References

[1] D. Balenson, D. Branstad, P. Dinsmore, M. Heyman, and C. Scace. DCCM cryptographic context negotiation protocol. Technical Report TIS report 0757, TIS labs at Network Associates, Inc., February 1999.

[2] D. Balenson, D. Branstad, D. McGrew, and A. Sherman. DCCM architecture and system design. Technical Report TIS report 0709, TIS labs at Network Associates, Inc., June 1998.

[3] D. Balenson, D. McGrew, and A. Sherman. Key management for large dynamic groups: One-way function trees and amortized initialization. draft-irtf-smug-groupkeymgmt-oft-00.txt, Internet Research Task Force, August 2000. Work in progress.

[4] A. Ballardie. Scalable multicast key distribution. RFC 1949 (Experimental), Internet Engineering Task Force, May 1996.

[5] D. Balneson, D. Branstad, D. McGrew, J. Turner, and M. Heyman. DCCM cryptographic context negotiation template. Technical Report TIS report 0745-2, TIS labs at Network Associates, Inc., February 1999.

[6] M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm. Group key management architecture. draft-ietf-msec-gkmarch-02.txt, Internet Engineering Task Force, March 2002. Work in progress.

[7] M. Baugher, R. Canetti, P. Rohatgi, and P. Cheng. MESP: Multicast encapsulating security payload. draft-ietf-msec-mesp-00.txt, Internet Engineering Task Force, October 2002. Work in progress.

[8] M. Baugher, T. Hardjono, H. Harney, and B. Weis. Group domain of interpretation for ISAKMP. draft-ietf-msec-gdoi-04.txt, Internet Engineering Task Force, March 2002. Work in progress.

[9] M. Bellare and P. Rogaway. Entity authentication and key distribution. In *Advances in Cryptology: Proceedings of Crypto 1993*. Springer-Verlag, 1993. LNCS 773.

[10] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation, December 1997.

[11] D. Boneh, G. Durfee, and M. Franklin. Lower bounds for multicast message authentication. In *Proceedings of EUROCRYPT*, pages 437–452, Innsbruck(Tyrol), Austria, May 2001. Springer-Verlag. LNCS 2045.

[12] B. Briscoe. MARKS: Zero side effect multicast key management using arbitrarily revealed key sequences. In *Proceedings of First International Workshop on Networked Group Communication (NGC)*, Pisa, Italy, November 1999.

[13] B. Briscoe and I. Fairman. NARK: Receiver-based multicast non-repudiation and key management. In *Proceedings of the First ACM Conference on E-commerce (EC)*, Denver, CO, November 1999.

[14] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In *Proceedings of EUROCRYPT*, pages 275–286, Perugia, Italy, May 1994. Springer-Verlag. LNCS 950.

[15] M. Burmester and Y. Desmedt. *Efficient and Secure Conference Key Distribution*, volume 1189, page . Springer – Verlag Inc., 1997.

[16] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and efficient constructions. In *Proceedings of IEEE INFOCOM*, New York, March 1999.

[17] R. Canetti, P. Rohatgi, and P. Cheng. Multicast data security transformations: Requirements, considerations, and proposed design. draft-irtf-smug-data-transforms-00.txt, Internet Research Task Force, June 2000. Work in progress.

[18] G. Caronni, M. Waldvogel, D. Sun, and B. Plattner. Efficient security for large and dynamic groups. Technical Report TIK Technical Report No. 41, Computer Engineering and Networks Laboratory, Swiss Federal Institute of Technology, February 1998.

[19] C. Castelluccia and G. Montenegro. Securing group management in IPv6 with cryptographically generated addresses. draft-irtf-gsec-sgmv6-00.txt, Internet Research Task Force, Feb 2001. Work in progress.

[20] I. Chang, R. Engel, D. Kandlur, D. Pendarakis, and D. Saha. Key management for secure Internet multicast using boolean function minimization techniques. In *Proceedings of IEEE INFOCOM*, New York, March 1999.

[21] W. Chen and L. R. Dondeti. Performance comparison of stateful and stateless group rekeying algorithms. In *Proceedings of Fourth International Workshop on Networked Group Communication (NGC)*, Boston, MA, October 2002.

