References

[1] M. Abadi, E. Allender, A. Broder, J. Feigenbaum, and L. Hemachandra. On generating solved instances of computational problems. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 297–310. Springer-Verlag, 1988.

[2] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffery I. Schiller, and Bruce Schneier. The risks of key recovery, key escrow, and trusted third party encryption. *World Wide Web Journal*, 2(3):241–257, 1997. Also in: Report in Centre for Democracy and Technology Policy Post, Vol. 3, no. 6, May 21, 1997. A revised edition appeared June 1998.

[3] Accredited Standards Committee X9. American National Standard X9.59-199x: Electronic Commerce for the Financial Services Industry: Account-Based Secure Payment Objects. Working Draft # 17, January 1999.

[4] C. Adams and S. Farrell. Internet X.509 public key infrastructure certificate management protocols. Internet Draft of the PKIX Working Group, May 1998.

[5] Carlisle Adams and Robert Zuccherato. A general, flexible approach to certificate revocation. Entrust white paper, June 1998.

[6] G.B. Agnew, R.C. Mullin, and S.A. Vanstone. An implementation of elliptic curve cryptosystems over $F_{2^{155}}$. *IEEE Journal on Selected Areas in Communications*, 11(5):804–813, June 1993.

[7] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation. In Hugo Krawczyk, editor, *Advances in Cryptology–CRYPTO '98*, Lecture Notes in Computer Science, pages 137–152. Springer-Verlag, 1998.

[8] American Bankers Association. X9.45-199x: Enhanced management controls using digital signatures and attribute certificates. Working draft, June 1997.

[9] American Bar Association. Digital signature guidelines; legal infrastructure for certification authorities and secure electronic commerce, August 1996. ISBN 1-57073-250-7.

[10] American Civil Liberties Union. Elements of effective self regulation for the protection of privacy and questions related to online privacy. Letter to Ms. Jane Coffin, Office of International Affairs, National Telecommunications and Information Administration, July 1998.

[11] American National Standards Institute. American National Standards Committee X.9.55-1995: Public key cryptography for the financial services industry, 1995.

[12] Ross Anderson and Markus Kuhn. Tamper resistance - a cautionary note. In *Second USENIX Workshop on Electronic Commerce*, pages 1–11, Oakland, California, November 1996. USENIX Association. ISBN 1-880446-83-9.

[13] Ross Anderson and Markus Kuhn. Low cost attacks on tamper resistant devices. In *Security Protocols, 5th International Workshop, Paris, France*, volume 1361 of *Lecture Notes in Computer Science*, pages 125–136. Springer-Verlag, April 1997.

[14] Ross Anderson and Serge Vaudenay. Minding your p's and q's. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology–ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 26–35. Springer-Verlag, 1996.

[15] Arthur Andersen Computer Risk Management. Report on companies' use of encryption & evaluations re. monitorable encryption systems. Background report for the Danish Ministry of Research and Information Technology, February 1998.

[16] Eric Bach. How to generate factored random numbers. *SIAM J. Computing*, 17(2):179–193, April 1988.

[17] Stewart Baker and Matthew Yeo. Survey of international electronic and digital signature initiatives. Steptoe & Johnson LLP, Internet Law and Policy Forum, version of April 14, 1999.

[18] Stewart A. Baker. Don't worry be happy – why Clipper is good for you. Wired 2.06, 1996.

[19] James Bamford. *The Puzzle Palace: A Report on America's Most Secret Agency*. Houghton Mifflin, Boston, 1982.

[20] Banksys / Groupement des Cartes Bancaires. Interoperable C-SET: Protocol specification. Deliverable: D 6.1, Issue 2, Version 0, November 1997.

[21] Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures, June 1998. Extended abstract in: Advances in Cryptology – Proceedings of Eurocrypt 98, Lecture Notes in Computer Science Vol. 1403, K. Nyberg ed., Springer-Verlag, 1998.

[22] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Ernest F. Brickell, editor, *Advances in Cryptology–CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 390–420. Springer-Verlag, 1992.

[23] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. Incremental cryptography: The case of hashing and signing. In Yvo G. Desmedt, editor, *Advances in Cryptology–CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 216–233. Springer-Verlag, 1994.

[24] Mihir Bellare, Markus Jakobsson, and Moti Yung. Round-optimal zero-knowledge arguments based on any one-way function. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 280–305. Springer-Verlag, 1997.

[25] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1988.

[26] J. Benaloh and M. Yung. Distributing the power of a government to enhance the privacy of voters. In *Proceedings of the 5th Symposium on Principles of Distributed Computing*, pages 52–62, New York, August 1986. ACM.

[27] Shimshon Berkovits, Santosh Chokhani, Judith A. Furlong, Jisoo A. Geiter, and Jonathan C. Guild. Public Key Infrastructure study. Final Report for the National Institute of Standards and Technology. Task performed by The MITRE Corporation, McLean, Virginia, April 1994.

[28] Ingrid Biehl, Bernd Meyer, and Christoph Thiel. Cryptographic protocols based on real-quadratic a-fields. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology–ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 15–25. Springer-Verlag, 1996.

[29] Eli Biham and Adi Shamir. The next stage of differential fault analysis: How to break completely unknown cryptosystems. Distributed on October 30th, 1996.

[30] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer-Verlag, 1997.

[31] David Birch. Exploiting Privacy Enhancing Technologies. Proceedings of UK Data Protection '99 IIR, London, July 1999. Draft of 5/7/99.

[32] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The role of trust management in distributed system security. In J. Vitek and C. Jensen, editors, *Secure Internet Programming: Security Issues for Distributed and Mobile Objects*, volume 1603 of *Lecture Notes in Computer Science*, pages 185–210. Springer, 1999.

[33] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In *Proceedings of the 17th Symposium on Security and Privacy*, pages 164–173, Los Alamitos, 1996. IEEE Computer Society Press.

[34] Daniel Bleichenbacher. Generating ElGamal signatures without knowing the secret key. In Ueli Maurer, editor, *Advances in Cryptology–EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 10–18. Springer-Verlag, 1996.

[35] Daniel Bleichenbacher, Eran Gabber, Phil Gibbons, and Yossi Matias. On personalized yet anonymous interaction. Manuscript 1997.

[36] D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $n^{0.292}$. In *Advances in Cryptology–EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag, 1999.

[37] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society*, 46(2):203–213, 1999.

[38] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer-Verlag, 1997.

[39] Dan Boneh and Matthew Franklin. Efficient generation of shared RSA keys. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 425–439. Springer-Verlag, 1997.

[40] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may be easier than factoring. In Kaisa Nyberg, editor, *Advances in Cryptology–EUROCRYPT '98*, volume 1233 of *Lecture Notes in Computer Science*, pages 59–71. Springer-Verlag, 1998.

[41] J.N.E. Bos and D. Chaum. SmartCash: a practical electronic payment system. Technical Report CS-R9035, Centrum voor Wiskunde en Infomatica, August 1990.

[42] Jurjen N.E. Bos. *Practical Privacy*. PhD thesis, Centrum voor Wiskunde en Informatica, March 1992. In: Verification of RSA Computations on a Small Computer, pages 103–116.

[43] Caspar Bowden and Yaman Akdeniz. Cryptography and democracy: Dilemmas of freedom. *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet*, pages 81–125, 1999.

[44] Joan Boyar, S.A. Kurtz, and M.W. Krentel. A discrete logarithm implementation of perfect zero-knowledge blobs. *Journal of Cryptology*, 2(2):63–76, 1990.

[45] Stefan Brands. Cryptographic methods for demonstrating satisfiable formulas from propositional logic. Patent PCT/NL96/00413. Filed November 1995.

[46] Stefan Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica, April 1993.

