US007205882B2

(12) **United States Patent**
Libin

(10) **Patent No.: US 7,205,882 B2**
(45) **Date of Patent: Apr. 17, 2007**

(54) **ACTUATING A SECURITY SYSTEM USING A WIRELESS DEVICE**

(75) Inventor: **Phil Libin**, Cambridge, MA (US)

(73) Assignee: **CoreStreet, Ltd.**, Cambridge, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 272 days.

(21) Appl. No.: **10/985,348**

(22) Filed: **Nov. 10, 2004**

(65) **Prior Publication Data**

US 2006/0097843 A1 May 11, 2006

(51) **Int. Cl.**

G05B 19/00	(2006.01)
G06F 7/00	(2006.01)
G08B 29/00	(2006.01)
H04B 1/00	(2006.01)
H04Q 1/00	(2006.01)

(52) **U.S. Cl.** **340/5.28**; 340/5.22; 340/5.6

(58) **Field of Classification Search** 340/5.22–5.28, 340/5.6–5.64, 5.7–5.74, 5.8–5.86; 455/420, 455/41.2, 557; 235/380; 70/63, 168
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,200,770	A	4/1980	Hellman et al.
4,218,582	A	8/1980	Hellman et al.
4,309,569	A	1/1982	Merkle
4,326,098	A	4/1982	Bouricius et al.
4,825,052	A	4/1989	Chemin et al.
4,879,747	A	11/1989	Leighton et al.
4,881,264	A	11/1989	Merkle
4,888,801	A	12/1989	Foster et al.
4,926,480	A	5/1990	Chaum
4,943,707	A	7/1990	Boggan
4,944,009	A	7/1990	Micali et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 618 550 A1	3/1994

(Continued)

OTHER PUBLICATIONS

**Facsimile message from Chini Krishnan of Integris Security, Inc. to Professor Silvio Micali, dated Feb. 17, 1997, 7 pages including cover sheet, submitted in attached sealed envelope as Proprietary Material Not Open to Public. To be opened only by Examiner or Other Authorized U.S. Patent and Trademark Office Employee.

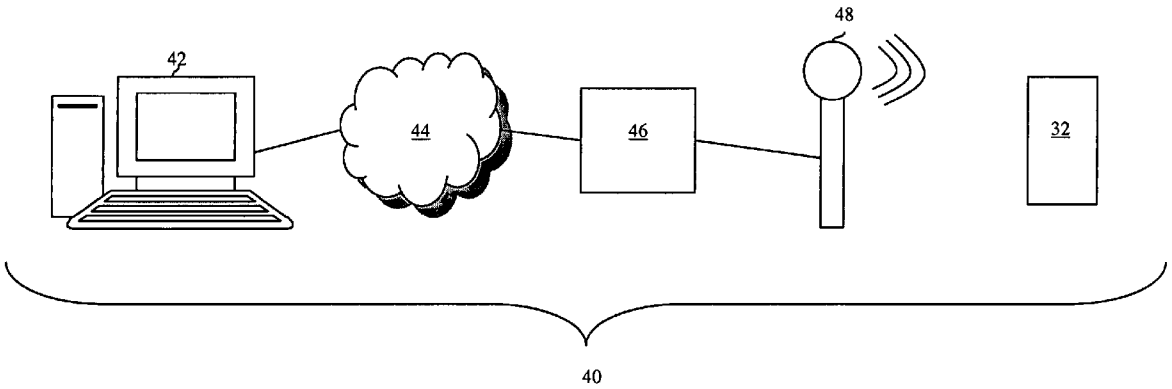
(Continued)

Primary Examiner—Wendy R. Garber
Assistant Examiner—Nam Nguyen
(74) *Attorney, Agent, or Firm*—Muirhead & Saturnelli, LLC

(57) **ABSTRACT**

Actuating a security system includes providing a first set of access codes to a wireless device and causing the wireless device to transmit the first set of access codes to a first controller that actuates the security system. The first set of access codes provided to the wireless device may expire. Actuating a security system may also include providing expiration dates for each of the first set of access codes provided to the wireless device. Actuating a security system may also include examining each of the expiration dates and, in response to a particular expiration date being prior to a current date, erasing from the wireless device a particular one of the first set of access codes that corresponds to the particular expiration date.

