References

[ABC$^+$98] R. Anderson, F. Bergadano, B. Crispo, J. Lee, C. Manifavas, and R. Needham. A new family of authentication protocols. *ACM Operating Systems Review*, 32(4):9–20, October 1998.

[AG00] N. Asokan and Philip Ginzboorg. Key-agreement in ad-hoc networks. *Computer Communications*, 23(17):1627–1637, November 2000.

[ALN97] M. Abadi, T. Lomas, and R. Needham. Strengthening passwords. SRC Technical Note 1997 - 033, December, Systems Research Center, December 1997.

[AMS97] R. Anderson, C. Manifavas, and C. Sutherland. NetCard – a practical electronic cash system. In *Security Protocols—International Workshop*, volume 1189 of *Lecture Notes in Computer Science*, pages 49–57. Springer-Verlag, Berlin Germany, April 1997.

[AST98] G. Ateniese, M. Steiner, and G. Tsudik. Authenticated group key agreement and friends. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 17–26. ACM Press, November 1998. A journal version of this paper appeared later in JSAC [AST00].

[AST00] G. Ateniese, M. Steiner, and G. Tsudik. New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications*, 18(4):628–639, April 2000.

[Atk95] R. Atkinson (editor). IP encapsulating security payload (ESP). Internet Request for Comment RFC 1827, Internet Engineering Task Force, August 1995. obsoleted by [KA98a].

[Atm02] Secure Microcontrollers for SmartCards. `http://www.atmel.com/atmel/acrobat/1065s.pdf`, 2002.

[ATW97] N. Asokan, G. Tsudik, and M. Waidner. Server-supported signatures. *Journal of Computer Security*, 5(1):91–108, 1997.

[BC95] C. Blundo and A. Cresti. Space requirements for broadcast encryption. In *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 287–298. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1995.

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, October 1988.

[BCC00a] F. Bergadano, D. Cavagnino, and B. Crispo. Chained stream authentication. In *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000*, volume 2012 of *Lecture Notes in Computer Science*, pages 144–157. Springer-Verlag, Berlin Germany, August 2000.

[BCC00b] F. Bergadano, D. Cavalino, and B. Crispo. Individual single source authentication on the mbone. In *2000 IEEE International Conference on Multimedia and Expo, ICME 2000*, pages 541–544, August 2000. A talk containing this work was given at IBM T. J. Watson Research Laboratory, August 1998.

[BCH$^+$00] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes. PGP in constrained wireless devices. In *Proceedings of the 9th USENIX Security Symposium*, pages 247–261. USENIX, August 2000.

[BCK96] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 1–15. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1996.

[BCK97] M. Bellare, R. Canetti, and H. Krawczyk. HMAC: Keyed-hashing for message authentication. Internet Request for Comment RFC 2104, Internet Engineering Task Force, February 1997.

[BD93] M. Burmester and Y. Desmedt. Towards practical "proven secure" authenticated key distribution. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 228–231. ACM Press, November 1993.

[BD95] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 275–286. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1995.

[BD97] M. Burmester and Y. Desmedt. Efficient and secure conference key distribution. In *Security Protocols—International Workshop*, volume 1189 of *Lecture Notes in Computer Science*, pages 119–129. Springer-Verlag, Berlin Germany, April 1997.

[BDF01] D. Boneh, G. Durfee, and M. Franklin. Lower bounds for multicast message authentication. In *Advances in Cryptology – EUROCRYPT '2001*, volume

2045 of *Lecture Notes in Computer Science*, pages 434–450. Springer-Verlag, Berlin Germany, 2001.

[BDJR97] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. In *Proceedings of the 38th Symposium on Foundations of Computer Science (FOCS)*, pages 394–403. IEEE Computer Society Press, 1997.

[Bel00] S. Bellovin. The ICMP traceback message. `http://www.research.att.com/~smb`, 2000.

[Ber91] S. Berkovits. How to broadcast a secret. In *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 535–541. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1991.

[BFH$^+$00] J. Byers, M. Frumin, G. Horn, M. Luby, M. Mitzenmacher, A. Roetter, and W. Shaver. FLID-DL: Congestion control for layered multicast. In *Second International Workshop on Networked Group Communication (NGC 2000)*, Palo Alto, California, November 2000.

[BHK$^+$99] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. UMAC: Fast and secure message authentication. In *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 216–233. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1999.

[BLMR98] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege. A Digital Fountain approach to reliable distribution of bulk data. In *Proceedings of the ACM SIGCOMM '98 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pages 56–67, 1998.

[BM92] S. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 72–84. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 1992.

