating mental tasks" and the abstract idea of "receiving and processing data," noting specifically that the elements of authenticating an identity and activation of an electronic device for use in transactions do not add "significantly more" to the claims beyond this abstract idea. Ex-1014 at 19. In addition, the examiner found that the incorporation of an implementing device into these claims "does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions." *Id*.

44. On November 29, 2017, Patent Owner conducted a telephonic interview with the examiner to discuss the § 101 rejection of the '126 application.

As explained in the summary of the interview dated December 5, 2017, the examiner was not persuaded by the applicant's position and the claims stand rejected. *Id*. at 5.

V. LEVEL OF ORDINARY SKILL

45. I understand that a person of ordinary skill in the relevant field is a hypothetical person to whom an expert in the relevant field could assign a routine task with reasonable confidence that the task would be successfully carried out. I further understand that the level of skill in the art is evidenced by prior art references.

46. The prior art demonstrates that a person of ordinary skill in the art, at the time the '813 patent was effectively filed, would have a Bachelor's Degree in electrical engineering, computer science, or a related scientific field, and approximately two years of work experience in the computer science field including, for example, operating systems, database management, encryption, security algorithms, and secure transaction systems, though additional education can substitute for less work experience and vice versa.

47. Based on my experience, I have an understanding of the capabilities of a person of ordinary skill in the relevant field. I have supervised and directed many such persons over the course of my career. Further, I had at least those capabilities myself at the time the patent was filed.

VI. GROUNDS FOR STANDING (37 C.F.R. § 42.304(A))

A. The '813 Patent Qualifies As A CBM Patent (37 C.F.R. § 42.301)

48. I have been informed that Section 18(d)(1) of the AIA on its face covers a wide range of finance-related activities, including activities that are financial in nature, incidental to a financial activity or complementary to a financial activity. I have been informed that under Section 18 of the AIA, the Board may institute a CBM review proceeding for any patent that qualifies as a CBM patent. I have been informed that section 18 of the AIA defines a "covered business method" as a claim that both (1) claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service; and (2) is not directed to a technological invention. In my opinion, the '813 patent satisfies both requirements for at least the reasons set forth below.

1. At Least One Claim Of The '813 Patent Is A Method Or Corresponding System Used In The Practice, Administration, Or Management Of A Financial Product Or Service

49. I have been informed that a patent qualifies for CBM review as long as "the subject matter of at least one claim is directed to a covered business method." I have been informed that the definition of "covered business method patent" is not limited to products and services of only the financial industry, or to

patents owned by or directly affecting the activities of financial institutions such as banks and brokerage houses. I have also been informed that the plain text of the statutory definition contained in § 18(d)(1) on its face covers a wide range of finance-related activities. I have been informed that the correct inquiry is not whether the claimed invention ***only*** has application in business contexts, but whether the claimed invention is a method or apparatus for performing data processing or other operations ***used*** in the practice, administration, or management of a financial product or service. I have been informed that the claims should be read in light of the specification when making this determination.

50. All claims of the '813 patent meet these requirements. For example, independent claims 1 and 24 (and those that depend from them) disclose a system and method for providing or denying access to information related to a user stored in a secure database in the context of a "financial transaction." Ex-1001, '813 patent at claims 1 and 24. The specification defines a financial transaction as including "transactions conducted on-line or at a point of sale using credit or debit accounts, banking transactions, purchases or sales of investments and financial instruments or generally the transfer of funds from a first account to a second account." *Id.* at 43:6-12. Similarly, dependent claims 7, 12-14, 17, 20-23, and 25-26 all explicitly recite financial transactions, user account numbers, purchases, and/or selection of products or services. *See id.* at claims 7, 12-14, 17, 20-23, and

25-26. And all independent claims recite a "point of sale" device. *See id.* at claims 1-26.

51. Moreover, the patent specification makes clear that the "accounts" recited in all patent claims can be financial in nature. *See, e.g.*, *id.* at 6:66-7:1 ("In still another aspect, a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction."); 7:47-50 ("authorizing the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated").

2. The '813 Patent Is Not Directed To A "Technological Invention"

52. I have been informed that a patent that otherwise qualifies as a CBM patent is nevertheless excluded from CBM review if it is directed to a "technological invention"—*i.e.*, if "the claimed subject matter as a whole" (1) "recites a technological feature that is novel and unobvious over the prior art" and (2) "solves a technical problem using a technical solution." In my opinion, the claims of the '813 patent do not meet either prong of the technological invention exclusion.

i. The '813 patent claims include only conventional technology components that were well known in the art.

53. I have been informed that the first prong of the test analyzes whether the differences between the claimed invention and the prior art are technological features. I understand that the Federal Circuit has affirmed the USPTO's listed characteristics that, if found, would preclude a finding of a "technological invention": 1) mere "recitation of known technologies"; 2) "reciting the use of known prior art technology"; and 3) "combining prior art structures to achieve the normal, expected, or predictable result of that combination."

54. The only arguably technological elements of the challenged claims are as follows:

'813 Patent Claim	Well-Known Technological Features
Independent Claim 1	Electronic ID device, biometric sensor, user interface, communication interface, processor, POS terminal, secure registry (database)
Dependent Claim 2	*No additional technological features*
Dependent Claim 3	*No additional technological features*
Dependent Claim 4	*No additional technological features*
Dependent Claim 5	Memory
Dependent Claim 6	*No additional technological features*

Dependent Claim 7	*No additional technological features*
Dependent Claim 8	*No additional technological features*
Dependent Claim 9	*No additional technological features*
Dependent Claim 10	*No additional technological features*
Dependent Claim 11	*No additional technological features*
Dependent Claim 12	*No additional technological features*
Dependent Claim 13	*No additional technological features*
Dependent Claim 14	*No additional technological features*
Dependent Claim 15	*No additional technological features*
Independent Claim 16	User interface, communication interface, interface with POS terminal, processor (implied), secure registry (database)
Dependent Claim 17	Memory
Dependent Claim 18	*No additional technological features*
Dependent Claim 19	*No additional technological features*
Dependent Claim 20	*No additional technological features*
Dependent Claim 21	*No additional technological features*
Dependent Claim 22	*No additional technological features*
Dependent Claim 23	*No additional technological features*
Independent Claim 24	Electronic ID device, POS terminal, processor (implied), secure registry (database)

Dependent Claim 25	User interface
Dependent Claim 26	*No additional technological features*

55. Under these guidelines, the '813 patent fails to disclose a "technological feature" because the claimed features—an electronic ID device (comprising a user interface, communication interface, and processor), database implementing an identity verification system and a POS device/terminal—were indisputably well known as of the patent's February 26, 2008 priority date and are implemented in a conventional manner. That is, the processor performs standard data operations such as comparing data, performing calculations, and executing commands, the user interface accepts user input, the communication interface communicates, and the secure registry database stores and controls access to conventional information such as a user's financial or medical records. *See*, *e.g.*, Ex-1001,'813 patent at cl. 16 (limitations reciting standard computer and networking functions "authenticating," "activating," "generating," "receiving," and "communicating").

