Research, analysis and application of electronic cash payment systems

# 吳聯鑫、曹偉駿

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

### ABSTRACT

In recent years the electronic payment system was getting more and more popular to pursue the convenience and efficiency instead of the traditional payment manner, The security of the electronic payment transaction is an extremely important issue. If the security is not eahanced, the consumer, business and bank will lose the confidence in employing the electronic payment system, and thus seriously influence the foundation of electronic commerce development. Electronic payment methods include credit card, account-based, and electronic cash models. Among the three kinds of payment manner, the electronic cash model is quite similar to the traditional cash payment and have the lowest cost margins, so it has the highest adaptability among the consumers and vendors. In addition, due to the rapid development of mobile communication and mobile devices ' high usage with its superior flexibility and functionality, electronic mobile device industry is booming. Owing to the fact that there are a wide variety of electronic payment technologies that cannot be used for all applications, this study will discuss and analyze the trends, benefits and concerns associated with electronic payment methods, focusing on the more commonly used commercial electronic cash payment system and academic research on the mechanisms of electronic payment methods. The objective of this thesis is to conclude with the result of relevant cash-based payment method comparisons, and further apply the most superior technology to the smart store.

Keywords : Electronic commerce, Electronic payment, Electronic cash, Mobile payment, Information security, Smart store

### Table of Contents

中文摘要...........................	英文摘要........................
iv 誌謝........................	/ 目錄
. vi 圖目錄	.viii 表目錄.....................
...ix 第一章 緒論....................	..1 1.1 研究背景..................
11.2 研究動機與目的	Σ流程..................4 1.4 研究架構
......................5 第二章 文獻探討..	6 2.1 電子付款類型 .
...............6 2.1.1 信用卡型付款方式..	
..........72.1.3 電子現金型付款方式.....	.......82.2 電子付款層面探討.......
10 2.2.1 技術層面	..10 2.2.2 經濟層面...............
11 2.2.3 社會層面	2 2.2.4 監控層面...................12
第三章 電子現金型付款系統分析比較 133.	1 智慧卡小額付款................13 3.2 行
動電子現金付款................4 3.3 商業與學術	衔之電子現金型付款系統分析比較 . . 15 第四章 電子現金
型付款系統應用	
..............25 4.3 智慧型商店付款機制...	
	......29 4.3.3 提款階段..........
	...32 4.3.5 交易階段..............
35 4.3.6 存款階段	36 4.3.7 追蹤階段..................
37 4.3.8 小結...................38 4.4	效益分析與探討...............39 第五章
結論與未來展望41 參考文獻	

### REFERENCES

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.