[BM93] S. Bellovin and M. Merritt. Augmented encrypted key exchange: A password-based protocol secure against dictionary atttacks and password file compromise. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 244–250. ACM Press, November 1993.

[BM94] D. Bleichenbacher and U. Maurer. Directed acyclic graphs, one-way functions and digital signatures. In *Advances in Cryptology – CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 75–82. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1994.

[BM96a] D. Bleichenbacher and U. Maurer. On the efficiency of one-time digital signatures. In *Advances in Cryptology – ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 196–209. Springer-Verlag, Berlin Germany, 1996.

[BM96b] D. Bleichenbacher and U. Maurer. Optimal tree-based one-time digital signature schemes. In *13th Symposium on Theoretical Aspects of Computer Science (STACS'96)*, volume 1046 of *Lecture Notes in Computer Science*, pages 363–374. Springer-Verlag, Berlin Germany, 1996.

[BMS96] C. Blundo, L. Mattos, and D. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. In *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 387–400. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1996.

[BMS99] D. Balenson, D. McGrew, and A. Sherman. Key management for large dynamic groups: One-way function trees and amortized initialization. Internet Draft, Internet Engineering Task Force, March 1999.

[BR93] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, November 1993.

[BR97] M. Bellare and P. Rogaway. Collision-resistant hashing: Towards making UOWHFs practical. In *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 470–484. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1997.

[Bra88] G. Brassard. *Modern Cryptology*, volume 325 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin Germany, 1988.

[Bri99] B. Briscoe. MARKS: Zero side-effect multicast key management using arbitrarily revealed key sequences. In *First International Workshop on Networked Group Communication*, pages 301–320, November 1999.

[BSUB98] M. Borella, D. Swider, S. Uludag, and G. Brewster. Internet packet loss: Measurement and implications for end-to-end QoS. In *1998 ICPP Workshop on Architectural and OS Support for Multimedia Applications Flexible Communication Systems*, pages 3–12. IEEE, August 1998.

[BW98] K. Becker and U. Wille. Communication complexity of group key distribution. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 1–6. ACM Press, November 1998.

[BW99] A. Biryukov and D. Wagner. Slide attacks. In *Proceedings of the 6th International Workshop on Fast Software Encryption*, volume 1636 of *Lecture*

Notes in Computer Science, pages 245–259. Springer-Verlag, Berlin Germany, March 1999.

[CEK$^+$99] I. Chang, R. Engel, D. Kandlur, D. Pendarakis, and D. Saha. Key management for secure internet multicast using boolean function minimization techniques. In *Proceedings IEEE Infocomm'99*, volume 2, pages 689–698, March 1999.

[CER97] CERT Coordination Center. CERT advisory CA-1997-28 IP denial-of-service attacks. Technical Report CA-1997-28, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, December 1997.

[CER01a] CERT Coordination Center. CERT advisory CA-2001-19 “Code Red” worm exploiting buffer overflow in IIS indexing service DLL. Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, July 2001.

[CER01b] CERT Coordination Center. CERT advisory CA-2001-23 continued threat of the “Code Red” worm. Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, July 2001.

[CGI$^+$99] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and some efficient constructions. In *INFOCOMM'99*, pages 708–716, March 1999.

[CGP01] N. Courtois, L. Goubin, and J. Patarin. Flash, a fast multivariate signature algorithm. In *Progress in Cryptology - CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 298–307. Springer-Verlag, Berlin Germany, April 2001.

[Che97] S. Cheung. An efficient message authentication scheme for link state routing. In *13th Annual Computer Security Applications Conference*, pages 90–98, 1997.

[CJ02] D. Coppersmith and M. Jakobsson. Almost optimal hash sequence traversal. In *Proceedings of the Fourth Conference on Financial Cryptography (FC '02)*, Lecture Notes in Computer Science. International Financial Cryptography Association (IFCA), Springer-Verlag, Berlin Germany, 2002.

[CMN99] R. Canetti, T. Malkin, and K. Nissim. Efficient communication-storage tradeoffs for multicast encryption. In *Advances in Cryptology – EUROCRYPT '99*, volume 1599 of *Lecture Notes in Computer Science*, pages 459–474. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1999.

[CRC00] R. Canetti, P. Rohatgi, and P. Cheng. Multicast data security transformations: Requirements, considerations, and prominent choices. Internet draft, Internet Engineering Task Force, 2000.

[CW79] L. Carter and M. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.

[CWI99] Security of e-commerce threatened by 512-bit number factorization. `http://www.cwi.nl/~kik/persb-UK.html`, August 1999. CWI press release.