84 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,995,081	A		2/1991	Leighton et al.
5,003,597	A		3/1991	Merkle
5,005,200	A		4/1991	Fischer
5,016,274	A		5/1991	Micali et al.
5,097,504	A		3/1992	Camion et al.
5,136,646	A		8/1992	Haber et al.
5,136,647	A		8/1992	Haber et al.
5,157,726	A		10/1992	Merkle et al.
5,214,702	A		5/1993	Fischer
5,231,666	A		7/1993	Matyas
5,245,652	A	*	9/1993	Larson et al. 379/102.06
5,261,002	A		11/1993	Perlman et al.
5,276,737	A		1/1994	Micali
5,299,263	A		3/1994	Beller et al.
5,307,411	A		4/1994	Anvret et al.
5,315,657	A		5/1994	Abadi et al.
5,315,658	A		5/1994	Micali
5,340,969	A		8/1994	Cox
5,351,302	A		9/1994	Leighton et al.
5,371,794	A		12/1994	Diffie et al.
5,382,778	A	*	1/1995	Takahira et al. 235/380
5,396,624	A		3/1995	Campbell, Jr.
RE34,954	E		5/1995	Haber et al.
5,420,927	A		5/1995	Micali
5,432,852	A		7/1995	Leighton et al.
5,434,919	A		7/1995	Chaum
5,450,493	A		9/1995	Maher
5,497,422	A		3/1996	Tysen et al.
5,499,296	A		3/1996	Micali
5,519,778	A		5/1996	Leighton et al.
5,537,475	A		7/1996	Micali
5,544,322	A		8/1996	Cheng et al.
5,551,027	A		8/1996	Choy et al.
5,553,145	A		9/1996	Micali
5,604,804	A		2/1997	Micali
5,606,617	A		2/1997	Brands et al.
5,610,982	A		3/1997	Micali
5,615,268	A		3/1997	Bisbee et al.
5,615,269	A		3/1997	Micali
5,629,982	A		5/1997	Micali
5,638,447	A		6/1997	Micali
5,659,616	A		8/1997	Sudia
5,659,617	A		8/1997	Fischer
5,666,414	A		9/1997	Micali
5,666,415	A		9/1997	Kaufman
5,666,416	A		9/1997	Micali
5,666,420	A		9/1997	Micali
5,677,955	A		10/1997	Doggett et al.
5,687,235	A		11/1997	Perlman et al.
5,699,431	A		12/1997	Van Oorschot et al.
5,717,757	A		2/1998	Micali
5,717,758	A		2/1998	Micali
5,717,759	A		2/1998	Micali
5,742,035	A		4/1998	Kohut
RE35,808	E		5/1998	Micali
5,748,738	A		5/1998	Bisbee et al.
5,768,379	A		6/1998	Girault et al.
5,774,552	A		6/1998	Grimmer
5,790,665	A		8/1998	Micali
5,790,790	A		8/1998	Smith et al.
5,793,868	A		8/1998	Micali
5,799,086	A		8/1998	Sudia
5,812,670	A		9/1998	Micali
5,825,880	A		10/1998	Sudia et al.
5,826,262	A		10/1998	Bui et al.
5,841,865	A		11/1998	Sudia
5,850,451	A		12/1998	Sudia
5,857,022	A		1/1999	Sudia
5,867,578	A		2/1999	Brickell et al.
5,903,882	A		5/1999	Asay et al.
5,936,544	A	*	8/1999	Gonzales et al. 340/5.22
5,960,083	A		9/1999	Micali
5,982,898	A		11/1999	Hsu et al.
5,995,625	A		11/1999	Sudia et al.
6,009,177	A		12/1999	Sudia
6,026,163	A		2/2000	Micali
6,044,462	A		3/2000	Zubeldia et al.
6,061,448	A		5/2000	Smith et al.
6,097,811	A		8/2000	Micali
6,119,137	A		9/2000	Smith et al.
RE36,918	E		10/2000	Micali
6,134,326	A		10/2000	Micali et al.
6,137,884	A		10/2000	Micali
6,141,750	A		10/2000	Micali
6,151,675	A		11/2000	Smith
6,189,103	B1		2/2001	Nevarez et al.
6,192,407	B1		2/2001	Smith et al.
6,209,091	B1		3/2001	Sudia et al.
6,216,231	B1		4/2001	Stubblebine
6,292,893	B1		9/2001	Micali
6,301,659	B1		10/2001	Micali
6,317,025	B1	*	11/2001	Leon et al. 340/5.21
6,385,655	B1		5/2002	Smith et al.
6,397,329	B1		5/2002	Aiello et al.
6,404,337	B1		6/2002	Van Till et al.
6,442,689	B1		8/2002	Kocher
6,470,086	B1		10/2002	Smith
6,480,096	B1	*	11/2002	Gutman et al. 340/5.31
6,487,599	B1		11/2002	Smith et al.
6,487,658	B1		11/2002	Micali
6,502,191	B1		12/2002	Smith et al.
6,516,411	B2		2/2003	Smith
6,529,956	B1		3/2003	Smith et al.
6,532,540	B1		3/2003	Kocher
6,609,196	B1		8/2003	Dickinson, III et al.
6,651,166	B1		11/2003	Smith et al.
6,658,568	B1		12/2003	Ginter et al.
6,671,805	B1		12/2003	Brown et al.
6,725,381	B1		4/2004	Smith et al.
6,748,529	B2		6/2004	Smith et al.
6,766,450	B2		7/2004	Micali
6,826,609	B1		11/2004	Smith et al.
6,873,824	B2	*	3/2005	Flick 455/41.2
6,975,202	B1	*	12/2005	Rodriguez et al. 340/5.25
7,012,503	B2	*	3/2006	Nielsen 340/5.6
2001/0011255	A1		8/2001	Assay et al.
2001/0050990	A1		12/2001	Sudia
2002/0013898	A1		1/2002	Sudia et al.
2002/0029200	A1		3/2002	Dulin et al.
2002/0029337	A1		3/2002	Sudia et al.
2002/0062438	A1		5/2002	Asay et al.
2002/0107814	A1		8/2002	Micali
2002/0123336	A1	*	9/2002	Kamada 455/420
2002/0165824	A1		11/2002	Micali
2002/0184182	A1		12/2002	Kwan
2003/0014365	A1		1/2003	Inada et al.
2003/0065921	A1		4/2003	Chang
2003/0212888	A1		11/2003	Wildish et al.
2003/0221101	A1		11/2003	Micali
2004/0049675	A1		3/2004	Micali et al.
2004/0111607	A1		6/2004	Yellepeddy
2004/0237031	A1		11/2004	Micali et al.
2005/0010783	A1		1/2005	Libin et al.
2005/0033962	A1		2/2005	Libin et al.
2005/0044376	A1		2/2005	Libin et al.
2005/0044386	A1		2/2005	Libin et al.
2005/0044402	A1		2/2005	Libin et al.
2005/0055548	A1		3/2005	Micali
2005/0055567	A1		3/2005	Libin et al.
2005/0114653	A1		5/2005	Sudia