[22] S. Cheung. An efficient message authentication scheme for link state routing. In *Proceedings of 13th annual computer security applications conference*, San Diego, CA, December 1997.

[23] B. Coan, V. Kaul, S. Narain, and W. Stephens. HASM: Hierarchical application-level secure multicast. draft-coan-hasm-00.txt, Internet Research Task Force, Nov 2001. Work in progress.

[24] S. E. Deering. Host extensions for IP multicasting. RFC 1112 (Standard), Internet Engineering Task Force, August 1989.

[25] S. E. Deering and D. R. Cheriton. Multicast routing in datagram internetworks and extended lans. *ACM Transactions on Computer Systems*, 8(2):85–110, May 1990.

[26] W. Diffie, P. van Oorschot, and M. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, June 1992.

[27] P. T. Dinsmore, D. M. Balenson, M. Heyman, P. S. Kruus, C. D. Scace, and A. T. Sherman. Policy-based security management for large dynamic groups: An overview of the DCCM project. In *Proceedings of the DARPA Information Survivability Conference & Exposition Volume I of II (DISCEX)*, pages 64–73, Hilton Head, SC, January 2000.

[28] L. R. Dondeti, S. Mukherjee, and A. Samal. A Dual Encryption Protocol for Scalable Secure Multicasting. In *Proceedings of the Fourth IEEE Symposium on Computers and Communications*, Red Sea, Egypt, July 1999.

[29] L. R. Dondeti, S. Mukherjee, and A. Samal. Comparison of scalable key distribution schemes for secure one-to-many group communication. In *Proceedings of IEEE GLOBECOM Global Internet Symposium*, Brazil, December 1999.

[30] L. R. Dondeti, S. Mukherjee, and A. Samal. Survey and Comparison of Secure Group Communication Protocols. Technical report, University of Nebraska-Lincoln, June 1999.

[31] L. R. Dondeti, S. Mukherjee, and A. Samal. DISEC: A distributed framework for scalable secure many-many communication. In *Proceedings of IEEE International Symposium on Computer Communications (ISCC)*, Antibes, France, July 2000.

[32] L. R. Dondeti, S. Mukherjee, and A. Samal. Scalable secure one-to-many group communication using dual encryption. *Computer Communications*, 23(17):1681–1701, November 2000.

[33] B. DeCleene et. al. Secure group communications for wireless networks. In *Proceedings of the IEEE MILCOM*, pages 113–117, Vienna, VA, October 2001.

[34] D. Farinacci, Y. Rekhter, D. Meyer, P. Lothberg, H. Kilmer, and J. Hall. Multicast source discovery protocol (MSDP). draft-ietf-msdp-spec-03.txt, Internet Engineering Task Force, Jan 2000. Work in progress.

[35] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol independent multicast - sparse mode (PIM-SM): Protocol specification (revised). draft-ietf-pim-sm-v2-new-05.txt, Internet Engineering Task Force, Mar 2002. Work in progress.

[36] A. Fiat and M. Naor. Broadcast Encryption. In *Advances in Cryptology: Proceedings of Crypto 1993*, pages 480–491, 1993. LNCS 773.

[37] R. Gennaro and P. Rohatgi. How to sign digital streams. In *Advances in Cryptology - CRYPTO*, pages 180–197, Santa Barbara, CA, August 1997. Springer-Verlag. LNCS 1294.

[38] P. Golle and N. Modadugu. Authenticating streamed data in the presence of random packet loss. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, pages 13–22, San Diego, CA, February 2001.

[39] L. Gong. Enclaves: Enabling secure collaboration over the Internet. *IEEE Journal on Selected Areas in Communications*, 15(3):567–575, April 1997.

[40] L. Gong and N. Shacham. Elements of trusted multicasting. In *Proc. IEEE Intl. Conf. on Network Protocols*, pages 23–30, Boston, MA, USA, October 1994.

[41] T. Hardjono. Multicast tunnels using IPsec ESP. In *Proceedings of the 10th IEEE Workshop on Local and Metropolitan Area Networks*, Sydney, Autralia, Nov 1999.

[42] T. Hardjono. Router-assistance for receiver access control in PIM-SM. In *Proceedings of IEEE International Symposium on Computer Communications (ISCC)*, Antibes, France, July 2000.

