REFERENCES

1. Adi Shamir (1979), 'How to share a secret', Communications of the ACM, Vol. 22, pp. 612-613.

2. Adi Shamir (1984), 'Identity-Based Cryptosystems and Signature Schemes', Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, pp. 47-53.

3. Asokan N., Shoup V. and Waidner M. (1998), 'Asynchronous protocols for optimistic fair exchange', In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 86-99.

4. Asokan N., Shoup V. and Waidner M. (2000), 'Optimistic fair exchange of digital signatures', IEEE Journal on Selected Area in Communications, pp. 45-56.

5. Avi Rubin (2004), 'Security consideration of remote e-voting over internet', Technical Report-2004.

6. Bao F., Deng R.H. and Mao W. (1998), 'Efficient and Practical Fair Exchange Protocols with Off-line TTP', In IEEE Symposium on Security and Privacy, pp. 124-132.

7. Bellare M. and Michali S. (1988), 'How to sign given any trapdoor function', Proceeding of 20th STOC-ACM, pp. 32-42.

8. Ben-Or M., Goldreich O., Micali S. and Rivest R. (1990), 'A fair protocol for signing contracts', IEEE Transactions on Information Theory, Vol. 36, No. 1, pp. 40-46.

9. Biehl I., Buchmann J.A., Meyer B., Thiel C. and Thiel C. (1994), 'Tools for proving zero knowledge', Advances in Cryptology - EuroCrypt-94, pp. 356-365.

10. Blakley G.R. (1979), 'Safeguarding cryptographic keys', Proceeding, AFIPS 1979 Nat. Computer Conference, Vol. 48, pp. 313-317.

11. Boldyreva A. and Jakobsson M. (2002), 'Theft-protected proprietary certificates', ACM Workshop on DRM '02.

12. Boneh D. and Franklin M.K. (2001), 'Identity-Based Encryption from the Weil Pairing', Advances in Cryptology - Proceedings of CRYPTO 2000, pp. 123-130.

13. Boyar J., Chaum D., Damgard I. and Pederson T. (1990), 'Convertible undeniable signatures', Advances in Cryptology – Crypto - 90, Lecture Notes in Computer Science, Vol. 537, pp.189-205.

14. Boyd C. (1986), 'Digital multi-signature, In Cryptography and Coding', Beker H.J. and Piper F.C. (Eds.), Clarendon Press, London, pp. 241-246.

15. Burmester M. and Magkos E. (2003), 'Towards Secure and Practical E-elections in the New Era, Secure Electronic Voting', Lecture Notes in Computer Science, pp. 63-76.

16. Burmester M.V.D., Desmedt Y., Piper F. and Walker M. (1989), 'A general zero knowledge scheme', Advance in Cryptology - Eurocrypt - 89, Lecture Notes in Computer Science, pp. 122-133.

17. Camenish J.L., Piveteare J.M. and Stadler M.A. (1994), 'Blind signature based on discrete logarithm problem', Advance in Cryptology-Eurocrypt - 94, Lecture Notes in Computer Science, pp. 428-432.

18. Cha, J. and Cheon J. (2003), 'An Identity-Based Signature from Gap Diffie-Hellman Groups', Proceedings of PKC 2003, LNCS 2567, pp 18-30.

19. Chang C.C., Jan J.K. and Kowng H.C. (1997), 'A digital signature scheme based upon the theory of Quadric Residues', Cryptologia - 01, pp. 55-69.

20. Chaum D., Fiat A. and Naor M. (1990), 'Untraceable Electronic Cash' (Extended Abstract), In Advances in Cryptology - CRYPTO'88, Lecture Notes in Computer Science ,Vol. 403, pp. 319-327.

21. Chaum D. (1982), 'Blind signature for untraceable payments', Advances in Cryptology – Crypto-82, Lecture Notes in Computer Science, pp. 199-203.

22. Chaum D. (1990), 'Zero knowledge undeniable signatures', Advance in Cryptology-Eurocrypt - 90, Lecture Notes in Computer Science, pp. 458-464.

23. Chaum D. (1991), ‘Group signatures’, Advance in Cryptology-Eurocrypt - 91, Lecture Notes in Computer Science, pp. 257-265.

24. Chaum D. (1995), ‘Designed confirmer signatures’, Advance in Cryptology-Eurocrypt - 94, Lecture Notes in Computer Science, Vol. 950, pp. 86-91.

25. Chaum D. and Van Autwerpan H. (1989), ‘Undeniable signatures’, Advance in Cryptology- Eurocrypt - 89, Lecture Notes in Computer Science, pp. 212-216.

