A Group-Oriented Proxy Authenticated Encryption Scheme with Key-Renewal Property

陳建鈞、曹偉駿

E-mail: 9314386@mail.dyu.edu.tw

ABSTRACT

Nowadays, enterprises use a variety of information technology to construct electronic enterprise environments in order to increase the benefit of organizations. However, enterprises should also consider the security of data transmitting on the Internet. This thesis will discuss the security of delegation and proxy in an electronic enterprise environment. The traditional proxy authenticated encryption scheme usually considers proxy authenticated conditions of one-to-one, one-to-many and many-to-one merely. However, the many-to-many condition should also be considered in the real electronic commerce. It is less efficient to construct a many-to-many proxy authenticated encryption scheme using many-to-one and one-to-many. Therefore, this thesis will integrate elliptic curve cryptosystems, self-certified public key cryptosystems and the group-oriented proxy authenticated encryption scheme to design a proper group-oriented proxy authenticated encryption scheme with key renewal suitable for the many-to-many condition. This scheme allows the original signer to delegate signing and encryption right to a specific signing group, and also allows original verifier to delegate verification and decryption right to another specific verification group. This thesis is based on elliptic curve cryptosystems, and therefore it can use less bits than other public key cryptosystems to achieve the same security degree and the requirement of its memory space is reduced substantially. In addition, the group-oriented proxy authenticated encryption scheme proposed in this thesis can use different proxy key in different periods to prevent the attack caused by the leak of a proxy key due to the proposed key renewal function.

Keywords : Elliptic Curve Cryptosystems ; Self-certified Public Key Cryptosystems ; Group-Oriented Proxy Authenticated Encryption Scheme ; Key Renewal

Table of Contents

REFERENCES

[1] 李廣凱，「安全且有效率之政府電子化採購機制研究」，大葉大學資訊管理研究所碩士論文，民國九十二年(指導教授:曹偉駿博士)。
[2] 吳宗成、許建隆及蔡國裕，「適用於群體導向應用之代理鑑別加密法」，第十三屆全國資訊安全會議，頁74-82，民國九十二年。
[3] 吳宗成、許建隆及蔡國裕，「適用於電子化企業環境之代理驗證鑑別加密法」，第十四屆全國資訊安全會議，頁201-210，民國九十三年。
[4] 許建隆，「適用於群體導向應用之鑑別加密法」，國立台灣科技大學資訊管理系博士論文，民國九十年(指導教授:吳宗成博士。) [5] 陳宗保，「行動電子商務環境下安全協定之研究」，大葉大學資訊管理研究所碩士論文，民國九十年(指導教授:曹偉駿博士)。
[6] 曹偉駿及周智禾，「無線虛擬私有網路環境下群體導向安全機制之設計」，2003電子商務與數位生活研討會，頁2345-2365，民國九十二年。
[7] 資策會FIND網際網路資訊情報網: http://www.find.org.tw/0105/howmany/index.asp [8] 劉彥含，「無線虛擬私有網路環境下群體導向安全機制之研究」，大葉大學資訊管理研究所碩士論文，民國九十年(指導教授:曹偉駿博士)。
[9] 賴溪松、韓亮及張真誠，「近代密碼學及其應用」，松崗電腦圖書資料股份有限公司，民國九十年。
[10] M. Abdalla and L. Reyzin,“ A new forward-secure digital signature scheme, ” Advances in Cryptology — Asiacrypt ’2000, pp. 116-129, 2000.
[11] D. Boneh and M. Franklin,“ Identity-based encryption from the weil pairing, ” Advance in Cryptology crypto ‘ 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001.
[12] W. Caelli, E. Dawson and S. Rea,“ PKI, elliptic curve cryptography and digital signatures, ” Computer & Security, Vol. 18, No. 1, pp. 47-66, 1999.
[13] T. S. Chen. K. H. Huang and Y. F. Chung,“ A practical authenticated encryption scheme based on the elliptic curve cryptosystem, ” Computer Standards & Interfaces, Vol. 26, pp. 461-469, 2004.
[14] W. Diffie and M. E. Hellman,“ New directions in cryptography, ” IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, 1976.
[15] M. Girault,“ Self-certified public keys, ” Advances in Cryptology: Eurocrypt ’91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, pp. 490-497, 1991.
[16] P. Horster, M. Michels and H. Petersen,“ Authenticated encryption schemes with low communication costs, ” Electronics Letters, Vol. 30, No. 15, pp. 1212-1213, 1994.
[17] C. L. Hsu and T. S. Wu,“ Efficient proxy signature scheme using self-certified public keys, ” Applied Mathematics and Computation, pp. 807-820, 2004.
[18] C. L. Hsu and T. C. Wu,“ Authenticated encryption scheme with (t, n) shared verification, ” IEE Proceedings Computers and Digital Techniques, Vol. 145, No. 2, pp. 117-120, 1998.
[19] C. L. Hsu, T. S. Wu and T. C. Wu,“ Improvements of generalization of threshold signature and authenticated encryption for group communications, ” Information Processing Letters, Vol. 81, No. 1, pp. 41-45, 2002.
[20] S. J. Hwang and C. C. Chen,“ New multi-proxy multi-signature schemes, ” Applied Mathematics and Computation, pp. 57-67, 2004.
[21] S. Kim, S. Park and D. Won,“ Proxy signature, revisited, ” Proceedings of International Conference on Information and Communications Security ICIS ’97, Springer-Verlag, pp.223-232, 1997.
[22] N. Koblitz,“ Elliptic curve cryptosystems, ” Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
[23] N. Koblitz, A. Menezes and S. Vanstone,“ The state of elliptic curve cryptography, Designs, ” Codes and Cryptography, pp. 173-193, 2000.
[24] M. Mambo and E. Okamoto,“ Proxy cryptosystems: delegation of the power to decrypt ciphertexts, ” IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, Vol. E80-A, No. 1, pp. 54-63, 1997.
[25] M. Mambo, K. Usuda and E. Okamoto,“ Proxy signature for delegation signing operation, ” Proceedings of the Third ACM Conference on Computer and Communications Security, pp. 48-57, 1996.
[26] M. Mambo, K. Usuda and E. Okamoto, E.,“ Proxy signature: delegation of the power to sign messages, ” IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, Vol. E79-A, No. 9, pp. 1338-1354, 1996.
[27] M. S. Hwang, J. L. Lu and I. C. Lin,“ A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem, ” IEEE Transactions on Knowledge and Data Engineering, Vol. 15, No. 6, pp. 1552 — 1560, 2003.
[28] 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.

