References

[1] P. Sadhukhan, P. K. Das, and S. Saha, "Hybrid mobility management schemes integrating mobile IP and SIP for seamless invocation of services in all-IP network," *Telecommunication Systems*, 2011. doi: 10.1007/s11235-011-9483-7.

[2] W. Znaidi and M. P. Minier, "Key establishment and management for WSNs," *Telecommunication Systems*, 2011. doi: 10.1007/s11235-010-9391-2.

[3] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad hoc networks," in *Proceedings of the Symposium on Applications and the Internet Workshop (SAINT'03)*, pp. 342–346, IEEE Computer Society, 2003.

[4] N. W. Wang, H. C. Chao, I. Y. Chen, and Y. M. Huang, "A novel user's authentication scheme for pervasive on-line media services," *Telecommunication Systems*, vol. 44, no. 3-4, pp. 181–190, 2011.

[5] C. C. Lee, I. E. Liao, and M. S. Hwang, "An efficient authentication protocol for mobile communications," *Telecommunication Systems*, vol. 46, no. 1, pp. 31–41, 2011.

[6] J. Park and Q. Jin, "Effective session key distribution for secure fast handover in mobile networks," *Telecommunication Systems*, vol. 44, no. 1-2, pp. 97–107, 2010.

[7] J. Kim and K. Kim, "A scalable and robust hierarchical key establishment for mission-critical applications over sensor networks," *Telecommunication Systems*, 2011. doi: 10.1007/s11235-011-9650-x.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology (Crypto'84)*, vol. 196, pp. 47–53, LNCS, Springer-Verlag, New York, 1984.

[9] S. H. Liaw, P. C. Su, H. K. C. Chang, E. H. Lu, and S. F. Pon, "Secured key exchange protocol in wireless mobile ad hoc networks," in *Proceedings of the International Carnahan Conference on Security Technology (CCST'05)*, pp. 171–173, 2005.

[10] N. Kettaf, H. Abouaissa, and P. Lorenz, "An efficient heterogeneous key management approach for secure multicast communications in ad-hoc networks," *Telecommunication Systems*, vol. 37, no. 1-3, pp. 29–36, 2008.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practices*. Pearson Education, Inc., 2007.

[12] S. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer-Verlag, New York, USA, 2004.

[13] A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

[14] X. Cao, W. Kou, Y. Yu, and R. Sun, "Identity-based authentication key agreement protocols without bilinear pairings," *IEICE Transaction on Fundamentals*, vol. E91, no. A12, pp. 3833–3836, 2008.

[15] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[16] R. W. Zhu, G. Yang, and D. S. Wong, "An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices," *Theoretical Computer Science*, vol. 9, no. 2, pp. 198–207, 2007.

[17] J. Nam, J. Lee, S. Kim, and D. Won, "DDH-based group key agreement in a mobile environment," *Journal of Systems and Software*, vol. 78, no. 1, pp. 73–83, 2005.

[18] Y. M. Tseng, "On the security of two group key agreement protocols for mobile devices," in *Proceedings of the International Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT'06)*, pp. 59–62, 2006.

[19] C. C. Lee, T. H. Lin, and C. S. Tsai, "A new authenticated group key agreement in a mobile environment," *Annals of Telecommunications*, vol. 64, no. 11-12, pp. 735–744, 2009.

[20] Q. F. Cheng, C. G. Ma, and F. S. Wei, "Analysis and improvement of a new authenticated group key agreement in a mobile environment," *Annals of Telecommunications*, vol. 66, no. 5-6, pp. 331–337, 2011.

[21] J. L. Tasi, "A novel authenticated group key agreement protocol for mobile environment," *Annals of Telecommunications*, vol. 66, no. 11-12, pp. 663–669, 2011.

[22] D. He, J. Chen, and J. Hu, "Identity-based digital signature scheme without bilinear pairings." Cryptology ePrint Archieve, Report 2011/079, 2011.

[23] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[24] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Proceedings of the Public Key Cryptography (PKC'04)*, vol. 2947, pp. 277–290, LNCS, Berlin/Heidelberg, 2004.

[25] C. P. Schnorr, "Efficient identification and signatures for smart cards," in *Proceedings of the Advances in Cryptology (Crypto'89)*, vol. 435, pp. 239–252, LNCS, Berlin/Heidelberg, 1990.

[26] M. Abe and T. Okamoto, "Provably secure partially blind signatures," in *Proceedings of the Advances in Cryptology (Crypto'00)*, vol. 1880, pp. 271–286, LNCS, Berlin/Heidelberg, 2000.

[27] D. Chaum, "Blind signatures for untraceable payments," in *Proceedings of the Advances in Cryptology (Crypto'82)*, pp. 199–203, LNCS, Berlin/Heidelberg, 1983.

[28] D. Chaum, "Online cash checks," in *Proceedings of the Advances in Cryptology (Eurocrypt'89)*, vol. 434, pp. 288–293, LNCS, Berlin/Heidelberg, 1989.

[29] M. Abe and E. Fujisaki, "How to date blind signatures," in *Proceedings of the Advances in Cryptology (Asiacrypt'96)*, vol. 1163, pp. 244–251, LNCS, Berlin/Heidelberg, 1996.