[47] Stefan Brands. Off-line cash transfer by smart cards. Technical Report CS-R9455, Centrum voor Wiskunde en Informatica, September 1994. Also in: Proceedings of the First Smart Card Research and Advanced Application Conference (October 1994), France, pages 101–117.

[48] Stefan Brands. Untraceable off-line cash in wallet with observers. In Douglas R. Stinson, editor, *Advances in Cryptology–CRYPTO '93*, volume 911, pages 302–318. Springer-Verlag, 1994.

[49] Stefan Brands. Off-line electronic cash based on secret-key certificates. In R. Baeza-Yates, E. Goles, and P.V. Goblete, editors, *Proceedings of the Second International Symposium of Latin American Theoretical Informatics*, volume 911, pages 131–166. Springer-Verlag, 1995.

[50] Stefan Brands. Restrictive blind issuing of secret-key certificates in parallel mode. Technical Report CS-R9523, Centrum voor Wiskunde en Informatica, March 1995.

[51] Stefan Brands. Restrictive blinding of secret-key certificates. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology–EUROCRYPT '95,* volume 921 of *Lecture Notes in Computer Science*, pages 231–247. Springer-Verlag, 1995.

[52] Stefan Brands. Secret-key certificates. Technical Report CS-R9510, Centrum voor Wiskunde en Informatica, February 1995.

[53] Stefan Brands. Secret-key certificates (continued). Technical Report CS-R9555, Centrum voor Wiskunde en Informatica, June 1995.

[54] Stefan Brands. Privacy-protected transfer of electronic information. U.S. Patent ser. no. 5,604,805, February 1997. Filed August 1993.

[55] Stefan Brands. Rapid demonstration of linear relations connected by Boolean operators. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 318–333. Springer-Verlag, 1997.

[56] Stefan Brands. Secret-key certificates. U.S. Patent ser. no. 5,606,617, February 1997. Filed October 1994.

[57] Stefan Brands. Secure cryptographic methods for electronic transfer of information. U.S. Patent ser. no. 5,668,878, September 1997. Filed August 1995.

[58] Stefan Brands. Electronic cash. In Mikhail J. Atallah, editor, *Algorithms and Theory of Computation Handbook*, chapter 44. CRC Press LLC, November 1998. ISBN 0-8493-2649-4.

[59] Stefan Brands and David Chaum. Distance-bounding protocols. In Tor Helleseth, editor, *Advances in Cryptology–EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer-Verlag, 1994.

[60] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, 1988.

[61] D.M. Bressoud. *Factorization and Primality Testing*. Springer-Verlag, New York, 1989.

[62] Ernest Brickell, Peter Gemmell, and David Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Proceedings of the 6th Annual Symposium on Discrete Algorithms*, pages 457–466, 1995.

[63] Ernest F. Brickell, David Chaum, Ivan B. Damgård, and Jeroen van de Graaf. Gradual and verifiable release of a secret. In Carl Pomerance, editor, *Advances in Cryptology–CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 156–166. Springer-Verlag, 1988.

[64] Murray J. Brown. Secure wireless messaging: A new approach to digital certificates. Wireless Magazine, October 1998.

[65] Mark E. Budnitz. Industry self-regulation of internet privacy: The sound of one hand clapping. Computers, Freedom & Privacy 1999, April 6–8, Washington DC.

[66] Mark E. Budnitz. Privacy protection for consumer transactions in electronic commerce: Why self-regulation is inadequate. 49 S. Caro. L. Rev. 847, 1998.

[67] Mike Burmester. A remark on the efficiency of identification schemes. In I.B. Damgård, editor, *Advances in Cryptology–EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 493–495. Springer-Verlag, 1991.

[68] W. E. Burr. Public key infrastructure (PKI) technical specifications: Part A - technical concept of operations. Working draft TWG-98-59, September 1998.

[69] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. OpenPGP message format. Network Working Group, Request for Comments no. 2440, November 1998.

[70] Jan Camenisch. *Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem*. PhD thesis, ETH, 1998. Reprinted as Vol. 2 in ETH Series in Information Security and Cryptography, edited by Ueli Maurer, Hartung-Gorre Verlag, Konstanz, ISBN 3-89649-286-1.

[71] Jan Camenisch, Ueli Maurer, and Markus Stadler. Digital payment systems with passive anonymity-revoking trustees. *Journal of Computer Security*, 5(1), 1997. Abbridged version in: Computer Security – ESORICS 96, Vol. 1146, pages 33–43, Springer-Verlag.

[72] Jan Camenisch, Jean-Marc Piveteau, and Markus Stadler. Blind signatures based on the discrete logarithm problem. In Alfredo De Santis, editor, *Advances in Cryptology–EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432. Springer-Verlag, 1995.

[73] Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. Springer-Verlag, 1997.

[74] Jan Camenisch and Markus Stadler. Proof systems for general statements about discrete logarithms. Technical Report TR 260, Institute for Theoretical Computer Science, ETH Zürich, March 1997.

[75] Duncan Campbell. Interception capabilities 2000. Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of economic information, April 1999.

[76] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *Proc.* 30*th ACM Symp. on Theory of Computing*. ACM Press, 1998.

[77] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist,

Gérard Guillerm, Paul Leyland, Joël Marchand, Francois Morain, Alec Muffett, Chris Putnam, Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit RSA modulus. To appear in: Proceedings of Eurocrypt 2000.

[78] Ann Cavoukian. Identity theft: Who's using your name? Information and Privacy Commissioner of Ontario, Canada, June 1997.

[79] Ann Cavoukian, Catherine Johnston, and David Duncan. Smart, optical and other advanced cards: How to do a privacy assessment. Joint report of the Information and Privacy Commissioner of Ontario and the Advanced Card Technology Association of Canada, 1996.

[80] CCITT. Recommendation X.500: The directory–overview of concepts, models and services, 1988.

[81] CCITT. Recommendation X.501: The directory–models, 1988.

[82] Center for Democracy and Technology. Policy vs. practice; a progress report on federal government privacy notice on the world wide web, April 1999.

[83] Center for Public Integrity. Nothing sacred: The politics of privacy, July 1998. ISBN: 1882583-12-4.

[84] M. Cerecedo, T. Matsumoto, and H. Imai. Efficient and secure multiparty generation of digital signatures based on discrete logarithms. *IEICE Trans. Fundamentals E76-A(4)*, pages 532–545, April 1993.

[85] Certicom. The elliptic curve cryptosystem for smart cards. Whitepaper no. 7, May 1998.

[86] B. Chalks. Privacy enhancement for Internet electronic mail – part IV: Key certification and related services. RFC 1424-C, February 1993.

[87] D. Chaum. Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology–AUSCRYPT '90*, volume 453 of *Lecture Notes in Computer Science*, pages 246–264. Springer-Verlag, 1990.

[88] D. Chaum. Achieving electronic privacy. *Scientific American*, 267(2):96–101, August 1992.

[89] D. Chaum, C. Crepeau, and I. Damgård. Multi-party unconditionally secure protocols. In *Proc. 20th ACM Symp. on Theory of Computing*, pages 11–19, Chicago, 1988. ACM Press.

[90] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 319–327. Springer-Verlag, 1988.

[91] David Chaum. Blind signatures for untraceable payments. In R.L. Rivest, A. Sherman, and D. Chaum, editors, *Advances in Cryptology–CRYPTO '82*, pages 199–203. Plenum Press, 1983.

[92] David Chaum. Blind signature system. In D. Chaum, editor, *Advances in Cryptology–CRYPTO '83*, page 153, New York, 1984. Plenum Press.

[93] David Chaum. Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.

[94] David Chaum. Blind signature systems. U.S. Patent ser. no. 4,759,063, July 1988. Filed August 1983.

[95] David Chaum. Blind unanticipated signature systems. U.S. Patent ser. no. 4,759,064, July 1988. Filed October 1985.