[CWS+99] G. Caronni, M. Waldvogel, D. Sun, N. Weiler, and B. Plattner. The VersaKey framework: Versatile group key management. *IEEE Journal on Selected Areas in Communications*, 17(9):1614–1631, September 1999.

[DA99] T. Dierks and C. Allen. The TLS protocol version 1.0. Internet Request for Comment RFC 2246, Internet Engineering Task Force, January 1999. Proposed Standard.

[Dal01] iButton: A Java-Powered Cryptographic iButton. `http://www.ibutton.com/ibuttons/java.html`, 2001.

[DBP96] H. Dobbertin, A. Bosselaers, and B. Preneel. RIPEMD-160: A strengthened version of RIPEMD. In *Proceedings of the 3rd International Workshop on Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 71–82. Springer-Verlag, Berlin Germany, 1996.

[DF92] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1992.

[DF02] Digital fountain corporation. `http://www.digitalfountain.com`, 2002.

[DFY92] Y. Desmedt, Y. Frankel, and M. Yung. Multi-receiver / multi-sender network security: Efficient authenticated multicast / feedback. In *Proceedings IEEE Infocom '92*, pages 2045–2054, 1992.

[DH79] W. Diffie and M. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, March 1979.

[DN93] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1993.

[DP00] R. Dhamija and A. Perrig. Déjà Vu: A user study. using images for authentication. In *Proceedings of the 9th USENIX Security Symposium*, pages 45–58. USENIX, August 2000.

[DR99] J. Daemen and V. Rijmen. AES proposal: Rijndael, March 1999.

[DvOW92] W. Diffie, P. van Oorschot, and M. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, pages 107–125, 1992.

[DY91] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. In *Advances in Cryptology – CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 177–188. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1991.

[EGM90] S. Even, O. Goldreich, and S. Micali. On-line/off-line digital signatures. In *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 263–277. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1990.

[FJ93] S. Floyd and V. Jacobson. Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on Networking*, 1(4):397—413, August 1993.

[FJM+95] S. Floyd, V. Jacobson, S. McCanne, C. Liu, and L. Zhang. A reliable multicast framework for light-weight sessions and application level framing. In *Proceedings of the ACM SIGCOMM 95*, pages 342–356, Boston, MA, August 1995.

[FKK96a] A. Freier, P. Kariton, and P. Kocher. The SSL protocol: Version 3.0. Internet draft, Netscape Communications, 1996.

[FKK96b] F. Fujii, W. Kachen, and K. Kurosawa. Combinatorial bounds and design of broadcast authentication. *IEICE Transactions*, E79-A(4):502–506, 1996.

[FN94] A. Fiat and M. Naor. Broadcast encryption. In *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 480–491. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1994.

[GB99] S. Goldwasser and M. Bellare. Lecture notes on cryptography. Summer Course "Cryptography and Computer Security" at MIT, 1996–1999, August 1999. Available at `http://www-cse.ucsd.edu/users/mihir/papers/gb.pdf`.

[GGM86] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986.

[GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer Security*, 28:270–299, 1984.

[GM01] P. Golle and N. Modadugu. Authenticating streamed data in the presence of random packet loss. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001)*, pages 13–22. Internet Society, February 2001.

[Gon97] L. Gong. Enclaves: Enabling secure collaboration over the Internet. *IEEE Journal on Selected Areas in Communications*, pages 567–575, 1997.

[GR97] R. Gennaro and P. Rohatgi. How to sign digital streams. In *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 180–197. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1997.

[GSE02] Group security research group (GSEC). `http://www.irtf.org/charters/gsec.html` and `http://www.securemulticast.org/smug-index.htm`, 2002. Research group in the Internet Engineering Task Force (IETF).

[GSW00] J. Garay, J. Staddon, and A. Wool. Long-lived broadcast encryption. In *Advances in Cryptology – CRYPTO '2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 333–352. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2000.

[Hal94] N. Haller. The S/Key one-time password system. In *Proceedings of the Symposium on Network and Distributed Systems Security*, pages 151–157. Internet Society, February 1994.

[HC98] D. Harkins and D. Carrel. The Internet key exchange (IKE). Internet Request for Comment RFC 2409, Internet Engineering Task Force, November 1998.

[HCM01] H. Harney, A. Colegrove, and P. McDaniel. Principles of policy in secure groups. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001)*, pages 125–135. Internet Society, February 2001.

[HH99] H. Harney and E. Harder. Logical key hierarchy protocol. Internet Draft, Internet Engineering Task Force, April 1999.

[HILL99] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. A preliminary version appeared in 21st STOC, 1989.

[HJP02] Y.-C. Hu, D. B. Johnson, and A. Perrig. Secure efficient distance vector routing in mobile wireless ad hoc networks. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA '02), June 2002.

