Bibliography

[1] M. Al-Ibrahim. An authentication scheme using a secret sharing technique. *The International Conference on Information Networking*, Proceedings(II):923–929, Feburary 2003.

[2] M. Al-Ibrahim. A Signcryption scheme based on secret sharing technique. In V. Gorodetsky, L. Popyack, and V. Skormin, editors, *proceedings of the Second MMM-ACNS 2003*, volume 2776 of LNCS, pages 279–288, Berlin, September 2003. Springer-Verlag.

[3] M. Al-Ibrahim and A. Cerny. Authentication of anycast communication. In V. Gorodetsky, L. Popyack, and V. Skormin, editors, *proceedings of the Second MMM-ACNS 2003*, volume 2776 of LNCS, pages 419–423, Berlin, 2003. Springer-Verlag.

[4] M. Al-Ibrahim and A. Cerny. Proxy and threshold one-time signature. In J. Zhou, M. Yung, and Y. Han, editors, *Applied Cryptography and Network Security (ACNS'03)*, volume 2846 of LNCS, pages 123–136. Springer-Verlag, 2003.

[5] M. Al-Ibrahim, H. Ghodosi, and J. Pieprzyk. Authentication of concast communication. In A. Menezes and P. Sarkar, editors, *Progress in Cryptology, third international conference on cryptology in India* INDOCRYPT'02*, Hyderabad: India*, volume 2551 of LNCS, pages 185–198. Springer-Verlag, 2002.

[6] M. Al-Ibrahim and J. Pieprzyk. Authenticating multicast streams in lossy channels using threshold techniques. In *Networking – ICN 2001*, volume 2094 of LNCS, pages 239–249. Springer-Verlag, 2001.

[7] M. Al-Ibrahim and J. Pieprzyk. Authentication of transit flows and k-sibling one-time signatures. In B. Jerman-Blazic and T. Klobucar, editors, *Advanced Communication and Multemedia Security*, volume IFIP TC6/TC11 Sixth Joint Working Conference, pages 41–55, Portroz, Slovenia, September 2002. Kluwer Academic Publisher.

[8] J. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In L. Kundsen, editor, *Advances in Cryptology - CRYPTO '02*, volume 2332 of LNCS, pages 83–107, Berlin, 2002. Springer-Verlag.

[9] R. Anderson and S. Vaudenay. Minding your p's and q's. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology Proceedings of Asiacrypt '96*, volume 1163 of LNCS, pages 26–35. Springer-Verlag, 1996.

[10] C. Asmuth and J. Bloom. A modular approach to key safeguarding. In *IEEE Transactions on Information Theory*, volume IT-29, pages 208–210, Mar 1983.

[11] A. Ballardie, S. Reeve, and N. Jain. Core-based trees (CBT) multicast - protocol specification. Internet Draft - RFC 1949, March 1996.

[12] T. Ballardie and J. Crowcroft. Multicast-specific security threats and countermeasures. *IEEE Digital Library*, 1995.

[13] T. Ballardie, P. Francis, and J. Crowcraft. Core-based trees (CBT): An architecture for scalable inter-domain multicast routing. *Proceedings of ACM SIGCOMM'93*, September 1993.

[14] M. Bellare, A. Desai, D. Pointcheval, and Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, *Advances in Cryptology - CRYPTO'98*, volume 1462 of, pages 26–45. Springer-Verlag, 1998.

[15] M. Bellare, J. Garay, and T. Rabin. Fast Batch Verification for Modular Exponentiation and Digital Signatures. In K. Nyberg, editor, *Advances in Cryptology Proceedings of EUROCRYPT'98*, volume 1403 of LNCS. Springer-Verlag, 1998.

[16] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the composition paradigm. In Y. Zheng and H. Wolfe, editors, *Advances in Cryptology - ASIACRYPT'00*, volume 1976 of LNCS, pages 531–545, Berlin, 2000. Springer-Verlag.

[17] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *First ACM Conference on Computer and Communication Security*, pages 62–73. Association for Computing Machinery, 1993.