2005/0154918	A1	7/2005	Engberg
2005/0155879	A1	7/2005	Engberg et al.
2005/0193204	A1	9/2005	Engberg et al.
2006/0097843	A1	5/2006	Libin

FOREIGN PATENT DOCUMENTS

EP	0 723 251	A2	1/1996
EP	0 798 671	A2	2/1997
EP	1 024 239	A1	1/1999
FR	2 774 833	A1	2/1998
WO	WO 98/26385		6/1998
WO	WO 98/43152		10/1998
WO	WO 00/22787		4/2000
WO	WO 01/06701	A1	1/2001
WO	WO 01/11812	A2	2/2001
WO	WO 01/11843		2/2001
WO	WO 01/25874	A2	4/2001

OTHER PUBLICATIONS

**Facsimile message from Chini Krishnan of Integris Security, Inc. to Professor Silvio Micali, dated Feb. 25, 1997, 13 pages including cover sheet, submitted in attached sealed envelope as Proprietary Material not Open to Public. To be Opened Only by Examiner or Other Authorized U.S. Patent and Trademark Office Employee.

"Distributed Certificate Validation: The answer to validation scalability, availability and cost issues," *CoreStreet White Paper*, published at www.corestreet.com, Jun. 12, 2003, 14 pp.

"Distributed OCSP: Security, Scalability, and Availability for Certificate Validation," *CoreStreet White Paper*, published at www.corestreet.com, 2002, 4 pp.

"Real Time Credential Validation: Secure, Efficient Permissions Management," *CoreStreet White Paper*, published at www.corestreet.com, 2002, 5 pp.

"Real Time Credential Validation: Secure, Efficient Permissions Management," *CoreStreet White Paper*, published at www.corestreet.com, 2002-2004, 5 pp.

"Identity Services Infrastructure™: A practical approach to ensuring trust and privacy in government and industry," *CoreStreet White Paper*, published at www.corestreet.com, 2006, 13 pp.