[HM97a] H. Harney and C. Muckenhirn. Group key management protocol (GKMP) architecture. Internet Request for Comment RFC 2094, Internet Engineering Task Force, July 1997.

[HM97b] H. Harney and C. Muckenhirn. Group key management protocol (GKMP) specification. Internet Request for Comment RFC 2093, Internet Engineering Task Force, July 1997.

[HPJ01] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole detection in wireless ad hoc networks. Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[HPJ02] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mobicom 2002)*, September 2002.

[HPS01] J. Hoffstein, J. Pipher, and J. Silverman. NSS: An NTRU lattice-based signature scheme. In *Advances in Cryptology – EUROCRYPT '2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 211–228. Springer-Verlag, Berlin Germany, 2001.

[HPT97] R. Hauser, A. Przygienda, and G. Tsudik. Reducing the cost of security in link state routing. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '97)*, pages 93–99. Internet Society, February 1997.

[HSW96] R. Hauser, M. Steiner, and M. Waidner. Micro-payments based on iKP. Research Report 2791, IBM Research, February 1996.

[HSW$^+$00] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 93–104, November 2000.

[HT96] R. Hauser and G. Tsudik. On shopping *incognito*. In *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, pages 251–257. USENIX, November 1996.

[HT00] T. Hardjono and G. Tsudik. IP multicast security: Issues and directions. *Annales de Telecom*, 2000.

[IEE97] IEEE Computer Society LAN MAN Standards Committee. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, 1997.

[ILL88] R. Impagliazzo, L. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21th Annual Symposium on Theory of Computing (STOC)*, pages 12–24. ACM Press, 1988.

[Jak02] M. Jakobsson. Fractal hash sequence representation and traversal. Cryptology ePrint Archive, `http://eprint.iacr.org/2002/001/`, January 2002.

[JV96] M. Just and S. Vaudenay. Authenticated multi-party key agreement. In *Advances in Cryptology – ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 36–49. Springer-Verlag, Berlin Germany, 1996.

[KA98a] S. Kent and R. Atkinson. IP encapsulating security payload (ESP). Internet Request for Comment RFC 2406, Internet Engineering Task Force, November 1998.

[KA98b] S. Kent and R. Atkinson. Security architecture for the Internet Protocol. Internet Request for Comment RFC 2401, Internet Engineering Task Force, November 1998.

[KKP99] J. Kahn, R. Katz, and K. Pister. Next century challenges: mobile networking for smart dust. In *International Conference on Mobile Computing and Networking (MOBICOM '99)*, pages 271–278, August 1999.

[KN93] J. Kohl and C. Neuman. The Kerberos network authentication service (V5). Internet Request for Comment RFC 1510, Internet Engineering Task Force, 1993.

[Knu98] D. Knuth. *Sorting and Searching, second edition*, volume 3 of *The Art of Computer Programming*. Addison-Wesley, 1998.

[KO97] K. Kurosawa and S. Obana. Characterization of (k,n) multi-receiver authentication. In *Proceedings of the 2nd Australasian Conference on Information Security and Privacy (ACISP '97)*, volume 1270 of *Lecture Notes in Computer Science*, pages 205–215. Springer-Verlag, Berlin Germany, 1997.

[KPT00] Y. Kim, A. Perrig, and G. Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 235–244. ACM Press, November 2000.

[Kuh00] M. Kuhn. Probabilistic counting of large digital signature collections. In *Proceedings of the 9th USENIX Security Symposium*, pages 73–83. USENIX, August 2000.

[Lab95] National Institute of Standards and Technology (NIST)(Computer Systems Laboratory). Secure hash standard. Federal Information Processing Standards Publication FIPS PUB 180-1, April 1995.

[Lam75] L. Lamport. Discussion with Whitfield Diffie. `http://research.compaq.com/SRC/personal/lamport/pubs/pubs.html#dig-sig`, 1975.

[Lam79] L. Lamport. Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.

[Lam81] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[LMS85] L. Lamport and P. Melliar-Smith. Synchronizing clocks in the presence of faults. *Journal of the ACM*, 32(1):52–78, 1985.

[LPB01] M. Li, R. Poovendran, and C. Berenstein. Optimization of key storage for secure multicast. In *35th Annual Conference on Information Sciences and Systems (CISS)*, March 2001.

[LRW00] H. Lipmaa, P. Rogaway, and D. Wagner. Counter mode encryption. `http://csrc.nist.gov/encryption/modes/`, 2000.

[LS98] M. Luby and J. Staddon. Combinatorial bounds for broadcast encryption. In *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 512–526. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1998.