[96] David Chaum. Privacy protected payments: Unconditional payer and/or payee untraceability. In D. Chaum and I. Schaumüller-Bichl, editors, *SMART CARD 2000*, pages 69–93. Elsevier Science Publishers B.V. (North-Holland), 1989.

[97] David Chaum. Card-computer moderated systems. U.S. Patent ser. no. 4,926,480, May 1990. Filed May 1988.

[98] David Chaum. One-show blind signature systems. U.S. Patent ser. no. 4,987,593, January 1991. Filed April 1990. Continuation of abandoned application Ser. No. 07/168,802, filed March 1988.

[99] David Chaum. Selected-exponent signature systems. U.S. Patent ser. no. 4,996,711, February 1991. Filed June 1989.

[100] David Chaum. Unpredictable blind signature systems. U.S. Patent ser. no. 4,991,210, February 1991. Filed May 1989.

[101] David Chaum. Zero-knowledge undeniable signatures. In I.B. Damgård, editor, *Advances in Cryptology–EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 458–464. Springer-Verlag, 1991.

[102] David Chaum. Designated-confirmer signature systems. U.S. Patent ser. no. 5,373,558, December 1994. Filed May 1993.

[103] David Chaum. Optionally moderated transaction systems. U.S. Patent ser. no. 5,276,736, January 1994. Filed July 1992.

[104] David Chaum. David Chaum on electronic commerce: How much do you trust Big Brother? *IEEE Internet Computing*, pages 8–16, November 1997.

[105] David Chaum. Limited-traceability systems. U.S. Patent ser. no. 5,712,913, January 1998. Filed February 1994.

[106] David Chaum, Ivan B. Damgård, and Jeroen van de Graaf. Multiparty computations ensuring privacy of each party's input and correctness of the result. In Carl Pomerance, editor, *Advances in Cryptology–CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 87–119. Springer-Verlag, 1988.

[107] David Chaum and Jan-Hendrik Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In A.M. Odlyzko, editor, *Advances in Cryptology–CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 118–168. Springer-Verlag, 1987.

[108] David Chaum, Jan-Hendrik Evertse, and Jeroen van de Graaf. An improved protocol for demonstrating possession of a discrete logarithm and some generalizations. In D. Chaum and W.L. Price, editors, *Advances in Cryptology–EUROCRYPT '87*, volume 304 of *Lecture Notes in Computer Science*, pages 127–141. Springer-Verlag, 1987.

[109] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology–CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer-Verlag, 1992.

[110] David Chaum and Hans van Antwerpen. Undeniable signatures. In G. Brassard, editor, *Advances in Cryptology–CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 212–216, 1990.

[111] David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. Technical report, University of Karlsruhe, February 1991. Interner Bericht 1/91.

[112] David Chaum, Eugène van Heijst, and Birgit Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. In J. Feigenbaum, editor, *Advances in Cryptology–CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 470–484. Springer-Verlag, 1992.

[113] Lidong Chen. Access with pseudonyms. In Ed Dawson and Jovan Golic, editors, *Cryptography: Policy and Algorithms*, number 1029 in Lecture Notes in Computer Science, pages 232–243. Springer-Verlag, 1995.

[114] S. Chokhani and W. Ford. Internet public key infrastructure certificate policy and certification practices framework. Internet Draft of the PKIX Working Group, work in progress, September 1997.

[115] Yang-hua Chu, Philip DesAutels, Brian LaMacchia, and Peter Lipp. PICS signed labels (DSig) 1.0 specification. W3C Recommendation, May 1998.

[116] Yang-hua Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust management for Web applications. *World Wide Web Journal*, 2:127–139, 1997.

[117] Roger Clarke. Chip-based ID: Promise and peril. Invited Address to a Workshop on 'Identity cards, with or without microprocessors: Efficiency versus confidentiality', at the International Conference on Privacy, Montreal, 23-26 September 1997.

[118] Roger Clarke. Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), February 1999. Version of 14 October 1998.

[119] J. Cohen and M. Fischer. A robust and verifiable cryptographically secure election scheme. In *Proceedings of 26th Symposium on Foundations of Computer Science*, pages 372–382, New York, October 1985. IEEE Computer Society.

[120] Chris Connolly. Smart cards: Big Brother's little helpers. Technical Report 66, Privacy Committee of New South Wales, August 1995. Also in: First Australian Computer Money Day, Newcastle, March 28, 1996.

[121] M.J. Coster. Some algorithms on addition chains and their complexity. Technical Report CS-R9024, Centrum voor Wiskunde en Informatica, June 1990.

[122] R.J.F. Cramer and T.P. Pedersen. Improved privacy in wallets with observers. In Tor Helleseth, editor, *Advances in Cryptology–EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 329–343. Springer-Verlag, 1994.

[123] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Yvo G. Desmedt, editor, *Advances in Cryptology–CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer-Verlag, 1994.

[124] Ronald Cramer, Matthew Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority secret-ballot elections with linear work. In Ueli Maurer, editor, *Advances in Cryptology–EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 72–83. Springer-Verlag, 1996.

[125] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118. Springer-Verlag, 1997. Also in: European Transactions on Telecommunications, Vol. 8, No. 5., September/OCtober 1997, pages 481-490.

[126] I.B. Damgård. Payment systems and credential mechanisms with provable security against abuse by individuals. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 328–335. Springer-Verlag, 1988.

[127] Ivan Bjerre Damgård. Practical and provably secure release of a secret. In Tor Helleseth, editor, *Advances in Cryptology–EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 200–217. Springer-Verlag, 1994.

[128] George Davida, Yair Frankel, Yiannis Tsiounis, and Moti Yung. Anonymity control in e-cash systems. In Rafael Hirschfeld, editor, *Financial Cryptography '97*, volume 1318. Springer-Verlag, February 1997.

[129] Simon Davies. Europe plans huge spy web. Telegraph Online, January 7, 1999.

[130] Simon Davies. Europe to U.S.: No privacy, no trade. *Wired magazine*, May 1998.

[131] Dorothy E. Denning. Descriptions of key escrow systems. Companion document to [132]. Version of February 26, 1997.

[132] Dorothy E. Denning and Dennis K. Branstad. A taxonomy for key recovery encryption systems. Version of May 11, 1997. Revision of "A Taxonomy of Key Escrow Encryption," Communications of the ACM, Vol. 39, No. 3, March 1996, pages 34–40.

[133] Department of Commerce of the National Telecommunications and Information Administration. Elements of effective self regulation for protection of privacy. *Federal Register*, 63(108):30729–30732, June 1998. Draft discussion paper.

[134] Yvo Desmedt. Major security problems with the "unforgeable" (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In *SecuriCom '88, SEDEP Paris*, pages 15–17, 1988.

[135] Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In Carl Pomerance, editor, *Advances in Cryptology–CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 16–20. Springer-Verlag, 1988.

[136] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-11(6):644–654, November 1976.

[137] Directorate-General XIII of the European Commission. Ensuring security and trust in electronic communication; towards a European framework for digital signatures and encryption. Communication to the European Parliament,

the Council, the Economic and Social Committee and the Committee of the Regions. COM (97) 503, October 1997.

[138] DoD Public Key Infrastructure Program Management Office. Public Key Infrastructure roadmap for the Department of Defense. Version 3.0, October 1999.

[139] DoD Public Key Infrastructure Program Management Office. X.509 Certificate Policy for the Department of Defense. Version 5.0, December 1999.

[140] S. Dusse, P. Hoffman, B. Ramsdell, and J. Weinstein. S/MIME version 2 certificate handling. Network Working Group, Request for Comments no. 2312, March 1998.

[141] S. Dusse, P. Hoffman, R. Ramsdell, L. Lundblade, and L. Repka. S/MIME version 2 message specification. Network Working Group, Request for Comments no. 2311, March 1998.