"The Roles of Authentication, Authorization & Cryptography in Expanding Security Industry Technology," Security Industry Association, *Quarterly Technical Update*, Dec. 2005, 32 pp.

"Important FIPS 201 Deployment Considerations: Ensuring Your Implementation is Future-Ready," *White paper*, published at www.corestreet.com, 2005-2006, 11 pp.

"Vulnerability Analysis of Certificate Validation Systems," *CoreStreet White Paper*, published at www.corestreet.com, 2006, 15 pp.

"The Role of Practical Validation for Homeland Security," *CoreStreet White Paper*, published at www.corestreet.com, 2002-2004, 3 pp.

"Distributed Certificate Validation," *CoreStreet White Paper*, published at www.corestreet.com, 2006, 16 pp.

"Certificate Validation Choices: Evaluation criteria for selecting the appropriate validation mechanism for your needs," *CoreStreet white paper*, published at www.corestreet.com, 2002-2004, 8 pp.

"Nonce Sense: Freshness and Security in OCSP Responses," *CoreStreet White Paper*, published at www.corestreet.com, 2003-2004, 2 pp.

"Sistema Distruito Per II Controllo Della Validita Dei Certificati Digitali: Prestazioni—Disponibilita'—Costi," *CoreStreet White Paper*, published at www.corestreet.com, visited Aug. 7, 2006, 17 pp.

"Analisi Della Vunlerabilita' Dei Sistemi Di Convalida Dei Certificati Digitali," *CoreStreet White Paper*, published at www.corestreet.com, visited Aug. 7, 2006, 17 pp.

Jon Shamah, "From eID to Identity Services Infrastructure—Practical implementations for sustainable success,"

"U.S. Department of Homeland Security First Responders Card Initiative," Transcript, *All Hazards Forum Conference and Exhibition*, Moderator Craig A. Wilson, Baltimore, Maryland, Oct. 26, 2005, 42 pp.

"Card-Connected System," *Functional Specification*, published at www.corestreet.com, 2005, 6 pp.

"Card-Connected System," *Architects and Engineers Specification*, published at www.corestreet.com, 2005, 11 pp.

"CoreStreet Validation Authority," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 2 pp.

"Responder Appliance 2400," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"Desktop Validation Client," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"Server Validation Extension," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"Path Builder System™: For Federated PKI," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"PKI Toolkit: Developer toolkit to enable certificate validation," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"MiniCRL," *CoreStreet data sheet*, published at www.corestreet.com, 2006, 1 p.

"PIVMAN™ System: Secure ID Checking," *CoreStreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"The PIVMAN™ System: Implementing secure ID checking for site control in emergencies," *CoreStreet Product Implementation Overview*, published at www.corestreet.com, 2006, 4 pp.

"The PIVMAN™ System: Deployment and use case overview," *CoreStreet Product Application Overview*, published at www.corestreet.com, 2006, 4 pp.

"Card-Connected™ Access Control," *Corestreet Data Sheet*, published at www.corestreet.com, 2006, 1 p.

"FIPS 201 Solutions," *Corestreet Solutions Overview*, published at www.corestreet.com, 2005, 1 p.

"Common Criteria Factsheet: Understanding the importance of certification," *Corestreet Fact Sheet*, published at www.corestreet.com, 2006, 1 p.

"Security Requirements for Cryptographic Modules," *Federal Information Processing Standards (FIPS) Publication 140-2*, Information Technology Laboratory, National Institute of Standards and Technology , Gaithersburg, MD 20899, May 25, 2001.

"Final Text of Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions," *ISO/IEC JTC 1/SC 21/WG 4 and ITU-T Q 15/7 Collaborative Editing Meeting on the Directory*, Dec. 1996, 54 pp.

Christoffersson et al., *Crypto User's Handbook, A Guide for Implementors of Cryptographics Protection in Computer Systems*, Elsevier Science Publishers B. V., 1988, pp. 8-85.

M. Ito, et al., "Secret Sharing Scheme Realizing General Access Structure," Dept. of Electrical Communications, Tohoku University, Sendai, Miyagi 9890, Japan, 1987, pp. 3.6.1-3.6.4.

L. Gong, "Securely replicating authentication services," *Proceedings of the International Conference on Distributed Computing Systems*, IEEE Computer Society Press, 1989. pp. 85-91.