[30] R. S. Anand and C. E. Madhavan, "An online, transferable e-cash payment system," in *Proceedings of the Progress in Cryptology (Indocrypt'00)*, vol. 1977, pp. 77–91, LNCS, Berlin/Heidelberg, 2000.

[31] M. Z. Ashrafi and S. K. Ng, "Privacy-preserving e-payments using one-time payment details," *Computer Standards and Interfaces*, vol. 31, pp. 321–328, 2009.

[32] M. Au, Q. Wu, W. Susilo, and Y. Mu, "Compact e-cash from bounded accumulator," in *Proceedings of the Topics in Cryptology (CT-RSA'07)*, vol. 4377, pp. 178–195, LNCS, Springer Berlin/Heidelberg, 2007.

[33] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact E-cash," in *Proceedings of the Advances in Cryptology (Eurocrypt'05)*, vol. 3494, pp. 566–591, LNCS, Berlin/Heidelberg, 2005.

[34] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal of Computing*, vol. 32, pp. 586–615, 2003.

[35] P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proceedings of the Advances in Cryptology (Crypto'02)*, vol. 2442, pp. 354–369, LNCS, Berlin/Heidelberg, 2002.

[36] P. Barreto, H. Kim, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups," in *Proceedings of the Selected Areas in Cryptography*, vol. 3006, pp. 17–25, LNCS, Berlin/Heidelberg, 2004.

[37] M. Girault, "Self-certified public keys," in *Proceedings of the Advances in Cryptology (Eurocrypt'91)*, vol. 547, pp. 490–497, LNCS, Berlin/Heidelberg, 1991.

[38] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of the Advances in Cryptology (Asiacrypt'03)*, vol. 2894, pp. 452–473, LNCS, Berlin/Heidelberg, 2003.

[39] S. H. Tan, S. H. Heng, and B. M. Goi, "Java implementation for pairing-based cryptosystems," in *Proceedings of the International Conference in Computational Science and Its Applications (ICCSA'10)*, vol. 6019, pp. 188–198, LNCS, Berlin/Heidelberg, 2010.

[40] M. Holbl and B. Brumen, "Two proposed identity-based three-party authenticated key agreement protocols from pairings," *Computers and Security*, vol. 29, no. 2, pp. 244–252, 2010.

[41] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Proceedings of the Advances in Cryptology (Crypto'93)*, vol. 773, pp. 232–249, LNCS, Berlin/Heidelberg, 1994.

[42] M. Ballare 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 (CCS'93)*, pp. 62–73, 1993.

[43] M. J. Beller and Y. Yacobi, "Fully-fledged two-way public key authentication and key agreement for low-cost terminals," *Electronics Letters*, vol. 29, no. 11, pp. 999–1001, 1993.

[44] I. C. Lin, C. C. Chang, and M. S. Hwang, "Security enhancement for the simple authentication key agreement algorithm," in *Proceedings of the 24th annual International Computer Software and Applications Conference (COMPSAC'02)*, pp. 113–115, IEEE Computer Society, 2002.

[45] H. Sun and B. Hsieh, "Security analysis of shim's authenticated key agreement protocols from pairings." Cryptology ePrint Archieve Report 2003/113, 2003.

[46] R. Lu, Z. Cao, and H. Zhu, "An enhanced authenticated key agreement protocol for wireless mobile communication," *Computer Standards and Interfaces*, vol. 29, no. 6, pp. 647–652, 2007.

[47] C. C. Chang and S. C. Chang, "An Improved Authentication Key Agreement Protocol Based on Elliptic Curve for Wireless Mobile Networks," in *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1375–1378, 2008.

[48] A. Sui, L. Hui, S. Yiu, K. Chow, W. Tsang, C. Chong, K. Pun, and H. Chan, "An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication," in *Proceedings of the IEEE Wireless and Communications and Networking Conference (WCNC'05)*, pp. 2088–2093, 2005.

[49] J. W. Lo, C. C. Lee, and M. S. Hwang, "A Secure and Efficient ECC-based AKA Protocol for Wireless Mobile Communications," *International Journal of*

Innovative Computing, Information and Control, vol. 6, no. 11, pp. 5249–5258, 2010.

[50] Q. Pu, "Cryptanalysis of Lu et al.'s Password-based Authenticated Key Agreement Protocol," in *Proceedings of the 2nd International Conference on Multimedia and Information Technology*, pp. 215–218, 2010.

[51] T. Y. Youn, E. S. Kang, and C. Lee, "Efficient three-party key exchange protocols with round efficiency," *Telecommunication Systems*, 2011. doi: 10.1007/s11235-011-9649-3.

[52] H. Guo, Z. Li, Y. Mu, and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," *Computers and Security*, vol. 27, no. 1-2, pp. 16–21, 2008.

[53] H. Guo, C. Xu, Y. Mu, and Z. Li, "A provably secure authenticated key agreement protocol for wireless communications," *Computers and Electrical Engineering*, vol. 38, no. 3, pp. 563–572, 2012.

[54] L. Chen and C. Kudla, "Identity based key agreement protocols from pairings," in *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, pp. 219–233, 2002.

