Provably Secure Fair Blind Signature Scheme with Message Recovery from Bilinear Pairings

郭啟志、曹偉駿

E-mail: 9314387@mail.dyu.edu.tw

ABSTRACT

The blind signature could be used in electronic payment systems to achieve the properties of unlinkability and anonymity. Unfortunately, this characteristic may be perverted the ability of scheme. Accordingly, Lee and Kim proposed a fair blind signature scheme with message recovery in 1999. However, the fairness of blind signature can not be achieved in Lee and Kim ’ s scheme. In this thesis, the proposed cryptosystem is constructed by using the pairing-based cryptosystem instead of modular exponentiation, and integrating the identity-based public key cryptosystems with the self-certified public key cryptosystems. In addition, we further employ the integrated cryptosystems to design a fair self-certified blind signature scheme with message recovery to improve the drawback on Lee and Kim''''s scheme. In the past few years, one of important research topics of network security protocol is security analysis; however, they still employ the method of heuristic security analysis. In fact, once such security analysis method is used, some previously proposed protocols originally judged to be secure may were found security holes later. Hence, we give security proofs on our proposed schemes such that it can withstand attacks by intruders. Finally, we analyze the performance of the proposed scheme and show that it is more efficient than previous other schemes.

Keywords : self-certified public key cryptosystems ; blind signature ; message recovery ; bilinear pairings ; provable security

Table of Contents

REFERENCES

[1] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, “ Efficient Algorithms for Pairing-Based Cryptosystems, ” Advances in Cryptology — CRYPTO 2002, LNCS, Vol. 2442, Springer-Verlag, pp. 354-368, 2002.

[2] D. Boneh and M. Franklin, “ Identity-Based Encryption from the Weil Pairing, ” Advances in Cryptology — CRYPTO 2001, LNCS, Vol. 2139, Springer-Verlag, pp. 213-229, 2001.

[3] D. Boneh, B. Lynn, and H. Shacham, “ Short Signatures from the Weil Pairing, ” Advances in Cryptology — ASIACRYPT 2001, LNCS, Vol. 2248, Springer-Verlag, pp. 514-532, 2001.