[142] Cynthia Dwork, Jeffrey Lotspiech, and Moni Naor. Digital signets: Self-enforcing protection of digital information. In *Proc.* 28*th ACM Symp. on Theory of Computing*. ACM Press, 1996.

[143] Electronic Privacy Information Center. Surfer beware: Personal privacy and the Internet, June 1997.

[144] Electronic Privacy Information Center. Surfer beware II: Notice is not enough, June 1998.

[145] Electronic Surveillance Task Force. Communications privacy in the digital age. Interim Report of the Digital Privacy and Security Working Group, June 1997.

[146] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31:469–472, July 1985.

[147] Carl Ellison. Establishing identity without certification authorities. 6th USENIX Security Symposium, San Jose, July 1996.

[148] Carl Ellison and Bruce Schneier. Ten risks of PKI: What you're not being told about Public Key Infrastructure. *Computer Security Journal*, 16(1), 2000.

[149] Carl M. Ellison. What do you need to know about the person with whom you are doing business? Written testimony before the House of Science and Technology Subcommittee Hearing on "Signatures in a Digital Age", October 1997.

[150] Carl M. Ellison. SPKI requirements. Internet draft, October 1998.

[151] Carl M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian M. Thomas, and Tatu Ylonen. SPKI certificate theory. Internet draft, work in progress, November 1998.

[152] Carl M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian M. Thomas, and Tatu Ylonen. Simple Public Key Certificate. Internet draft, work in progress, 1998.

[153] EPIC and Privacy International. Privacy and human rights: An international survey of privacy laws and practice. Released by Global Internet Liberty Campaign. Primary authors: David Banisar and Simon Davies, October 1998.

[154] Richard A. Epstein. Testimony before the Senate Judiciary Subcommittee on the Constitution, Federalism and Property Rights. Hearings on “Privacy in the Digital Age: Encryption and Mandatory Access”, March 1998.

[155] European Commission. Report of the Working Party on Illegal and Harmful Content on the Internet, November 1996.

[156] European Commission. A European initiative in electronic commerce. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, April 1997. COM(97) 157.

[157] European Parliament. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, pages 31–45, November 1995.

[158] Carol H. Fancher. Smart cards: As potential applications grow, computers in the wallet are making unobtrusive inroads. *Scientific American*, pages 40–45, August 1996.

[159] Federal Bureau of Investigation. The Digital Telephony and Privacy Improvement Act, March 1994.

[160] Federal Bureau of Investigation. The Digital Telephony and Privacy Improvement Act (update), June 1994.

[161] Federal Card Services Task Force. Federal smart card implementation plan; ”the future is in the cards”. Electronic Processes Initiatives Committee, January 1998.

[162] Federal Deposit Insurance Corporation. Online privacy of consumer personal information, August 1998.

[163] Federal Public Key Infrastructure Steering Committee. Access with trust. Government Information Technology Services Board, Office of Management and Budget, September 1998.

[164] Federal Trade Commission. Consumer Identity Fraud meeting. Official Transcript Proceedings before the Federal Trade Commission, August 1996. Washington, D.C.

[165] Federal Trade Commission. Privacy online: A report to Congress, June 1998.

[166] Federation of European Direct Marketing. Codes of practice, direct marketing and on-line services, November 1997.

[167] Jalal Feghhi, Peter Williams, and Jalil Feghhi. *Digital Certificates : Applied Internet Security*. Addison-Wesley, October 1998. ISBN 0201309807.

[168] Uriel Feige, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[169] Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. In *Proc. 22nd ACM Symp. on Theory of Computing*, pages 416–426, May 1990.

[170] Uriel Feige and Adi Shamir. Zero-knowledge proofs of knowledge in two rounds. In G. Brassard, editor, *Advances in Cryptology–CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 526–544. Springer-Verlag, 1990.

[171] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A.M. Odlyzko, editor, *Advances in Cryptology–CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer-Verlag, 1987.

[172] Warwick Ford and Michael Baum. *Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption*. Prentice Hall, April 1997. ISBN: 0134763424.

[173] Yair Frankel, Yiannis Tsiounis, and Moti Yung. "Indirect discourse proofs": Achieving efficient fair off-line e-cash. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology–ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 286–300. Springer-Verlag, 1996.

[174] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The SSL protocol, version 3.0. Internet draft, Netscape Communications, November 1996.

[175] Richard L. Fricker. The INSLAW octopus, March 1993.

[176] A. Michael Froomkin. It came from Planet Clipper: The battle over cryptographic key ”escrow”. Page 15 of the 1996 Law of Cyberspace issue of the University of Chicago Legal Forum.

[177] A. Michael Froomkin. The essential role of trusted third parties in electronic commerce. *Oregon Law Review*, 75(1):49–115, 1996.

[178] E. Fujisaki and Tatsuaki Okamoto. Practical escrow cash system. In *Proceedings of the 1996 Cambridge Workshop on Security Protocols*, pages 33–48. Springer-Verlag, June 1996.

[179] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO ’97*, volume 1294 of *Lecture Notes in Computer Science*, pages 16–30. Springer-Verlag, 1997.

[180] Simson Garfinkel. The downside of digital IDs. Hotwired, October 9, 1996.

[181] Simson L. Garfinkel. 2048: Privacy, identity, and society in the next century. Unpublished book, 1997.

[182] Dan Geer. Risk management is where the money is. *Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy*, 20(6), November 1998.

[183] General Accounting Office. Identity fraud: Information on prevalence, cost, and Internet impact is limited. Briefing Report, May 1998. GAO/GGD-98-100BR.

[184] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Robust threshold DSS signatures. In N. Koblitz, editor, *Advances in Cryptology–CRYPTO ’96*, volume 1109 of *Lecture Notes in Computer Science*, pages 354–371. Springer-Verlag, 1996.

[185] Marc Girault. Self-certified public keys. In D.W. Davies, editor, *Advances in Cryptology–EUROCRYPT ’91*, volume 547 of *Lecture Notes in Computer Science*, pages 490–497. Springer-Verlag, 1992.

[186] Beth Givens. Identity theft – how it happens, its impact on victims, and legislative solutions. Presentation of the Privacy Rights Clearinghouse, May 1997.

[187] Brian Gladman, Carl Ellison, and Nicholas Bohm. Digital signatures, certificates & electronic commerce. Version 1.1, June 1999.

[188] Global Network Navigator. The seduction of Crypto AG: How the NSA held the keys to a top-selling encryption machine, 1997.

[189] Ian Goldberg and Adam Shostack. Freedom network 1.0 architecture. Zero-Knowledge Systems, Inc. white paper, November 1999.

[190] Ian Goldberg, David Wagner, and Eric A. Brewer. Privacy-enhancing technologies for the Internet. In *COMPCON '97*. IEEE, February 1997.

[191] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(1):691–729, 1991.

[192] Oded Goldreich, Birgit Pfitzmann, and Ronald L. Rivest. Self-delegation with controlled propagation - or - what if you lose your laptop. In Hugo Krawczyk, editor, *Advances in Cryptology–CRYPTO '98*, Lecture Notes in Computer Science, pages 153–168. Springer-Verlag, 1998.

[193] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989.

[194] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988.

[195] David Goodman and Colin Robbins. Understanding LDAP & X.500. Distributed by the European Electronic Messaging Association, Version 2.0, August 1997.

[196] Daniel M. Gordon. A survey of fast exponentiation methods. *Journal of Algorithms*, 27:129–146, April 1998.

[197] J. Orlin Grabbe. The White House “Big Brother” data base & how Jackson Stephens precipitated a banking crisis, 1997.

[198] Group of Experts on Information Security and Privacy. Draft background report for the ministerial declaration in the protection of privacy on global networks. Background report for the OECD Ministerial Conference on 7-9 October 1998 in Ottawa, Canada, September 1998.