[Lub96] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton Computer Society Notes, 1996.

[LV99] A. Lenstra and E. Verheul. Selecting cryptographic key sizes. `http://www.cryptosavvy.com`, November 1999. A shorter version of the report appeared in the proceedings of the Public Key Cryptography Conference (PKC2000) and in the Autumn '99 PricewaterhouseCoopers CCE newsletter. A revised version appeared later in the Journal of Cryptology.

[LV00] A. Lenstra and E. Verheul. Key improvements to XTR. In *Advances in Cryptology – ASIACRYPT '2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 220–233. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2000.

[LV01] A. Lenstra and E. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001.

[LYGL01] X. Li, Y. Yang, M. Gouda, and S. Lam. Batch rekeying for secure group communications. In *Proceedings of the tenth international World Wide Web conference on World Wide Web*, pages 525–534, October 2001.

[Man96] U. Manber. A simple scheme to make passwords based on one-way functions much harder to crack. *Computers and Security*, 15(2):171–176, 1996.

[McD01] P. McDaniel. *Policy Management in Secure Group Communication*. PhD thesis, Univerity of Michigan, 2001.

[Mer78] R. Merkle. Secure communication over insecure channels. *Communications of the ACM*, 21(4):294–299, April 1978.

[Mer80] R. Merkle. Protocols for public key cryptosystems. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 122–134. IEEE Computer Society Press, April 1980.

[Mer88] R. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology – CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1988.

[Mer90] R. Merkle. A certified digital signature. In *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1990.

[Mic96] S. Micali. Efficient certificate revocation. Technical Report MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science, March 1996.

[Mil92] D. Mills. Network Time Protocol (version 3) specification, implementation and analysis. Internet Request for Comment RFC 1305, Internet Engineering Task Force, March 1992.

[Mil94] D. Mills. Improved algorithms for synchronizing computer network clocks. In *Proceedings of the Conference on Communications Architectures, Protocols and Applications, SIGCOMM 94*, pages 317–327, London, England, 1994.

[Mit97] S. Mittra. Iolus: A framework for scalable secure multicasting. In *ACM SIGCOMM'97*, pages 277–288, September 1997.

[MKOM90] S. Miyaguchi, S. Kurihara, K. Ohta, and H. Morita. 128-bit hash function (N-hash). *NTT Review*, 2(6):128–132, 1990.

[MMO85] S. Matyas, C. Meyer, and J. Oseas. Generating strong one-way functions with cryptographic algorithm. *IBM Technical Disclosure Bulletin*, 27:5658–5659, 1985.

[MMSA$^+$96] L. Moser, P. Melliar-Smith, D. Agarwal, R. Budhia, and C. Lingley-Papadopoulos. Totem: A fault-tolerant multicast group communication system. *Communications of the ACM*, 39(4):54–63, April 1996.

[MNSS88] S. Miller, B. Neuman, J. Schiller, and J. Saltzer. Kerberos authentication and authorization system. Technical report, MIT, October 1988. Project Athena Technical Plan.

[MP99] R. Molva and A. Pannetrat. Scalable multicast security in dynamic groups. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 101–112. ACM Press, November 1999.

[MP00] R. Molva and A. Pannetrat. Scalable multicast security with dynamic recipient groups. *ACM Transactions on Information and System Security*, 3(3):136–160, August 2000.

[MP02] M. Mitzenmacher and A. Perrig. Bounds and improvements for biba signature schemes. Technical Report TR-02-02, Harvard Computer Science Technical Report, 2002.

[MPH99] P. McDaniel, A. Prakash, and P. Honeyman. Antigone: A flexible framework for secure group communication. In *Proceedings of the 8th USENIX Security Symposium*, pages 99–114. USENIX, August 1999.

[MRR99] M. Moyer, J. Rao, and P. Rohatgi. A survey of security issues in multicast communications. *IEEE Network*, 13(6):12–23, November/December 1999.

[MS98] D. McGrew and A. Sherman. Key establishment in large dynamic groups using one-way function trees. Manuscript, May 1998.

[MS01] S. Miner and J. Staddon. Graph-based authentication of digital streams. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 232–246. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 2001.

[MSE02] Multicast security (msec). `http://www.ietf.org/html.charters/msec-charter.html` and `http://www.securemulticast.org/msec-index.htm`, 2002. Working group within the Internet Engineering Task Force (IETF).

[Mul02] Source-Specific Multicast. `http://www.ietf.org/html.charters/ssm-charter.html`, 2002.

[MvOV97] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[Nao90] M. Naor. Bit commitment using pseudo-randomness (extended abstract). In *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 128–137. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1990.

