網路電子拍賣機制之研究

黃正炎、陳澤雄 ; 余心淳

E-mail: 9225034@mail.dyu.edu.tw

ABSTRACT

網際網路技術發展一日千里，不但跨越了地域的限制，也造就地球村的可能，是現代通訊、商務發展、及種種生活機制上的一大利器。藉由網際網路技術的應用，本文所提出一套英式拍賣機制，將參與拍賣活動的互動三方加以連結，包括：註冊單位(Registration Manager)、拍賣商(Auction Manager)及競標者(Bidder)。其中，註冊單位主要是對競標者身分進行確認與認證，拍賣商負責核發競標者之競標資格與拍賣進行中之秩序維護。該機制包含以下安全特性：(1)匿名性(2)可追蹤性(3)不可陷害性(4)不可偽造性(5)不可否認性(6)公平性(7)可公開驗證性(8)在不同拍賣回合中無關聯性(9)同一拍賣回合中之關聯性(10)投標有效率(11)單次註冊(12)容易註銷。同時，為因應網際網路的應用環境，在所提出的方法中，由於考量競標資訊在網路傳輸中必須耗費的時間成本，因此以佈告欄的方式供註冊單位及拍賣商公佈競標資訊，取信於參與競標之競標者，並且應用橢圓曲線密碼系統，取其低運算量及短金鑰在有限硬體環境中之優越性，有助於拍賣商伺服器端運算量之簡化，進而提昇競標者在投標活動中的競價效率，使競標活動得以更有效、更便捷的方式進行。

Keywords : 橢圓曲線密碼系統 ; 英式拍賣 ; 佈告欄 ; 匿名性 ; 公開驗證性

Table of Contents

封面內頁 簽名頁 授權書1..... iii 授權書2..... iv 中文摘要..... v 英文摘要..... vi 誌謝..... vii 目錄..... viii 圖目錄..... x 表目錄..... xi 第一章 緒論..... 1 1.1 研究背景與動機..... 1 1.2 研究目的..... 3 1.3 論文架構..... 4 第二章 文獻探討..... 6 2.1 拍賣的種類..... 6 2.2 數學理論..... 8 2.2.1 單向函數及單向暗門函數..... 8 2.2.2 解離散對數問題..... 8 2.2.3 因數分解問題..... 9 2.2 密碼系統..... 9 2.3.1 公開金鑰密碼系統..... 9 2.3.2 RSA密碼系統..... 10 2.3.3 ElGamal數位簽署..... 11 2.3.4 橢圓曲線密碼系統..... 12 2.3.5 Diffie-Hellman..... 14 第三章 相關研究文獻回顧..... 16 3.1 Omote與Miyaji之英式拍賣機制..... 16 3.2 Lee、Kim與Ma之英式拍賣機制..... 21 3.3 吳、陳與張之英式拍賣機制..... 26 第四章 我們所提之英式拍賣機制..... 32 4.1 系統模型..... 32 4.2 使用指數運算之方法..... 39 4.3 使用橢圓曲線之方法..... 47 第五章 安全性分析與效能評估..... 55 5.1 安全性分析..... 55 5.2 效能分析與比較..... 63 第六章 結論與未來研究方向..... 68 6.1 結論..... 68 6.2 未來研究方向..... 69 參考文獻..... 70

REFERENCES

[1] M. Kumar and S. Feldman.,“ Internet Auctions, ” Proceedings of the Third USENIX Workshop on Electronic Commerce, pp. 49-60, 1998.

[2] T. Mullen and M. Wellman.,“ The auction manager: Market middleware for large-scale electronic commerce, ” Proceedings of the Third USENIX Workshop on Electronic Commerce, pp. 49-60, 1998.

[3] K. Nguyen and J. Traore.,“ An Online Public Auction Protocol Protecting Bidder Privacy, ” Proceedings of Australasian Conference on Information Security and Privacy 2000, pp. 427-442, 2000.

[4] 吳宗成， 陳奎聿， 林祚儀， “適用於網際網路環境之英式拍賣機制， ”第十二屆全國資訊安全會議， pp.331-337， 2002。

[5] V. S. Miller,“ Uses of Elliptic Curves in Cryptography, ” Advances in Cryptology-CRYPTO ’85, Proceedings, Lecture Notes in Compute Science, New York, NY:Springer-Verlag, No. 218, pp. 417-426, 1985.