[199] Group of Experts on Information Security and Privacy. Draft ministerial declaration on the protection of privacy on global networks. Scheduled for transmission to the OECD Ministerial Conference of 7–9 October 1998 in Ottawa, Canada, September 1998.

[200] Richard A. Guida. Truth about PKI isn't always common knowledge. GCN Spotlight, May 3, 1999.

[201] Louis C. Guillou and Jean-Jacques Quisquater. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. In C.G. Günther, editor, *Advances in Cryptology–EUROCRYPT '88*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128. Springer-Verlag, 1988.

[202] Louis Claude Guillou and Jean-Jacques Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 216–231. Springer-Verlag, 1988.

[203] C. Gülcü and G. Tsudik. Mixing email with Babel. Symposium on Network and Distributed System Security, San Diego, February 1996.

[204] Peter Gutmann. How to recover private keys for Microsoft Internet Explorer, Internet Information Server, Outlook Express, and many others - or - where do your encryption keys want to go today?, 1997.

[205] John Hagel and Mark Singer. *Net Worth: Shaping Markets When Customers Make the Rules*. Harvard Business Press, 1999.

[206] Nicky Hager. Exposing the global surveillance system. *CovertAction Quarterly*, pages 11–17, 1996.

[207] Nicky Hager. *Secret Power - New Zealand's Role in the International Spy Network*. Craig Potton Publishing, Nelson, New Zealand, 1996.

[208] J. Håstad, A.W. Schrift, and A. Shamir. The discrete logarithm modulo a composite hides O(n) bits. *JCSS*, 47(3):376–404, 1993.

[209] Pat Hensley, Max Metral, Upendra Shardanand, Donna Converse, and Mike Myers. Proposal for an Open Profiling Standard. Submitted to W3C, June 1997.

[210] I.N. Herstein. *Topics in Algebra*. John Wiley & Sons, New York, 2 edition, 1975. ISBN 0-471-02371-X.

[211] Austin Hill and Gus Hosein. The privacy risks of public key infrastructures. Presented at the 21st Data Protection Commissioner's Conference in Hong Kong, September 13, 1999.

[212] Robert Holmes. Privacy: Philosophical foundations and moral dilemmas. In *Proceedings of the 16th International Conference on Data Protection–Facing Dilemmas*, September 1994.

[213] John D. Howard. *An Analysis Of Security Incidents On The Internet, 1989 – 1995*. PhD thesis, Carnegie Mellon University, April 1997.

[214] P. J. Hustinx. Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS). Adopted by the Data Protection Working Party of the European Union on 16 June, 1998.

[215] Computer Security Institute. 1998 computer crime and security survey. Conducted by CSI with the participation of the San Francisco office of the FBI's International Computer Crime Squad, March 1998.

[216] International Telecommunication Union. ITU-T recommendation X.509, information technology – open systems interconnection – the directory: Authentication framework, June 1997.

[217] International Working Group on Data Protection in Telecommunications. Data protection and privacy on the Internet – report and guidance. Adopted at the 20th Meeting in Berlin ("Budapest - Berlin Memorandum"), November 1996.

[218] ITU & ISO/IEC. Working document on amendments for certificate extensions, January 1998. Collaborative meeting on the Directory, Phoenix Arizona.

[219] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Ueli Maurer, editor, *Advances in Cryptology–EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 143–154. Springer-Verlag, 1996.

[220] Markus Jakobsson and Moti Yung. Revokable and versatile electronic money. In *Third ACM Conference on Computer and Communications Security*, pages 76–87. ACM Press, 1996.

[221] Markus Jakobsson and Moti Yung. Applying anti-trust policies to increase trust in a versatile e-money system. Financial Cryptography '97, February 1997.

[222] Markus Jakobsson and Moti Yung. Distributed "magic ink" signatures. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 450–464. Springer-Verlag, 1997.

[223] Don Johnson and Alfred Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, University of Waterloo, Canada, Dept. of C&O, August 1999.

[224] Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 150–164. Springer-Verlag, 1997.

[225] Burt Kaliski and Matt Robshaw. The secure use of RSA. *CryptoBytes*, 2(3), 1995.

[226] C. Kaufman. DASS - distributed authentication security service. Network Working Group, Request for Comments no. 1507, September 1993.

[227] Jane Kaufman Winn. Couriers without luggage: Negotiable instruments and digital signatures. *South Carolina Law Review*, 49(4), 1998.

[228] Jane Kaufman Winn and Carl Ellison. Regulating the use of electronic authentication procedures by US consumers in the global electronic marketplace. Comment P994312 to the Federal Trade Commission, March 1999.

[229] John Kelsey, Bruce Schneier, and David Wagner. Protocol interactions and the chosen protocol attack. Security Protocols Workshop, Cambridge, 1997.

[230] S. Kent. Privacy enhancement for Internet electronic mail – part II: Certificate-based key management. RFC 1422, February 1993.

[231] Anthony L. Kimery. Big Brother wants to look into your bank account. Wired Magazine, December 1993.

[232] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*, pages 441–462. Addison-Wesley Publishing Company, 2 edition, 1981. ISBN 0-201-03822-6.

[233] N. Koblitz. A family of Jacobians suitable for discrete log cryptosystems. In S. Goldwasser, editor, *Advances in Cryptology–CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 94–99. Springer-Verlag, 1988.

[234] Neil Koblitz. Elliptic curve implementation of zero-knowledge blobs. *Journal of Cryptology*, 4(3):207–213, 1991.

[235] Paul Kocher. Quick introduction to Certificate Revocation Trees (CRTs). ValiCert whitepaper, 1997.

[236] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. In N. Koblitz, editor, *Advances in Cryptology–CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer-Verlag, 1996.

[237] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology–CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.

[238] Loren M. Kohnfelder. Towards a practical public-key cryptosystem. Master's thesis, MIT Laboratory for Computer Science, May 1978.

[239] Oliver Kömmerling and Markus G. Kuhn. Design principles for tamper-resistant smartcard processors. In *Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99)*, pages 9–20. USENIX Association, May 1999. ISBN 1-880446-34-0.

[240] David W. Kravitz, Peter S. Gemmell, and Ernest F. Brickell. Off-line compatible electronic cash method and system. U.S. Patent ser. no. 5,832,089, November 1998. Filed June 1995.

[241] Hugo Krawczyk and Tal Rabin. Chameleon hashing and signatures, September 1997.

[242] Markus Kuhn. Sicherheitsanalyse eines Mikroprozessors mit Busverschlüsselung. Master's thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, July 1996.

[243] Art Kunkin. The Octopus Conspiracy: Has the U.S. been spying on your bank accounts? World Wide Free Press, 1996.

[244] L. Lamport. Constructing digital signatures from a one-way function. Technical Report CSL–98, SRI International, October 1979.

[245] Peter Lenoir. Timing attack on classical RSA using Montgomery multiplications. Rump session of CRYPTO '97, August 1997.

[246] Arjen K. Lenstra and Adi Shamir. Analysis and optimization of the TWINKLE factoring device. To appear in: Proceedings of Eurocrypt 2000.

[247] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. Proceedings of the 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC2000), Melbourne, Australia, January 2000. An earlier version appeared in: PricewaterhouseCoopers Cryptographic Centre of Excellence (CCE) Quarterly Journal, autumn '99 issue.

[248] Garby Leon. Inslaw, the continuing caper, 1996.

[249] Lawrence Lessig and Paul Resnick. The constitutionality of mandated access control: A model. Circulating Draft 4, April 14, 1999. Earlier version in: Proceedings of the Telecommunications Policy Research Conference (1998).

[250] R. Levien and A. Aiken. Attack resistant trust metrics for public key certification. In *Proceedings of the 7th USENIX Security Symposium*. USENIX Press, January 1998.

[251] Jamie Lewis. Public Key Infrastructure architecture. The Burton Group, Network Strategy Report, July 1997.

