基於行動代理人之整合電子付款的行動電子拍賣機制

蘇雍超、曹偉駿

E-mail: 9422479@mail.dyu.edu.tw

摘 要

與日俱增的消費者期望著能透過手持行動裝置享受行動商務(m-commerce)的各樣式服務。在電子商務中，電子拍賣是越來越普及與重要的線上交易活動之一，目前許多學者也針對電子拍賣的安全性提出相關機制加以解決。在有線的環境中，運用代理人技術以協助拍賣雖已蔚然成風，不過，行動拍賣機制卻鮮少探討行動代理人機密資訊的防護，除此之外，目前的電子拍賣機制之研究少有探討到拍賣後的付款機制，因此，本研究使用低運算量之『植基於ECC的自我認證公開金鑰密碼系統』，以設計出以行動代理人為基礎之整合式行動電子拍賣機制。因此，藉由本機制將可降低拍賣與付款過程中，手持裝置的運算量與網路通訊的傳輸量。而在安全性方面，本研究藉由代理鑑別金鑰隱藏議價者的私鑰，改善過去使用行動代理人議價的安全拍賣機制皆未解決的議價者私鑰外洩之問題，使其滿足日益發展的行動商務環境之安全需求，並克服手持裝置硬體先天上的限制。基於上述，本機制整合安全的電子付款與行動電子拍賣，使得整個流程既便捷又安全，讓使用者將更樂於參與行動電子拍賣，進而促使行動商務更加蓬勃發展。

關鍵詞 : 行動商務 ; 行動代理人 ; 電子付款 ; 電子拍賣 ; 橢圓曲線密碼系統

目錄

第一章 緒論.....1 1.1 研究背景與動機.....1 1.2 研究目的.....2 1.3 研究流程.....3 1.4 論文架構.....5 第二章 文獻探討.....6 2.1 行動代理人安全性.....6 2.2 電子拍賣機制.....12 2.3 電子付款機制.....16 2.4 植基於ECC的自我認證公開金鑰密碼系統.....29 第三章 以行動代理人為基礎之整合式行動電子拍賣機制..34 3.1 初始階段.....35 3.2 註冊階段.....38 3.3 提款階段.....40 3.4 拍賣階段.....41 3.5 宣佈階段.....43 3.6 金鑰託管階段.....45 3.7 付款階段.....49 3.8 存款階段.....50 3.9 追蹤階段.....51 3.10 討論.....52 第四章 安全性與複雜度分析.....54 4.1 安全性分析.....54 4.2 複雜度分析.....67 第五章 系統雛形建構.....78 第六章 結論.....84 參考文獻.....85

參考文獻

[1]邱筱雅，「電子商務的付款機制:研究文獻回顧與評述」，交通大學資訊管理研究所碩士論文，民國85年。

[2]邵敏華、黃景彰，「SET使用的密碼學技巧:優缺點之評估」，資訊安全通訊，民國88年。

[3]段正明、李鎮樟，「電子付款的分析與探討，電腦與通訊」，民國85年。

[4]吳琮璠、謝清佳，「資訊管理」，智勝文化事業，民國87年。

[5]H. S. Bierman and L. Fernandez, Game theory with economic applications, Addison Wesley, 1993.

[6]A. Cervera,“ Analysis of J2ME? for developing mobile payment systems, ” IT University of Copenhagen, 2002.

[7]T.S. Chen,“ An English auction scheme in the online transaction environment, ” Computers & Security, Vol. 23, No. 5, pp. 389 – 399, 2004.

[8]C.C. Chang and Y.F. Chang,“ Efficient anonymous auction protocols with freewheeling bids, ” Computers & Security, Vol. 22, No. 8, pp. 728 – 734, 2003.

[9]W. Caelli, E. Dawson and S. Rea,“ PKI, elliptic curve cryptography and digital signatures, ” Computer & Security, Vol. 18, No. 1, pp. 47 – 66, 1999.

[10]D.M. Chess, B. Grosof, C.G. Harrison, D. Levine, C. Parris, and G. Tsudik,“ Itinerant agents for mobile computing, ” IEEE Personal Communications, Vol. 2, No. 5, pp. 34 – 49, 1995.

[11]eBay, http://www.ebay.com, 2001.

[12]T. ElGamal,“ A public key cryptosystem and a signature scheme based on discrete logarithms, ” IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469 – 472, 1985.

[13]L. Ferreira and R. Dahab,“ A scheme for analyzing electronic payment systems, ” Computer Security Applications Conference, pp. 137 – 146, 1998.