56. The named inventor did not claim to have invented a new computer, processor, database, or Internet system. Instead, he leveraged known technology to claim methods for verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction. Indeed, the

'813 patent repeatedly touts the generic nature of its components and implementation, emphasizing that the claimed invention is not tied to any particular technology, but can be implemented in "a general-purpose computer system" using "a commercially available microprocessor" running "any commercially available operating system." Furthermore, the USR itself is not a special database; rather, the USR database "may be any kind of database," which can communicate using "any [network] protocol." Ex-1001, '813 patent at 10:1, 10:9-24, 11:4-17.

57. The '813 prosecution history provides further evidence that the '813 claims are not technically distinguishable from the prior art. For example, the amendments made to overcome prior art during prosecution were all non-technical in nature and the claims were ultimately allowed based on a non-technical distinction over the prior art. *See* Ex-1008, '813 Patent File History, 12/17/2012 Amendment/Req. Reconsideration After Non-Final Rejection (amending claim to add conventional access restriction (e.g., biometric or passcode authorization) to use of processor); Ex-1011, '813 Patent File History, 03/07/2013 Response After Final Action (rolling limitation of claim 2 requiring communication with generic POS device into claim 1).

ii. The '813 patent does not solve a technical problem with a technical solution.

58. The '813 patent also fails the second prong of the technological invention test because it does not solve a technical problem with a technical solution. I understand that this prong requires a review of the patent's specification to determine what problem the claimed invention purportedly solves. If the problem is nontechnical, the patent does not meet the technological invention exception. Moreover, I understand that where the specification recognizes that technology known in the art could be used to reach the desired result, the patent does not solve a technical problem with a technical solution.

59. The '813 patent states at the outset that it is directed to a system for "authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges and providing other services in response to such identifications/verifications." Ex-1001, '813 patent at 1:36-46 (describing the "field of invention"). How to control access to information stored in a particular location is a problem as old as society itself. Although humans have more recently employed computers to make identity verification more precise and transactions more secure, the underlying problem of ensuring that people conducting transactions are who they claim to be is inherently non-technical.

60. Moreover, the patent does not provide a novel "technical solution" to this purported problem. Instead, it merely claims using wholly conventional and generic computers to perform common functions like receiving information, comparing received values to stored values, and controlling access to stored information based on the result. *See, e.g.*, Ex-1001, '813 patent at 11:36-45 ("A comparison by the user or the code generator between the provided number and an expected number can validate, to the user (or other entity) or the code generator, that communication is with the database and not an imposter."); *see also id.* at 10:1-23, Fig. 1. This does not constitute a technical solution to the problem identified above. Moreover, as explained above, all amendments made during prosecution were nontechnical in nature. Thus, the claimed subject matter of the '813 patent, taken as a whole, does not solve a technical problem using a technical solution.

VII. PROPOSED CLAIM CONSTRUCTIONS FOR CBM REVIEW (37 C.F.R. § 42.304(b)(3))

61. I understand that for purposes of this covered business method review proceeding, in comparing the claim language to the prior art, I am to construe that claim language as a person of ordinary skill in the art at the time of the alleged invention would do in light of the specification. I also understand that in proceedings before the Board, patent claims are to be given their broadest

reasonable interpretation, consistent with the teachings of the specification and file history.

62. I have reviewed the claim constructions explicitly set forth in the Petition from that perspective and, in my opinion, believe the constructions are consistent with the broadest reasonable interpretation in light of the specification. At this time, I have no opinion as to whether these constructions would be the proper constructions for any district court litigation involving the '813 patent.

A. Biometric Input (All Challenged Claims)

63. I understand that Apple's proposed construction for "biometric input" as used in the '813 patent means "information about a user's physical characteristics, such as fingerprint, voice print, signature, iris or facial scan, DNA analysis, or personal photograph."

64. This construction is consistent with the plain meaning of the term, and is further supported by the specification, which describes biometric information

using substantially identical language.[2] Ex-1001, '813 patent at 4:29-34 ("biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis"); 31:64-66 ("biometric information can be fingerprint information, a voiceprint, DNA codes of the first user"). Consistent with the use of the biometric input in the specification, Webster's Dictionary defines biometric authentication as "[a] method of authentication that requires a biological scan of some sort, such as a retinal scan or voice recognition." Ex-1018, Webster's Dictionary, 65. Similarly, Microsoft Computer Dictionary defines biometrics as

[2] The '813 patent specification includes one passage that describes a "personal identification number (PIN)" as an example of biometric information. Ex-1001, '813 patent at 13:12-15. That passage is inconsistent with other statements in the intrinsic record that describe biometric information as information that relates to a user's physical characteristics and distinct from a PIN. For example, the specification elsewhere distinguishes PIN numbers from biometric information. Ex-1001, '813 patent at 4:29-34 ("The identity of the user possessing the identifying device may be verified at the point of use via any combination of a memorized PIN number or code, biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device").

"the science of measuring and analyzing human biological characteristics. In computer technology, biometrics relates to authentication and security techniques that rely on measurable, individual biological stamps to recognize or verify an individual's identity. For example, fingerprints, handprints, or voice-recognition might be used to enable access to a computer, to a room, or to an electronic commerce account. Ex-1019, Microsoft Computer Dictionary, 50.

B. Secret Information

65. I understand that Apple's proposed construction for "secret information" as used in the '813 patent means "information known and input by an authorized user, such as a PIN, a phrase, a password, or a passcode of the user."

66. This construction is consistent with the specification and claims. For example, the abstract and specification describe secret information as "known to the user," Ex-1001, '813 patent at Abstract, 7:4-7, which may comprise "a PIN, a phrase, a password, etc." *Id.* at 12:25-29, 42:29-36. The secret information is part of the claimed authentication process. *See*, *e.g.*, *id.* at Claim 1 ("the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information"). It is input by a user via the user interface (*id.* at 7:4-7, 51:7-15), and then combined with other pieces of information, such as biometric data, to create encrypted authentication information, which is transmitted to the

secure registry for identity verification. *Id.* at 7:25-30; *see also*, *e.g.*, *id.* at claim 1. In some embodiments, the secret information may include identifying information concerning an account (*id.* at 50:21-22) or a PIN number (*id.* at 50:40-44).

67. That the information is known and input by an authorized user is consistent with the overall purpose of the invention, which is to provide an identification system "that will enable a person to be accurately identified … and/or authenticated without compromising security, to gain access to secure systems and/or areas." *Id.* at 3:57-64 (Summary of the Invention). If the information were known and used by others, then the security of the system would be compromised.

C. Authentication Information

68. I understand that Apple's proposed construction for "authentication information" as used in the '813 patent means "information used by the electronic ID device and/or the secure registry to verify the identity of an individual."

69. This construction is consistent with the plain meaning of the term and the patent specification. The patent uses the terms "verification," "identification," and "authentication" interchangeably. *Id.* at 3:57-64 ("There is thus a need for an identification system that will enable a person to be accurately identified ('identification' sometimes being used hereinafter to mean either identified or verified) and/or authenticated without compromising security, to gain access to

secure systems and/or areas."). According to the specification and claims, authentication information is generated from a combination of a "non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information." *Id.* at 7:13-18.