[18] M. Bellare and P. Rogaway. Collision-resistant hashing: towards making universal one-way hash functions practical. In Burton S. Kaliski, editor, *Advances in Cryptology Proceedings of CRYPTO'97*, volume 1294 of LNCS, pages 470–484. Springer-Verlag, 1997.

[19] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *20th Annual Symposium on the Theory of Computing*, pages 1–10, 1988.

[20] Bertsekas and R. Gallagher. *Data Network*. Prentice Hall, 1992.

[21] B. Blakley, G. Blakley, A. Chan, and J. Massey. Threshold schemes with disenrollment. In E. Brickell, editor, *Advances in Cryptology Proceedings of CRYPTO '92*, volume 740 of LNCS, pages 540–548. Springer-Verlag, 1993.

[22] G. Blakley. Safeguarding cryptographic keys. In *Proceedings of AFIPS 1979 National Computer Conference*, pages 313–317. AFIPS, 1979.

[23] G. Blakley and C. Meadows. Security of Ramp schemes. In G. Blakley and D. Chaum, editors, *Advances in Cryptology Proceedings of CRYPTO '84*, volume 196 of LNCS, pages 242–268. Springer-Verlag, 1985.

[24] D. Bleichenbacher. Generating ElGamal signatures without knowing the secret key. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of LNCS, pages 10–18, Berlin, 1996. Springer-Verlag.

[25] A. Boldyreva, A. Palacio, and B. Warinschi. Secure proxy signature schemes for delegation of signing rights. Interner Draft, Feburary 2003. http://www.eprint.iacr.org/2003/096.

[26] J.N.E. Bos and D.Chaum. Provably unforgeable signatures. In Ernest F. Brickell, editor, *Advances in Cryptology Proceedings of CRYPTO'92*, volume 740 of LNCS, pages 1–14. Springer-Verlag, 1992.

[27] C. Boyd. Digital Multisignatures, in *cryptography and coding*. IEE Proc. - Computer and Digital Technology, pages 241–246, 1989.

[28] E. Brickell, D. Gordon, K. McCurley, and D. Wilson. Fast Exponentiation with Precomputation. In R. Rueppel, editor, *Advances in Cryptology Proceedings of EUROCRYPT'92*, volume LNCS No. 658. Springer-Verlag, 1993.

[29] R. Burden and J. Faires. *Numerical Analysis*. PWS-Kent, New York, 1989.

[30] B. Cain, S. Deering, and A. Thyagarajan. Internet group management protocol: Version 3. Internet Draft, August expired 2000. draft-ietf-idmr-igmp-v3-00.txt.

[31] R. Canetti, J. Garay, G. Itkins, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and some efficient constructions. In *IEEE INFOCOM'99*. IEEE Digital Library, 1999.

[32] G. Caronni, M. Waldvogel, D. Sun, and B. Plattner. Efficient security for large and dynamic groups. In *Proceedings of the Seventh Workshop on Enabling Technologies*. IEEE Computer Society Press, 1998.

[33] C. Charnes, J. Pieprzyk, and R. Safavi-Naini. Conditionally secure secret sharing schemes with disenrolment capability. In *Proceedings of the 2nd ACM Conference on Computer and Communication Security*, pages 89–95, Fairfax, Virginia, November 2-4 1994.

[34] D. Chaum. Private signature and proof systems. United States Patent, pages 5,493,614, 1996.

[35] L. Chen and T. P. Pedersen. New group signature schemes. *Advances in Cryptology Proceedings of EUROCRYPT '94*, 950 of LNCS:171–181, 1994.

[36] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of 26th IEEE Symposium on Foundations of Computer Science*, pages 383–395. IEEE Computer Society, 1985.

[37] H. Chu, L. Qiao, and K. Nahrstedt. Secure multicast protocol with copyright protection. *Proceedings of ACM SIGCOMM'02*, 32(2), April 2002.

[38] C. Colbourn and J. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC press, 1996.

[39] Coppersmith, D. Franklin, M. K., Patarin, J., and M. K. Reiter. Low-exponent RSA with related messages. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of LNCS, pages 1–9, Berlin, 1996. Springer-Verlag.

[40] R. Cramer and I. Damgård. New generation of secure and practical RSA-based signatures. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of LNCS, pages 173–185, Berlin, 1996. Springer-Verlag.

