

# Multiple Banks Issuing E-cash Systems Based on Partially Blind Signature Scheme

陳昭安、曹偉駿

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

## ABSTRACT

In recent years, more and more people use portable mobile appliances with the function of the Internet roaming due to the rapid growth of mobile communication. Mobile phones highly prevail in our society and their devices are easy to install, to change and to use, so mobile commerce will surely be the trend of the future. Therefore, the secure transaction issue of mobile commerce is becoming more and more important. Because the bandwidth of mobile appliance is smaller and its ability of computation is worse, the promotion of effectiveness is mostly focused on the payment system of mobile commerce, but its security is ignored. Transaction expenditure is thus higher in order to solve the problem. However, in the mobile payment system there should be three properties which are security, easy-to-use and low-cost to stimulate consumers to use it and the bosses to invest in it. Therefore, in this study we design partially blind signature scheme based on secure and efficient ECC based self-certified public cryptosystem. And we apply the scheme in the mobile e-cash system issued together by multiple banks. The scheme can not only reduce the impact of great growth of bank database, but also effectively solve the problems of time limitation and amount recognition of signed e-cash. Besides, the e-cash system issued together by multiple banks makes e-cash operate under universal verification and centralized management. In such a manner, it raises consumers' confidence to use e-cash payment and promote the development of mobile commerce.

Keywords : mobile e-cash ; partially blind signature ; ECC based self-certified public key cryptosystem ; multiple banks issuing

## Table of Contents

中文摘要	iii	英文摘要	iii
iv 誌謝辭	vi	內容目錄	vi
viii 表目錄	ix	圖目錄	ix
x 第一章 緒論	1	第一節 研究背景與動機	1
1 第二節 研究目的	2	第三節 研究流程	2
2 第四節 論文架構	4	第二章 文獻探討	4
5 第一節 電子付款機制	5	第二節 公開金鑰密碼系統	5
16 第三節 ECC based self-certified public key cryptosystem	16	第五節 多銀行聯合發行	16
17 第四節 部分盲簽章	21	第一節 多銀行聯合發行之行動電子現金系統安全需求	25
22 第三章 多銀行聯合發行的行動電子現金系統安全需求	25	第二節 植基於ECC based self-certified public key cryptosystem發展部分盲簽章機制	27
29 第四節 小結	41	第三節 多銀行聯合發行的行動電子現金付款機制	41
43 第一節 安全性分析	43	第四章 安全性與複雜度分析	43
52 第五章 結論	62	第二節 複雜度分析	62
63 參考文獻	62		62

## REFERENCES

- 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, Springer-Verlag, 547, 491-497. GiSMo. (2008). Millicom international cellular sa announce secure internet shopping with your mobile phone [Online]. Available: [http://www.mobico.com/oldnews/9911/millicom\\_international\\_cellular\\_.htm](http://www.mobico.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 Annual Joint 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., & Wu, 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://eps.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/home/index.htm> [2008, February 19]. Tsauro, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. *Applied Mathematics and Computation*, 168(1), 447-464. Tsauro, 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.