26. Chaum M.L., Hwang T., Lee N. and Jiun-Jang Tsai (2000), ‘(t, n) threshold multi-signature scheme and generalized multi-signature scheme, where suspected forgery implies traceability of the adversarial shareholders’, Cryptologia - 24, Vol. 3, pp. 250-268.

27. Chen L. and Pederson T.P. (1994), ‘New group signature signatures’, Advance in Cryptology -Eurocrypt - 94, Lecture Notes in Computer Science , pp.171-181.

28. Chou-Chen Yang and Hang Wen Yang (2005), ‘Cryptanalysis of Security Enhancement for anonymous secure e-voting over network’, Journal of Applied Sciences, Vol. 5, pp. 794-797.

29. Clifford Cocks (2001), ‘An Identity Based Encryption Scheme Based on Quadratic Residues’, Proceedings of the 8th IMA International Conference on Cryptography and Coding, pp. 234-142.

30. Damgard I.B. (1987), ‘Collision free hash function and public key signature scheme’, Advance in Cryptology - Eurocrypt - 87, Lecture Notes in Computer Science, pp. 203-216.

31. Desmedt Y. (1988), ‘Society and group oriented cryptography’, Advances in Cryptology –Crypto - 87, Lecture Notes in Computer Science, pp. 120-127.

32. Desmedt Y. (1994), ‘Threshold cryptography’, European Transactions on Telecommunications and Related Technologies, Vol. 5, pp. 35-43.

33. Desmedt Y. and Frankel Y. (1990), ‘Threshold cryptosystems’, Advances in Cryptology –Crypto- 89, Lecture Notes in Computer Science, Vol. 293, pp. 307-315.

34. Desmedt Y. and Frankel Y. (1991), 'Shared generation of authenticators and signatures', Advances in Cryptology – Crypto - 91, Springer Verlag, pp. 457-469.

35. Diffie W. (1988), 'The first ten years of Public Key Cryptography', In Contemporary Cryptology: The Science of Information Integrity, pp. 135-175.

36. Diffie W. and Hellman M. (1976), 'New directions in Cryptography', IEEE Trans. Information Theory, Vol. 31, pp. 644-654.

37. Dowland P.S., Furenell S.M., Illingworth H.M. and Reynolds P.L. (1999), 'Computer crime and abuse: A survey of public attitudes and awareness', Computer and Security, Vol. 18, pp. 715-726.

38. Due Liem V. (2003), 'A new threshold blind signature scheme from Pairings', Journal of Applied Sciences, pp. 293-297.

39. ElGamal T. (1985), 'A PKC and a signature scheme based on discrete logarithm', IEEE Transinformation Theory, Vol. 31, pp. 469-472.

40. Even S., Goldreich O. and Lempel A. (1995), 'A randomized protocol for signing contracts', Communication of ACM, Vol. 28, pp. 637-647.

41. Fangguo Zhang and Kwangjo Kim (2002), 'ID-Based Blind Signature and Ring Signature from Pairings',Volume 2501, pp. 533-547.

42. Fangguo Zhang and Kwangjo Kim,(2003), 'Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings', Volume 2727, pp. 312-323.

43. Fiat A. and Shamir A. (1986), 'How to prove yourself, Practical solution to identification and signature problem', Advances in Cryptology - Crypto – 86, Lecture Notes in Computer Science, Vol. 263, pp. 186-194.

44. Frankal Y. and Desmedt Y. (1992), 'Parallel reliable threshold multi-signature', Technical Report, Department of EE and CS, University of Wisconsin.

45. Gennaro R., Jarecki Hkrawczyk S. and Rabin T. (1996), 'Robust threshold DSS signature', Advances in Cryptology–EuroCrypt - 96, Lecture Notes in Computer Science, pp. 354-371.

46. Giuseppe Ateniese and Cristina Nita-Rotaru (2002), 'Stateless-Recipient Certified E-mail System based on Verifiable Encryption', RSA Conference- 2002, pp. 145-152.

47. Gnanaguruparan G. and Kak S. (2002), 'Recursive Hiding of the secrets in the visual Cryptography', Cryptologia–25, pp. 68-75.

48. Goldrich O. (1986), 'Two remark concerning the GMR signature scheme', Advance in Cryptology - Crypto – 86, Lecture Notes in Computer Science, pp. 104-110.

49. Goldwasser, Michali S. and Yao A. (1983), 'Strong signature scheme', Proceeding of the 15th STOC - ACM, pp. 431-439.

50. Goldwasser S., Michali S. and Rivest R. (1985), 'A paradoxical signature scheme', 25th IEEE Symposium of Foundation on the Computing, pp. 441-344.

