基於部分盲簽章之多銀行聯合發行的行動電子現金系統

陳昭安、曹偉駿

E-mail: 9707320@mail.dyu.edu.tw

摘 要

近年來行動通訊的快速發展，越來越多人使用具上網功能的可攜式行動通訊設備。基於行動電話極高的普及率，加上行動裝置本身所具有的自由度、機動性，行動商務勢必是未來的趨勢。也正因如此，更增添了行動商務交易安全議題的重要性。 由於行動裝置的頻寬較小、運算能力較差，目前適用於行動商務之付款系統，多半著重於提升效率但卻忽略其安全性，或是需要較高的交易成本。然而，一個行動付款系統需具備安全、易於使用及費用低廉三項特質才能吸引消費者使用，驅使業者投資。因此，本論文將植基於既安全且高效率之ECC based self-certified public key cryptosystem設計出部分盲簽章機制，並將其應用於多銀行聯合發行的行動電子現金系統。除了能改善銀行資料庫大量成長的衝擊，更有效解決了已簽署之電子現金難以辨識其額度與時效的問題。而聯合發行的導入，使電子現金具備了統一的驗證與集中的管理之特性，能提升消費者對行動電子付款的信心，進而促進行動商務的發展。

關鍵詞 : 行動電子現金;部分盲簽章;自我認證公開金鑰密碼系統;多銀行聯合發行

目錄

參考文獻

Abe, M., & Fujisaki, E. (1996). How to date blind signatures. Proceedings of Advances in Cryptology-Asiacrypt ’ 96, LNCS, Springer-Verlag, 1163, 244-251. Cao, T., Lin, D., & Xue R. (2005). A randomized RSA-based partially blind signature scheme for electronic cash. Computers & Security, 24, 44-49. Carmenisch, J. L., Piveteau, J. M., & Sradler, M. A. (1994). Blind signatures based on the discrete logarithm problem. Proceedings of Rump Session of Eurocrypt ’ 94, Springer-Verlag, 428-432. Cervera, A. (2002). Analysis of J2ME^(TM) for developing mobile payment systems. Copenhagen: University of Copenhagen. Chaum, D. (1983). Blind signature for untraceable payments. Proceedings of Advances in Cryptology: Crypto ’ 82, 199-203. Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable electronic cash. Proceedings of Advances in Cryptology: Crypto ’ 88, 319-327. Chien, H. Y., Jan, J. K., & Tseng Y. M. (2001). RSA-based partially blind signature with low computation. Proceedings of the Eighth International Conference on Parallel and Distributed Systems, 385-389. Dhem, J. F., Veithen, D., & Quisquater, J. J. (1996). SCALPS: Smart card for limited payment systems. Micro, IEEE, 16(3), 42-51. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469-472. Ferreira, L., & Dahab, R. (1998). A scheme for analyzing electronic payment systems. Proceedings of Computer Security Applications Conference, 137-146. Girault, M. (1991). Self-certified public keys. Proceedings of Advances in Cryptology-EuroCrypt ’ 91, LNCS, Spring-Verlag, 547, 491-497. GiSMo. (2008). Millicom international celluar sa announce secure internet shopping with your mobile phone [Online]. Available: http://www.mobic.com/oldnews/9911/millicom_international_cellular_.htm [2008, February 17]. Harn, L. (1994). New digital signature scheme based on discrete logarithm. Electronics Letters, 30(5), 396-398. Horster, P., Michels, M., & Petersen, H. (1995). Cryptanalysis of the blind signatures based on the discrete logarithm problem. Electronics Letters, 31(21), 1827. Hu, Z. Y., Liu, Y. W., Hu, X., & Li, J. H. (2004). Anonymous micropayments authentication (AMA) in mobile data network. Proceedings of INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, 46-53. Kim, M. A., Lee, H. K., Kim, S. W., Lee, W. H., & Kang, E. K. (2002). Implementation of anonymity-based e-payment system for m-commerce. Proceedings of IEEE 2002 International Conference on Communication, Circuits and Systems and West Sino Expositions, 1, 363-366. Kim, S., & Oh, H. (2001). An atomic micropayment system for a mobile computing environment. IEICE Transactions information & Systems, 84(6), 709-716. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(17), 203-209. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptograph designs. Codes and Cryptography, 19, 173-193. Lee, M., Ahn, G., Kim, J., Park, J., Lee, B., Kim, K., & Lee, H. (2002). Design and implementation of an efficient fair off-line e-cash system based on elliptic curve discrete logarithm problem. Journal of Communications and Networks, 4(2), 81-89. Lu, E. W., & Wuu, L. C. (2004). Multiple banks electronic payment systems by group blind signatures. Journal of Internet Technology, 5(1), 41-46. Lysyanskaya, A., & Ramzan Z. (1998). Group blind digital signature: a scalable solution to electronic cash. Proceedings of Financial Cryptography (FC ’ 98), 1465, 184-197. Miller, V. S. (1986). Use of elliptic curves in cryptography. Proceedings of Advances in Cryptology: Crypto ’ 85, Springer- Verlag, 417-426. Mobipay. (2008). Creating a mobile payment standard based on a co-operation between financial institutions and telcos [Online]. Available: http://epso.jrc.es/presentations.html[2008, February 17]. Mohammed, E., Emarah, A. E., & El-shennawy, K. H. (2000). A blind signature scheme based on ElGamal signature. Proceedings of Seventeenth National Radio Science Conference, C25.1-C25.6. Paiement CB sur mobile. (2008). Paiement CB sur mobile [Online]. Available: http://www.mercatel.info/espadhaccueil.html[2008, February 18]. Paybox. (2008). Business and technical information regarding the security at paybox [Online]. Available: http://paybox.net/ [2008, February 16]. Paybox. (2008). Die paybox-gruppe strukturiert um [Online]. Available: http://www.paybox.de [2008, February 16]. Paypal. (2008). X.com [Online]. Available: http://www.paypal.com [2008, February 16]. Pedersen, T. P. (1991). Distributed provers with applications to undeniable signature. Proceedings of Advances in Cryptology – EUROCRYPT ’ 91, LNCS, Springer-Verlag, 547, 221-238. Petersen, H., & Poupard, G. (1997). Efficient fair cash with off-line extortion prevention. Proceedings of ICICS ’ 97, LNCS, Springer-Verlag, 1334, 463-477. Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. Journal of Cryptology, 13, 361-396. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital structures and public-key cryptosystem. Communication of ACM, 21(2), 120 – 126. Sandholm, T., & Huai, Q. (2000). Nomad: mobile agent system for an internet-based auction house. IEEE Internet Computing, 4(2), 80-86. Towergroup. (2008). Mobile commerce: financial institutions and mobile carriers define their roles in the new M-World [Online]. Available: http://www.towergroup.com/research/ho- me/ index.htm [2008, February 19]. Tsaur, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Mathematics and Computation, 168(1), 447-464. Tsaur, W. J., & Lin, S. J. (2004). Designing key recovery and escrow schemes in electronic commerce environments. Journal of Internet Technology, 5(1), 33-39. Vodafone m-pay bill. (2008). Vodafone m-pay bill [Online]. Available: http://mpay-bill.vodafone.co.uk [2008, February 18]. Wang, C., Li, Q., & Yang, X. (2007). Fair e-cash system without trustees for multiple banks. Proceedings of Computational Intelligence and Security Workshops, 585-587. Weber, Dr. R. (2001). Security / Electronic commerce. SIEMENS, 1. Zhang, J., Ma, L., & Wang, Y. (2007). A fair and transferable off-line electronic cash system with multiple banks. Proceedings of IEEE International Conference on e-Business Engineering, 189-194.