International Search Report from PCT/US 96/17374, dated Feb. 19, 1997, 3 pp.

C.J. Mitchell and F.C. Piper, "Key Storage in Secure Networks," *Discrete Applied Mathematics*, vol. 21, No. 3, 1988, pp. 215-228.

D. Otway and O. Rees, "Efficient and timely mutual authentication," *SIGOPS Oper Syst. Rev.* vol. 21, No. 1, Jan. 1987, pp. 8-10.

"The Digital Signature Standard," National Institute of Standards and Technology (NIST), Proposal and Discussion, *Comm. of the ACM*, 35 (7), Jul. 1992, pp. 36-54.

F. T. Leighton, "Failsafe Key Escrow Systems," *Technical Memo 483, MIT Lab. for Computer Science*, 1994, 9 pp.

B. Fox and B. LaMacchia, "Certificate Revocation: Mechanics and Meaning," *Proceedings of Financial Cryptography '98* , Lecture Notes in Computer Science 1465, Springer-Verlag, Jan. 1998, pp. 158-164.

R. Blom, "An optional class of symmetric key generation schemes,"

C. Blundo, et al., "Perfectly Secure Key Distribution for Dynamic Conferences" *Proceedings of Advances in Cryptology: CRYPTO '92*, Springer-Verlag, Berlin, 1993, pp. 471-486.
D. Beaver, "Multiparty Protocols Tolerating Half Faulty Processors," *Proceedings of Advances in Cryptology* '89, Lecture Notes In Computer Science 435, G. Brassard, Ed. Springer-Verlag, London, 1990, pp. 560-572.
B. Schneier, *Applied Cryptography* 2nd ed.; John Wiley & Sons, Inc., 1996, pp. 42-65, 574-576, 591, 593.
"Escrowed Encryption Standard (EES)," *Federal Information Processing Standards (FIPS) Publication 185*, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899, Feb. 1994.
S. Chokhani, "Toward a National Public Key Infrastructure," *IEEE Communications Magazine*, vol. 32, No. 9, Sep. 1994, pp. 70-74.
M. Gasser, et al., "The Digital Distributed System Security Architecture," *Proc. 12thNational Computer Security Conference*, 1989, pp. 305-319.
R. L. Rivest, et al., "SDSI—A Simple Distributed Security Infrastructure," 1996, pp. 1-39.
D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Technical Note Programming Techniques and Data Structures, *Communications of the ACM*, vol. 24, No. 2, Feb. 1981, pp. 84-88.
R. Gennaro, et al., "Robust Threshold DSS Signatures," *Proc. of Advances in Cryptology: EUROCRYPT '96*, Lecture Notes in Computer Science 1070, 1996, 20 pp.
"Federal Public Key Infrastructure (PKI) Technical Specifications: Part D—Interoperability Profiles," (DRAFT) *Federal PKI Technical Working Group, Inc.,* Cygnacom Solutions, 1995, 91 pp.
N. Nazario, "Federal Public Key Infrastructure (PKI) Version 1 Technical Specifications: Part B—Technical Security Policy," *PKI Technical Working Group*, 1996, 21 pp.
S. Chokhani and W. Ford, "Certificate Policy and Certification Practice Statement Framework," (DRAFT) *CygnaCom Solutions, Inc.,* Nov. 1996, 80 pp.
William E. Burr, et al., "A Proposed Federal PKI Using X.509 V3 Certificates," *National Institute of Standards and Technology (NIST)*, Gaithersburg, MD 20899, 1996, 8 pp.
W.E. Burr, "Public Key Infrastructure (PKI) Technical Specifications (Version 1): Part C—Concept of Operations," (DRAFT) Feb. 1996, 30 pp.
Warwick Ford, "Public-Key Infrastructure Standards," *PP Presentation*, 1996, 15 pp.
William T. Polk, "Minimum Interoperability Specifications for PKI Components," *NIST presentation*, 1996, 13 pp.
Santosh Chokhani, Ph.D., "Security Considerations in Using X.509 Certificates," *PP Presentation*, 1996, 11 pp.
Donna F. Dodson, "PKI Implementation Projects," *NIST Presentation*, 1996, 17 pp.
William E. Burr, et al., "A Proposed Federal PKI Using X.509 V3 Certificates," *NIST Presentation*, 1996, 12 pp.
Noel A. Nazario, et al., "Management Model for the Federal Public Key Infrastructure," *NIST Presentation*, 1996, 9 pp.
Noel A. Nazario, "Security Policies for the Federal Public Key Infrastructure," *NIST Presentation*, 1996, 11 pp.
William Burr, et al., "Minimum Interoperability Specification for PKI Components," *Output of NIST's Cooperatve Research and Development Agreements for Public Key Infrastructure development with AT&T, BBN, Certicom, Cylink, DynCorp, IRE, Motorola, Northern Telecom, Spyrus, and VeriSign*, DRAFT Version 1, 1996.