70. The construction is also consistent with how the term is used in the specification. For example, the patent specification describes how authentication information is used as follows:

> According to one embodiment, the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry.

Id. at 50:14-20. The authentication information is also discussed as transmitted by the POS device: "In a further embodiment, the communication link wirelessly transmits the encrypted authentication information to a point-of-sale (POS) device, and the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry."

D. Point-of-Sale Device

71. I understand that Apple's proposed construction for "point-of-sale device" as used in the '813 patent means "a device located at a point of sale

capable of transmitting and/or receiving information related to a financial transaction."

72. This construction is consistent with the patent specification. The background of the invention refers to "a substantial installed base of interfaces (for example, at points of sale, at automatic teller machines ("ATM"), and the like) that include magnetic card readers," which it states are likely to be replaced by "RF devices that transmit information wirelessly" in the future. *Id.* at 3:18-36. When discussing the claimed invention, the specification later discloses that the electronic ID device "communicat[es] the encrypted authentication information … to a secure registry via a point-of-sale (POS) device to authenticate or not authenticate the device with the secure registry," and that the secure registry ultimately "authoriz[es] the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated" or "deni[es] the POS device from initiation of the financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is not successfully authenticated." *Id.* at 7:35-54; *see also id.* at 45:4-17, 50:23-33, 51:7-26.

73. The POS device also transmits and receives information about the financial transaction in addition to authentication information. *Id.* at 40:52-56

("For example, where the system 100 is employed in conjunction with a check-authorization process, the converter device 102 may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale."); 43:12-15 ("The system includes a user device 352, a point-of sale ("POS") device 354 and a universal secure registry 356 which can communicate with one another wirelessly, and/or over a network 357."); 51:7-26 ("…communicating the encrypted authentication information from the device to a secure registry via a point-of-sale (POS) device … to initiate a financial transaction involving a transfer of funds to or from the account selected by the user…."); 43:54-57 ("In general, the POS device 354 may be any type of POS device as known to those of ordinary skill in the art. In accordance with some embodiments, the POS device 354 includes a display 368, a user interface 370 and a communication link 372."). *see also* Fig. 31 below.

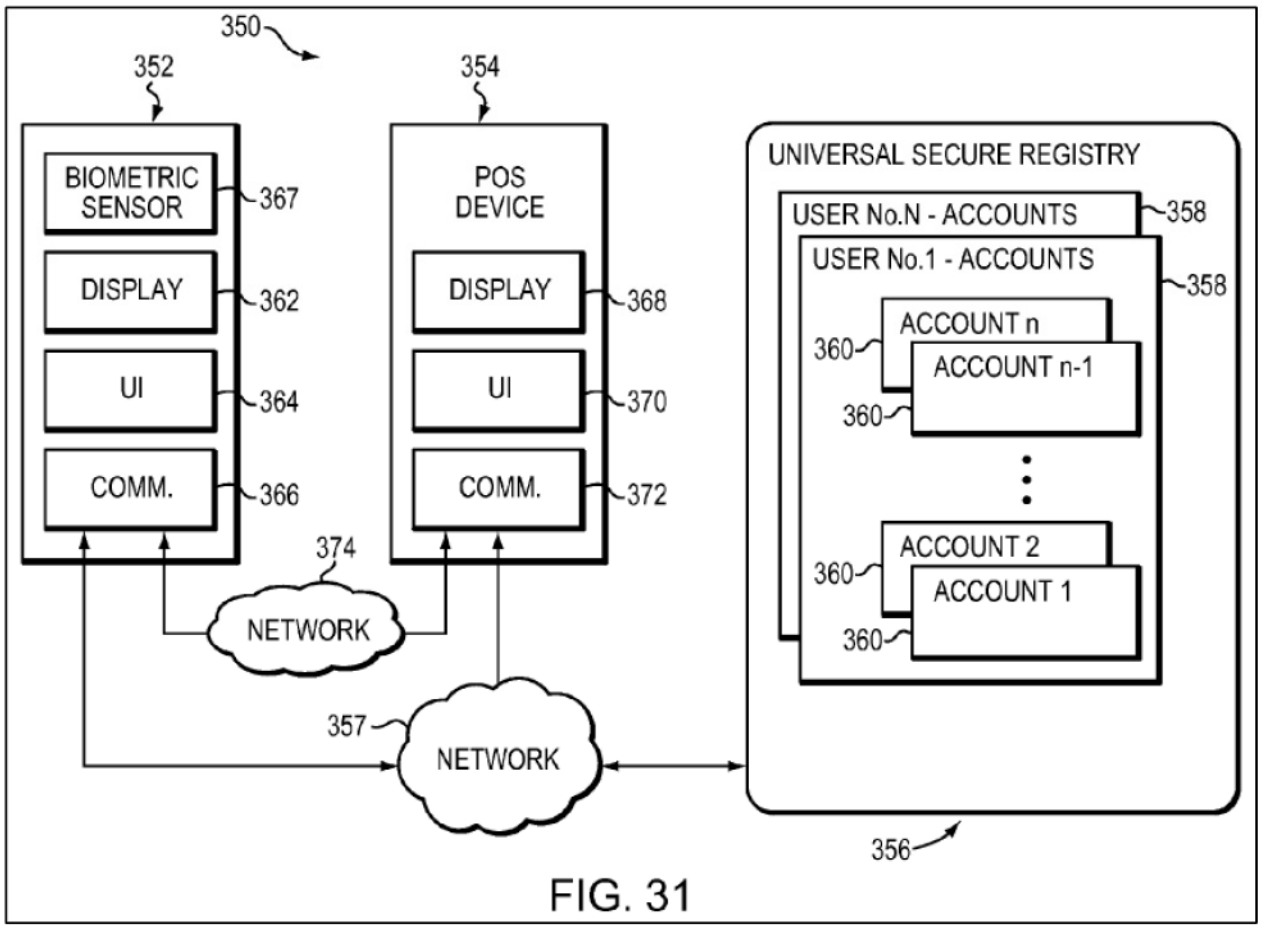

FIG. 31

E. Secure Registry (All Challenged Claims)

74. I understand that Apple's proposed construction for "secure registry" as used in the '813 patent means "a database with access restrictions."

75. The construction is consistent with the '813 claims. For example, claim 1 describes the secure registry as receiving encrypted authentication information, and claim 16 describes the secure registry as used to authenticate an electronic ID device. Claim 20 further describes the secure registry as capable of identifying a user and a selected account using the encrypted authentication information. This construction is further supported by the specification, which

describes the claimed invention as a "Universal Secure Registry." The Universal Secure Registry is described as a "database" throughout the specification. *See also id.* at 4:12-20 (describing the invention as a database); Fig. 1 (depicting the USR as a database filled with entries about persons); 9:61-63 ("In the illustrated embodiment, the database 24 contains a universal secure registry database"); 49:37-41 ("Although the above-described system 350 employs the USR 356 to facilitate the preceding operations, the above approach may be employed with alternative systems that include a secure database with the user's account information.").