[6] N. Koblitz,“ Elliptic Curve Cryptosystems, ” Mathematics of Computation, Vol. 48, pp. 203-209, 1987.

[7] A. J. Menezes, T. Okamoto, and S. A. Vanstone,“ Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, ” IEEE Transactions on Information Theory, Vol. 39, pp. 1639-1646, 1993.

[8] J. S. Brickell and K. S. McCurely,“ ECC: Do We Need to Count?, ” Advances in Cryptology-ASIACRYPT ’99, Lecture Notes in Computer Science, Springer-Verlag, No. 1716, pp. 122-134, 1999.

[9] K. Omoto and A. Miyaji,“ An Anonymous auction Protocol with a single non-trusted Center Using Binary Trees, ” Proceedings of

Information Security Workshop 2000, pp.108-120, 2000.
[10] K. Omote and A. Miyaji, “ A Practical English Auction with One-Time Registration, ” Proceedings of Australasian Conference on Information Security and Privacy 2001, pp. 221-234, 2001.
[11] Stuart G. Stubblebine and Paul F. Syverson, “ Fair On-line Auction Without Special Trusted Parties, ” Proceedings of Financial Cryptography ’99, pp. 230-240, 1999.
[12] K. Omote and A. Miyaji, “ A Practical English Auction with Simple Revocation, ” IEICE TRANS. Fundamentals, Vol. E85-A, No. 5, pp. 1054-1061, May 2002.
[13] N. Koblitz, A. Menezes, and S. Vanstone, “ The State of Elliptic Curve Cryptography, ” Designs, Codes and Cryptography, Vol. 19, pp. 173-193, 2000.
[14] M. Franklin and M. Reiter. , “ The Design and Implementation of a Secure Auction Service, ” IEEE Transactions on Software Engineering, Vol. 5, No. 22, pp. 302-312, 1996.
[15] K. Chida, K. Kobayashi, and H. Morita. “ Efficient Sealed-Bid Auctions for Massive Numbers of Bidders with Lump Comparison, ” Proc. ISC2001, pp. 408-419, 2001.
[16] K. Kobayashi, H. Morita, K. Suzuki, and M. Hakuta, “ Efficient Sealed-Bid Auction by Using One-Way Functions, ” IEICE Transactions Fundamentals. Vol. E84-A, No.1, pp. 289-294, Jan. 2001.
[17] M. Kudo, “ Secure Electronic Sealed-Bid Auction Protocol with Public Key Cryptography, ” IEICE Trans. Fundamentals, Vol. E81-A, No. 1, pp. 20-27, Jan. 1998.
[18] K. Omote and A. Miyaji, “ An Anonymous sealed-bid Auction with a Feature of entertainment, ” Trans. IPS Japan, Vol. 42, No. 8, pp. 2049-2056, 2001.
[19] B. Lee, K. Kim, and J. Ma, “ Efficient Public Auction with One-Time Registration and Public Verifiability, ” Proceedings of the International Conference on INDOCRYPT 2001, pp. 162-174, 2001.
[20] 梁高榮， ”農產品交易工程學， ” 五南出版社，2000。
[21] 賴松溪，韓亮與張真誠， ”近代密碼學及其應用， ” 松崗圖書資料公司，2001年10月。
[22] W. Diffie and M. E. Hellman, “ New Directions in Cryptography, ” IEEE Transaction on Information Theory, Vol. IT-22, No.6, pp. 644-654, Nov. 1976.
[23] C. P. Schnorr, “ Efficient Identification and Signature for smart Cards, ” Lecture Notes in Computer Science 435, Advances in Cryptology: Cryptology ’89, Berlin: Springer Verlag, pp. 339-351, 1990.
[24] T. ElGamal, “ A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, ” IEEE Trans. On Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.
[25] J. Camenisch and M. Stadler, “ Efficient Group Signature Schemes for Large Groups, ” In Advances in Cryptology- CRYPTO ’97, pp. 410-424, 1997.