[43] T. Hardjono, M. Baugher, and H. Harney. Group key management for IP multicast: Model and architecture. In *IEEE 10th International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2001)*, MIT, Cambridge, MA, June 2001. IEEE.

[44] T. Hardjono, M. Baugher, and H. Harney. Group security association (GSA) management in IP multicast. In *Proceedings of the 16th International Conference on Information Security (IFIP/SEC)*, Paris, France, June 2001.

[45] T. Hardjono and B. Cain. PIM-SM security: Interdomain issues and solutions. In Bart Preneel, editor, *Communications and Multimedia Security (CMS'99)*, Leuven, Belgium, September 1999. Kluwer.

[46] T. Hardjono and B. Cain. Simple key management protocol for PIM. draft-ietf-pim-simplekmp-01.txt, Internet Engineering Task Force, February 2000. Work in progress.

[47] T. Hardjono, B. Cain, and N. Doraswamy. A framework for group key management for multicast security. draft-ietf-ipsec-gkmframework-03.txt, Internet Engineering Task Force, August 2000. Work in progress.

[48] T. Hardjono, B. Cain, and I. Monga. Intra-domain group key management protocol. draft-ietf-ipsec-intragkm-02.txt, Internet Engineering Task Force, February 2000. Work in progress.

[49] T. Hardjono, R. Canetti, M. Baugher, and P. Dinsmore. Secure IP multicast: Problem areas, framework and building blocks,. draft-irtf-smug-framework-01.txt,, Internet Research Task Force, September 2000. Work in progress.

[50] T. Hardjono and H. Harney. Group security policy management for IP multicast and group security. In *IFIP Networking*, Pisa, Italy, May 2002. Poster.

[51] T. Hardjono, H. Harney, P. McDaniel, A. Colegrove, and P. Dinsmore. Group security policy token. draft-ietf-msec-gspt-00.txt, Internet Engineering Task Force, September 2001. Work in progress.

[52] T. Hardjono and G. Tsudik. IP multicast security: issues and directions. November 2000.

[53] T. Hardjono, L. Vicisano, and L. Dondeti. Security considerations for NORM protocols, March 2001. Internet draft in preparation.

[54] T. Hardjono and B. Whetten. Security requirements for TRACK. draft-ietf-rmt-pi-track-security-00.txt, Internet Engineering Task Force, June 2000. Work in progress.

[55] D. Harkins and D. Carrel. The Internet key exchange (IKE). RFC 2409 (Proposed Standard), Internet Engineering Task Force, November 1998.

[56] D. Harkins and N. Doraswamy. A secure scalable multicast key management protocol (MKMP). draft-ieft-ipsec-mkmp-00.txt, Internet Engineering Task Force, November 1997. expired.

[57] H. Harney, M. Baugher, and T. Hardjono. GKM building block: Group security association (GSA) definition. draft-irtf-smug-gkmbb-gsadef-01.txt, Internet Research Task Force, Sept 2000. Work in progress.

[58] H. Harney, A. Colegrove, E. Harder, U. Meth, and R. Fleischer. Group secure association key management protocol. draft-ietf-msec-gsakmp-sec-00.txt, Internet Engineering Task Force, March 2001. Work in progress.

[59] H. Harney, A. Colegrove, and P. McDaniel. Principles of policy in secure groups. In *Proceedings of network and distributed systems security 2001 Internet society*, San Diego, CA, February 2001.

[60] H. Harney and E. Harder. Multicast security management protocol (MSMP) requirements and policy. draft-harney-msmp-sec-00.txt, Internet Engineering Task Force, March 1999. Work in progress.

[61] H. Harney and C. Muckenhirn. Group key management protocol (GKMP) architecture. RFC 2094 (Experimental), July 1997.

[62] H. Harney and C. Muckenhirn. Group key management protocol (GKMP) specification. RFC 2093 (Experimental), July 1997.

[63] R. Hauser, T. Przygienda, and G. Tsudik. Reducing the cost of security in link-state routing. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, February 1997.

[64] H. He, B. Cain, and T. Hardjono. Upload authentication information using IGMPv3. draft-he-magma-igmpv3-auth-00.txt, Internet Research Task Force, November 2001. Work in progress.

[65] H. He, T. Hardjono, and B. Cain. Simple multicast receiver access control. draft-irtf-gsec-smrac-00.txt, Internet Research Task Force, November 2001. Work in progress.