VIII. CLAIMS 1-26 OF THE '813 PATENT ARE UNPATENTABLE UNDER 35 U.S.C. § 101 (37 C.F.R. § 42.304(b)(4))

76. I understand that in *Alice Corp. Pty. v. CLS Bank Int'l*, the Supreme Court raised the bar for establishing subject matter eligibility for computer-implemented inventions under 35 U.S.C. § 101, unanimously affirming the judgment of the Federal Circuit invalidating claims directed toward computer-based schemes to manage "settlement risk" in financial transactions. I understand the Court confirmed that, in light of "the ubiquity of computers," limiting a claim covering an abstract concept to a "wholly generic computer implementation" is insufficient to transform the idea into a patent-eligible invention. 134 S. Ct. at 2358.

77. I understand that *Alice* articulates a two-step framework for distinguishing patents that claim ineligible abstract ideas from those that claim eligible applications of those ideas. I understand that in step one, the court must determine whether the claims at issue are directed to a patent-ineligible abstract concept. *Id.* If the claim is directed to an abstract idea, the analysis proceeds to step two. I understand that in step two, the elements of the claim must be searched, both individually and as an "ordered combination," for an "inventive concept"—i.e., an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself. I understand that a patentee cannot circumvent the prohibition on patenting abstract ideas by limiting the idea to "a particular technological environment," or by adding "insignificant postsolution activity," or "well-understood, routine, conventional" features, *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S. Ct. 1289, 1299 (2012). Thus, "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Alice*, 134 S. Ct. at 2358.

A. *Alice* Step 1: The '813 Patent Claims Are Directed to the Abstract Idea Of Verifying an Account Holder's Identity Based On Codes And/Or Information Related to an Account Holder Before Enabling a Transaction

78. The '813 patent fails the first step of *Alice* because the claims are directed to the abstract idea of verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction.

1. Independent Claim 1

79. The claim 1 of the '813 patent, which USR has characterized as "exemplary" of the other patent claims, recites in its preamble:

> An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:

Ex-1001, '813 patent at claim 1. The electronic ID device's processor is configured to perform a two-step authentication process prior to allowing the user access to the selected account, first, locally via biometric or secret information, and

then apparently[3] remotely via encrypted authentication information transmitted to the secure registry.

80. Although claim 1 is limited to a computer system, the underlying problem that the claim purports to solve is age old: verifying the identity of individuals and other entities seeking access to certain privileges. *Id.* at 1:36-46 ("Embodiments of the invention generally relate to systems, methods, and apparatus for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges and providing other services in response to such identifications/verifications."). I understand that limiting this pre-Internet problem to using a computer database cannot confer patent eligibility.

81. The claimed verification method is also directed to an abstract concept for the additional reason that the claim recites nothing more than a mental process. For example, a person in possession of a spreadsheet containing the same

[3] The specification discusses the use of encrypted authentication information to verify a user's identity before authorizing a transaction. ('813 patent at 51:7-26.) '813 claims 1-23, however, stop short of discussing the authentication process that the specification describes as taking place at the USR. Claim 24 includes limitations regarding "authorizing" and "denying" a transaction.

information as the Electronic ID device could perform the same comparison between a received value and an expected value to determine whether to grant a particular user access to an Electronic ID device, generate encrypted authentication information, and send that on to a database. As a result, in my opinion, the identity verification system claimed in claim 1 is drawn to an unpatentable abstract idea.

82. The patent specification also fails to meaningfully limit the breadth of the claimed abstract idea. More specifically, the patent specification does not limit the claims to specific hardware or software, but instead emphasizes the broad range of systems in which the invention can be implemented. *Id.* at 10:1-4 ("The computer system may be a general purpose computer system"); 10:24-26 ("the database may be any kind of database"); 10:58-60 ("It should also be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language"); 11:24-28 ("Communication between the interface centers 27 and the computer system may take place according to any protocol"). Moreover, although the '813 patent places significant emphasis on database security (*see*, *e.g.,* '813 patent at Abstract ("The user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. The processor is configured to generate a non-predictable

value and encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and communicate the authentication information via the communication link to the secure registry."); 1:12-19 (describing the "field of invention" as relating to "**selectively** granting privileges and providing other services in response to such **identifications/verifications**."), it imposes no limits on *how* to implement such security in the database, how to communicate with the secure database, or how to implement these concepts in the Electronic ID device. For example, the specification provides only a generic description of prior art encryption and security protocols used by the claimed invention to protect transmissions to/from the database as well as the information stored in the database. *Id.* at 4:1-5 ("Transactions to and from the database may take place using a public key/private key security system to enable users of the system and the system itself to encrypt transaction information during the transactions. . . ."); 4:21-36 ("Access to the USR system may be by smart card, such as a SecurID™ card, or any other secure access device."); 11:28-35 ("To enhance security, especially where communication takes place over a publicly accessible network such as the Internet, communications facilitating or relating to transmission of data from/to the USR database 24 or the computer system 10 may

be encrypted using an encryption algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption algorithm.").

83. Finally, as explained above, the Patent Office recently found that four continuation applications of the '813 patent, which contain claims covering substantially the same subject matter as those of the '813 patent, were invalid under §101 because they were directed to the abstract idea of "receiving and processing data." *See* Exs-1014-1017. The examiner further found that the elements of authenticating an identity and activation of an electronic device for use in transactions do not add "significantly more" to the claims beyond this abstract idea. *Id.* Rather, taken alone or as an ordered combination, the claims did not "provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment" and "require[] no more than a generic computer to perform generic computer functions."

84. For the foregoing reasons, claim 1 of the '813 patent is directed to the unpatentable abstract idea of verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction.

2. The Remaining Claims

85. The remaining claims of the '813 patent all claim the same abstract idea. All three independent claims (1, 16, 24) commonly claim a system/method of authenticating user identity to grant access to an Electronic ID device. Claim

16 is directed to a method performed by substantially the same system recited in system claims 1 and 24.[4] *See id.* at claims 1, 16, and 24. I understand that it is well established that method claims "in the guise of a device" do "not overcome the Supreme Court's warning to avoid permitting a 'competent draftsman' to endow abstract claims with patent-eligible status." Thus, all three independent claims are directed to the same abstract idea: verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction.

86. The dependent claims of the '813 patent are likewise directed to the same abstract idea because they contain conventional components used in conventional ways or only ancillary post-solution limitations. For example, claim 2 requires a discrete code (which is nothing more than a secret key) to be associated with the electronic ID device. Claim 3 requires the biometric input to be transmitted to the secure registry as a prerequisite to creating authentication

[4] Minor differences between the independent claims exist, but in my opinion, all are merely incidental to the core identity verification function. For example, claims 16 and 24 contain additional limitations relating to the authorization or denial of a financial transaction by a point of sale device that are not present in claims 1 or 16.

information. Claims 4 and 7 require the secret information to include specific information such as identifying information (claim 4) or a PIN number (claim 7). Claims 5-10 cover an embodiment including a memory that stores information relevant to biometric authentication (claim 5), requires biometric authentication prior to any user input (claim 6), requires the secret information to include a PIN (claim 7), limits access to data on the electronic ID device pending authentication (claim 8), encryption of stored data stored data (claim 9), or generate a "seed" value to generate encrypted authentication information (claim 10). Claim 11 requires the use of specific types of biometric information. Claim 12 requires generation of account identifying information that does not include the user's account number. Claims 13-15, 17, 22, 23, 25, and 26 require user interface features such as indicators to be displayed in the user interface for each user account (claims 13 and 17), options for purchase (claims 14, 22, and 25), and the ability to select a product or service (claims 15, 23, and 26). Claim 18 requires authentication prior to activation of the electronic ID device. Claim 19 requires a seed value to be generated from biometric, secret, and/or a serial number. Claim 20 requires encryption that is decipherable by the secure registry. Claim 21 requires generating an account identifier used to create the encrypted authentication information.