[Nat77] National Bureau of Standards (NBS). Specification for the Data Encryption Standard. Federal Information Processing Standards Publication 46 (FIPS PUB 46), January 1977.

[Nat80] National Institute of Standards and Technology (NIST). DES model of operation. Federal Information Processing Standards Publication 81 (FIPS PUB 81), December 1980.

[Nat91] National Institute of Standards and Technology (NIST). Digital Signature Standard (DSS), Federal Register 56. Draft Tech. Rep. FIPS PUB 186, August 1991.

[NES99] NESSIE: New European Schemes for Signatures, Integrity, and Encryption. `http://www.cryptonessie.org`, 1999.

[Ope01] OpenSSL. The OpenSSL project. `http://www.openssl.org/`, 2001.

[Pax99] V. Paxson. End-to-end Internet packet dynamics. *IEEE/ACM Transactions on Networking*, 7(3):277–292, June 1999.

[PB99] R. Poovendran and J. Baras. An information theoretic analysis of rooted-tree based secure multicast key distribution schemes. In *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 624–638. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1999.

[PCB$^+$02] Adrian Perrig, Ran Canetti, Bob Briscoe, J.D. Tygar, and Dawn Song. TESLA: Multicast source authentication transform introduction. Internet Draft, Internet Engineering Task Force, February 2002. Work in progress.

[PCST01] A. Perrig, R. Canetti, D. Song, and J. D. Tygar. Efficient and secure source authentication for multicast. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2001)*, pages 35–46. Internet Society, February 2001.

[PCTS00] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. Efficient authentication and signature of multicast streams over lossy channels. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 56–73. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 2000.

[PCTS02] A. Perrig, R. Canetti, J.D̃. Tygar, and D. Song. The tesla broadcast authentication protocol. *RSA CryptoBytes*, 5(Summer), 2002.

[Ped97] T. Pedersen. Electronic payments of small amounts. In *Security Protocols—International Workshop*, volume 1189 of *Lecture Notes in Computer Science*, pages 59–68. Springer-Verlag, Berlin Germany, April 1997.

[Per99] A. Perrig. Efficient collaborative key management protocols for secure autonomous group communication. In *International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)*, July 1999.

[Per01] A. Perrig. The BiBa one-time signature and broadcast authentication protocol. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 28–37. ACM Press, November 2001.

[PGV97] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1997.

[PKB99] K. Pister, J. Kahn, and B. Boser. Smart dust: Wireless networks of millimeter-scale sensor nodes, 1999. In 1999 UC Berkeley Electronics Research Laboratory Research Summary.

[Poo99] R. Poovendran. *Key Management for Secure Multicast Communications*. PhD thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park, 1999.

[Pre93] B. Preneel. *Analysis and design of cryptographic hash functions*. PhD thesis, Katholieke Universiteit Leuven (Belgium), 1993.

[Pro02] Proxim, Inc. Data sheet for Proxim Harmony 802.11a CardBus Card. Sunnyvale, CA. Available at: `http://www.proxim.com/products/all/harmony/docs/ds/harmony_11a_cardbus.%pdf`, 2002.

[PS98] G. Poupard and J. Stern. Security analysis of a practical "on the fly" authentication and signature generation. In *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 422–436. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1998.

[PS99a] A. Perrig and D. Song. Hash visualization: A new technique to improve real-world security. In *International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)*, pages 131–138, July 1999.

[PS99b] G. Poupard and J. Stern. On the fly signatures based on factoring. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 37–45. ACM Press, November 1999.

[PS00a] A. Perrig and D. Song. A first step towards the automatic generation of security protocols. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '00)*, pages 73–83. Internet Society, February 2000.

[PS00b] A. Perrig and D. Song. Looking for diamonds in the desert — extending automatic protocol generation to three-party authentication and key agreement protocols. In *13th IEEE Computer Security Foundations Workshop*, pages 64–76. IEEE Computer Society Press, July 2000.

[PST01] A. Perrig, D. Song, and J. D. Tygar. ELK, a new protocol for efficient large-group key distribution. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 247–262. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 2001.

[PSW$^+$01] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. In *Seventh Annual International Conference on Mobile Computing and Networks (MobiCOM 2001)*, pages 189–199, 2001.

[PSW$^+$02] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, September 2002.

[Rab78] M. Rabin. Digitalized signatures. In *Foundations of Secure Computation*, pages 155–168. Academic Press, 1978.

[Rab90] M. Rabin. The information dispersal algorithm and its applications. In *Sequences: Combinatorics, Compression, Security and Transmission*, pages 406–419. Springer-Verlag, Berlin Germany, 1990.