Farrell, et al., "Internet Public Key Infrastructure Part III: Certificate Management Protocols," *Internet Draft, PKIX Working Group*, Dec. 1996.
W. Polk, ed., "Requirements for the Federal Public Key Infrastructure (Version 1) Part A: Requirements," 1996, 19 pp.
Warwick Ford, "A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications," *NORTEL/Bell-Northern Research, National Institute of Standards, and Technology*, 1995, 94 pp.
L. Harn, "Group-Oriented (t, n) threshold digital signature scheme and digital multisignature," *IEEE Proc-Comput. Digit. Tech.,* vol. 141, No. 5, Sep. 1994, pp. 307-313.
Oded Goldreich, "Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme," *Laboratory for Computer Science, Massachusetts Institute of Technology MIT/LCS/TM-315*, Sep. 1986, 10 pp.
S. Goldwasser, et al., "The Knowledge Complexity of Interactive Proof Systems," *Society for Industrial and Applied Mathematics (SIAM) J. Comput.,* vol. 18, No. 1, Feb. 1989, pp. 186-208.
"X9-Financial Services: American National Standard X9.55-1995," *American National Standards Institute, Accredited Standards Committee X9(Working Draft)*, Jul. 3, 1996, 41 pp.
S. Micali, et al., "An Efficient Zero-Knowledge Method for Answering Is He In Or Out? Questions," *Abstract of talk given at International Computer Science Institute*, Berkeley, CA, Dec 1995.
"Information technology—Open Systems Interconnection—The Directory: Authentication framework," *International Standard ISO/IEC 9594-8*, 1995, 41 pp.
Z. Galil, et al., "Partitioned Encryption and Achieving Simultaneity by Partitioning," *Information Processing* Letters 26 (1987/88), Oct. 1986, pp. 81-88.
Paul Neil Feldman, "Optimal Algorithms for Byzantine Agreement," *Thesis submitted for Doctor of Philosophy in Mathematics at the Massachusetts Institute of Technology*, May 1988.
B. Chor, et al., "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults," *IEEE*, 1985, pp. 383-395.
D. Chaum, "Security Without Identification: Transaction Systems To Make Big Brother Obsolete," Communications of the ACM, vol. 28, No. 10, Oct. 1985, pp. 1030-1044.
V. Varadharajan, "Notification: A Partical Security Problem in Distributed Systems," *Proc. of the 14thNational Computer Security Conference*, National Institute of Standards and Technology/National Computer Security Center, Oct. 1-4, 1991, pp. 386-396.
Silvio Micali, "Computationally-Sound Proofs," *Laboratory for Computer Science, Massachusetts Institute of Technology*, Apr. 11, 1995, 56 pp.
Silvio Micali, *Proc. of Advances in Cryptology-CRYPTO '92* , Lecture Notes in Computer Science 740, Aug. 1992, pp. 113-138.
J. L. Abad-Peiro, et al., "Designing a Generic Payment Service," *IBM Research Division, Zurich Research Laboratory*, Nov. 1996, 26 pp.
R. Ankney, "A Certificate-Based Authorization Model," *Fisher International*, Sep. 25, 1995, 20 pp.
D. Chaum, et al., "Multiparty Unconditionally Secure Protocols," ACM-0-89791-264, 1988, pp. 11-19.
O. Goldreich, et al., "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems," *Journal of the Association for Computing Machinery*, vol. 38, No. 1, Jul. 1999, pp. 691-729.
M. K. Franklin, et al., "Fair Exchange with a Semi-Trusted Third Party," *Proc.of the 4thACM Conference on Computer and Communications Security*, Apr. 1997, 6 pp.
A. Fiat, et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," *Proc. of Advances in Cryptology: Proc. Crypto '86*, Lecture Notes in Computer Science 263, 1987, pp. 186-194.
D. Dolev, et al., "Non-Malleable Cryptography," ACM 089791-397-3, 1991, pp. 542-552.
Richard A. DeMillo, et al., "Cryptology in Revolution: Mathematics and Models," *Lecture Notes Prepared for the American Mathematical Society Short Course Held in San Francisco*CA, Jan. 5-6, 1981, ISBN 0-8218-0041-8, 1983, pp. 152-155.
Ivan Bjerre Damgdrd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," *Proc. of Advances in Cryptology—CRYPTO '88*, 1988, pp. 328-335.
O. Goldreich, et al., "How To Play Any Mental Game or A Completeness Theorem for Protocols with Honest Majority," ACM 0-89791-221-7, 1987, pp. 218-229.
Y. Frankel, et al., "Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash," *Proc. of Advances in Cryptology,*