51. Goldwasser S., Michali S. and Rivest R. (1998), 'A digital signature secure against adaptive chosen message attacks', SIAM Journal on Computing , Vol. 17, pp. 281-308.

52. Guillou L.C. and Quisquater J.J. (1988), 'A paradoxical identity based on signature scheme resulting from zero knowledge', Advances in Cryptology Crypto – 88, Lecture Notes in Computer Science, pp. 216-231.

53. Guillou L.C. and Quisquater J.J. (1988), 'A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory', Advances in Cryptology – Eurocrypt - 88, Lecture Notes in Computer Science, Vol. 330, pp.123-128.

54. Hard Jono T. and Zheng Y. (1992), 'A practical digital multi-signature scheme based on discrete logarithm', Advance in Cryptology – Auscrypto- 92, Lecture Notes in Computer Science, pp. 16-21.

55. Harn L. (1993), '(t,n) threshold signature and digital multi-signature', Proceeding of Workshop on Cryptography and data security, Chung Cheng Institute of Technology, ROC, pp. 61-73.

56. Harn L. (1994), 'Group oriented (t, n) threshold signature scheme and digital multi-signature', IEEE, Proceedings of the Computer Digital Technology, Vol. 141, pp. 307-313.

57. Harn L. and Kiesler T. (1989), 'New Scheme for Digital Multi-signature', Electronic Letters, Vol. 25, pp. 1002-1003.

58. Harn L. and Yang S. (1992), 'Group oriented undeniable signature scheme without the assistance of a mutually trusted party', Advance in Cryptology- Auscrypt - 92, Lecture Notes in Computer Science, pp. 133-142.

59. Hellman M.E. (1979), 'The mathematics of public key cryptography', Scientific American, Vol. 241, pp. 130-139.

60. Hill L. (1929), 'Cryptography in an algebraic alphabet', American Mathematical Monthly, Vol. 36, pp.15-30.

61. Hwang M., Lin I. and Lie E.J. (2000), 'A secure nonrepudiable threshold signature Scheme with Known Signers', International Journal of Informatica, Vol. 11, pp. 1- 8.

62. Hwang T., Li C. and Lee N. (1993), 'Remark on the threshold RSA signature scheme', Advance in Cryptology - Crypto – 93, Lecture Notes in Computer Science, pp. 413-419.

63. Hwang T., Li C. and Lee N. (1995), '(t, n) Threshold signature scheme based on discrete logarithm', Advance in Cryptology – Eurocrypt - 94, Lecture Notes in Computer Science, pp. 191-200.

64. Hwang T. and Chen C.C. (2001), 'A new proxy multi-signature signature scheme', International Workshop on Cryptography and Network Security, pp. 26-28.

65. Itakura K. and Nakamura K. (1983), 'A public key cryptosystem, suitable for digital multisignatures', NEC Research and Development, pp. 1-8.

66. Ivan Damgård and Mads Jurik (2003), 'A Length-Flexible Threshold Cryptosystem with Applications', ACISP 2003, pp. 350-364.

67. Ivan Damgård and Mats Jurik (2001), 'A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System', Public Key Cryptography, pp. 119-136.

68. Jac C.C. and Jung H.C. (2002), 'An identity based signature from gap Diffie Hellman groups', www.iacr.org .

69. Jackson W.A., Martin K.M. and O'Keefe C.M. (1995), 'Efficient secret sharing scheme without mutually trusted party', Advance in Cryptology – Eurocrypt - 95, Lecture Notes in Computer Science, pp. 183-193.

70. Jakobsson M., Juels A. and Nguyen P. (2002), 'Proprietary Certificates', Proceedings of The Cryptographers', Track at the RSA Conference 2002, Lecture Notes in Computer Science, Vol. 2271, pp. 231-242.

71. Jan Camenish and Victor Shoup (2003), 'Practical Verifiable Encryption and Decryption of Discrete Logarithms', Proceedings of Crypto 2003, pp. 10-32.

72. Javier Herranz and German Saez (2003),'Verifiable Secret Sharing for General Access Structures, with Application to Fully Distributed Proxy Signatures', Lecture Notes in Computer Science, Volume 2742, Financial Cryptography, pp. 286-302.

73. Ji-Hye Park, Young-Seol Kim and Jik Hyun Chang (2007), 'A Proxy Blind Signature Scheme with Proxy Revocation', Computational Intelligence and Security Workshops, CISW 2007, pp. 761-764.