[RBD00a] O. Rodeh, K. Birman, and D. Dolev. Optimized rekey for group communication systems. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '00)*, pages 37–48. Internet Society, February 2000.

[RBD00b] O. Rodeh, K. Birman, and D. Dolev. A study of group rekeying. Technical Report TR2000-1791, Computer Science Department, Cornell University, March 2000.

[RBH$^+$98] O. Rodeh, K. Birman, M. Hayden, Z. Xiao, and D. Dolev. The architecture and performance of security protocols in the ensemble group communication system. Technical Report TR98-1703, Computer Science Department, Cornell University, September 1998.

[RBvR94] M. Reiter, K. Birman, and R. van Renesse. A security architecture for fault-tolerant systems. *ACM Transactions on Computer Systems*, 12(4):340–371, November 1994.

[Rei93] M. Reiter. *A Security Architecture for Fault-Tolerant Systems*. PhD thesis, Department of Computer Science, Cornell University, August 1993.

[Riv92] R. Rivest. The MD5 message-digest algorithm. Internet Request for Comment RFC 1321, Internet Engineering Task Force, April 1992.

[Riv94] R. Rivest. The RC5 encryption algorithm. In *Proceedings of the 1st International Workshop on Fast Software Encryption*, volume 809 of *Lecture Notes in Computer Science*, pages 86–96. Springer-Verlag, Berlin Germany, 1994.

[Riz00] L. Rizzo. PGMCC: a TCP-friendly single-rate multicast congestion control scheme. In *SIGCOMM 2000*, pages 17–28, August 2000.

[RMTR02] Reliable Multicast Transport (RMT). `http://www.ietf.org/html.charters/rmt-charter.html`, 2002.

[Roh99] P. Rohatgi. A compact and fast hybrid signature scheme for multicast packet. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 93–100. ACM Press, November 1999.

[RR02] Leonid Reyzin and Natan Reyzin. Better than biba: Short one-time signatures with fast signing and verifying. In *Seventh Australasian Conference on Information Security and Privacy (ACISP 2002)*, July 2002.

[RS60] I. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8:300–304, 1960.

[RS97] R. Rivest and A. Shamir. PayWord and MicroMint: Two simple micropayment schemes. In *Security Protocols—International Workshop*, volume 1189 of *Lecture Notes in Computer Science*, pages 69 – 88. Springer-Verlag, Berlin Germany, April 1997.

[RSA78] R. 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.

[RSW96] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timed-release crypto, March 1996. Published at `http://theory.lcs.mit.edu/~rivest/RivestShamirWagner-timelock.ps`.

[Sch91] C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[Sch96] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, second edition, 1996.

[Sim90] G. Simmons. A Cartesian product construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology*, 2(2):77–104, 1990.

[SKJ00] S. Setia, S. Koussih, and S. Jajodia. Kronos: A scalable group re-keying approach for secure multicast. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 215–228. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 2000.

[SLWL90] B. Simons, J. Lundelius-Welch, and N. Lynch. An overview of clock synchronization. In B. Simons and A. Spector, editors, *Fault-Tolerant Distributed Computing*, number 448 in LNCS, pages 84–96. Springer-Verlag, Berlin Germany, 1990.

[SMS00] A. Selcuk, C. McCubbin, and D. Sidhu. Probabilistic optimization of LKH-based multicast key distribution schemes. Internet Draft, Internet Engineering Task Force, January 2000.

[SNW98] R. Safavi-Naini and H. Wang. New results on multireceiver authentication codes. In *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 527–541. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1998.

[SNW99] R. Safavi-Naini and H. Wang. Multireceiver authentication codes: Models, bounds, constructions and extensions. *Information and Computation*, 151(1/2):148–172, 1999.

[SP01] D. Song and A. Perrig. Advanced and authenticated marking schemes for IP traceback. In *Proceedings IEEE Infocomm 2001*, pages 878–886, April 2001.

[SSDW90] D. Steer, L. Strawczynski, W. Diffie, and M. Wiener. A secure audio teleconference system. In *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 520–528. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1990.

[SSV01] J. Snoeyink, S. Suri, and G. Varghese. A lower bound for multicast key distribution. In *Proceedings IEEE Infocomm 2001*, pages 422–431, April 2001.

[STW96] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman key distribution extended to groups. In *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pages 31–37. ACM Press, March 1996. Appeared as revised and extended journal version as [STW00].

[STW98] M. Steiner, G. Tsudik, and M. Waidner. CLIQUES: A new approach to group key agreement. In *18th International Conference on Distributed Computing Systems (ICDCS'98)*, pages 380–387. IEEE Computer Society Press, May 1998. Appeared as heavily revised and extended journal version in [STW00].