[55] N. P. Smart, "An identity based authenticated key agreement protocol based on the weil pairing," *Electronics Letters*, vol. 38, no. 13, pp. 630–632, 2002.

[56] N. McCullagh and P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement," in *Proceedings of the Topics in Cryptology (CT-RSA'05)*, vol. 3376, pp. 262–274, LNCS, Berlin/Heidelberg, 2005.

[57] Y. J. Choie, E. Jeong, and E. Lee, "Efficient identity-based authenticated key agreement protocol from pairings," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 179–188, 2005.

[58] S. Wang, Z. Cao, and F. Cao, "Efficient Identity-based Authenticated Key Agreement Protocol with PKG Forward Secrecy," *International Journal of Network Securitys*, vol. 7, no. 2, pp. 181–186, 2008.

[59] S. Wang, Z. Cao, K. K. R. Choo, and L. Wang, "A proposed identity-based key agreement protocol and its security proof," *Information Sciences*, vol. 179, no. 3, pp. 307–318, 2009.

[60] C. L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Computers and Security*, vol. 22, no. 1, pp. 68–72, 2003.

[61] M. Peyravian and N. Zunic, "Methods for protecting password transmission," *Computers and Security*, vol. 19, no. 5, pp. 466–469, 2000.

[62] J. J. Hwang and T. C. Yeh, "Improvement on Peyravian-Zunic's password authentication schemes," *IEICE Transactions on Communications*, vol. E85, no. B4, pp. 823–825, 2002.

[63] L. Zhu, S. Yu, and X. Zhang, "Improvement upon mutual password authentication scheme," in *Proceedings of the International Seminar on Business and Information Management (ISBIM'08)*, vol. 1, pp. 400–403, 2008.

[64] J. H. Yang and C. C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computes and Security*, vol. 28, no. 3-4, pp. 138–143, 2009.

[65] E. J. Yoon and K. Y. Yoo, "Robust ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC," in *Proceedings of the International Conference on Computational Science and Engineering*, pp. 633–640, 2009.

[66] T. H. Chen, Y. C. Chen, and W. K. Shih, "An advanced ECC ID-based remote mutual authentication scheme for mobile devices," in *Proceedings of the*

7th International Conference on Ubiquitous, Autonomic and Trusted Computing, pp. 116–120, 2010.

[67] S. Song, M. Abid, H. Moustafa, and H. Afifi, "Performance evaluation of an authentication solution for IMS services access," *Telecommunication Systems*, 2011. doi: 10.1007/s11235-011-9543-z.

[68] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing," *Electronics Letters*, vol. 39, no. 8, pp. 653–654, 2003.

[69] E. Ryu, E. Yoon, and K. Yoo, "An efficient ID-based Authenticated Key Agreement Protocol from Pairings," in *Proceedings of the Networking'04*, vol. 3042, pp. 1458–1463, LNCS, Berlin/Heidelberg, 2004.

[70] C. Boyd and K. K. R. Choo, "Security of Two-Party Identity-based Key Agreement," in *Proceedings of the Progress in Cryptology (Mycrypt'05)*, vol. 3715, pp. 229–243, LNCS, Berlin/Heidelberg, 2005.

[71] G. Xie, "Cryptanalysis of Noel Mccullagh and P. S. L. M. Barreto's two-party identity-based key agreement." Cryptology ePrint Archieve, Report 2004/308, 2004.

[72] S. Li, Q. Yuan, and J. Li, "Towards security two-part authenticated key agreement protocols." Cryptology ePrint Archieve, Report 2005/300, 2005.

[73] M. Hölbl, T. Welzer, and B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Science*, vol. 78, no. 1, pp. 142–150, 2012.

[74] B. T. Hsieh, H. M. Sun, T. Hwang, and C. T. Lin, "An improvement of saeednia's identity based key exchange protocol," in *Proceedings of the Information Security Conference*, pp. 41–43, 2002.

[75] S. Saeednia, "Improvement of Gunther's identity-based key exchange protocol," *Electronics Letters*, vol. 36, no. 18, pp. 1535–1536, 2000.

[76] Y. M. Tseng, J. K. Jan, and C. H. Wang, "Cryptanalysis and improvement of an identity based key exchange protocol," *Journal of Computers*, vol. 14, no. 3, pp. 7–22, 2002.

[77] M. Hölbl and T. Welzer, "Two improved two-party identity-based authenticated key agreement protocols," *Computer Standards and Interfaces*, vol. 31, pp. 1056–1060, 2003.

[78] Y. M. Tseng, "An efficient two-party identity-based key exchange protocol," *Informatica*, vol. 18, no. 1, pp. 125–136, 2007.

[79] S. Zhang, Q. Cheng, and X. Wang, "Impersonation attack on two identity-based authenticated key exchange protocols," in *Proceedings of the WASE International Conference on Information Engineering*, pp. 113–116, 2010.

[80] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Conference on Advances in Cryptology (Crypto'01)*, vol. 2139, pp. 213–229, LNCS, Berlin/Heidelberg, 2001.

[81] S. Wang, Z. Cao, K. K. R. Choo, and L. Wang, "An improved identity-based key agreement protocol and its security proof," *Information Sciences*, vol. 179, pp. 307–318, 2009.