74. Julie Ann Staub (2005), 'Analysis of Chaum's voter verifiable election scheme' (Master of Science Thesis).

75. Kim J. and Kim K. (2001), 'An efficient and provably secure threshold blind signature scheme', www.caislab.icu.ac.kr.

76. Kobolitz N. (1987), 'Elliptic curve cryptosystem', Mathematics of Computation, Vol. 48, pp. 203-209.

77. Lal S. and Awasthi A.K. (2003), 'A scheme for obtaining warrant message from the digital proxy signature scheme', Report No. 2003/73, http://www.eprint.iacr.org

78. Lal S. and Awasthi A.K. (2003), 'Proxy blind signature scheme', Report No. 2003/72, http://www.eprint.iacr.org

79. Lal S. and Kumar M. (2003), 'A directed signature scheme and its application', Proceedings, National Conference on Information Security, pp. 124-132.

80. Lal S. and Kumar M. (2003), 'Some applications of directed signature scheme', South East Asian Journal of Mathematics and Mathematical Science, Vol. 1, pp. 13-26.

81. Lanford S.K. (1995), 'Differential linear cryptanalysis and threshold signatures', Advance in Cryptology - Crypto - 94, Lecture Notes in Computer Science, pp. 17-25.

82. Lanford S.K. (1995), 'Threshold DSS signatures without a trusted party', Advance in Cryptology - Crypto - 95, Lecture Notes in Computer Science, pp. 397-400.

83. Langford S.K. (1996), 'Weaknesses in some threshold cryptosystems', Advance in Cryptology - Crypto - 96, Lecture Notes in Computer Science, pp. 74-82.

84. Lee B. and Kim H. (2001), 'Strong proxy signature scheme and its applications', Proceeding of SCIS, pp. 603-608.

85. Lim C.H. and Lee P.J. (1996), 'A directed signature scheme and its application to threshold cryptosystems', Security Protocol, In Proceedings of International Workshop, (Cambridge, United Kingdom), Lecture Notes in Computer Science, Vol. 1189, pp. 131-138.

86. Lin I., Hwang M. and Chang C. (2003), 'Security enhancement for anonymous secure e-voting over a network', Computer Standard and Interfaces, Vol. 25, pp. 131-139.

87. Mambo, Usuda and Okamoto (1996), 'Proxy Signatures for Delegating Signing Operation', Proceedings of the 3rd ACM Conference on Computer and Communications Security, pp. 48-57.

88. Ming Yang and Yumin Wang (2008), 'A new efficient ID-based proxy blind signature scheme', Journal of Electronics, Vol. 25, pp. 162-169.

89. Mu Y. and Varadharajan V. (1998), 'Anonymous secure e-voting over a network', Proceedings of the 14th Annual Computer Security Applications Conference, ACSAC'98, pp. 293-299.

90. Riza Aditya (2005), 'Secure electronic voting with flexible ballot structure', Ph.D. thesis.

91. Sakai, R., Ohgishi, K., Kasahara, M., (2000), 'Cryptosystems based on pairing' , SICS 2000, Symposium on Cryptography and Information Security, pp 26-28.

92. Shaobin Wang,Fan Hong and Guohua Cui,'Secure Efficient Proxy Blind Signature Schemes Based DLP',Proceedings of the Seventh IEEE International Conference on E-Commerce Technology, CEC 2005, pp. 452 - 455.

93. Smart NP (2002) , 'Identity-based authenticated key agreement protocol based on Weil pairing', Electronics Letters, 2002 - ieeexplore.ieee.org.

94. Stinson Douglas R. and Strobl Reto (2001), 'Provably secure distributed schnorr signatures and a (t, n) threshold scheme for implicit certificates', Lecture notes in computer science , Information security and privacy : (Sydney, 11-13 July 2001), vol. 2119, pp. 417-434

95. Tan, Z., Liu, Z. and Tang, C. (2002), 'Digital proxy blind signature schemes based on DLP and ECDLP', In MM Research Preprints 21, pp. 212-217.

96. Yi L., Bai G. and Xiao G (2001), 'Proxy multi-signature Scheme: A new type of proxy signature scheme', Electronic Letter - 36, pp. 527-528.

97. Yu-Yi Chen, Jinn-Ke Jan and Chin-Ling Chen (2004), 'The design of a secure anonymous Internet voting system', Computer and Security, Vol. 23, pp. 330-337.

98. Zhang F. and Kim K. (2003), 'Efficient ID-based blind signature and proxy signature from pairings', ACISP 2003, Lecture Notes in Computer Science, pp. 172-178.

99. Zhang K. (1997), 'Threshold proxy signature schemes', Information Security Workshop' pp. 191-197.