[29] V. S. Miller, “ Use of elliptic curves in cryptography, ” Advances in Cryptology Crypto ’ 85, Lecture Notes in Computer Science 218, Springer-Verlag, pp. 417-426, 1986.
[30] K. Nyberg and R. A. Rueppel, “ Message recovery for signature based on the discrete logarithm problem, ” Advances in Cryptology Eurcrypt ’ 94, pp. 182-193, 1995.
[31] A. Shamir, “ How to share a secret, ” Communications of the ACM, Vol. 22, pp. 612-613, 1979.
[32] A. Shamir, “ Identity-based cryptosystems and signature schemes, ” Advances in Cryptology: Crypto ’ 84, pp. 47-53, 1985.
[33] H. M. Sun and B. J. Chen, “ Time-stamped proxy signatures with traceable receivers, ” Workshop on Information Security ISW ’ 99, pp. 247-253, 1999.
[34] H. M. Sun, “ Design of time-stamped proxy signatures with traceable receivers, ” IEE Proceedings — Computers and Digital Techniques, Vol. 147, No. 6, pp. 462-466 , 2000.
[35] W. J. Tsaur, “ Designing an efficient wireless public key infrastructure in mobile internet environments, ” Proceedings of the 6th World Multiconference on Systemics, Cybernetics, and Informatics (SCI 2002), Orlando, Florida, USA, Vol. X, pp. 516-521, 2002.
[36] S. Vanstone, “ Elliptic curve cryptosystem — the answer to stong, fast public key cryptography for securing constrained environments, ” Information Security Technical Report, Vol. 2, No. 2, Elsevier, pp. 78-87, 1997.
[37] C. T. Wang, C. C. Chang and C. H. Lin, “ Generalization of threshold signature and authenticated encryption for group communications, ” IEICE Transaction on Fundamentals of Electronics, Communications and Computer Science, Vol. E83-A, pp. 1228-1237, 2000.
[38] T. C. Wu, C. L. Hsu and K. Y. Tsai, “ Anonymous proxy authenticated encryption scheme for group-oriented applications, ” Proceedings of the Thirteenth National Conference on Information Security, pp. 74-82, 2003.
[39] L. Yi, G. Bai and G. Xiao, “ Proxy multi-signature scheme: a new type of proxy signature scheme, ” Electronics Letters, Vol. 36, No. 6, pp. 527-528, 2000.
[40] F. Zhang, Q. Li and Y. Wang, “ A new secure electronic auction scheme, ” Eurocumm 2000, Information System for Enhanced Public Safety and Security IEEE/AFCEA, pp. 54-56, 2000.