[252] Chae Hoon Lim and Pil Joong Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Burton S. Kaliski Jr., editor, *Advances in Cryptology–CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 249–263. Springer-Verlag, 1997.

[253] Anna Lysyanskaya, Ronald Rivest, Amit Sahai, and Stefan Wolf. Pseudonym systems. To appear in: Proceedings of SAC 99, 1999.

[254] Wayne Madsen. Crypto AG: The NSA's Trojan Whore? CovertAction Quarterly, Winter 1998, no. 63.

[255] Gary T. Marx. Privacy and technology. Revision of paper in The World and I, September 1990 and Telektronik January 1996.

[256] Masons Sollicitors and Privy Council Agents. Handbook on cost effective compliance with Directive 95/46/EC, 1998.

[257] MasterCard & Visa. SET secure electronic transaction specification, version 1.0. Book 1: Business Description, Book 2: Programmer's Guide, Book 3: Formal Protocol Definition, May 1997.

[258] Ueli M. Maurer and Stefan Wolf. Diffie-Hellman oracles. In N. Koblitz, editor, *Advances in Cryptology–CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 268–282. Springer-Verlag, 1996.

[259] Kevin S. McCurley. The discrete logarithm problem. In *Proc. of Symposia in Applied Mathematics: Cryptography and Computational Number Theory*, volume 42, pages 49–74. American Mathematical Society, August 1990.

[260] P. D. McDaniel and S. Jamin. Windowed certificate revocation. Technical Report Technical Report CSE-TR-413-99, Dept. of Electrical Engineering and Computer Science, University of Michigan, November 1999. Also in: Proceedings of IEEE Infocom 2000. IEEE, March 2000. Tel Aviv, Israel.

[261] P. D. McDaniel and A. Rubin. A response to 'can we eliminate certificate revocation lists?'. Technical Report Technical Report 99.8.1, AT&T Research Labs, 1999. Also in: Financial Cryptography 2000, February 2000, Anguilla.

[262] Niall McKay. Europe is listening. Wired News, December 2, 1998.

[263] A.J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, New York, 1993.

[264] Alfred Menezes. Elliptic curve cryptosystems. *RSA Laboratories*, 1(2), 1995. CryptoBytes.

[265] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proc. 23rd ACM Symp. on Theory of Computing*, pages 80–89, New Orleans, 1991. ACM Press.

[266] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, New York, 1997.

[267] Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology–CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. Springer-Verlag, 1988.

[268] Silvio Micali. Efficient certificate revocation. Technical Report TM-542, Laboratory of Computer Science, Massachusetts Institute of Technology, November 1995.

[269] Silvio Micali and Leonid Reyzin. Signing with partially adversarial hashing. MIT Laboratory for Computer Science, Februari 27, 1998.

[270] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. Internet public key infrastructure Online Certificate Status Protocol – OCSP. IETF Draft, August 1998.

[271] David Naccache, David M'Raïhi, Serge Vaudenay, and Dan Raphaeli. Can D.S.A. be improved? – complexity trade-offs with the digital signature standard. In Alfredo De Santis, editor, *Advances in Cryptology–EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 77–85. Springer-Verlag, 1995.

[272] Yasushi Nakayama, Hidemi Moribatake, Masayuki Abe, and Eichiro Fujisaki. An electronic money scheme; a proposal for a new electronic money scheme which is both secure and convenient. IMES Discussion paper series, Bank of Japan, June 1997. Discussion Paper No. 97-E-4.

[273] Moni Naor and Kobbi Nissim. Certificate revocation and certificate update. Technical report, Weizmann Institute of Science, January 1999. Preliminary version in: Proceedings of the 7th USENIX Security Symposium, 1998.

[274] Nathan Associates Inc. The cost of government-driven key escrow encryption, June 1998. Prepared by the Family, Industry, and Community Economics group, and commissioned by the Business Software Alliance.

[275] National Institute of Standards and Technology. FIPS PUB 140-2: Security requirements for cryptographic modules. Federal Information Processing Standard Publication, U.S. Department of Commerce, January 11, 1994. (Supersedes FIPS PUB 140-1 of January 1994).

[276] National Institute of Standards and Technology. Secure hash standard (SHA), April 1995. Federal Information Processing Standards Publication, FIPS PUB 180-1.

[277] National Institute of Standards and Technology. Digital signature standard (DSS). Federal Information Processing Standards Publication, FIPS PUB 186-1, December 1998.

[278] National Research Council. Cryptography's role in securing the information society. Prepublication copy, May 1996. Kenneth Dam and Herbert Lin, Editors.

[279] National Security Agency. Threat and vulnerability model for key recovery. Unofficial NSA document, February 18, X3, 1998.

[280] L. O'Connor. An analysis of exponentiation based on formal languages. In Jacques Stern, editor, *Advances in Cryptology–EUROCRYPT '99*, Lecture Notes in Computer Science. Springer, 1999.

[281] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology–EUROCRYPT '84*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314. Springer-Verlag, 1985.

[282] Andrew Odlyzko. Discrete logarithms: The past and the future. Version of July 18, 1999. To appear in: Designs, Codes, and Cryptography (1999).

[283] Andrew M. Odlyzko. The future of integer factorization. Technical Report 2, RSA Laboratories, July 1995.

[284] Office of Technology Assessment. Federal government information technology: Electronic surveillance and civil liberties. U.S. Congress, Office of Technology Assessment, OTA-CIT-293, Washington, DC: U.S. Government Printing Office, October 1985.

[285] Office of Technology Assessment. Electronic record systems and individual privacy, June 1986. OTA-CIT-296 (Washington, DC: U.S. Government Printing Office).

[286] Office of Technology Assessment. Electronic surveillance in a digital age, July 1995. OTA-BP-ITC-149 (Washington, DC: U.S. Government Printing Office).

[287] Office of the Privacy Commissioner of Canada. Privacy framework for smart card applications, July 1996.

[288] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, *Advances in Cryptology–CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer-Verlag, 1992.

[289] Tatsuaki Okamoto and Kazuo Ohta. Divertible zero knowledge interactive proofs and commutative random self-reducibility. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology–EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 134–149. Springer-Verlag, 1989.

[290] Lewis Willian Oleinick. *Computerized Governmental Database Systems containing Personal Information and the Right to Privacy*. PhD thesis, University of Texas at Austin, December 1993.

[291] OMB Watch. A delicate balance: The privacy and access practices of federal government World Wide Web sites, June 1998. ISBN: 1882583-12-4.

[292] Paul Van Oorschot, Warwick Ford, Stephen Hillier, and Josanne Otway. Method for efficient management of Certificate Revocation Lists (CRLs) and update information. U.S. Patent ser. no. 5,699,431, December 1997. Filed November 1995.

[293] OpenCard Consortium. OpenCard framework general information web document. IBM Germany, October 1998. Second Edition.

[294] Organisation for Economic Co-operation and Development. Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal information, September 1980.

[295] Organisation for Economic Co-operation and Development. Cryptography policy guidelines, March 1997.

[296] Organisation for Economic Co-operation and Development. Inventory of approaches to authentication and certification in a global networked society. Document of the Working Party on Information Security and Privacy, October 1999.

[297] PC/SC Workgroup. Interoperability specification for ICCs and personal computer systems, part 1–8. Revision 1.0, December 1997.

[298] Torben Pryds Pedersen. *Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem*. PhD thesis, Aarhus University, March 1992. DAIMI PB–388.

[299] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology–CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140. Springer-Verlag, 1992.

[300] Radia J. Perlman and Charles Kaufman. Method of issuance and revocation of certificates of authenticity used in public key networks and other systems. U.S. Patent ser. no. 5,261,002, November 1993. Filed March 1992.

[301] Birgit Pfitzmann. *Fail-Stop Signature Schemes*. PhD thesis, Institut für Informatik, Universität Hildesheim, May 1994.