[82] K. K. R. Choo, C. Boyd, Y. Hitchcock, and G. Maitland, "On session identifiers in provably secure protocols: the Bellare-Rogaway three-party key distribution protocol revisited," in *Proceedings of the SCN'04*, vol. 3352, pp. 351–366, LNCS, Berlin/Heidelberg, 2005.

[83] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of the Advances in Cryptology (Crypto'85)*, vol. 218, pp. 417–426, LNCS, Springer-Verlag, New York, 1985.

[84] N. Koblitz, "Elliptic curve cryptosystem," *Journal of Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[85] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," *Computer Communications*, vol. 27, no. 17, pp. 1730–1737, 2004.

[86] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[87] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[88] J. Nam, S. Kim, and D. Won, "A weakness in the Bresson-Chevassut-Essiari-Pointcheval's group key agreement scheme for low-power mobile devices," *IEEE Communications Letters*, vol. 9, no. 5, pp. 429–431, 2005.

[89] J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," *Journal of Cryptology*, vol. 20, no. 1, pp. 485–113, 2003.

[90] D. Boneh, "The Decision Diffie-Hellman problem," in *Proceedings of the Third Algorithmic Number Theory Symposium*, vol. 1423, pp. 48–63, LNCS, Berlin/Heidelberg, 1998.

[91] Y. M. Tseng, "A resource-constrained group key agreement protocol for imbalanced wireless networks," *Computers and Security*, vol. 26, no. 4, pp. 331–337, 2007.

[92] M. Manulis, K. Suzuki, and B. Ustaoglu, "Modeling Leakage of Ephemeral Secrets in Tripartite/Group Key Exchange," in *Proceeding of the 12th international conference onInformation, Security and Cryptology (ICISC'09)*, vol. 5984, pp. 16–33, LNCS, Berlin/Heidelberg, 2010.

[93] W. Yuan, L. Hu, H. Li, and J. Chu, "Cryptanalysis of Lee et al.'s authenticated group key agreement," in *Proceedings of the Advanced in Control Engineering and Information Science*, vol. 15, pp. 1421–1425, 2011.

[94] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proceedings of the Advances in Cryptology (Eurocrypt'01)*, vol. 2045, pp. 453–474, LNCS, Berlin/Heidelberg, 2001.

[95] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *Proceedings of the 6th IMA International Conference on Cryptography and Coding*, vol. 1335, pp. 30–45, LNCS, Springer-Verlag, New York, 1997.

[96] J. Zhao and D. Gu, "Provably secure three-party password-based authenticated key exchange protocol," *Information Sciences*, vol. 184, no. 1, pp. 310–323, 2012.

[97] Z. Cheng, M. Nistazakis, R. Comley, and L. Vasiu, "On the in distinguishability-based security model of key agreement protocols-simple cases." Cryptology ePrint Archieve Report 2005/129, 2005.

[98] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes," in *Proceedings of the Cryptology and Network Security (CANS'05)*, vol. 3810, pp. 13–25, LNCS, Berlin/Heidelberg, 2005.

[99] Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: Security model and efficient construction," in *Proceedings of the Applied*

Cryptography and Network Security (ACNS'06), vol. 3989, pp. 293–308, LNCS, Berlin/Heidelberg, 2006.

[100] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateles signature revisited," in *Proceedings of the 12th Australasian Conference on Information Security and Privacy (ACISP'07)*, vol. 3989, pp. 308–322, LNCS, Berlin/Heidelberg, 2007.

[101] D. Yum and P. Lee, "Generic construction of certificateless signature," in *Proceedings of the International Conference on Information Security and Privacy*, vol. 3108, pp. 200–211, LNCS, Berlin/Heidelberg, 2004.

[102] M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Proceedings of the International Conference on Computational Intelligence and Security*, vol. 3802, pp. 110–116, LNCS, Berlin/Heidelberg, 2005.

[103] W. S. Yap, S. H. Heng, and B. M. Goi, "An efficient certificateless signature scheme," in *Proceedings of the Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4097, pp. 322–331, LNCS, Berlin/Heidelberg, 2006.

[104] K. Choi, J. Park, J. Hwang, and D. Lee, "Efficient certificateless signature schemes," in *Proceedings of the Applied Cryptography and Network Security (ACNS'07)*, vol. 4521, pp. 443–458, LNCS, Berlin/Heidelberg, 2007.

[105] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu, "A certificateless signature scheme for mobile wireless cyber-physical systems," in *Proceedings of the International Conference on Distributed Computing Systems Workshops (ICDCS'08)*, pp. 489–494, 2008.

[106] L. Zhang and F. Zhang, "A new provably secure certificateless signature scheme," in *Proceedings of the IEEE International Conference on Communications (ICC'08)*, pp. 1685–1689, 2008.

[107] F. Li and P. Liu, "An efficient certificateless signature scheme from bilinear parings," in *Proceedings of the International Conference on Network Computing and Information Security*, pp. 35–37, 2011.

[108] B. Hu, D. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Proceedings of the Information Security and Privacy*, vol. 4058, pp. 235–246, LNCS, Berlin/Heidelberg, 2006.