87. As noted above, claims 10 and 19 cover an embodiment that requires the generation of a "seed" value as part of the generation of encrypted authorization information. Seed values, which are essentially values input to a pseudo-random number generator, were well known in the art, and have been used in security and encryption application for decades. The '813 patent leaves unspecified how the seed value is generated and/or used. As such, the use of seed values does not alter the abstract nature of the claims.

88. At bottom, the dependent claims do not alter the abstract nature of the independent claims because none of the additional limitations explains or limits the abstract idea of verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction. To the contrary, all narrowing required by these dependent claims—variations on codes and biometric data (claims 2, 4, 7, and 11), conditions on access (claims 3, 6, 8, and18), storage of data (claims 5, 9), different types of encryption (claims 10, 19, 20, and 21), variations on account identifying information (claim 12), and user interface features (claims 13-15, 17, 22, 23, 25, and 26)—is incidental to the core abstract concept and therefore insufficient to lend patentability.

89. All challenged claims cover the use of "biometric information" as part of the verification process. "Biometric information" is defined in the patent to encompass nearly any physical characteristic of a user, from highly specific

information such as fingerprints and DNA to more rudimentary forms of authentication like a picture of the user. Ex-1001, '813 patent at 42:29-36, 12:19-31. But whether authentication is performed using encrypted authentication information or a user's physical characteristics (or both) likewise does not change the abstract nature of the claimed invention. Authentication based on physical characteristics remains an abstract longstanding practice.

90. All challenged claims also require the user to select between one of multiple accounts, but that does not affect the abstract nature of the claim. Rather, "account selection" is merely an abstract process no different from selecting a credit card in one's wallet. *Id.* at 45:9-12 (describing the system as an "electronic wallet"); *see also id.* at 44:39-46. Moreover, the patent makes no effort to explain how a particular account is selected, except to generically describe a user interface for doing so.

91. Finally, the challenged claims are no less abstract because they require multiple pieces of information (secret information, biometric information, and a non-predictable value) to be combined to create "encrypted authentication information." I understand that the Federal Circuit has held that generating a data set by taking existing information and organizing this information into a new form recites an ineligible abstract idea. Moreover, the '813 patent does not claim a novel way to generate encrypted authentication information from biometric

information, secret information, and/or a non-predictable value. Instead, the patent leaves completely unspecified the methods for combining such information. *Id.* at 12:45-63; 46:46-67. In addition, the abstract process of verifying a person's identity routinely requires consideration of multiple factors. One simple example is the combination of a person's physical characteristics *and* his or her knowledge of a password before allowing entry to a restricted area. Thus, even when multiple pieces of information are used together to perform verification, the underlying "fundamental" process is still abstract.

92. For at least the reasons given above, in my opinion, the claims of the '813 patent fail the first step of the *Alice* test.

B. *Alice* Step 2: The Remaining Limitations Of The '813 Patent Claims Add Nothing Inventive To The Abstract Idea Of Verifying An Account Holder's Identity Based on Codes And/Or Information Related To The Account Holder Before Enabling A Transaction

93. The '813 patent also fails the second step of the *Alice* test. The patent takes the abstract idea of verifying an account holder's identity based on codes and/or information related to the account holder before enabling a transaction and adds nothing but the instruction to automate the process using conventional, generic computer hardware. As described above, all claims of the '813 patent are directed to systems and methods implemented using generic hardware and database software that was well known at the time of filing. Indeed, the written

description emphasizes that the claimed invention can be implemented in "a general-purpose computer system" and is "not limited to a particular computer platform, particular processor, or … high level programming language." *Id.* at 10:1, 10:24-26, 10:58-60, 11:24-28, Fig. 1. This generic database is protected using known methods, and may be accessed by providing information sufficient to verify the user's identity. *Id.* at 4:37-40 ("According to one embodiment of the invention, a method of controlling access to a plurality of secure computer networks using a secure registry system located remotely from the to [sic] secure computer networks is disclosed."). The database with which it interacts can be "any kind of database," and it can run on any operating system employing a general purpose "wide area network … such as the internet." *Id.* at 10:24; 9:51-54. Moreover, the database can be used in multiple contexts, including financial, medical and others. *Id.* at 11:66-12:9. These general-purpose elements are neither inventive nor do they add "significantly more" than the abstract idea of verification, as I understand *Alice* requires.[5]

[5] In my view, the claims would similarly not pass muster under the "machine or transformation" test. First, as described throughout this petition, the claims do not cover any particular machine, but instead are drafted broadly to cover any generic computing device employing a number of general-purpose computer

94. As explained below, the limitations of each of the challenged claims, considered separately or as an ordered combination, do not meaningfully limit the scope of the underlying abstract idea to which the claims are directed.

1. Independent Claim 1

95. All elements of exemplary claim 1 were well known and conventional by the priority date of the '813 patent.

96. As an initial matter, the patent itself admits that the use of biometric information, secret information, non-predictable values and encryption were known in the prior art. *Id.* at 2:59-63 ("Recently, such devices have seen technological advances that increase their capabilities and improve their security. For example, such devices may now include embedded processors, integral biometric sensors that sense one or more biometric feature…"); 3:40-43 ("The bridge device includes a slot for receiving the smart card, a key pad whereby the user may enter information (e.g., a PIN number), and a credit card sized extension member."); 4:7-11 ("For example, in one embodiment, a smart card such as the

---

components. And second, the claims do not transform any article from one state to another, but instead merely manipulate data, which I understand the Federal Circuit has found does not constitute "transformation" of an article from one state to another.

Secure ID™ card from RSI Security, Inc. may be provided with the user's private key and the USR system's public key to enable the card to encrypt messages being sent to the USR system and to decrypt messages from the USR system 10."). Accordingly, the encrypted authentication information itself cannot supply an inventive concept at *Alice* step 2. Likewise, none of the individual claim elements that implement use of that encrypted authentication information to control access to the user's account is a technological innovation, as described in the previous section and below.

97. The specification also makes clear that the other components recited by claim 1 are conventional. The biometric sensor recited in the first limitation is a generic device "configured to receive a biometric input provided by the user" such as "fingerprint, voice print, signature, iris or facial scan, or DNA analysis." Ex-1001, '813 patent at 7:1-3, 4:32-33, 26:52-57, 5:30-34. The user interface is similarly generic, as the specification describes that it is merely "configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from a plurality of accounts." *Id.* at 7:4-7; *see also id.* at 27:25-29, 50:3-9. The communication interface is also described generically as "any of a receiver and a transmitter suitable for wireless communication such as via RF and/or optical signals." *Id.* at 43:21-33, 9:51-54, 50:9-11. And the point of sale terminal with which the system

can interact is also generic. *Id.* at 50:23-28 ("the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry. Further, the POS device can include a magnetic stripe reader"); 51:7-26.