S. Micali, "A Secure and Efficient Digital Signature Algorithm," *Technical Memo, Laboratory for Computer Science, Massachusets Institute of Technology*Cambridge, MA 02139, Mar. 1994, 12 pp.
"Initial EFF Analysis of Clinton Privacy and Security Proposal," *Society for Electronic Access, The Electronic Frontier Foundation*, Apr. 1993, 3 pp.
L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, Technical Note Operating Systems, vol. 24, No. 11, Nov. 1981, pp. 770-772.
J. Linn, "Privacy Enhancement for Internet Electronics Mail: Part I—Message Encipherment and Authentication Procedures," *Network Working Group Request for Comments: 1040*, Jan. 1988, 28 pp.
S. Kent, "Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Managements," *Network Working Group Request for Comments: 1422*, Feb. 1993, 30 pp.
T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, No. 4, Jul. 1985, pp. 469-472.
R. Hauser, et al., "Lowering Security Overhead in Link State Routing," *Computer Networks*, vol. 31, Elsevier, Apr. 1999, pp. 885-894.
S. Herda, "Non-repudiation: Constituting evidence and proof in digital cooperation," *Computer Standards & Interfaces*, vol. 17, Elsevier, 1995, pp. 69-79.
S.G. Stubblebine, "Recent-Secure Authentication: Enforcing Evocation in Distributed Systems, Security and Privacy," *Proc. of the 1995 IEEE Smposium on Security and Privacy*, Section 5, 1995, pp. 224-235.
Ronald L. Rivest and Adi Shamir, "PayWord and MicroMint: Two simple micropayment schemes," *MIT Laboratory for Computer Science 545 Technology Square*, Cambridge, Mass 02139; *Wezmann Institute of Science Applied Mathematics Department*, Rehovot, Israel, Apr. 27, 2001, 19 pp.
R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Programming Techniques, vol. 21. No. 2, Feb. 1978, pp. 120-126.
M. Bellare, et al., "Incremental cryptography: the case of hashing and signing," *Proc. of Advances in Cryptology—CRYPTO '94*, Lecture Notes in Computer Science 839, Springer-Verlag, 1994, pp. 216-233.
M. Bellare and S. Micali, "How to Sign Given Any Trapdoor Permutation," *J. of the Assoc. for Computing Machinery*, vol. 39, No. 1, Jan. 1992, pp. 214-233.
J. C. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret (Extended Abstract)," *Proc of Advances in Cryptology—CRYPTO '86*, Lecture Notes in Computer Science 263, Springer-Verlag,1986, pp. 216-233.
W. Johnston, et al., "Authorization and Attribute Certificates for Widely Distributed Access Control," *IEEE 7thInternational Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 1998, 6 pp.
P. Janson and M. Waidner, "Electronic Payment over Open Networks," *IBM Zurich Research Laboratory*, Apr. 18, 1995, 9 pp.
E. D. Karnin, et al., "On Secret Sharing Systems," *IEEE Transactions on Information Therory*, vol. IT-29, No. 1, Jan. 1983, pp. 35-41.
S. Micali, and R. L. Rivest, R. L., "Micropayments Revisited," *Proc. of the Cryptographer's Track At the RSA Conference on Topics in Cryptology* (Feb. 18-22, 2002), Lecture Notes In Computer Science 2271. Springer-Verlag, London, 2002, 149-163.
Silvio Micali, "Enhanced Certificate Revocation," *Technical Memo MIT/LCS/TM-542b, Laboratory for Computer Science, Massachusetts Institute of Technology*, Mar. 22, 1996, 10 pp.
R. Housley, et al., "Internet Public Key Infrastructure Part I: x.509 Certificate and CRL Profile," *Internet Engineering Task Force, PKIX Working Group, Internet Draft*, Mar. 26, 1996, 76 pp.
T. Elgamal, et al., "Securing Communications on the Intranet and Over the Internet," White Paper, *Netscape Communications Corporation*, Jul. 1996, 19 pp.