[109] X. Cao, K. G. Paterson, and W. Kou, "An attack on a certificateless signature scheme." Cryptology ePrint Archieve, Report 2006/367, 2006.

[110] Z. Zhang and D. Feng, "Key replacement attack on a certificateless signature scheme." Cryptology ePrint Archieve, Report 2006/453, 2006.

[111] H. Guozheng and H. Fan, "Attacks against two provably secure certificateless signature schemes," in *Proceedings of the WASE International Conference on Information Engineering*, pp. 246–249, 2009.

[112] F. Zhang, S. Li, S. Miao, Y. Mu, W. Susilo, and X. Huang, "Cryptanalysis on two certificateless signature schemes," *International Journal of Computers, Communications and Control*, vol. 4, pp. 586–591, 2010.

[113] Z. Eslami and M. Talebi, "A new untraceable off-line electronic cash system," *Electronic Commerce Research and Applications*, vol. 10, no. 1, pp. 59–66, 2011.

[114] S. Chow, L. Hui, S. Yiu, and K. Chow, "Two improved partially blind signature schemes from bilinear pairings," in *Proceedings of the Information Security and Privacy*, vol. 3574, pp. 355–411, LNCS, Berlin/Heidelberg, 2005.

[115] C. I. Fan and C. L. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E81, no. A5, pp. 818–824, 1998.

[116] F. Zhang, R. Safavi-Naini, and W. Susilo, "Efficient verifiably encrypted signature and partially blind signature from bilinear pairings," in *Proceedings of the Progress in Cryptology (Indocrypt'03)*, vol. 2904, pp. 191–204, LNCS, Springer Berlin/Heidelberg, 2003.

[117] H. F. Huang and C. C. Chang, "A new design of efficient partially blind signature scheme," *The Journal of Systems and Software*, vol. 73, no. 3, pp. 397–403, 2003.

[118] F. Zhang and X. Chen, "Cryptanalysis of Huang-Chang partially blind signature scheme," *The Journal of Systems and Software*, vol. 76, no. 3, pp. 323–325, 2005.

[119] X. Hu and S. Huang, "Analysis of ID-based restrictive partially blind signatures and applications," *The Journal of Systems and Software*, vol. 81, no. 11, pp. 1951–1954, 2008.

[120] Y. M. Tseng, T. S. Wu, and J. D. Wu, "Forgery attacks on an ID-based partially blind signature scheme," *IAENG International journal of Computer science*, vol. 35, no. 3, 2008.

[121] X. Chen, F. Zhang, and S. Liu, "ID-based restrictive partially blind signatures and applications," *Journal of Systems and Software*, vol. 80, no. 2, pp. 164–171, 2007.

[122] X. Lin, R. Lu, H. Zhu, P. Ho, and X. Sherman, "Provably secure self-certified partially blind signature scheme from bilinear pairings," in *Proceedings of the IEEE International Conference on Communications (ICC'08)*, vol. 3810, pp. 1530–1535, IEEE Computer Society, 2008.

[123] J. Zhang and S. Gao, "Cryptoanlaysis of a self-certified partially blind signature and a proxy blind signature," in *Proceedings of the WASE International Conference on Information Engineering*, pp. 184–187, IEEE Computer Society, 2009.

[124] J. J. Hwang, T. C. Yeh, and J. B. Lib, "Securing on-line credit card payments without disclosing privacy information," *Computer Standards and Interfaces*, vol. 73, no. 2, pp. 119–129, 2003.

[125] Y. Li and X. Zhang, "Securing credit card transactions with one-time payment scheme," *Electronic Commerce Research and Applications*, vol. 4, no. 4, pp. 413–426, 2005.

[126] M. Stirland, "Smartcards in secure electronic commerce," *Information Security Technical Report*, vol. 3, no. 2, pp. 41–54, 1998.

[127] W. K. Chen, "Efficient on-line electronic checks," *Applied Mathematics and Computation*, vol. 162, no. 3, pp. 1259–1263, 2005.

[128] W. Chen, B. Qin, Q. Wu, L. Zhang, , and H. Zhang, "ID-based partially blind signatures: A scalable solution to multi-bank E-cash," in *Proceedings of the International Conference on Signal Processing Systems*, pp. 433–437, 2009.

[129] L. Zhang, F. Zhang, B. Qin, and S. Liu, "Provably-secure electronic cash based on certificateless partially-blind signatures," *Electronic Commerce Research and Applications*, vol. 10, no. 5, pp. 323–325, 2011.

[130] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[131] R. Song and L. Korba, "How to make e-cash with non-repudiation and anonymity," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, IEEE Computer Society, pp. 167–172, 2004.

[132] T. Nakanishi and Y. Sugiyama, "An efficient on-line electronic cash with unlinkable exact payments," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88, no. A10, pp. 2769–2779, 2005.

[133] L. Shi, B. Carbunar, and R. Sion, "Conditional E-cash," in *Proceedings of the 1st International Conference on Financial Cryptography and Data Security and 1st International Conference on Usable Security*, vol. 4886, pp. 15–28, LNCS, Berlin/Heidelberg, 2007.