[41] J. Daemen and V. Rijmen. The design of Rijndael, AES. In J. Daemen and V. Rijmen, editors, *Fast Software Encyption '02*, volume 2365 of LNCS, Berlin, 2002. Springer-Verlag.

[42] I. Damgård. A design principle for hash functions. In G. Brassard, editor, *Advances in Cryptology Proceedings of CRYPTO'89*, volume 435 of LNCS, pages 416–427. Springer-Verlag, 1990.

[43] I. B. Damgård. A design principle for hash functions. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of LNCS, pages 416–427, Berlin, 1989. Springer-Verlag.

[44] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85*, volume 218 of LNCS, pages 18–27, Berlin, 1986. Springer-Verlag.

[45] M. De Soete, J. Quisquater, and K. Vedder. A signature with shared verification scheme. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of LNCS, pages 253–262, Berlin, 1989. Springer-Verlag.

[46] S. Deering. Host extension for IP multicasting. Internet Draft, August 1989. RFC 1112.

[47] S. Deering. *Multicast Routing in a Datagram Internetworks*. PhD thesis, Stanford University, USA, December 1991.

[48] S. Deering and D. R. Cheriton. Multicast routing in datagram interntworks and extended LANs. *IEEE/ACM Transactions on Networking*, 4(2):153–162, April 1996.

[49] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C-G Lim, and L. Wei. An architecture for wide-area multicasting routing. *ACM SIGCOMM '94*, pages 126–135, October 1994.

[50] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C-G Lim, and L. Wei. The pim architecture for wide-area multicasting routing. *IEEE/ACM Transactions on Networking*, 4(2):153–162, April 1996.

[51] D. Denning. Digital signature with RSA and other public-key cryptosystems. *Communications of the ACM*, 27(4):388–392, 1984.

[52] Y. Desmedt. Society and group oriented cryptography: A new concept. In C. Pomerance, editor, *Advances in Cryptology Proceedings of CRYPTO'87*, volume 293 of LNCS, pages 120–127. Springer-Verlag, 1988.

[53] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, *Advances in Cryptology Proceedings of CRYPTO'89*, volume 435 of LNCS, pages 307–315. Springer-Verlag, 1990.

[54] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology Proceedings of CRYPTO'91*, volume 576 of LNCS, pages 457–469. Springer-Verlag, 1992.

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

[56] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976.

[57] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. Blakley and D. Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO '84*, volume 196 of LNCS, pages 10–18, Berlin, 1985. Springer-Verlag.

[58] Wu-Chi Feng. *Buffering Techniques for Delivery of Compressed Vedio in Demand Systems*. Kluwer Academic Publisher, 1997.

[59] W. Fenner. Internet group management protocol: Version 2. Internet Draft, August expired 1998. draft-ietf-idmr-igmp-v2-08.txt.

[60] A. Fiat. Batch RSA. *Journal of Cryptology*, 10 no. 2:75–88, 1997.

[61] A. Fiat and A. Shamir. How to prove yourself: Practical solution to identification and signature problems. In *Advances in Cryptology Proceedings of CRYPTO'86*, volume 263 of LNCS, pages 186–194. Springer-Verlag, 1987.

[62] M. Garey and D. Johnson. *Computers and Intractibilty*. Freeman, 1979.

[63] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of LNCS, pages 354–371, Berlin, 1996. Springer-Verlag.

[64] R. Gennaro and P. Rohatchi. How to sign digital streams. In Burton S. Kaliski, editor, *Advances in Cryptology Proceedings of CRYPTO'97*, volume 1249 of LNCS, pages 180–197. Springer-Verlag, 1997.

[65] H. Ghodosi and J. Pieprzyk. Repudiation of cheating and nonrepudiation of Zhang's proxy signature schemes. In J. Pieprzyk, R. Safavi-Naini, and J. Seberry, editors, *Information Security and Privacy ACISP'99*, volume 1587 of LNCS, pages 129–134, Berlin, 1999. Springer-Verlag.

[66] S. Goldwasser, S. Micali, and R. Rivest. A Digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17 (2):281 – 308, 1988.