[302] Birgit Pfitzmann and Ahmad-Reza Sadeghi. Self-escrowed cash against user blackmailing. 4th International Conference on Financial Cryptography (FC '00), to be published by Springer-Verlag, February 2000. An earlier German version appeared in: Verlässliche IT-Systeme, GI-Fachtagung VIS '99.

[303] Birgit Pfitzmann and Michael Waidner. How to break and repair a "provably secure" untraceable payment system. In J. Feigenbaum, editor, *Advances in Cryptology–CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 338–350. Springer-Verlag, 1992.

[304] Birgit Pfitzmann and Michael Waidner. Strong loss tolerance of electronic coin systems. *ACM Transactions on Computer Systems*, 15(2):194–213, May 1997. Extended version appeared as: Hildesheimer Informatik-Berichte 15/95, University of Hildesheim, June 1995.

[305] David Pointcheval. *Les Preuves de Connaissance et leurs Preuves de S écurité*. PhD thesis, University of Caen, December 1996.

[306] David Pointcheval and Jacques Stern. Provably secure blind signature schemes. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology–ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 252–265. Springer-Verlag, 1996.

[307] David Pointcheval and Jacques Stern. Security proofs for signature schemes. In Ueli Maurer, editor, *Advances in Cryptology–EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398. Springer-Verlag, 1996.

[308] Patrick S. Poole. Echelon: America's spy in the sky. Fourth installment in the Free Congress Foundation/Center for Technology Policy's The Privacy Papers series, October 1998.

[309] Guillaume Poupard and Jacques Stern. Generation of shared RSA keys by two parties. In *Advances in Cryptology–ASIACRYPT '91*, volume 1514 of *Lecture Notes in Computer Science*, pages 11–24. Springer-Verlag, 1998.

[310] Guillaume Poupard and Jacques Stern. Security analysis of a practical “on the fly” authentication and signature generation. In Kaisa Nyberg, editor, *Advances in Cryptology–EUROCRYPT ’98*, volume 1403 of *Lecture Notes in Computer Science*, pages 422–436. Springer-Verlag, 1998.

[311] Privacy Commissioner of the Commonwealth of Australia. Smart cards: Implications for privacy. Information Paper No. 4, December 1995.

[312] Privacy International. Identity Cards: Frequently asked questions, August 1996.

[313] Privacy Working Group. Privacy and the National Information Infrastructure: Principles for providing and using personal information, June 1995. Publication of the Information Policy Committee of the Information Infrastructure Task Force.

[314] Public Interest Research Group. Mistakes do happen: Credit report errors mean consumers lose, March 1998.

[315] Charles D. Raab, Colin J. Bennett, Robert M. Gellman, and Nigel Waters. Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method of several categories of transfer - final report. Study carried out for the European Commission. Tender No. XV/97/18/D, September 1998.

[316] Cristian Radu, Rene Govaerts, and Joos Vandewalle. A restrictive blind signature scheme with applications to electronic cash. In P. Horster, editor, *Proceedings of the IFIP TC6/TC11 international conference on communications and multimedia security II*, pages 196–207. Chapman and Hall, 1996.

[317] Cristian Radu, Rene Govaerts, and Joos Vandewalle. Efficient electronic cash with restricted privacy. In Rafael Hirschfeld, editor, *Financial Cryptography ’97*, volume 1318. Springer-Verlag, February 1997.

[318] Joel R. Reidenberg and Paul M. Schwartz. Data protection law and on-line services: Regulatory responses. Study prepared as part of the project “Vie privée et sociétée de l information: Etude sur les problèmes posés par les nouveaux services en ligne en matière de protection des données et de la vie privée,” commissioned by Directorate General XV of the Commission of the European Communities, December 1998.

[319] Lawrence A. Reinert and Stephen C. Luther. Tokeneer; user authentication techniques using public key certificates. Part 1: Certificate options. National Security Agency, Central Security Service, R22 INFOSEC Engineering, December 1997.

[320] Lawrence A. Reinert and Stephen C. Luther. Tokeneer; authentication protocol for smartcards. National Security Agency, Central Security Service, R22 INFOSEC Engineering, January 1998.

[321] M. Reiter and S. Stubblebine. Toward acceptable metrics of authentication. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 10–20, Oakland, CA, May 1997. IEEE.

[322] Michael K. Reiter and Aviel D. Rubin. Crowds: Anonymity for Web transactions. ACM Transactions on Information and System Security, April 1998. Also as: DIMACS 95-15, June 1997, AT&T Labs–Research, Murray Hill, New Jersey.

[323] Ronald L. Rivest. Can we eliminate certificate revocation lists? In Rafael Hirschfeld, editor, *Financial Cryptography '98*, volume 1465, February 1998.

[324] Ronald L. Rivest and Butler Lampson. SDSI - a Simple Distributed Security Infrastructure. Working document defining SDSI version 1.1., October 1996.

[325] Ronald L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[326] Ronald L. Rivest and Robert D. Silverman. Are “strong” primes needed for RSA? Submitted draft, November 1998.

[327] Marc Rotenberg. Communications privacy. Prepared Statement Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, United States of House of Representatives, Washington, D.C., March 26, 1998.

[328] Marc Rotenberg. On the European Union Data Directive and Privacy. Testimony and Statement for the Record Before the Committee on International Relations, U.S. House of Representatives, May 7, 1998.

[329] Marc Rotenberg, editor. *The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments*. Electronic Privacy Information Center, 1998.

[330] RSA Laboratories. PKCS #6: Extended-certificate syntax standard. Version 1.5, November 1993.

[331] R. J. Rummel. *Death by Government: Genocide and Mass Murder in the Twentieth Century*. Transaction Publishers, New Jersey, 1994. ISBN: 1560009276.

[332] Dick Russell. Spook wars in cyberspace–is the FBI railroading Charles Hayes?, June 1997.

[333] Tomas Sander and Amnon Ta-Shma. Flow control: A new approach for anonymity control in electronic cash systems. In *Financial Cryptography '99*. Springer-Verlag, February 1999.

[334] Alfredo De Santis, Giovanni De Crescenzo, Giuseppe Persiano, and Moti Yung. On monotone formula closure of SZK. In *Proc. 35th IEEE Symp. on Foundations of Comp. Science*, pages 454–465, Santa Fe, 1994.

[335] T. Satoh and K. Arako. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Preprint, 1997.

[336] Bruce Schneier and Adam Shostack. Breaking up is hard to do: Modeling security threats for smart cards. First USENIX Symposium on Smart Cards, USENIX Press, 1999.

[337] Claus P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4:161–174, 1991.

[338] Claus P. Schnorr. Security of 2^t-root identification and signatures. In N. Koblitz, editor, *Advances in Cryptology–CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 143–156. Springer-Verlag, 1996.

[339] Claus P. Schnorr and Markus Jakobsson. Security of discrete log cryptosystems in the random oracle $+$ generic model. Presented at the Conference on The Mathematics of Public-Key Cryptography, The Fields Institute, Toronto, Canada, June 1999.

[340] Berry Schoenmakers. Efficient proofs of Or. Unpublished manuscript, September 1993.

[341] Berry Schoenmakers. An efficient electronic payment system withstanding parallel attacks. Technical Report CS-R9522, Centrum voor Wiskunde en Informatica, March 1995.

[342] Berry Schoenmakers. Sharp interval proofs and other predicates. Submitted for publication, February 1997.

[343] Ari Schwartz. Smart cards at the crossroads: Authenticator or privacy invader? *At Home With Consumers*, 19(3), December 1998.

[344] Scientific and Technological Options Assessment. An appraisal of technologies of political control. STOA Interim Study (PE 166.499), September 1998.

[345] Adi Shamir. Factoring large numbers with the TWINKLE device. EUROCRYPT '99 rump session talk. Extended abstract distributed on May 5, 1999.

