適用電子商務環境之金鑰恢復與託管機制研究

林幸君、曹偉駿

E-mail: 9222447@mail.dyu.edu.tw

摘 要

在電子商務環境中，一個安全的交易環境是不可或缺的，而安全的密碼系統正提供我們一個很好的解決方案。在這些密碼系統中，使用者的保障皆依賴在金鑰的安全管理上。所以，金鑰安全管理的相關議題對於密碼系統而言是十分重要的。本論文所要探討的課題即是密碼系統中的金鑰恢復與金鑰託管機制。由於金鑰恢復與金鑰託管機制之運作需要繁複的金鑰運算與訊息傳遞。 而本論文提出之金鑰恢復與託管機制，利用橢圓曲線密碼系統中金鑰長度較短與計算速度快之優點，以及自我認證公開金鑰密碼系統中有效率的驗證公鑰正確性之優點，讓此機制不必依靠系統中心就能達到身份確認以及提高效率性。另外我們在電子現金系統中加入託管的功能，設計出託管電子現金系統，避免電子現金完全匿名可能產生之犯罪行為，我們所設計的託管電子現金系統除了具有防範網路犯罪之功能(如洗錢、勒索)，並且能迅速地找出犯罪者，還給受害者一個公道。

關鍵詞 : 橢圓曲線密碼系統、自我認證公開金鑰密碼系統、金鑰恢復機制、金鑰託管機制、電子現金系統、託管電子現金系統

目錄

參考文獻

[1] 張明聖, 「商業性金鑰恢復與金鑰託管機制之研究」, 中央大學資訊工程研究所碩士論文, 民國90年。

[2] 張真誠、韓亮、賴溪松, 「近代密碼學及其應用」, 松崗圖書資料公司, 民國88年。

[3] 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90年。

[4] 楊泰岳, 「適用單雙向通訊之金鑰託管系統之研究」, 台灣科技大學電子工程研究所碩士論文, 民國89年。

[5] 賴溪松、李永振、樊國楨, 「美國Escrowed Encryption Standard簡介」, 資訊安全通訊, 民國85年。

[6] Y. Y. Al-Salqan, "Cryptographic key recovery," Proceedings of 6th IEEE Workshop on Future Trends of Distributed Computing Systems, pp. 34-37, 1997.

[7] M. Bellare and S. Goldwasser, "Encapsulated key escrow," In MIT/LCS/TR-688, 1996.

[8] M. Bellare, S. Goldwasser, "Verifiable partial key escrow," Proceedings of 4th ACM Conference on Computer and Communications Security, 1997.

[9] T. Beth, H. Knobloch, M. Otten, G. J. Simmons, and P. Wichmann, " Towards acceptable key escrow systems," Proceedings of 2nd ACM Conference on Computer and Communications Security, pp. 51-58, 1994.

[10] M. Blaze, "Protocol failure in the escrowed encryption standard," Proceedings of 2nd ACM Conference on Computer and Communications Security, pp. 59-67, 1994.

[11] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," Advances in Cryptology-Crypto'2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001.

[12] C. Boyd, "Enforcing traceability in software," In Information and Communication Security-First International Conference, ICICS'97, Springer-Verlag, pp. 398-408, 1997.

[13] S. Brands, "Electronic cash systems based on the representation problem in groups of prime order, Technical Report CS-R9323, CWI, 1993.

[14] S. Brands, "Untraceable of off-line cash in wallets with observers," Advances in Cryptology-Crypto'93, LNCS, Springer-Verlag, Vol. 773, pp. 302- 318, 1993.

[15] M. Burmester, Y. Desmedt and J. Seberry, "Equitable key escrow with limited time span (or, How to enforce time expiration cryptographically)," Advanced in Cryptology-Asiacrypt'98, Springer-Verlag, LNCS, Vol. 1514, pp. 380-391, 1998.

[16] W. Caelli, E. Dawson, and S. Rea, "PKI, Elliptic Curve Cryptography and digital signatures," Computer & Security, Vol. 18, No. 1, 1999, pp. 47-66.

[17] Y. S. Chang, T. C. Wu and S. C. Huang, "ElGamal-like digital signature and multisignature schemes using self-certified public keys," Journal of Systems and Software, pp. 99-105, 2000.

[18] D. Chaum, "Blind signature for untraceable payments," Advances in Cryptology-CRYPTO'82, LNCS, pp.199-203, 1983.

[19] A. J. Clark, S. S. Limited, "Key recovery—why, how, who?," Computers and Security, Vol. 16, No. 8, pp. 669-674, 1997.

[20] D. E. Denning and D.K. Branstad, "A taxonomy for key escrow encryption systems," Communications of the ACM, Vol. 39, No. 3, pp. 34-40, 1996.

[21] D. E. Denning and M. Smid, "Key escrowing today," IEEE Communications, Vol. 32, pp. 58-68, 1994.

[22] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, No. 6, pp. 644-654, 1976.