[67] P. Golle and N. Modadugu. Authenticating streamed data in the presence of random packet loss. In *ISOC Network and Distributed System Security Symposium*, volume NDSS. ACM press, 2001.

[68] L. Gong and N. Shacham. Elements of trusted multicasting. *IEEE Digital Library*, 1994.

[69] L. Gong and N. Shacham. Trade-offs in routing private multicast traffic. *IEEE Digital Library*, 1995.

[70] N. Gruschka, F. Reuter, and N. Luttenberger. Checking and signing XML documents on JAVA smart cards. In J. Quisquarter and B. Schneier, editors, *CARDIS 04, 6th Smart Card Research and Advanced Application IFIP Conference*. Kluwer Academic Publisher, 2004.

[71] M. Hall. *Combinatorial Theory*. A Wiley-Interscience Publication John Wiley and Sons, 1986.

[72] H. Handschuth and P. Paillier. Smart card crypto-coprocessors for public-key cryptography. In J. Quisquarter and B. Schneier, editors, *Smart Card Research and Applications*, volume 1820 of LNCS, pages 386–394. Springer-Verlag, 2000.

[73] T. Hardjono and B. Cain. A secure group membership verification protocol for IP multicast. *IEEE Digital Library*, 1999.

[74] T. Hardjono, B. Cain, and N. Doraswamy. A framework for key management for multicast security. *Internet-Draft*, IETF(draft-ietf-ipsec-gkmframework-02.txt), 2000.

[75] L. Harn. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. IEE Proc.-Comput. Digit. Tech., 141:307–313, September 1994.

[76] L. Harn. Batch verifying multiple DSA-type digital signature. *Electronics Letters*, Vol. 34(9):870–871, 1998.

[77] L. Harn. Batch verifying multiple RSA digital signature. *Electronics Letters*, Vol. 34(12):1219–1210, 1998.

[78] Harney and Harder. Multicast security management protocol requirement and policy.

[79] H. Harney and C. Muckenhirn. Group key management protocol (GKMP) architecture. Internet Draft, November 1997. RFC-2094.

[80] J. Håstad. Solving simultaneous modular equations of low degree. *SIAM Journal on Computing*, 17(2):336–341, April 1988.

[81] C. Hedrick. Routing information protocol. RFC 1058, June 1988.

[82] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. In D. Coppersmith, editor, *Advances in Cryptology Proceedings of CRYPTO'95*, volume 963 of LNCS, pages 339–352. Springer-Verlag, 1995.

[83] Hinden.
IP next generation overview. http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html, March 1996.

[84] T. Hwang, S. Shi, and Chi-Hwai. A simple multiproxy signature scheme. In *Tenth National Conference on Information Security*, pages 134–138. Springer-Verlag, 2000.

[85] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, pages 143–154, Berlin, 1996. Springer-Verlag. LNCS Volume 1070.

[86] B.S. Kaliski. The MD2 message-digest algorithm. *RFC 1319*, April 1992. RSA Laboratories.

[87] E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. In *IEEE Transactions on Information Theory*, volume IT-29, pages 35–41, Jan 1983.

[88] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402, November 1998. Networking Group, IETF.

[89] S. Kent and R. Atkinson. IP Encapsulation security payload. RFC 2406, November 1998. Networking Group, IETF.

[90] S. Kent and R. Atkinson. Security architecture for the internet security. RFC 2401, November 1998. Networking Group, IETF.

[91] H. Kim, J. Baek, B. Lee, and K. Kim. Secret computation with secrets for mobile agent using one-time proxy signature. *Proc. of SCIS'01*, April 2001.

[92] S. Kim, Park, and Won. Proxy signatures, revisited. In *International Conference in Information and Communication Security ICICS'97*, volume 1334, pages 223–232. Springer-Verlag, 1997.

[93] S. Kothari. Generalized linear threshold scheme. In G. Blakely and D. Chaum, editors, *Advances in Cryptology Proceedings of CRYPTO '84*, volume 196 of LNCS, pages 231–241. Springer-Verlag, 1985.

[94] H. Krawczyk. The order of encryption and authentication for protecting communications. In *Advances in Cryptology - CRYPTO '01*, volume 2139 of LNCS, pages 310–331, Berlin, 2001. Springer-Verlag.