[346] Adi Shamir. Identity-based cryptosystems and signature schemes. In G.R. Blakley and D.C. Chaum, editors, *Advances in Cryptology–CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1985.

[347] Adi Shamir. Memory efficient variants of public-key schemes for smart card applications. In Alfredo De Santis, editor, *Advances in Cryptology–EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 445–449. Springer-Verlag, 1995.

[348] Adi Shamir and Nicko van Someren. Playing hide and seek with stored keys. In *Financial Cryptography '99*. Springer-Verlag, February 1999.

[349] Jenny Shearer and Peter Gutmann. Government, cryptography, and the right to privacy. *Journal of Universal Computer Science*, 2(3), March 1996.

[350] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc.* 26*th ACM Symp. on Theory of Computing*, pages 124–134, Santa Fe, 1994. IEEE.

[351] Victor Shoup. On the security of a practical identification scheme. In Ueli Maurer, editor, *Advances in Cryptology–EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 344–353. Springer-Verlag, 1996.

[352] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology–EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer-Verlag, 1997.

[353] Robert D. Silverman. A cost-based security analysis of symmetric and asymmetric key lengths. *News and Advice Bulletin*, (13), April 2000.

[354] Gustavus J. Simmons. The Prisoners' Problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology–CRYPTO '83*, pages 51–67. Plenum Press, 1984.

[355] Gustavus J. Simmons. The subliminal channel and digital signature. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology–EUROCRYPT '84*, volume 209 of *Lecture Notes in Computer Science*, pages 364–378. Springer-Verlag, 1985.

[356] Solveig Singleton. Privacy as censorship – a skeptical view of proposals to regulate privacy in the private sector. *Cato Policy Analysis*, January 1998.

[357] Nigel Smart. The discrete logarithm problem on elliptic curves of trace one. Internal Note at Hewlett-Packard Laboratories, 1997.

[358] Smart Card Forum. Consumer privacy and smart cards - a challenge and an opportunity. Prepared by the Legal & Public Policy Committee, 1997.

[359] South African Law Commission. Review of security legislation; the Interception and Monitoring Prohibition Act (ACT no. 127 of 1992). Discussion Paper 78, Project 105, November 1998. ISBN 0-621-28847-0.

[360] Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch. Fair blind signatures. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology–EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 209–219. Springer-Verlag, 1995.

[361] Standards Australia. Strategies for the implementation of a Public Key Authentication Framework (PKAF) in Australia. PKAF Report, Miscellaneous Publication SAA MP75-1996, October 1996.

[362] Statewatch. European Union & FBI launch global surveillance system. Report, January 1997.

[363] Marc Strassman and Robert D. Atkinson. Jump-starting the digital economy (with department of motor vehicles-issued digital certificates). Policy Briefing of the Democratic Leadership Council & The Progressive Policy Institute, June 1999.

[364] Res Strehle. *Verschlüsselt - Der Fall Hans Beühler*. Werd Verlag, Zürich, 1994. U.S. Library of Congress #: DS318.84.B84S77 1994.

[365] S. Stubblebine. Recent-secure authentication: Enforcing revocation in distributed systems. In *Proceedings of the 1995 IEEE Symposium on Research in Security and Privacy*, pages 224–234, May 1995.

[366] Kathleen M. Sullivan. Testimony on behalf of Americans for Computer Privacy before the Senate Judiciary Subcommittee on the Constitution, Federalism and Property Rights. Hearings on “Privacy in the Digital Age: Encryption and Mandatory Access”, March 1998.

[367] Peter P. Swire. Financial privacy and the theory of high-tech government surveillance. Draft of September 24, 1998.

[368] Paul Syverson, D. Goldschlag, and M. Reed. Anynonymous connections and onion routing. In *Symposium on Security and Privacy*. IEEE, 1997.

[369] Kazuo Takaragi, Kunihiko Miyazaki, and Masashi Takahashi. A threshold digital signature issuing scheme without secret communication. Presented at the November 1998 meeting of the IEEE P1363 Working Group, November 1998.

[370] Task Force on Electronic Commerce. The protection of personal information – building Canada s information economy and society. Industry Canada/Justice Canada, January 1998.

[371] The Baltimore Sun. NSA's crypto sting. Issue of December 10, 1995.

[372] The Washington Weekly. NSA, CIA, and U.S. NAVY all use PROMIS software. Published in the March 31, 1997 issue.

[373] The Working Party on the Protection of Individuals with regard to the processing of personal data. Recommendation 3/97; anonymity on the Internet. Discussion paper adopted by the Working Party on 3 December 1997 at the 8th meeting.

[374] Yiannis S. Tsiounis. *Efficient Electronic Cash: New Notions and Techniques*. PhD thesis, Northeastern University, June 1997.

[375] United States Government. Privacy and electronic commerce. Draft, June 1998.

[376] U.S. Federal Reserve. Order approving notices to engage in nonbanking activities. Press release, November 10, 1999.

[377] U.S. General Services Administration. Access Certificates for Electronic Services (ACES). Draft Request for Proposals, Solicitation Number TIBA98003, Office of Governmentwide Policy, Federal Technology Service, March 1998.

[378] U.S. General Services Administration and Federal Telecommunications Service and Office of Information Security. Access Certificates for Electronic Services (ACES). Request For Proposals, January 1999.

[379] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4, 1985.

[380] E. van Heijst and T.P. Pedersen. How to make efficient fail-stop signatures. In R.A. Rueppel, editor, *Advances in Cryptology–EUROCRYPT '92*, volume 658 of *Lecture Notes in Computer Science*, pages 366–377. Springer-Verlag, 1993.

[381] Christine Varney. You call this self-regulation? Wired News, June 9, 1998.

[382] Eric R. Verheul and Marc P. Hoyle. Tricking the Chaum-Pedersen protocol. Submitted for publication, August 1997.

[383] J. von zur Gathen and M. Nöcker. Exponentiation in finite fields: Theory and practice. *Proc. AAECC-12*, pages 88–113, 1997. To appear in: Springer LNCS.

[384] S. S. Wagstaff Jr. Greatest of the least primes in arithmetic progression having a given modulus. *Mathematics of Computation*, 33(147):1073–1080, July 1979.

[385] M. Wahl. A summary of the X.500(96) user schema for use with LDAPv3. Network Working Group, Request for Comments no. 2256, December 1997.

[386] Gerard Walsh. Review of policy relating to encryption technologies. Publication suppressed by the Australian Attorney-General's Department in February 1997, censored version released to the Electronic Frontier Association under the Freedom of Information Act, June 1997.

[387] Alan Westin. *Privacy and Freedom*. New York: Atheneum, 1967.

[388] A. Wheeler and L. Wheeler. Internet Public Key Infrastructure: PKI Account Authority Digital Signature Infrastructure, November 1998.

[389] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36:553–558, 1990.

[390] Michael J. Wiener. Performance comparison of public-key cryptosystems. *CryptoBytes*, 4(1):1–5, 1998.

[391] Julie L. Williams. Remarks before the Banking Roundtable Lawyers Council, on the treatment of confidential customer information and privacy issues, Washington, D.C., May 8, 1998.

[392] Norman A. Willox. Identity theft: Authentication as a solution. National Fraud Center, Inc., March 2000.

[393] World Wide Web Consortium. Platform for Privacy Preferences (P3P) Syntax Specification. Second public W3C Working Draft, edited by M. Marchiori and D. Jaye, July 1998.

[394] Tom Wright. Smart cards. Publication of the Information and Privacy Commissioner of Ontario, April 1993.

[395] Eric C. Zimits and Christopher Montano. Public Key Infrastructure: Unlocking the Internet's economic potential. *IStory*, 3(2), April 1998. The Hambrecht and Quist Internet Research Group.

[396] Phil R. Zimmerman. *The Official PGP User's Guide*. MIT Press, Boston, 1995.