電子現金型付款系統研析與應用

吳聯鑫、曹偉駿

E-mail: 345514@mail.dyu.edu.tw

摘 要

近年來電子付款系統越來越普及為了追求方便與效率，而取代傳統付款方式成為便利付款的趨勢，電子付款在交易時的安全是極重要的議題，因為各方之間的交易轉移沒有直接接觸，若電子付款系統存在安全疑慮，則可能會降低消費者、商家和銀行使用電子付款系統的信心，因而嚴重影響電子商務發展的基礎。一般電子付款方式包括信用卡型、帳戶型、以及電子現金型，在此三種付款類型中，由於電子現金型比較接近傳統現金付款方式，而且其邊際成本較另外二者低，故較易為使用者與系統商所接受。此外，近年來行動通訊的快速發展，基於行動電話極高的普及率，以及行動裝置本身所具有的自由度與機動性，行動商務正蓬勃發展當中。有鑑於電子現金付款技術的相關研究頗多，亦各具特色，將之應用於實際情況時無法一體適用，故本研究將探討電子付款趨勢以及其種類與優缺點，特別針對目前商業上較多人使用的電子現金型付款系統與學術上提出的電子現金型付款機制分別進行分析比較，並從中選擇較具優越性的系統應用於智慧型商店。

關鍵詞 : 電子商務、電子付款、電子現金、行動付款、資訊安全、智慧型商店

目錄

參考文獻

一、中文部份 [1]悠遊卡股份有限公司，“ EasyCard, ”2010, http://www.tscc.com.tw/default.aspx (2010/6/10) [2]財團法人資訊工業策進會，“ 智慧型商店, ”2011, http://www.find.org.tw/distribution/home.aspx (2011/02/01) 二、英文部份 [3]S. Brands, “ Electronic cash on the Internet ”, Proceedings of the 1995 Symposium on Network and Distributed System Security (SNDSS'95), pp. 64-84, 1995.

[4]S. Brands, “ Untraceable off-line cash in wallets with observers, ” Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, pp. 302-318, 1994.

[5]D. Chaum, “ Blind signature for untraceable payments, ” Proceedings of Advances in Cryptology: Crypto ’ 82, pp. 199-203, 1983.

[6]D. Chaum, A. Fiat and M. Naor, “ Untraceable electronic cash, ” Proceedings of Advances in Cryptology: Crypto ’ 88, pp. 319-327, 1988.

[7]C. L. Chen and M. H. Liu, “ A traceable E-cash transfer system against blackmail via subliminal channel, ” Electronic Commerce Research and Applications, vol. 8, no. 6, pp. 327-333, 2009.

[8]L. Erreira and R. Dahab, “ A scheme for analyzing electronic payment systems, ” Proceedings of Computer Security Applications Conference,

pp. 137-146, 1998.
[9]P. Horster, M, Michels and H. Petersen, “ Cryptanalysis of the blind signatures based on the discrete logarithm problem, ” Electronics Letters, vol. 31, p. 1827, 1995.
[10]Z. Y. Hu, Y. W. Liu, X. Hu and J. H. Li, “ Anonymous micropayments authentication (AMA) in mobile data network, ” Proceedings of IEEE INFOCOM 2004, pp. 46-53, 2004.
[11]icash, “ IcashWave “ , 2010, http://www.icash.com.tw/howtouse.asp (2010/6/11) [12]W. S. Juang, “ RO-cash: An efficient and practical recoverable pre-paid offline e-cash scheme using bilinear pairings, ” The Journal of Systems and Software, vol. 83, no. 4, pp. 638-645, 2010.
[13]M. A. Kim, H. K. Lee, S. W. Kim, W. H. Lee and E. K. Kang, “ 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, vol. 1, pp. 363-366, 2002.
[14]C. Kim, W. Tao, N. Shin and K. Kim, “ An empirical study of customers ’ perceptions of security and trust in e-payment systems, ” Electronic Commerce Research and Applications, vol. 9, no. 1, pp. 84-95, 2010.
[15]Z. Y. Lee, H. C. Yu and P. J. Ku, “ An analysis and comparison of different types of electronic payment systems ” Management of Engineering and Technology, vol. 2, pp. 38 – 45, 2001.
[16]E. W. Lu and L. C. Wuu, “ Multiple banks electronic payment systems by group blind signatures, ” Journal of Internet Technology, vol. 5, no. 1, pp. 41-46, 2004.
[17]F. C. Lin, H. W. Yu, C. H. Hsu and T. C. Weng, “ Recommendation system for localized products in vending machines, ” Expert Systems with Applications , vol. 38, pp. 9129-9138, 2011.
[18]T. Okamota and K. Ohita, “ Universal electronic cash, ” Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, pp. 324-337, 1991.
[19]C. Popescu and H. Oros, “ A fair off-line electronic cash system with anonymity revoking trustee, ” Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, pp. 409-416, 2004.
[20]C. Popescu, “ An electronic cash system based on group blind signatures, ” Informatica, vol. 17, no. 4, pp. 551-564, 2006.
[21]W. J. Tsaur and S. J. Lin, “ Designing key recovery and escrow schemes in electronic commerce environments, ” Journal of Internet Technology, vol. 5, no. 1, pp. 33-39, 2004.
[22]W. J. Tsaur and H. C. Tsai, “ Multiple Banks Issuing Mobile E-cash Systems, ” Proceedings of the 15th Mobile Computing Workshop, Taiwan, pp. 145-154, 2010.
[23]W. J. Tsaur, “ Several security schemes constructed using ECC-based self-certified public key cryptosystems, ” Applied Mathematics and Computation, vol. 168, no. 1, pp. 447-464, 2005.
[24]B. Von Solms and D. Naccache, “ On blind signatures and perfect crimes, ” Computers and Security, vol. 11, no. 6, pp. 581-583, 1992.
[25]Visa, “ VisaWave, ” 2010, http://www.visa-asia.com/ap/tw/index.shtml (2010/6/10) [26]C. Wang, Q. Li and X. Yang, “ Fair e-cash system without trustees for multiple banks, ” Proceedings of Computational Intelligence and Security Workshops, pp. 585-587, 2007.
[27]C. Wang and R. Lu, “ An ID-based transferable off-line e-cash system with revokable anonymity, ” Proceedings of International Symposium on Electronic Commerce and Security, pp. 758-762, 2008.
[28]J. Zhang, L. Ma and Y. Wang, “ A fair and transferable off-line electronic cash system with multiple banks, ” Proceedings of IEEE International Conference on e-Business Engineering, pp. 189-194, 2007.