[66] I. Ingemarsson, D. T. Tang, and C. K. Wong. A conference key distribution system. *IEEE Transactions on Information Theory*, IT-28(5):714–720, 1982.

[67] N. Ishikawa, N. Yamanouchi, and O. Takahashi. IGMP extensions for authentication of IP multicast senders and receivers. draft-ishikawa-igmp-auth-01.txt, Internet Engineering Task Force, August 1998. Work in progress.

[68] P. Judge and M. Ammar. Gothic: A group access control architecture for secure multicast and anycast. In *Proceedings of IEEE INFOCOM*, New York, NY, June 2002.

[69] P. Karn and W. Simpson. Photuris: Session-key management protocol. RFC 2522 (Experimental), Internet Engineering Task Force, March 1999.

[70] S. Kent and R. Atkinson. IP authentication header (AH). RFC 2402 (Proposed Standard), Internet Engineering Task Force, November 1998.

[71] S. Kent and R. Atkinson. IP encapsulating security payload (ESP). RFC 2406 (Proposed Standard), Internet Engineering Task Force, November 1998.

[72] S. Kent and R. Atkinson. Security architecture for the Internet protocol. RFC 2401 (Proposed Standard), Internet Engineering Task Force, November 1998.

[73] K. P. Kihlstrom, L. E. Moser, and P. M. Melliar-Smith. The SecureRing protocols for securing group communication. In *Proceedings of the IEEE 31st Hawaii International Conference on System Sciences*, pages 317–326, Kona, Hawaii, Jan 1998.

[74] K. Koyama and K. Ohta. Identity-based conference key distribution systems. In C. Pomerance, editor, *Advances in Cryptology - CRYPTO (Lecture Notes in Computer Science No. 293)*, pages 175–184. G. Goos and J. Hartmanis, Springer-Verlag, 1987.

[75] K. Koyama and K. Ohta. Security of improved identity-based conference key distribution systems. In C. G. Gunther, editor, *Proceedings of EU-*

ROCRYPT (Lecture Notes in Computer Science No. 330), pages 11–19. Springer-Verlag, 1988.

[76] H. Krawczyk. SKEME: A versatile secure key exchange mechanism for the Internet. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, 1996.

[77] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: keyed-hashing for message authentication. RFC 2104 (Informational), Internet Engineering Task Force, February 1997.

[78] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11), November 1981.

[79] J. Lotspiech, M. Naor, and D. Naor. Subset difference based key management for secure multicast. draft-irtf-smug-subsetdifference-00.txt, Internet Research Task Force, July 2001. Work in progress.

[80] S. H. Low, N. F. Maxemchuk, and S. Paul. Anonymous credit cards and their collusion analysis. *IEEE/ACM Transactions on Networking*, December 1996.

[81] C. Madson and R. Glenn. The use of HMAC-MD5-96 within ESP and AH. RFC 2403 (Proposed Standard), Internet Engineering Task Force, November 1998.

[82] C. Madson and R. Glenn. The use of HMAC-SHA-1-96 within ESP and AH. RFC 2404 (Proposed Standard), Internet Engineering Task Force, November 1998.

[83] D. Malki, M. Merritt, and O. Rodeh. Secure reliable multicast protocols in a WAN. In *Proceeding of ICDCS*, Baltimore, Maryland, May 1997. IEEE.

[84] D. Malki and M. Reiter. A high-throughput secure reliable multicast protocol. Technical Report TR 96-1-1, AT&T Laboratories, Murray Hill, NJ, July 1996.

[85] G. Malkin. RIP version 2. RFC 2453 (Standard), Internet Engineering Task Force, November 1998.

[86] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol (ISAKMP). RFC 2408 (Proposed Standard), Internet Engineering Task Force, November 1998.

[87] L. McCarthy. RTP profile for source authentication and non-repudiation of audio and video conferences. draft-mccarthy-smug-rtp-profile-src-auth-00.txt, Internet Engineering Task Force, May 1999. Work in progress.

[88] P. McDaniel and A. Prakash. Antigone: implementing policy in secure group communication. Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, University of Michigan, May 2000.

[89] P. McDaniel and A. Prakash. Ismene: Provisioning and policy reconciliation in secure group communication. Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, University of Michigan, December 2000.