[134] J. Camenisch, A. Lysyanskaya, and M. Meyerovich, "Endrosed e-cash," in *Proceedings of the IEEE Symposium on Security and Privacy (SP'07)*, pp. 101–115, 2007.

[135] D. Chaum, A. Fiat, and A. Naor, "Untraceable electronic cash," in *Proceedings of the Advances in Cryptology (Crypto'88)*, vol. 403, pp. 319–327, LNCS, Berlin/Heidelberg, 1990.

[136] K. Q. N. V. Varadharajan and Y. Mu, "On the design of efficient RSA-based offline electronic cash schemes," *Theoretical Computer Science*, vol. 226, no. 1-2, pp. 173–184, 1999.

[137] H. Wang and Y. Zhang, "Untraceable off-line electronic cash flow in ecommerce," in *Proceedings of the 24th Australasian Computer Science Conference (ACSC'01)*, pp. 191–198, IEEE Computer Society, 2001.

[138] W. Qiu, K. Chen, and D. Gu, "A new offiine privacy protecting E-cash system with revokable anonymity," in *Proceedings of the 5th International Conference on Information Security*, vol. 2433, pp. 177–190, LNCS, Berlin/Heidelberg, 2002.

[139] C. Popescu, "An off-line electronic cash system with revocable anonymity," in *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (MELECON'04)*, vol. 2, pp. 763–767, IEEE Computer Society, 2004.

[140] X. Hou and C. H. Tan, "Fair traceable off-line electronic cash in wallets with observers," in *Proceedings of the 6th International Conference on Advanced Communication Technology*, pp. 595–599, IEEE Computer Society, 2004.

[141] Y. Hanatani, Y. Komano, K. Ohta, and N. Kunihiro, "Provably secure electronic cash based on blind multisignature schemes," in *Proceedings of the Financial Cryptography and Data Security*, vol. 4107, pp. 236–250, LNCS, Berlin/Heidelberg, 2006.

[142] S. Canard, A. Gouget, and J. Traor, "Improvement of efficiency in (unconditional) anonymous transferable E-cash," in *Proceedings of the Financial Cryptography and Data Security*, vol. 5143, pp. 202–214, LNCS, Berlin/Heidelberg, 2008.

[143] S. Canard and A. Gouget, "Multiple denominations in E-cash with compact transaction data," in *Proceedings of the Financial Cryptography and Data Security*, vol. 6052, pp. 82–97, LNCS, Berlin/Heidelberg, 2010.

[144] G. Fuchsbauer, D. Pointcheval, and D. Vergnaud, "Transferable constant-size fair E-cash," in *Cryptology and Network Security*, vol. 5888, pp. 226–247, LNCS, Berlin/Heidelberg, 2009.

[145] Y. Chen, J. S. Chou, H. M. Sun, and M. H. Cho, "A novel electronic cash system with trustee-based anonymity revocation from pairing," *Electronic Commerce Research and Applications*, vol. 10, no. 6, pp. 673–682, 2011.

[146] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Proceedings of the Advances in Cryptology (Asiacrypt'02)*, vol. 2501, pp. 629–637, LNCS, Berlin/Heidelberg, 2002.

[147] Z. Huang, K. Chen, and Y. Wang, "Efficient identity-based signatures and blind signatures," in *Proceedings of the 4th International Conference on Cryptology and*

Network Security (CANS'05), vol. 3810, pp. 120–133, LNCS, Berlin/Heidelberg, 2005.

[148] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[149] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM Operating Systems Review*, vol. 36, no. 4, pp. 23–29, 2002.

[150] W. C. Ku, C. M. Chen, and H. L. Lee, "Weaknesses of Lee-Li-Hwang's hash-based password authentication scheme," *ACM Operating Systems Review*, vol. 37, no. 4, pp. 19–25, 2003.

[151] E. J. Yoon, E. K. Ruy, and K. Y. Roo, "A secure user authentication scheme using hash functions," *ACM Operating Systems Review*, vol. 38, no. 3, pp. 62–68, 2004.

[152] W. C. Ku, C. M. Chen, and L. Hui, "Cryptanalysis of a variant of Peyravian-Zunic's password authentication scheme," *IEICE Transactions on Communications*, vol. E86, no. B5, pp. 1682–1684, 2002.

[153] M. Peyravian and C. Jeffries, "Secure remote user access over insecure networks," *Computer Communications*, vol. 29, no. 5, pp. 660–667, 2006.

[154] K. A. Shim, "Security flaws of remote user access over insecure networks," *Computer Communications*, vol. 30, no. 1, pp. 117–121, 2006.

[155] Y. F. Chang, C. C. Chang, and Y. L. Liu, "Password authentication without the server public key," *IEICE Transactions on Communications*, vol. E87, no. B10, pp. 3088–3091, 2004.

[156] T. C. Group, "TCG Specification Architecture Overview [EB/OL]." http://www.trustedcomputinggroug.org/, 2007.

[157] Z. H. Shen, "A new modified remote user authentication scheme using smartcards," *Applied Mathematics*, vol. 23, no. 3, pp. 371–376, 2008.