[14]GiSMo, http://www.mobic.com/oldnews/9911/millicom_international_cellular_.htm.
[15]M. Gini, A. Jaiswal and Y. Kim, " Design and implementation of a secure multi-agent marketplace, " Electronic Commerce Research and Applications, Vol. 3, No. 4, pp. 355 – 368, 2004.
[16]M. Girault, " Self-certified public keys, " Advances in Cryptology – EuroCrypt'91, LNCS, Vol. 547, pp. 491-497, 1991.
[17]L. Harn, " New digital signature scheme based on discrete logarithm, " Electronics Letters, Vol. 30, No. 5, pp. 396 – 398, 1994.
[18]M.N. Huhns and J.M. Vidal, " Online auctions, " IEEE Internet Computing, Vol. 3, No. 3, pp. 103 – 105, 1999.
[19]Z.Y. Hu, Y.W. Liu, X. Hu and J.H. Li, " Anonymous micropayments authentication (AMA) in mobile data network, " INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, 2004.
[20]W.A. Jansen, " Countermeasures for mobile agent security " , Computer Communications, Vol. 23, No. 17, pp. 1667 – 1676, 2000.
[21]E. Kountz, " Celling mobile payments: what carrier positioning in mobile micropayments means for FSIs, " ACI and Towergroup, 2002.
[22]N. Koblitz, " Elliptic curve cryptosystems, " Mathematics of Computation, Vol. 48, No. 17, pp. 203 – 209, 1987.
[23]K.D. Kotay and D. Kotz, " Transportable agents " , Proceedings of the CIKM Workshop on Intelligent Information Agents, Third International Conference on Information and Knowledge Management, 1994.
[24]S. Kim and H. Oh, " An atomic micropayment system for a mobile computing environment, " IEICE Transactions Information & Systems, Vol.84, No. 6, 2001.
[25]N. Koblitz, A. Menezes and S. Vanstone, " The state of elliptic curve cryptograph, " Designs, Codes and Cryptography, Vol. 19, No. 2-3, pp. 173-193, 2000.
[26]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, " IEEE 2002 International Conference on Communication, Circuits and Systems and West Sino Expositions, 2002.
[27]I.C. Lin, H.H. Ou and M.S. Hwang, " Efficient access control and key management schemes for mobile agents, " Computer Standards & Interfaces Vol. 26, No. 5, pp. 423 – 433, 2004.
[28]V.S. Miller., " Use of elliptic curves in cryptography, " Advances in Cryptology:Crypto ' 85, pp. 417 – 426, 1986.
[29]Mobipay, http://epso.jrc.es/conference/presentations.html [30]P.J. Marques, L.M. Silva and J.G. Silva, " Secure mechanisms for using mobile agents in electronic commerce, " Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, pp. 378 – 383, 1999.
[31]K. Nyberg and R. Ruppel, " Message recovery for signature scheme based on the discrete logarithm problem, " Designs, Codes and Cryptography, Vol. 7, No. 1/2, pp. 61 – 81, 1996.
[32]Paiement CB sur mobile, http://www.mercatel.info/esp-adh- accueil.html.
[33]Paybox, http://www.paybox.de.
[34]Paypal. X.com, http://www.paypal.com.
[35]T.P.Pedersen, " Distributed provers with applications to undeniable signature, " Advances in Cryptology EUROCRYPT, LNCS, Vol. 547, pp. 221-238, 1991.
[36]R. Rivest, A. Shamir and L. Adleman, " A method for obtaining digital structures and public-key cryptosystem, " Communication of ACM, Vol. 21, No. 2, pp. 120 – 126, 1978.
[37]B. Schneier, Applied Cryptography, second ed., New York: John Wiley, 1996.
[38]K.M. Sim and E. Wong, " Toward market-driven agents for electronic auction, " IEEE Transations on Systems, Man, And Cybernetics —Part A: Systems And Humans, Vol. 31, No. 6, pp. 474 – 484, 2001.
[39]T. Sandholm and Q. Huai, " Nomad: mobile agent system for an internet-based auction house, " IEEE Internet Computing, Vol. 4, No. 2, pp. 80 – 86, 2000.
[40]D.H. Shih, S.Y. Huang and D.C. Yen, " A new reverse auction agent system for m-commerce using mobile agents, " Computer Standards & Interfaces, Vol. 27, No. 4, pp. 383 – 395, 2005.
[41]M. Sandirigama, A. Shimizu and M.T. Noda, " Simple and secure coin (SAS-Coin)—a practical micropayment system, " IEICE Transactions Fundamentals, Vol. 83, No. 12, pp. 2679 – 2688, 2000.
[42]W.J. Tsaur, " Several security schemes constructed using ECC-based self-certified key cryptosystems, " Applied Mathematics and Computation, Available online 2004.
[43]Vodafone m-pay bill, http://mpay-bill.vodafone.co.uk.
[44]S. Vanstone, " Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments, " Elsevier Information Securtiy Technical Report, Vol. 2, No. 2, pp. 78 – 87, 1997.
[45]W. Vickrey, " Counterspeculation, auctions, and competitive sealed tenders, " Journal of Finance, Vol. 16, pp. 8 – 37, 1961.
[46]J. E. White, " Mobile agents make a network an open platform for third-party developers, " IEEE Computer, Vol. 27, No. 11, pp. 89 – 90, 1994.
[47]R. Weber, " Security/Electronic Commerce, " SIEMENS, 2001.
[48]Yahoo Auction, http://auctions.yahoo.com/, 2001.
[49]M. Yokoo and K. Suzuki, " Secure multi-agent dynamic programming based on homomorphic encryption and its application to

combinatorial auctions, ” In Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems, pp. 112 – 119 , 2002.
[50]X. Yi and C. K. Siew, “ Secure agent-mediated online auction framework, ” International Journal of Information Technology, Vol. 7, No. 1, pp. 1 – 13, 2001.