[90] P. McDaniel and A. Prakash. Methods and limitations of security policy reconciliation. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 73–87, Oakland, CA, May 2002. IEEE Computer Society.

[91] 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, Washington, D.C., August 1999.

[92] P. McDaniel, A. Prakash, J. Irrer, S. Mittal, and T. Thuang. Flexibly constructing secure groups in Antigone 2.0. In *Proceedings of DARPA Information Survivability Conference and Exposition II*, pages 55–67, Anaheim, CA, June 2001.

[93] D. A. McGrew and A. T. Sherman. Key establishment in large dynamic groups using one-way function trees. *Submitted to IEEE Transactions on Software Engineering*, May 1998.

[94] A. Meissner, L. Wolf, and R. Steinmetz. A novel group integrity concept for multimedia multicasting. In *Proceedings of the 8th International Workshop on Interactive Distributed Multimedia Systems (IDMS)*, pages 233–244, Lancaster, UK, September 2001. Springer-Verlag. LNCS 2158.

[95] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. Series on discrete mathematics and its applications. CRC Press, 1997.

[96] R. C. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology - Crypto*, pages 369–378, Berlin, August 1987. Springer-Verlag. LNCS 293.

[97] R. C. Merkle. A certified digital signature. In *Advances in Cryptology - Crypto*, pages 218–238, Berlin, August 1989. Springer-Verlag. LNCS 435.

[98] D. Meyer. Administratively scoped IP multicast. RFC 2365 (Best Current Practice), Internet Engineering Task Force, July 1998.

[99] K. Miller, K. Robertson, A. Tweedly, and M. White. Starburst multicast file transfer protocol (MFTP) specification. draft-miller-mftp-spec-03.txt, Internet Research Task Force, April 1998. Work in progress.

[100] S. Miner and J. Staddon. Graph-based authentication of digital streams. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 232–246, Oakland, CA, May 2001.

[101] S. Mittra. Iolus: A framework for scalable secure multicasting. In *Proceedings of ACM SIGCOMM*, pages 277–288, Cannes, France, September 1997.

[102] A. Van Moffaert and O. Paridaens. Security issues in Internet group management protocol version 3 (IGMPv3). draft-irtf-gsec-igmpv3-security-issues-01.txt, Internet Research Task Force, Feb 2002. Work in progress.

[103] A. Van Moffaert and O. Paridaens. Security issues in protocol independent multicast - sparse mode (PIM-SM). draft-irtf-gsec-pim-sm-security-issues-01.txt, Internet Research Task Force, Feb 2002. Work in progress.

[104] R. Molva and A. Pannetrat. Scalable multicast security in dynamic groups. In *6th ACM conference on computer and communication security*, Singapore, November 1999.

[105] I. Monga and T. Hardjono. Group security association (GSA) definition for IP multicast. draft-irtf-smug-gsadef-00.txt, Internet Engineering Task Force, February 1999. Work in progress.

[106] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *Advances in cryptology - CRYPTO*, Santa Barbara, CA, August 2001. Springer-Verlag Inc. LNCS 2139.

[107] H. Orman. The OAKLEY key determination protocol. RFC 2412 (Informational), Internet Engineering Task Force, November 1998.

[108] J. Park, E. Chong, and H. Siegel. Efficient multicast packet authentication using signature amortization. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, May 2002.

[109] R. Perlman. *Network layer protocols with byzantine robustness*. PhD dissertation, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, August 1988.

[110] A. Perrig, R. Canetti, B. Briscoe, J. D. Tygar, and D. Song. TESLA: multicast source authentication transform. draft-irtf-smug-tesla-00.txt, Internet Research Task Force, November 2000. Work in progress.

[111] A. Perrig, R. Canetti, D. Song, and J. D. Tygar. Efficient and secure source authentication for multicast. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, pages 35–46, San Diego, CA, February 2001.

[112] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 56–73, Oakland, CA, May 2000.

[113] D. Piper. The Internet IP security domain of interpretation for ISAKMP. RFC 2407 (Proposed Standard), Internet Engineering Task Force, November 1998.

[114] O. Rodeh, K. Birman, and D. Dolev. Optimized group rekey for group communication systems. In *Proceedings of Network and Distributed System Security Symposium*, San Diego, CA, February 3-4 2000.