[95] P. Kruus and J. Macker. Techniques and issues in multicast security. *Proceedings MILCOM'98*, 1998.

[96] C. Laih, L. Harn, J. Lee, and T. Hwang. Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space. In G. Brassard, editor, *Advances in Cryptology Proceedings of CRYPTO '89*, volume 435 of LNCS, pages 286–297. Springer-Verlag, 1990.

[97] L. Lamport. Constructing digital signatures from a one-way function. *Technical report CSL-98, SRI international*, 1979.

[98] B. Lee, H. Kim, and K. Kim. Secure mobile agent using strong non-designated porxy signature. In *Information Security and Privacy, ACISP'01*. Springer-Verlag, 2001.

[99] B. Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. In *Symposium on Cryptography and Information Security SCIS'2001*, 2001.

[100] N. Lee, T. Hwang, and C. Wang. On Zhang's nonrepudiation proxy signature schemes. In C. Boyd and E. Dawson, editors, *Information Security and Privacy ACISP'98*, volume 1438 of LNCS, pages 415–422, Berlin, 1998. Springer-Verlag.

[101] C. Li, T. Hwang, and N. Lee. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94*, volume 950 of LNCS, pages 194–204, Berlin, 1995. Springer-Verlag.

[102] C. Lim and P. Lee. Security of interactive DSA batch verification. *Electronics Letters*, Vol. 30(19):1592–1593, 1994.

[103] J. Lin and R. Chang. A comparison of the internet multicast routing protocols. *Computer Communications*, 22:144–155, 1999.

[104] D. Malkhi and M. Reiter. A high-throughput secure reliable multicast protocol. *Journal of Computer Security*, 5:113–127, 1997.

[105] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operation. *IEICE Trans. Fundamentals*, E79-A, no.9:1338–1354, 1996.

[106] C. Meadows. Some threshold schemes without central key distributors. *Congressus Numerantium*, 46:187–199, 1985.

[107] A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.

[108] R. Merkle. A certified digital signature. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of LNCS, pages 218–238, Berlin, 1989. Springer-Verlag.

[109] M. Mignotte. How to share a secret. In T. Beth, editor, *Cryptography*, volume 149 of Workshop on Cryptography, pages 371–375. Springer-Verlag, 1983.

[110] S. Mittra. The iolus framework for scalable secure multicasting. In *Proceedings of SIGCOMM '97*, 1997.

[111] J. Moy. OSPF, extensions to multicasting. Internet Draft, March 1994. RFC-1584.

[112] J. Moy. OSPF version 1. Internet Draft, March 1994. RFC-1584.

[113] J. Moy. OSPF version 2. Internet Draft, April 1998. RFC-2328.

[114] M. Naor and M. Yung. Universal hash functions and their cryptographic applications. volume 21st ACM *S*ymposium on Theory of *C*omputing, pages 33–43, Seattle, USA, 1989.

[115] National Institute of Standards and Technology (NIST). FIPS publication 180: Secure Hash Standards (SHS). *National Institute of Standards and Technology (NIST)*, May 1993.

[116] K. Nyberg and R. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94*, volume 950 of LNCS, pages 182–193, Berlin, 1995. Springer-Verlag.

[117] A. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In T. Beth, N Cot, and I Ingemarsson, editors, *Advances in Cryptology: Proceedings of EUROCRYPT '84*, volume 209 of LNCS, pages 224–316, Berlin, 1984. Springer-Verlag.

[118] National Bureau of Standards. Data Encryption Standard. Technical Report 46 ed, U.S. Department of Commerce, US, Jan 1977.

[119] T. Okamat and D. Pointcheval. The Gap-Problems: a new class of problems for the security of cryptographic schemes. In *Public Key Cryptography (PKC'01)*, volume 1992 of LNCS, pages 104–118, Berlin, 2001. Springer-Verlag.

[120] S. Paul. *Multicasting on the internet and its applications.* Kluwer Academic Publisher, 1998.

[121] A. Perrig. The BiBa one-time signature and broadcast authentication protocol. *ACM, CCS'01*, November 2001.

[122] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. In *Computer and Communication Security'00.* ACM press, May 2000.