[158] Y. L. Jia, A. M. Jhou, and M. X. Gao, "A new mutual authentication scheme based on nonce and smartcards," *Computer Communications*, vol. 31, no. 10, pp. 2205–2209, 2008.

[159] W. S. Juang and W. K. Nien, "Efficient password authenticated key agreement using bilinear pairings," *Mathematical and Computer Modelling*, vol. 47, no. 11-12, pp. 1238–1245, 2008.

[160] S. K. Kim and M. G. Chung, "More secure remote user authentication scheme," *Computer Communications*, vol. 32, no. 6, pp. 1018–1021, 2009.

[161] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards and Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[162] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.

[163] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[164] X. M. Wang, W. F. Zhang, J. S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 29, no. 5, pp. 507–512, 2007.

[165] T. Xiang, K. W. Wong, and X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 74, no. 5, pp. 657–661, 2008.

[166] H. C. Hsiang and W. K. Shiho, "Weaknesses and improvements of the Yoon-RyuYoo remote user authentication scheme using smart cards," *Computer Communications*, vol. 32, no. 4, pp. 649–652, 2009.

[167] M. Joye and F. Olivier, *Side-channel analysis, Encyclopedia of Cryptography and Security*. Kluwer Academic Publishers, 2005.

[168] H. R. Chung, W. C. Ku, and M. J. Tsaur, "Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments," *Computer Standards and Interfaces*, vol. 31, no. 4, pp. 863–868, 2009.

[169] Y. Chen, J. S. Chou, and C. H. Huang, "Comments on five smart card based password authentication protocols," *International Journal of Computer Science and Information Security*, vol. 8, no. 2, pp. 129–132, 2010.

[170] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the Advances in Cryptology (Crypto'99)*, vol. 1666, pp. 388–397, LNCS, Berlin/Heidelberg, 1999.

[171] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[172] W. C. Ku, M. H. Chaing, and S. T. Chang, "Weaknesses of Yoon-Ryu-Yoo's hash-based password authentication scheme," *ACM Operating Systems Review*, vol. 39, no. 1, pp. 85–89, 2005.

[173] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card," *Computer Networks*, vol. 49, no. 4, pp. 535–540, 2005.

[174] Y. P. Liao and S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards and Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[175] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 44, no. 1-2, pp. 223–228, 2006.

[176] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards and Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.

[177] I. E. Liao, C. C. Lee, and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," in *Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP'05)*, 2005.

[178] Z. Gao and Y. Tu, "An improvement of dynamic ID-based remote user authentication scheme with smart cards," in *Proceedings of the 7th World Congress on Intelligent Control and Automation*, vol. 8, pp. 4562–4567, 2008.

[179] Y. V. Wang, J. Y. Liu, X. F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 32, no. 4, pp. 583–585, 2009.

[180] H. C. Hsiang and W. K. Shiha, "Improvement of the secure dynamic ID-based remote user authentication scheme for multi-server environment," *Computer Standards and Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[181] M. A. Ahmed, D. R. Lakshmi, and S. A. Sattar, "Cryptanalysis of a more efficient and secure dynamic ID-based remote user authentication scheme," *International Journal of Network Security and Its Applications*, vol. 1, no. 3, pp. 32–37, 2009.

[182] T. Y. Chen, M. S. Hwang, C. C. Lee, and J. K. Jan, "Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment," in *Proceedings of the 4th International Conference on Innovative Computing, Information and Control (ICICIC'09)*, pp. 725–728, 2009.

[183] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[184] E. R. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," *Journal of Cryptology*, vol. 17, no. 4, pp. 277–296, 2004.

[185] T. H. Chen, W. B. Lee, and H. B. Chen, "A round-and computation-efficient three-party authenticated key exchange protocol," *Journal of Systems and Software*, vol. 81, no. 9, pp. 1581–1590, 2008.

[186] R. Lu and Z. Cao, "Simple three-party key exchange protocol," *Computers and Security*, vol. 26, pp. 94–97, 2007.

[187] R. C. W. Phan, W. C. Yau, and B. M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)," *Information Sciences*, vol. 178, pp. 2849–2856, 2008.

[188] Q. Pu, X. Zhao, and J. Ding, "Crypproceedings of thetanalysis of a three-party authenticated key exchange protocol using elliptic curve cryptography," in *Proceedings of the International Conference on Research Challenges in Computer Science*, pp. 7–10, 2009.

[189] Z. Tan, "An enhanced three-party authentication key exchange protocol for mobile commerce environments," *Journal of Communications*, vol. 5, no. 5, pp. 430–434, 2010.

[190] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, vol. 6, pp. 213–241, 2007.

[191] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Transaction on Wireless Communication*, vol. 11, no. 6, pp. 4136–4144, 2007.

[192] C. Kudla and K. G. Paterson, "Modular security proofs for key agreement protocols," in *Proceedings of the Advances in Cryptolog (Asiacrypt'05)*, pp. 549–565, LNCS, Berlin/Heidelberg, 2005.

[193] S. Wang, Z. Cao, Z. Cheng, and K. K. R. Choo, "Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode," *Science in China Series F: Information Sciences*, vol. 58, no. 8, pp. 1358–1370, 2009.