S. Berkovits. et al., "Public Key Infrastructure Study," Final Report,
M. Ben-Or, et al., "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," ACM-0-89791-264, 1988, 10 pp.
M. Ben-Or, et al., "A Fair Protocol for Signing Contracts," *IEEE Transactions on Information Theory*, vol. 36, No. 1, Jan. 1990, pp. 40-46.
G. R. Blakley, "Safeguarding cryptographic keys," *AFIPS—Proc. of the National Computer Conference*, vol. 48, 1979, pp. 313-317.
J. Camenisch, et al., "An Efficient Fair Payment System," ACM-089791-892-0, 1996, 7 pp.
J. Camenisch, et al., "Digital Payment Systems with Passive Anonymity-Revoking Trustees," *Computer Security—ESORICS '96*, Lecure Notes in Computer Science 1146, Springer Verlag, 1996, pp. 33-43.
M. Blum, "How to Exchange (Secret) Keys," *ACM Transactions on Computer Systems*, vol. 1, No. 2, May 1983, pp. 175-193.
H. Bürk, et al., "Digital Payment Systems Enabling Security and Unobservability," *Computers & Security*, vol. 8, Elsevier Science, 1989, pp. 399-416.
G. Brassard, et al., "Minimum Diclosure Proofs of Knowledge," *J. of Computer and Systems Sciences*, vol. 37, 1988, pp. 156-189.
D. Chaum, et al., "Untraceable Electronic Cash," *Proc. of the 8th Annual international Cryptology Conference on Proc. of Advances in Cryptology* (Aug. 21-25,1988), Lecture Notes In Computer Science 403, Springer-Verlag, 1990, pp. 319-327.
P. Cheng, et al., "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX," *IBM Thomas J. Watson Research Center*, Yorktown Heights, NY, 10598, Apr. 28, 1995, 14 pp.
R. DeMillo, et al., "Protocols for Data Security," *Computer, IEEE*, Feb. 1983, pp. 39-50.
E-mail from Martin Hellman "Re: Clipper-Chip Escrow-System Flaws," Apr. 16, 1993, 1 p.
E-mail from Martin Hellman, "Clipper Chip," Apr. 17, 1993, 2 pp.
E-mail from Dorothy Denning, "Re: Clipper Chip," Apr. 18, 1993, 3 pp.
Y. Desmedt, et al., "Threshold cryptosystems," *Proc. of Advances in Cryptology—CRYPTO 89*, Lecture Notes in Computer Science 435, Springer-Verlag, 1990, pp. 307-315.
W. Diffie, et al., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, Nov. 1976, pp. 644-654.
S. Dukach, "SNPP: A Simple Network Payment Protocol," *Proc. of the Eighth Annual Computer Security Applications Conference*, Dec. 1992, 6 pp.
S. Even, et al., "A Randomized Protocol for Signing Contracts," *Communications of the ACM, Programming Techniques and Data Structures*, vol. 28, No. 6, Jun. 1985, pp. 637-647.
S. Even, et al., "On-line/Off-line Digital Signatures," *Proc. of Advances in Cryptology*, Springer-Verlag New York, pp. 263-275.
S. Even, et al., "Secure Off-line Electronic Fund Transfer Between Nontrusting Parties," *Computer Science Department, Technion, Israel Institute of Technology*, Haifa, Israel 32000, Jan. 31, 1988, 10 pp.
O. Goldreich, et al., "Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design," *Proc of 27th Symp. on Foundation of Computer Science*, 1986, pp. 174-187.
P. Feldman, "A Practical Scheme for Non-interactive Verifiable Secret Sharing," *IEEE Symposium on Foundations of Computer Science*, 1987, pp. 427-437.
A. Fiat, "Batch RSA," *Proc. of Advances in Cryptology—CRYPTO '89*, Lecture Notes on Computer Science 435, Springer-Verlag, 1989, pp. 175-185.
S. Goldwasser, et al., "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," *Society for Industrial and Applied Mathematics (SIAM) J. Comput.*, vol. 17, No. 2, Apr. 1988, pp. 281-308.
L. C. Guillou, et al., "A 'Paradoxical' Identity-Based Signature Scheme Resulting from Zero-Knowledge," *Proc. of Advances in*

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.