[STW00] M. Steiner, G. Tsudik, and M. Waidner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 11(8):769–780, August 2000.

[SWKA00] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical network support for IP traceback. In *Proceedings of the 2000 ACM SIGCOMM Conference*, August 2000. An early version of the paper appeared as techreport UW-CSE-00-02-01 available at: `http://www.cs.washington.edu/homes/savage/traceback.html`.

[SWP00] D. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 44–55. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, May 2000.

[Ten00] D. Tennenhouse. Embedding the Internet: Proactive computing. *Communications of the ACM*, 43(5):43–50, 2000.

[Tri02] Trimble Navigation Limited. Data sheet and specifications for Trimble Thunderbolt GPS Disciplined Clock. Sunnyvale, California. Available at `http://www.trimble.com/thunderbolt.html`, 2002.

[TSPL01] W. Trappe, J. Song, R. Poovendran, and K. Liu. Key distribution for secure multimedia multicast via data embedding. In *IEEE ICASSP 2001*, May 2001.

[TT00] W. Tzeng and Z. Tzeng. Round-efficient conference-key agreement protocols with provable security. In *Advances in Cryptology – ASIACRYPT '2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 614–628. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2000.

[TT01] W. Tzeng and Z. Tzeng. Robust key-evolving public key encryption schemes. Report 2001/009, Cryptology ePrint Archive, 2001.

[vM39] R. von Mises. Über Aufteilungs- und Besetzungswahrscheinlichkeiten. *Revue de la Faculté des Sciences de l'Université d'Istanbul*, 4:145—163, 1939.

[vRBM96] R. van Renesse, K. Birman, and S. Maffeis. Horus: A flexible group communication system. *Communications of the ACM*, 39(4):76–83, April 1996.

[WGL97] C. Wong, M. Gouda, and S. Lam. Secure group communications using key graphs. Technical Report TR-97-23, University of Texas at Austin, Department of Computer Sciences, August 1997.

[WGL98] C. Wong, M. Gouda, and S. Lam. Secure group communications using key graphs. In *Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 68–79, 1998. Appeared in ACM SIGCOMM Computer Communication Review, Vol. 28, No. 4 (Oct. 1998).

[WHA99] D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. Internet Request for Comment RFC 2627, Internet Engineering Task Force, June 1999.

[Win84] R. Winternitz. A secure one-way hash function built from DES. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 88–90. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, April 1984.

[WL98] C. Wong and S. Lam. Digital signatures for flows and multicasts. In *IEEE ICNP '98*, 1998.

[WL00] C. Wong and S. Lam. Keystone: A group key management service. In *International Conference on Telecommunications, ICT 2000*, 2000.

[WLLP01] B. Warneke, M. Last, B. Liebowitz, and K. Pister. Smart dust: Communicating with a cubic-millimeter computer. *IEEE Computer*, pages 44–51, January 2001.

[WN94] D. Wheeler and R. Needham. TEA, a tiny encryption algorithm. `http://www.ftp.cl.cam.ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html`, November 1994.

[XMZY97] X. Xu, A. Myers, H. Zhang, and R. Yavatkar. Resilient multicast support for continuous-media applications. In *IEEE 7th International Workshop on Network and Operating Systems Support for Digital Audio and Video, NOSSDAV 97*, pages 183–194, 1997.

[Yee94] B. Yee. *Using Secure Coprocessors*. PhD thesis, School of Computer Science, Carnegie Mellon University, May 1994. CMU-CS-94-149.

[YLZL01] Y. Yang, X. Li, X. Zhang, and S. Lam. Reliable group rekeying: A performance analysis. In *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, SIGCOMM 2001*, pages 27–38, 2001.

[YMKT99] M. Yajnik, S. Moon, J. Kurose, and D. Towsley. Measurement and modelling of the temporal dependence in packet loss. In *Proceedings IEEE Infocom '99*, March 1999.

[YT95] B. Yee and J. D. Tygar. Secure coprocessors in electronic commerce applications. In *Proceedings of the First USENIX Workshop on Electronic Commerce*. USENIX, July 1995.

[Yuv97] G. Yuval. Reinventing the Travois: Encryption/MAC in 30 ROM bytes. In *Proceedings of the 4th International Workshop on Fast Software Encryption*, volume 1267 of *Lecture Notes in Computer Science*, pages 205–209. Springer-Verlag, Berlin Germany, 1997.

[Zha98] K. Zhang. Efficient protocols for signing routing messages. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98)*. Internet Society, March 1998.