98. The claimed processor is also a generic piece of computer hardware. *Id.* at 10:58-60 ("It should also be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language"). The claimed functions -- "receiv[ing]" biometric input, "activat[ing]" the electronic ID device, "generat[ing]" a nonpredictable value and encrypted authentication information by combining biometric, secret, and other information, and "communicat[ing]" with the secure registry -- are all rudimentary computer functions. None of these functions provides the "inventive step" required at *Alice* step 2.

99. These claim limitations fail to meaningfully limit the breadth of the underlying abstract idea because they do not identify ***how*** to verify an account holder's identity. In my opinion, automation of these overbroad abstract limitations through computer software cannot constitute an inventive concept.

100. Even when the elements of claim 1 are considered as a system designed to implement an ordered combination, they do not recite meaningfully more than the underlying abstract idea—i.e., verifying an account holder's identity based on codes and/or information related to the account holder before enabling a

transaction—because they again only add conventional components implementing routine steps to the abstract idea. Even when put together, the elements only claim a rudimentary identity verification system that is no different in any substantial way from those that already existed in the prior art. In sum, it is my opinion that these claim limitations amount to nothing more than a conventional computer performing rudimentary computer functions as part of verifying a user's identity in a transaction.

101. Finally, as explained above, the patent office recently found that four continuation applications of the '813 patent, which contain claims covering substantially the same subject matter as those of the '813 patent, were invalid under §101 because they were directed to the abstract idea of "receiving and processing data." *See* Exs-1014-1017. The examiner further found that the elements of authenticating an identity and activation of an electronic device for use in transactions do not add "significantly more" to the claims beyond this abstract idea. *Id.* Rather, taken alone or as an ordered combination, the claims did not "provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment" and "require[] no more than a generic computer to perform generic computer functions.

102. For the reasons given above, the limitations of claim 1 do not meaningfully limit the abstract idea to which the claim is directed. Therefore,

under the standard set forth in *Alice*, claim 1 of the '813 patent claims patent ineligible subject matter.

2. Independent Claims 16 and 24

103. Claims 16 and 24 cover methods of performing authentication via interactions with a secure registry and a POS device. The claimed method steps are substantially identical to the capabilities claimed in system claim 1. There is no meaningful distinction between these independent claims under § 101. Thus, the limitations of claims 16 and 24 necessarily fail to confer patent eligibility for the same reasons that the limitations of claim 1 do.

3. Dependent Claims

104. The dependent claims of the '813 patent also do not contain an inventive concept. As discussed above, these claims contain only post-solution limitations and additional method steps that were conventional and well known in the art.

105. None of the dependent claims recites inventive methods for using conventional hardware, and the only additional hardware recited is conventional memory, which has been in use for decades. Instead, these claims contain only post-solution limitations to and variations on the claimed method and system. *See*, *e.g.*, Ex-1001, '813 patent at claims 2, 4, 7, and 11 (claiming variations on codes and biometric data), claims 3, 6, 8, and 18 (claiming different conditions for access

to the secure registry), claims 5 and 9 (claiming basic data storage), claims 10, 19, 20, and 21 (claiming varying methods for generating encrypted authentication information), claim 12 (claiming variations on account identifying information), claims 13-15, 17, 22, 23, 25, and 26 (claiming well-known user interface features).

106. I understand that it is well established that limiting an abstract idea to one field of use or adding token postsolution component does not make the concept patentable, and the Federal Circuit has applied this rule in numerous contexts.

IX. AVAILABILITY FOR CROSS-EXAMINATION

107. 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.

X. RIGHT TO SUPPLEMENT

108. I reserve the right to supplement my opinions in the future to respond to any arguments that the Patent Owner raises and to take into account new information as it becomes available to me.

XI. JURAT

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

Dated: April 18, 2018

Dr. Victor Shoup

APPENDIX A

Victor Shoup
Curriculum Vitae December 14, 2017

Department of Computer Science
Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012
Tel: (646) 403-7853; email: victor@shoup.net
URL: http://www.shoup.net

Employment History

Visiting Reseach Scientist, Cryptography Research Group, IBM T. J. Watson Research Lab, Yorktown Heights, New York, April 2012–present.

Professor, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Jan. 2007–present.

Associate Professor, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Sept. 2002–Jan. 2007.

Research Scientist, Network Security Group, IBM Zurich Research Lab, Feb. 1997–Aug. 2002.

Research Scientist, Security Research Group, Bellcore, Morristown, N. J., June 1995–Jan. 1997.

Alexander von Humboldt research fellow, Universität des Saarlandes, Germany, Sept. 1993–June 1995.

Postdoctoral fellow, Univ. of Toronto, Computer Science Department, Sept. 1990–Aug. 1993.

Postdoctoral fellow, AT&T Bell Laboratories, Murray Hill, N. J., Sept. 1989–Sept. 1990.

Education

Ph. D., Computer Science, Univ. of Wisconsin–Madison, 1989; *advisor:* Eric Bach; *thesis title:* Removing randomness from computational number theory; *areas of study:* programming languages, compilers, operating systems, theory of computing, algebra.

M. S., Computer Science, Univ. of Wisconsin–Madison, 1985.

B. S., Mathematics, Computer Science, Univ. of Wisconsin–Eau Claire, 1983.

Awards and Honors

1. 2016: *IACR Fellow* — "For fundamental contributions to public-key cryptography and cryptographic security proofs, and for educational leadership." (`http://www.iacr.org/fellows/2016/`)
2. 2015: *Richard D. Jenks Memorial Prize for Excellence in Software Engineering Applied to Computer Algebra* — "For NTL: A library for doing number theory." (`http://www.sigsam.org/awards/jenks/awardees/2015/`)
3. 2011: *AsiaCrypt best paper award*, and *IBM Pat Goldberg best paper award* — A Framework for Practical Universally Composable Zero-Knowledge Protocols, with Jan Camenisch and Stephan Krenn.

Invited Lectures

1. *Coxeter Lecture Series*, The Fields Institute for Research in Mathematical Sciences, Toronto, Canada, October 2015.
2. *Historical Papers in Cryptography Seminar Series*, Summer 2015 program on Cryptography, Simons Institute, Berkeley, California, August 2015. (`http://simons.berkeley.edu/crypto2015/historical-papers-seminar-series`).
3. The Sixth International Conference on Provable Security, Chengdu, China, September 2012.
4. 5th Workshop on Hot Topics in Privacy Enhancing Technologies, Vigo, Spain, July 2012.
5. Applied Cryptography and Network Security, New York, June 2005.
6. Crypto 2004, Santa Barbara, August 2004.
7. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, August 2003.
8. RSA Conference 2002, Cryptographer's Track, February 2002.
9. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, September 2001.
10. International Symposium on Symbolic and Algebraic Computation, London, Canada, July 2001.
11. LMS Durham Symposium on Computational Number Theory, Durham, England, August 2000.
12. Conference on The Mathematics of Public-Key Cryptography, Toronto, Canada, June 1999.

13. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, November 1997.

14. Fourth Annual Conference on Finite Fields and Applications, Waterloo, Ontario, August 1997.

15. IMACS Symposium on Symbolic Computation, Lille, France, June 1993.

16. Workshop on Number Theory and Algorithms, MSRI, Berkeley, CA, March 1990.

17. Summer Meeting of the AMS—Special Session on Cryptography and Number Theory, Boulder, CO, August 1989.

Books (author)

1. *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 517 pages, June 2005. Revised second edition, 2008. The electronic version of the book is (and will remain) freely available at `http://www.shoup.net/ntb`.

Books (editor)

1. *Advances in Cryptology – CRYPTO 2005 (LNCS 3621)*, Springer, 568 pages, August 2005.

Patents

1. Method for reducing a value modulo a shared secret, with J. Algesheimer, J. Camenisch. US Patent Number 7194089, March 20, 2007.

2. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections when a client requests a server to propose a message encoding scheme, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 7039946, May 2, 2006.

3. Agreement and atomic broadcast in asynchronous networks, with C. Cachin, K. Kursawe, F. Petzold. US Patent Number 6931431, August 16, 2005.

4. Method of achieving multiple processor agreement in potentially asynchronous networks, with C. Cachin, K. Kursawe. US Patent Number 6957332, Oct 18, 2005.

5. Piggy-backed key exchange protocol for providing secure low-overhead browser connections from a client to a server using a trusted third party, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6775772, August 10, 2004.

6. Method of achieving optimistic multiple processor agreement in potentially asynchronous networks, with K. Kursawe. US Patent Number 6754845, June 22, 2004.

7. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections to a server with which a client shares a message encoding scheme, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6751731, June 15, 2004.

8. Practical non-malleable public-key cryptosystem, with R. Cramer. US Patent Number 6697488, February 24, 2004.

9. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections when a server will not use a message encoding scheme proposed by a client, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6694431, February 17, 2004.

10. Session key distribution using smart cards, with A. Rubin. US Patent Number 5809140, September 15, 1998.

Standards

1. Editor, ISO/IEC Standard on Encryption Algorithms (18033, Part 2: Asymmetric Encryption).

Software

1. Author and maintainer of *NTL*, a free, high-performance, *C++* library for number theoretic computations. *NTL* consists of approximately 140,000 lines of source code, and has been used and cited in numerous research articles, and in a number of university courses around the world (the software has averaged well over 500 downloads a month for many years, and a quick Google Scholar search reveals several hundred research citations). For more information, visit `http://www.shoup.net/ntl`.

2. Co-author of *HElib*, a library that implements the Brakerski-Gentry-Vaikuntanathan homomorphic encryption scheme. For more information, visit `https://github.com/shaih/HElib`.

Other Professional Activities

1. Program Chair, Crypto 2005.

2. Program committee member:

   - Crypto 2000, 2003,
   - RSA 2001,
   - Eurocrypt 1999,
   - International Symposium on Symbolic and Algebraic Computation (ISSAC) 1999,
   - Foundations of Computer Science (FOCS) 1994.

Research Articles

These are my research articles that have appeared in journals and/or refereed conferences. They are all available on-line at `http://www.shoup.net/papers`. Authors on multi-author papers are in alphabetical order, except for papers [38] and [44], where all authors are in the order indicated.

1. Implementing BP-Obfuscation Using Graph-Induced Encoding, with Shai Halevi, Tzipora Halevi, and Noah Stephens-Davidowitz, *ACM CCS 2017.*

2. Bootstrapping for HElib, with Shai Halevi, *Eurocrypt 2015.*

3. Algorithms in HElib, with Shai Halevi, *Eurocrypt 2014.*

4. Practical and employable protocols for UC-Secure circuit evaluation over $\mathbf{Z}_n$, with J. Camenisch and R. Enderlein. *ESORICS 2013.*

5. GNUC: A New Universal Composability Framework, with D. Hofheinz. *J. Cryptology*, 2013.

6. Practical chosen ciphertext secure encryption from factoring, with D. Hofheinz and E. Kilz. *J. Cryptology 26(1):102–118*, 2012.

7. A Framework for Practical Universally Composable Zero-Knowledge Protocols, with J. Camensisch and S. Krenn. *Asiacrypt 2011.*

8. Anonymous Credentials on Java Card, with P. Bichsel, J. Camenisch, and T. Gross. *21st Fraunhofer SIT-Smartcard Workshop*, 2011.

9. Credential authenticated identification and key exchange, with J. Camenisch, N. Casati, and T. Gross. *CRYPTO 2010.*

10. Simple and efficient public-key encryption from computational Diffie-Hellman in the standard model, with K. Haralambiev, T. Jager, and E. Kiltz. *PKC 2010.*

11. Anonymous credentials on a standard Java Card, with P. Bichsel, J. Camenisch, and T. Gross. *ACM CCS 2009.*

12. A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack, with Y. Desmedt, R. Gennaro, and K. Kurosawa. *J. Cryptology 23(1):91-120*, 2010

13. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks, with J. Camenisch and N. Chandran. *Eurocrypt 2009.*

14. Efficient constructions of composable commitments and zero-knowledge proofs, with Y. Dodis and S. Walfish. *CRYPTO 2008.*

15. The Twin Diffie-Hellman problem and applications, with D. Cash and E. Kiltz. *Eurocrypt 2008.*

16. Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation, with M. Bellare and T. Kohno. In *Proc. 13th ACM Conf. on Computer and Communications Security*, 2006.

17. Optimistic asynchronous atomic broadcast, with K. Kursawe, in *Proc. ICALP 2005.*

18. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM, with M. Abe, R. Gennaro, K. Kurosawa, in *Proc. Eurocrypt 2005.*

19. Anonymous identification in *ad hoc* groups, with Y. Dodis, A. Nicolosi, and A. Kiayias, in *Proc. Eurocrypt 2004.*

20. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, with R. Cramer, *SIAM Journal on Computing* 33:167–226, 2003.

21. Practical verifiable encryption of and decryption of discrete logarithms, with J. Camenisch, in *Proc. Crypto 2003.*

22. A secure signature scheme from bilinear maps, with D. Boneh and I. Mironov, in *Proc. RSA CT-2003.*

23. Efficient computation modulo a shared secret with application to the generation of shared safe-prime products, with J. Algesheimer and J. Camenisch, in *Proc. Crypto 2002.*

24. Universal hash proofs and a paradigm for chosen ciphertext secure public key encryption, with R. Cramer, in *Proc. Eurocrypt 2002.*

25. OAEP reconsidered, *Journal of Cryptology* 15(4):223–249, 2002. Extended abstract in *Proc. Crypto 2001.*

26. Secure and efficient asynchronous broadcast protocols, with C. Cachin, K. Kursawe, and F. Petzold, in *Proc. Crypto 2001.*

27. Factorization in $Z[x]$: the searching phase, with J. Abbott and P. Zimmermann, in *Proc. 2000 International Symposium on Symbolic and Algebraic Computation.*

28. Random oracles in Constantinople: practical asynchronous Byzantine agreement using cryptography, with C. Cachin and K. Kursawe, in *Proc. 2000 Principles of Distributed Computing.* To appear, *Journal of Cryptology.*

29. Algorithms for exponentiation in finite fields, with S. Gao, J. von zur Gathen, and D. Panario, *Journal of Symbolic Computation* 29:879–889, 2000.