[4] J. L. Camenisch, J. M. Pivetuau, and M. A. Stadler, " Blind Signature Based on the Discrete Logarithm Problem, " Preprint, presented at the Rump session of EUROCRYPTt ' 94, 1994.
[5] J. C. Cha and J. H. Cheon, " An identity-based Signature from Gap Diffie-Hellman Groups, " Public Key Cryptography — PKC 2003, LNCS, Vol. 2139, Springer-Verlag, pp. 18-30, 2003.
[6] D. Chaum, " Blind Signature for Untraceable Payments, " Advances in Cryptology — CRYPOT ''82, pp. 199-203, 1983.
[7] X. F. Chen, F. G. Zhang, and K. Kim, " ID-based Multi-Proxy Signature and Blind Multisignature from Bilinear Pairings, " Proceedings of KIISC Conference 2003, Korea, pp. 11-19, 2003.
[8] M. Y. Chung, " Message Recovery Fair Blind Signature Schemes, " Ms.D. Thesis, Department of Computer Science, National Chung Hsing University, 2002.
[9] Cybercash web site, URL: http://www.cybercash.com.
[10] W. Diffie and M. E. Hellman, " New Directions in Cryptography, " IEEE Transactions on Information Theory, Vol. IT-22, pp. 644-654, 1976.
[11] R. Dutta, R. Barua, P. Sarkar, " Pairing-Based Cryptography : A Survey, " Cryptology ePrint Archive, Report, 2004.
[12] T. ElGamal, " A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm, " IEEE Transactions on Information Theory, Vol. IT-30, No. 4, pp. 469-472, 1985.
[13] C. I. Fan, W. K. Chen, and Y. S. Yeh, " Randomization Enhanced Chaum ' s Blind Signature Scheme, " Computer Communications, Vol. 23, pp. 1677-1680, 2000.
[14] G. Frey, M. Muller, and H. G. Ruck, " The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems, " IEEE Transactions on Information Theory, Vol. 45, No. 5, pp. 1717-1719, 1999.
[15] S. D. Galbraith, K. Harrison, and D. Soldera, " Implementing the Tate pairing, " Algorithmic Number Theory Symposium, ANTS-V, LNCS, Vol. 2369, Springer-Verlag, pp. 324-337, 2002.
[16] M. Girault, " Self-Certified Public Keys, " Proceedings of EUROCRYPT ''91, LNCS, Vol. 547, Springer-Verlag, pp. 491-497, 1991.
[17] F. Hess, " Efficient Identity Based Signature Schemes Based on Pairings, " SAC 2002, LNCS, Vol. 2595, Springer-Verlag, pp. 310-324, 2002.
[18] P. Horster, M. Michels, H. Petersen, " Meta-ElGamal Signature Schemes, " proceedings of the 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, 1994.
[19] J. E. Hsien, P. W. Ko and C. Y. Chen, " Comments on Lee and Kim''s Message Recovery Fair Blind Signature Scheme, " Proceedings of the tenth National Conference on Information Security, Chinese Cryptology and Information Security Association (CCISA), Taiwan, pp. 123-125, 2000.
[20] M. S. Hwang, C. C. Lee, and Y. C. Lai, " An Untraceable Blind Signature Scheme, " IEIEC Transactions on Fundamentals, Vol. E86-A, No. 7, pp. 1902-1906, 2003.
[21] A. Joux, " A One-Round Protocol for Tripartite Diffie-Hellman, " Algorithm Number Theory Symposium, ANTS-IV, LNCS, Vol. 1838, Springer-Verlag, pp. 385-394, 2000.
[22] A. Joux, " The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems, " Algorithm Number Theory Symposium, ANTS-VI, LNCS, Vol. 2369, Springer-Verlag, pp. 20-32, 2002.
[23] W. S. Juang and C. L. Lei, " Partially Blind Threshold Signatures Based on Discrete Logarithm, " Computer Communications, Vol. 22, pp. 73—86, 1999.
[24] S. Kim, S. Oh, S. Park, and D. Won, " On Saeednia''s Key-exchange Protocols, " KICS (Korean Institute of Communication Sciences) Conference, Vol. 17, No. 2, pp. 1001-1004, 1998.
[25] N. Koblitz, A. Menezes, S. Vanstone, " The State of Elliptic Curve Cryptography, " Designs, Codes and Cryptography, pp. 173-193, 2000.
[26] H. W. Lee and T. Y. Kim, "Fair Blind Signature with Message Recovery Based on Oblivious Transfer Protocol," Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC ''99, pp. 97-111, 1999.
[27] C. L. Lin, " Provably Secure Password Authenticated Key Exchanges, " Ph.D. Thesis, Department of Computer Science and Information Engineering Notional Cheng Kung University, 2003.
[28] C. Y. Lin, T. C. Wu and F. G. Zhang, " Proxy Signature and Proxy Multi-Signature from Bilinear Pairings, " 2003 International Conference on Informatics, Cybernetics and Systems, Kaohsiung, Taiwan, 2003.
[29] W. Mao, " Modern Cryptography: Theory and Practice, " Prentice Hall PTR, 2003.
[30] A. J. Menezes, T. Okamoto, and S. Vanstone, " Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, " IEEE Transactions on Information Theory, Vol. 39, pp. 1639-1646, 1993.
[31] S. Mitsunari, R. Sakai and M. Kasahara, " A New Traitor Tracing, " IEICE Transactions on Fundamentals, Vol. E85-A, No.2, pp. 481-484, 2002.
[32] H. Petersen and P. Horster, " Self-Certified Keys: Concepts and Applications " , Proceedings of Communications and Multimedia Security ''97, Chapman & Hall, pp. 102-116, 1997.