[115] O. Rodeh, K. Birman, M. Hayden, Z. Xiao, and D. Dolev. Ensemble security. Technical Report TR98-1703, Cornell University, September 1998.

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

[117] S. Setia, S. Koussiah, S. Jajodia, and E. Harder. Kronos: A scalable rekeying approach for secure multicast. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, May 2000.

[118] S. Setia, S. Zhu, and S. Jajodia. A comparative performance analysis of reliable group rekey transport protocols for secure multicast. In *Proceedings of Performance 2002*, Rome, Italy, September 2002.

[119] C. Shields and J. J. Garcia-Luna-Aceves. KHIP – a scalable protocol for secure multicast routing. In *Proceedings of ACM SIGCOMM*, Cambridge, MA, September 1999.

[120] T. Shiroshita, O. Takahashi, and M. Yamashita. Integrating layered security into reliable multicast. In *Proceedings of the Third International Workshop on Protocols for Multimedia Systems*, Madrid, October 1996.

[121] K. E. Sirois and S. T. Kent. Securing the Nimrod routing architecture. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, February 1997.

[122] M. Sloman and E. Lupu. Security and management policy specification. *IEEE Network, special issue on policy-based networking*, 16(2):10–19, March/April 2002.

[123] B. R. Smith, S. Murthy, and J. J. Garcia-Luna-Aceves. Securing distance vector routing protocols. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, February 1997.

[124] W. Stallings. *Network and Internetwork Security*. Prentice-Hall Inc., 1995.

[125] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman key distribution extended to group communications. In *Proceedings of the Third ACM Conference on Computer and Communications Security*, New Delhi, March 1996.

[126] M. Steiner, G. Tsudik, and M. Waidner. CLIQUES: A New Approach to Group Key Agreement. Technical report, IBM Research Division, December 1997.

[127] M. Valdvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner. The VersaKey framework: versatile group key management. *IEEE JSAC Special Issue on Service Enabling Platforms For Networked Multimedia Systems*, 17(9), September 1999.

[128] C. Villamizar, C. Alaettinoglu, D. Meyer, S. Murphy, and C. Orange. Routing policy system security. draft-ietf-rps-auth-01.txt, Internet Engineering Task Force, May 1998. Work in progress.

[129] D. Wallner, E. Harder, and R. Agee. Key management for multicast: issues and architectures. RFC 2627(Informational), Internet Engineering Task Force, June 1999.

[130] L. Wei. Authenticating PIM version 2 messages. draft-ietf-pim-v2-auth-01.txt, Internet Engineering Task Force, May 1999. Work in progress.

[131] B. Weis. The use of RSA signatures within ESP and AH. draft-bew-ipsec-signatures-00.txt, Internet Engineering Task Force, October 2002. Work in progress.

[132] B. Whetten, T. Montgomery, and S. Kaplan. A high perfomance totally ordered multicast protocol. In K. P. Birman, F. Mattern, and A. Schipper, editors, *Theory and Practice in Distributed Systems: International Workshop*, pages 33–57. Springer-Verlag, 1995.

[133] C. K. Wong, M. Gouda, and S. S. Lam. Secure group communications using key graphs. In *Proceedings of ACM SIGCOMM*, Vancouver, Canada, September 1998.

[134] C. K. Wong, M. Gouda, and S. S. Lam. Secure group communications using key graphs. *IEEE/ACM Transactions on Networking*, 8(1):16–30, February 2000.

[135] C. K. Wong and S. S. Lam. Digital signatures for flows and multicasts. *IEEE/ACM Transactions on Networking*, 7(4):502–513, August 1999.

[136] Y. R. Yang, X. S. Li, X. B. Zhang, and S. S. Lam. Reliable group rekeying: design and performance analysis. In *Proceedings of ACM SIGCOMM*, San Diego, CA, August 2001.

[137] K. Zhang. Efficient protocols for signing routing messages. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, pages 29–35, San Diego, CA, 1998.

[138] X. B. Zhang, Y. R. Yang, S. S. Lam, and D. Y. Lee. Protocol design for scalable and reliable group rekeying. In *Proceedings of SPIE conference on scalability and traffic control in IP networks*, Denver, C0, August 2001.