30. A composition theorem for universal one-way hash functions, in *Proc. Eurocrypt 2000.*

31. Using hash functions as a hedge against chosen ciphertext attack, in *Proc. Eurocrypt 2000.*

32. Practical threshold signatures, in *Proc. Eurocrypt 2000.*

33. Signature schemes based on the Strong RSA Assumption, with R. Cramer, *ACM Transactions on Information and System Security (ACM TISSEC)* 3(3):161–185, 2000. Extended abstract in *Proc. 6th ACM Conf. on Computer and Communications Security*, 1999.

34. Efficient computation of minimal polynomials in algebraic extension of finite fields, in *Proc. 1999 International Symposium on Symbolic and Algebraic Computation.*

35. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, with R. Cramer, in *Proc. Crypto '98.*

36. Optimistic fair exchange of digital signatures, with N. Asokan and M. Waidner, *IEEE Journal on Selected Areas in Communications* 18(4):593–610, 2000. Extended abstract in *Proc. Eurocrypt '98.*

37. Asynchronous protocols for optimistic fair exchange, with N. Asokan and M. Waidner, in *Proc. of the IEEE Symp. on Research in Security and Privacy*, 1998.

38. Securing threshold cryptosystems against chosen ciphertext attack, by V. Shoup and R. Gennaro, *Journal of Cryptology* 15(2):75–96, 2002. Extended abstract in *Proc. Eurocrypt '98.*

39. Fast polynomial factorization over high algebraic extensions of finite fields, with E. Kaltofen, in *Proc. 1997 International Symposium on Symbolic and Algebraic Computation.*

40. Private information storage, with R. Ostrovsky, in *Proc. 29th ACM Symposium on Theory of Computation*, 1997.

41. Lower bounds for discrete logarithms and related problems, in *Proc. Eurocrypt '97.*

42. On fast and provably secure message authentication based on universal hashing, in *Proc. Crypto '96.*

43. On the security of a practical identification scheme, *Journal of Cryptology* 12(4):247–260, 1999. Extended abstract in *Proc. Eurocrypt '96.*

44. Session-key distribution using smart cards, by V. Shoup and A. Rubin, in *Proc. Eurocrypt '96.*

45. Subquadratic-time factorization of polynomials over finite fields, with E. Kaltofen, *Mathematics of Computation* 67(223):1179–1197, 1998. Extended abstract in *Proc. 27th ACM Symposium on Theory of Computation,* 1995.

46. A new polynomial factorization algorithm and its implementation, *Journal of Symbolic Computation* 20:363-397, 1995.

47. Counting the number of points on elliptic curves of characteristic greater than three, with F. Lehmann, M. Mauerer, and V. Mueller, in *Proc. First Algorithmic Number Theory Symposium*, 1994.

48. Primality testing with fewer random bits, with R. Peralta, *Computational Complexity* 3:355–367, 1993.

49. Factoring polynomials over finite fields: asymptotic complexity vs. reality, in *Proc. IMACS Symposium*, Lille, France, 1993.

50. Fast construction of irreducible polynomials over finite fields, *Journal of Symbolic Computation* 17:371–391, 1994. Extended abstract in *Proc. 4th Annual Symposium on Discrete Algorithms*, 1993.

51. Computing Frobenius maps and factoring polynomials, with J. von zur Gathen, *Computational Complexity* 2:187–224, 1992. Extended abstract in *Proc. 24th ACM Symposium on Theory of Computing*, 1992.

52. Smoothness and factoring polynomials over finite fields, *Information Processing Letters* 39:39–42, 1991.

53. A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic, in *Proc. 1991 International Symposium on Symbolic and Algebraic Computation.*

54. Lower bounds for polynomial evaluation and interpolation problems, with R. Smolensky, *Computational Complexity* 6:301–311, 1997. Extended abstract in *Proc. 31st Annual Symposium on Foundations of Computer Science*, 1991.

55. Constructing nonresidues in finite fields and the Extended Riemann Hypothesis, with J. Buchmann, *Mathematics of Computation* 65(215):1311–1326, 1996. Extended abstract in *Proc. 23rd ACM Symposium on Theory of Computation*, 1991.

56. On the deterministic complexity of factoring polynomials over finite fields, *Information Processing Letters* 33:261–267, 1990.

57. Hiding instances in zero-knowledge proof systems, with D. Beaver and J. Feigenbaum, in *Proc. Crypto '90.*

58. Factoring polynomials using fewer random bits, with E. Bach, *Journal of Symbolic Computation* 9:229–239, 1990.

59. Searching for primitive roots in finite fields, *Mathematics of Computation* 58:369-380, 1992. Extended abstract in *Proc. 22nd ACM Symposium on Theory of Computation*, 1990.

60. New algorithms for finding irreducible polynomials over finite fields, *Mathematics of Computation* 54:435–447, 1990. Extended abstract in *Proc. 29th Annual Symposium on Foundations of Computer Science*, 1988.

APPENDIX B

Exhibit Number	Description
1001	U.S. Patent No. 8,577,813
1003	*Universal Secure Registry, LLC v. Apple Inc. et al.*, No. 17-585-VAC-MPT (D. Del.), ECF No. 1, Complaint
1004	U.S. Patent No. 8,001,055
1005	'813 Patent File History, 09/20/2011 Documents Submitted With 371 Applications
1006	'813 Patent File History, 09/26/2011 Petition Automatically Granted by EFS
1007	'813 Patent File History, 08/15/2012 Non-Final Rejection
1008	'813 Patent File History, 12/17/2012 Response to Office Action
1009	'813 Patent File History, 01/17/2013 Final Rejection
1010	'813 Patent File History, 03/19/2013 Applicant Initiated Interview Summary
1011	'813 Patent File History, 03/07/2013 Response After Final Action
1012	'813 Patent File History, 03/19/2013 Notice of Allowance and Fees Due
1013	Plaintiff's Answering Brief in Opposition to Defendants' Motion to Dismiss, Case No. 17-cv-00585 (D. Del.)
1014	Excerpts from File History of U.S. Patent Appl. No. 14/071,126
1015	Excerpts from File History of U.S. Patent Appl. No. 15/045,408
1016	Excerpts from File History of U.S. Patent Appl. No. 15/661,955
1017	Excerpts from File History of U.S. Patent Appl. No. 15/661,943
1018	Webster's New World Dictionary of Computer Terms Eighth Edition Copyright 2000 (Date Stamped by Library of Congress March 28, 2000)

1019	Microsoft Computer Dictionary Fourth Edition Copyright 1999
1020	U.S. Provisional Application No. 60/775,046
1021	U.S. Provisional Application No. 60/812,279
1022	U.S. Provisional Application No. 60/859,235
1023	U.S. Provisional Application No. 61/031,529