[33] R. Rivest and A. Shamir, “ PayWord and MicroMint: Two Simple Micropayment Schemes, ” Proceedings of RSA''96 Conference, 1996.
[34] R. Rivest, A. Shamir, and L. Adleman, “ A Method for obtaining digital signatures and public-key cryptosystems, ” Communications of the ACM, Vol,21, pp. 120-126, 1978.
[35] S. Saeednia, “ Identity-Based and Self-Certified Key Exchange Protocols, ” Proceedings of the Second Australasian Conference on Information Security and Privacy, ACISP ''97, LNCS, Springer-Verlag, pp. 303-313, 1997.
[36] R. Sakai, K. Ohgishi, and M. Kasahara, “ Cryptosystems Based on Pairing, ” Proceedings of Symposium on Cryptography and Information Security, SCIS 2000, 2000.
[37] R. Sakai and M. Kasahara, “ Cryptosystems Based on Pairing Over Elliptic Curve, ” Proceedings of Symposium on Cryptography and Information Security, SCIS 2003, 8C-1, Japan, 2003.
[38] C. P. Schnorr, “ Efficient Identification and Signatures for Smart Cards, ” Advances in Cryptology — CRYPTO ''89, pp. 339-351, 1990.
[39] C. P. Schnorr, “ Security of Blind Discrete Log Signatures against Interactive Attacks, ” ICICS 2001, LNCS, Vol. 2229, Springer-Verlag, pp. 1-12, 2001.
[40] A. Shamir, “ Identity-based Cryptosystems and Signature schemes, ” Advances in Cryptology — CRYPTO ''84, pp. 47-53, 1985.
[41] C. E. Shannon, “ A Mathematical Theory of Communication, ” Bell System Technical Journal, Vol. 27, pp. 379-423, 1948.
[42] C. E. Shannon, “ A Mathematical Theory of Communication, ” Bell System Technical Journal, Vol. 27, pp. 623-656, 1948.(Continued from July 1948 issue.) [43] Z. Shao, “ Improved User Efficient Blind Signatures, ” Electronic Letters, Vol. 36, No. 16, pp. 1372—1374, 2000.
[44] N. Smart, “ Cryptography: an Introduction, ” Mc Graw Hill, 2003.
[45] N. P. Smart, “ An Identity Based Authenticated Key Agreement Protocol Based on the Weil pairing, ” Electronic Letters, Vol. 38, No. 13, pp. 630-632, 2002.
[46] M. Stadler, J. M. Piveteau, J. Camenisch, “ Fair Blind Signature, ” Advances in Cryptology — EUROCRYPT ''95, LNCS, Vol. 921, Springer-Verlag, 1995.
[47] W. Stallings, “ Cryptography and Network Security: Principles and Practices — Third Edition, ” Prentice Hall, 2003.
[48] W. J. Tsaur and C. H. Chou, “ An Efficient and Secure Fair Blind Signature Scheme with Message Recovery, ” Information Security Conference 2003, pp. 54-62, 2003.
[49] Y. M. Tseng, J. K. Jan, and H. Y. Chien, “ Digital Signature with Message Recovery Using Self-certified Public Keys and its Variants, ” Applied Mathematics and Computation, Vol. 136, pp.203-214, 2003.
[50] S. F. Tzenga, M. S. Hwang, “ Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, ” Computer Standards and Interfaces, Vol. 26, pp. 61-71, 2004.
[51] E. Verheul, Self-blindable Credential Certificates from the Weil Pairing, Advances in Cryptology — ASIACRYPT 2001, LNCS, Vol. 2248, Springer-Verlag, pp. 533-551, 2001.
[52] F. G. Zhang and K. Kim, “ Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings, ” ACISP''03, Wollongong, Australia, LNCS, Vol. 2727, Springer-Verlag, pp. 312-323, 2003.
[53] F. G. Zhang and K. Kim, “ ID-Based Blind Signature and Ring Signature from Pairings, ” Advances in Cryptology — ASIACRYPT 2002, LNCS, Vol. 2501, Springer-Verlag, pp. 533-547, 2002.
[54] F. G. Zhang, S. N. Reihaneh and W. Susilo, “ An Efficient Signature Scheme from Bilinear Pairings and Its Applications, ” PKC 2004, Singapore. LNCS, Vol. 2947, Springer-Verlag, pp. 277-290, 2004.
[55] F. G. Zhang, S. N. Reihaneh and W. Susilo, “ Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings, ” INDOCRYPT 2003, New Delhi. LNCS, Vol. 2904, Springer-Verlag, pp. 191-204, 2003.
[56] T. C. Wu, Y. S. Chang, and T. Y. Lin, “ Improvement of Saeednia''s Self-certified Key Exchange Protocols, ” Electronic Letters, Vol. 34, No. 11, pp. 1094-1095, 1998.
[57] T. S. Wu and C. L. Hsu, “ Convertible Authenticated Encryption Scheme, ” Journal of Systems and Software, Vol. 62, No. 3, pp. 205-209, 2002.