[194] Y. F. Chung, K. H. Huang, F. Lai, and T. S. Chen, "ID-based digital signature scheme on the elliptic curve cryptosystem," *Computer Standards and Interfaces*, vol. 29, no. 6, pp. 601–604, 2007.

[195] A. W. Fan and S. X. Lu, "An improved elliptic curve digital signature algorithm," *Applied Mechanics and Materials*, vol. 34-35, pp. 1024–1027, 2010.

[196] I. Ingemaresson and C. K. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. 28, no. 5, pp. 5714–720, 1982.

[197] M. S. Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, 1995.

[198] Y. M. Tseng, "Cryptanalysis and improvement of key distribution system for VSAT satellite communications," *Informatica*, vol. 13, no. 3, pp. 369–376, 2002.

[199] Y. M. Tseng, "A scalable key management scheme with minimizing key storage for secure group communications," *International Journal of Network Management*, vol. 13, no. 6, pp. 419–425, 2003.

[200] Y. M. Tseng, "A robust multi-party key agreement protocol resistant to malicious participants," *The Computer Journal*, vol. 48, no. 4, pp. 480–487, 2005.

[201] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," *IEEE Transaction on Information Theory*, vol. 54, no. 5, pp. 2007–2025, 2005.

[202] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," in *Proceedings of the 5th IFIP-TC6 International Conference on Mobile and Wireless Communications Networks (MWCN'03)*, pp. 59–62, IEEE Computer Society, 2003.

[203] C. Boyd and J. Nieto, "Round-Optimal Contributory Conference Key Agreement," in *Proceedings of the Public Key Cryptography (PKC'03)*, vol. 2567, pp. 161–174, LNCS, Berlin/Heidelberg, 2002.

[204] J. Herranz and J. L. Villar, "An Unbalanced Protocol for Group Key Exchange," in *Proceedings of the Trust and Privacy in Digital Business*, vol. 3184, pp. 172–180, LNCS, Berlin/Heidelberg, 2004.

[205] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless public key encryption without pairing," in *Proceedings of the Information Security*, vol. 3650, pp. 134–148, LNCS, Berlin/Heidelberg, 2005.

[206] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communication of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[207] L. Lamport, "Constructing digital signatures from a one-way function." Technical Report CSL-983, SRI International Computer Science Laboratory, 1979.

[208] R. Merkle, "A certified digital signature," in *Proceedings of the Advances in Cryptology (Crypto'89)*, vol. 435, pp. 218–238, LNCS, Berlin/Heidelberg, 1990.

[209] M. O. Rabin, "Digitalized signatures as intractable as factorization," 1979. Technical Report MIT/LCS/TR-212, MIT Laboratory for Computer Science.

[210] X. Hu and S. Huang, "An efficient ID-based partially blind signature scheme," in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, vol. 3, pp. 291–296, IEEE Computer Society, 2007.

[211] D. He, Y. Chen, J. Chen, R. Zhang, and W. Han, "A new two-round certificateless authenticated key agreement protocol without bilinear pairings," *Mathematical and Computer Modelling*, vol. 54, no. 11-12, pp. 3143–3152, 2011.

[212] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, pp. 361–396, 2000.

[213] D. He, J. Chen, and J. Hu, "A pairing-free certificateless authenticated key agreement protocol," *International Journal of Communication Systems*, vol. 25, no. 2, pp. 221–230, 2012.

[214] D. He, J. Chen, and J. Hu, "An id-based proxy signature schemes without bilinear pairings," *Annals of Telecommunications*, vol. 66, no. 11-12, pp. 657–662, 2011.

[215] Y. H. Yan, D. S. Wang, J. P. Li, and L. G. Li, "Cryptanalysis of a remote user authentication scheme based on bilinear pairing," in *Proceedings of the ICACIA'09*, 2009.

[216] M. Hou, Q. Xu, G. Shanqing, and H. Jiang, "Cryptanalysis of identity-based authenticated key agreement protocols from parings," *Journal of Networks*, vol. 5, no. 7, pp. 826–855, 2010.

[217] C. M. Swanson, "Security in key agreement: two-party certificateless schemes," Master's thesis, University of Waterloo, Canada, 2008.

[218] T. Mandt and C. Tan, "Certificateless authenticated two-party key agreement protocols," in *Proceedings of Advances in Computer Science (ASIAN'06)*, vol. 4435, pp. 37–44, LNCS, Berlin/Heidelberg, 2008.

[219] B. T. Hsieh, H. M. Sun, and T. Hwang, "On the security of some password authentication protocols," *Informatica*, vol. 14, no. 2, pp. 195–204, 2003.

[220] S. T. Wu, J. H. Chiu, and B. C. Chieu, "ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography," in *Proceedings of IEEE International Conference on Electro Information Technology*, pp. 5–9, 2005.

[221] Z. Jia, Y. Zhang, H. Shao, Y. Lin, and J. Wang, "A remote user authentication scheme using bilinear pairings and ECC," in *Proceedings of the ISDA'06*, pp. 1091–1096, 2006.

[222] P. E. Abichar, A. Mhamed, and B. Elhassan, "A fast and secure elliptic curve based authenticated key agreement scheme for low power mobile communications," in *Proceedings of the International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 235–240, 2007.