[23] R. Ganesan, "The Yaksha security system," Communications of the ACM, vol. 39, pp. 55-60, 1996.

[24] M. Girault, "Self-certified public keys," Advances in Cryptology-EuroCrypt'91, LNCS, Vol. 547, Spring-Verlag, pp. 491-497, 1991.

[25] J. Kennedy, S. M. Matyas, Jr. and N. Zunic, "Key recovery functional model," Computers & Security, Vol. 19, pp. 31-36, 2000.

[26] J. Kim, S. Kim, H. Kwon, and S. Lee, "Forward-secure commercial key escrow systems," Tenth IEEE International Workshops on Enabling Technologies:Infrastructure for Collaborative Enterprises, pp. 211-216, 2001.

[27] D. F. Knuth, "Seminumerical Algorithms," The Art of Computer Programming, Addison-Wesley, Vol. 2, 1981.

[28] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, Vol. 48, No. 17, pp. 203-209, 1987.

[29] D. Kugler and H. Vogt, "Marking : A Privacy Protecting Approach Against Blackmailing", International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1992, Springer-Verlag, pp. 137-152, 2001.

[30] M. Lee, G. Ahn, J. Kim, J. Park, B. Lee, K. Kim, and H. Lee, "Design and implementation of an efficient fair off-line E-Cash system based on elliptic curve discrete logarithm problem," Journal of Communications and Networks, Vol. 4, 2002.

[31] S. Lim, H. Ham, M. Kim, and T. Kim, " Design of key recovery system using multiple agent technology for electronic commerce," IEEE International Symposium on Industrial Electronics Conferences, pp. 1351-1356, 2001.

[32] W. Mao, "Publicly verifiable partial key escrow," International Conference on Information and Communications Security, Springer-Verlag, LNCS , pp. 409-413, 1997.

[33] V. S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology-Crypto'82, Springer-Verlag, 1986.

[34] J. Nechvatal, "A public-key-based key escrow system," Journal of Systems and Software, Vol. 35, pp. 73-83, 1996.

[35] J. M. Nieto, K. Viswanathan, C. Boyd, and E. Dawson, "Key recovery system for the commercial environment," International Journal of Information Security, Vol. 1, pp. 161-174, 2002.

[36] NIST, "Escrowed encryption standard," FIPS PUB 185, 1994.

[37] T.P.Pedersen, "Distributed provers with applications to undeniable signature," Advances in Cryptology-EUROCRYPT'91, LNCS, Vol. 547, Springer-Verlag, pp. 221-238, 1991.

[38] H. Petersen and G. Poupard, "Efficient fair cash with off-line extortion prevention," Proceedings of ICICS'07, LNCS 1334, Springer-Verlag, pp. 463-477, 1997.

[39] S. Saeednia, "Identify-based and self-certified key-exchange protocols," Proceedings of ACISP'97, Information Security and Privacy, LNCS, Vol. 1270, Springer-Verlag, pp. 303-313, 1997.

[40] A. Shamir, "Partial key escrow:A New Approach to Software Key Escrow," NIST Key Escrow Standards meeting, 1995.

[41] J. Shaoquan and Z. Yufeng, "Partial key escrow monitoring scheme," The International Workshop on Cryptographic Technique and E-Commerce'99, HongKong, 2002.

[42] M. Smith, P. VanOorschot, and M. Willet, "Cryptographic information recovery using key recovery," Computers & Security, Vol. 19, pp. 21-27, 2000.

[43] B. von Solms and D. Naccache, "On blind signatures and perfect crimes," Computers and Security, Vol. 11, No. 6, pp. 581-583, 1992.

[44] C. J. Tsao, Y. H. Lin, C. Y. Chen and C. Y. Ku, "An efficient escrow electronic cash system based on Yacobi's scheme," Proceedings of 2000 Workshop on Internet & Distributed System, pp. 398-406, 2000.

[45] W. J. Tsaur and C. H. Ho, "A Secure Electronic Payment System Based on Efficient Public Key Infrastructure," Proceedings of the 2002

International Workshop for Asian Public Key Infrastructures (IWAP 2002), Taipei, Taiwan, 2002.

[46] S. Vanstone, "Elliptic Curve Cryptosystem—the answer to strong, fast public key cryptography for securing constrained environments," Information Security Technical Report, Vol. 2, No. 2, Elsevier, 1997, pp. 78-87.

[47] K. Viswanathan, C. Boyd and E. Dawson, "Strong binding for software key escrow," International Workshops on Parallel Processing, IEEE Press., 1999.

[48] H Wang, and Y. Zhang "Untraceable off-line electronic cash flow in e-commerce," Proceedings of Computer Science Conference, pp. 191-198, 2001.

[49] H. C. Yu, K. H. Hsi and P. J. Kuo, "Electronic payment systems : an analysis and comparison of types," Technology in Society, pp. 331-347, 2002.

[50] P. L. Yu and C. L. Lei, "A proxy deposit protocol for e-cash systems," Proceedings of the 11th Conference on Information Security, pp. 289-295, 2001.