Integrating E-Payment into Mobile Auction Scheme based on Mobile Agents

蘇雍超、曹偉駿

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

ABSTRACT

More and more mobile consumers expect to participate in various services of m-commerce using handheld devices. Electronic auction is getting popular and also is one of important online transactions in e-commerce. In addition, many researchers have presented some schemes to resolve the security of e-auction. Under an Internet environment, using agent techniques to assist participants of an auction to bid autonomously has become common practice. However, only few mobile auction schemes can protect the security of information for mobile agent. Besides, the previously proposed auction schemes are also to rarely state subsequent payment when the auction has been finished. Therefore, in this thesis we employ efficient " ECC-based self-certified public key cryptosystems " to design an integrated mobile e-auction scheme with e-payment based on the technology of mobile agent. Besides, our proposed scheme can reduce the computational overhead of handheld devices and provide low communicational cost. As far as the security of our proposed scheme is concerned, by hiding a private key into a proxy authenticated key, this thesis improves previously proposed mobile agent based e-auction schemes that result in bidder ' s private key disclosed. Hence, this thesis can satisfy the security requirements of m-commerce environment, and overcome hardware limitations of handheld devices. In summary, our proposed integrated scheme can make the whole e-auction process not only efficient but also secure. It also makes users have much desire to join in mobile e-auction actively, and therefore stimulates a boom in m-commerce.

Keywords : mobile commerce ; mobile agent ; electronic payment ; electronic auction ; elliptic curve cryptosystems

Table of Contents

REFERENCES

[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.