[123] J. Pieprzyk and D. Pointcheval. Parallel cryptography. In *ACISP'03*, volume 2727 of LNCS, pages 387–401. Springer-Verlag, 2003.

[124] J. Pieprzyk and B. Sadeghiyan. *Design of Hashing Algorithms*. Springer-Verlag, Berlin, 1993.

[125] J. Pieprzyk, H. Wang, and C. Xing. Multiple-time signature schemes secure against adaptive chosen message attack. March 2003.

[126] D. Pointcheval and J. Stern. Security proofs for signature schemes. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of LNCS, pages 387–398, Berlin, 1996. Springer-Verlag.

[127] B. Quinn. IP multicast applications: Challenges and solutions. Internet Draft, November 1998. Expires May 1999.

[128] M.O. Rabin. Digitalized signatures. *Foundations of Secure Computation*, pages 155–168, 1978.

[129] L. Reyzin and N. Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. In J. Sebbery and Ri Safavi Naini, editors, *Seventh Australasian Conference on Information Security and Privacy ACISP'02*, volume 2384 of LNCS, pages 144–152. Springer-Verlag, 2002.

[130] R. Rivest. The MD4 message digest algorithm. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90*, volume 537 of LNCS, pages 303–312, Berlin, 1990. Springer-Verlag.

[131] R. Rivest. The MD5 message-digest algorithm. *RFC 1321*, April 1992.

[132] 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.

[133] P. Rohatchi. A compact and fast hybrid signature scheme for multicast packet authentication. In *Computer and Communications Security'99*, volume 6th of ACM Conference. ACM press, 1999.

[134] J. Rompel. One-way functions are necessary and sufficient for signatures. In *proceedings 22nd ACM Symposium on Theory of Computing*, pages 387–394, Baltimore, Maryland, 1990.

[135] P. Rooij. Efficient Exponentiation using Precomputation and Vector Addition Chains. In A. Santis, editor, *Advances in Cryptology Proceedings of EUROCRYPT'94*, volume 950 of LNCS. Springer-Verlag, 1994.

[136] A. Santis and M. Yung. On the design of provably-secure cryptographic hash functions. In I. Damgård, editor, *Advances in Cryptology Proceedings of EUROCRYPT'90*, volume 473 of LNCS, pages 412–431. Springer-Verlag, 1991.

[137] C. Schnorr. Efficient identification and signatures for smart cards. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology - EUROCRYPT'89*, volume 434 of LNCS, pages 688–689, Berlin, 1989. Springer-Verlag.

[138] C. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4 no. 3:161–174, 1991.

[139] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[140] R. Shankran, V. Varadharjan, and M. Hitchens. Secure multicast extensions for mobile networks. *IEEE Digital Library*, 1999.

[141] C. Shields and J. Garcia-Luna-Aceves. KHIP : a scalable protocol for secure multicast routing. *Computer Communication Review, ACM SIGCOMM'99*, 29(4), October 1999.

[142] V. Shoup. OAEP reconsidered. In Joe Kilian, editor, *Advances in Cryptology Proceedings of Crypto '01*, volume 2139 of LNCS, pages 239–259. Springer-Verlag, 2001.

[143] G. Simmons. Robust shared secret schemes or 'how to be sure you have the right answer even though you don't know the question. In *18th Annual Conference on Numerical Mathematics and Computing*, volume 68 of Congressus Numerantium, pages 215–248, Manitoba, Canada, May 1989.

[144] G. Simmons. How to (really) share a secret. In S. Goldwasser, editor, *Advances in Cryptology Proceedings of CRYPTO '88*, volume 403 of LNCS, pages 390–448. Springer-Verlag, 1990.

[145] G. Simmons. An introduction to shared secret and/or shared control schemes and their application. In G. Simmons, editor, *Contemporary Cryptology - The Science of Information Integrity*, pages 441–497, New York, 1992. IEEE Press.

[146] G. Simmons and M. Norris. Prelimenary comments on the MIT publi-key cryptosystem. In *Cryptologia*, volume 1, pages 406–414, 1977.

[147] B. Smith and J. Garcia-Luna-Aceves. Securing the border gateway routing protocol. *IEEE Digital Library*, 1997.

[148] B. Smith, J. Garcia-Luna-Aceves, and S. Murthy. Securing distance-vector routing protocols. *IEEE Digital Library*, 1996.

[149] M. De Soete and K. Vedder. Some new classes of geometric threshold schemes. In C. Ginther, editor, *Advances in Cryptology Proceedings of EUROCRYPT '88*, volume 330 of LNCS, pages 389–401. Springer-Verlag, 1988.

[150] M. Stadler. Publicly verifiable secret sharing. In *Advances in Cryptology Proceedings of EUROCRYPT '96*, volume 1070 of LNCS, pages 190–199, Berlin, 1996. Springer-Verlag.

[151] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman key distribution extended to group communication. In *3rd ACM Conference on Computer and Communications Security*, pages 276–285, New Delhi, India, March 14-16 1996.

[152] Z. Steinfeld and Y. Zheng. A Signcryption scheme based on integer factorization. In J.Pieprzyk, E. Okamoto, and J. Seberry, editors, *Third International Workshop, Information Security ISW '00, Wollongong - Australia*, volume 1975 of LNCS, pages 308–322, Berlin, 2000. Springer-Verlag.

[153] D. Stinson. Attack on a concast signature scheme. Manuscript.

[154] D. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

[155] D. Stinson and S. Vanstone. A combinatorial approach to threshold schemes. *SIAM J. Disc. Math.*, 1:230–236, May 1988.

[156] B. Szuprowicz. *Webcasting and Push technology strategies: Effective Communications for Intranets and Extranents.* Computer Technologies Research Group, 1998.

[157] D. Vergnaud and F. Laguillaumie. Multi-designated verifiers signature schemes. In *pre-print*, 2004.

[158] D. Vergnaud and F. Laguillaumie. Some remarks on recent advances in designated verifier signature schemes. In *pre-print*, 2004.

[159] D. Waitzman, C. Portridge, and S. Deering. Distance vector multicast routing protocol. Internet Draft, March 1988. RFC-1075.

[160] D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. Internet Draft, September 1998.

[161] G. Wang, F. Bao, J. Zhou, and R. Deng. Security analysis of some proxy signatures. Internet draft, January 2004. http://www.eprint.iacr.org.

[162] H. Wang and J. Pieprzyk. Efficient one-time proxy signature scheme. In C. Laih and C. Chang, editors, *Asiacrypt'03*, volume 2894 of LNCS. Springer-Verlag, 2003.

[163] C. Wong, M. Gouda, and S. Lam. Secure group communications using key graphs. In *Proceedings of ACM SIGCOMM'98*, pages 68–79, Vancouver, Canada, September 1998.

[164] C. Wong and S. Lam. Digital signatures for flows and multicasts. *IEEE/ACM Transaction on Networking*, 7(4), August 1999.

[165] Y. Wu, Di Ma, and C. Xu. Efficient object-based stream authentication. In P. Sarkar A. Menezes, editor, *Progress in Cryptology, INDOCRYPT 2002, Third International Conference on Cryptology in India*, volume 2551 of LNCS, pages 354–367, Berlin, 2002. Springer-Verlag.

[166] S. Yen and C. Laih. Improved digital signature suitable for batch verification. *IEEE Trans. on Computers*, vol. 44(5):729–370, May 1995.

[167] K. Zhang. Threshold proxy signature scheme. In *Proc. of 1st International Information Security Workshop*, 1997.

[168] Y. Zheng. *Principles for Designing Secure Block Ciphers and One-Way Hash Functions*. PhD thesis, Electrical and Computer Engineering, Japan, 1990.

[169] Y. Zheng. Digital Signcryption or how to achieve cost (signature & encryption << cost (signature) + cost (encryption). In Burt Kaliski, editor, *Advances in Cryptology - CRYPTO '97*, volume 1294 of LNCS, pages 165–179, Berlin, 1997. Springer-Verlag.

[170] Y. Zheng, T. Hardjono, and J. Pieprzyk. The sibling intractable function family (SIFF): notion, construction and applications. *IEICE Trans. Fundamentals*, E76-A:4–13, January 1993.