設計植基於自我驗證公開金鑰系統之安全線上電子拍賣機制

胡國新、曹偉駿

E-mail: 9015627@mail.dyu.edu.tw

摘 要

現在大部分看到的拍賣網站都是屬於離線式 (OFF-LINE)的拍賣。但我們在一般日常生活中所見到的拍賣活動是屬於英式拍賣，亦即所有競標者於同一時間，聚集在同一地點進行競標，由出席的競標者以喊價的方式來決定得標者及得價之價格與數量。這和現行的網站拍賣機制多不相同，所以本論文以英式拍賣為主軸，建立出可以適用於這類拍賣的安全機制。現行多數拍賣網站中，如拍賣王、EBAY等，其交易安全是以SSL(SECURE SOCKET LAYER)安全機制為基礎，且其電子憑證是由公正的第三單位所簽發，也就是說僅達到GIRAULT [18]所提出的LEVEL 2安全等級 (即公正第三單位有機會偽造出一不存在的使用者)。 本論文採用自我驗證的方式來達成即使是認證中心也無法假扮使用者，再加上參與競標者對拍賣會議主持人使用假名，使主持人也無法得知何人參與拍賣。因本論文所要探討的是即時的線上拍賣問題，所以除了安全性是否周延的顧慮之外，還必須兼顧安全機制運算上的效率。而橢圓曲線公開金鑰密碼系統較現存的其它公開金鑰密碼系統運算更快速，且以較少的位元數可達到相同的安全度。因此，本論文發展出一套以橢圓曲線密碼系統為基礎的自我驗證公開金鑰系統，並據以建構出各種安全機制，應用在線上拍賣上，藉以提高線上拍賣的安全機制之效率，使即時性的安全線上拍賣成為可行的方案。

關鍵詞 : 電子商務，資訊安全，自我驗證公開金鑰系統，拍賣，橢圓曲線密碼系統

目錄

第一章　緒論 1 第一節 研究動機 1 第二節 研究背景及目的 2 第三節 論文架構 4 第二章　文獻探討 6 第一節 拍賣的種類 6 第二節 數學理論及密碼背景 9 第三節 公開金鑰密碼系統 13 第三章 具自我驗證之線上拍賣安全機制 23 第一節 線上拍賣的安全需求 24 第二節 植基於橢圓曲線密碼系統之具自我驗證公開金鑰系統 26 第三節 線上拍賣的安全機制 31 第四章 安全及計算複雜度分析 33 第一節 植基於橢圓曲線密碼系統之具自我驗證公開金鑰系統及其相關安全機制的安全度分析 33 第二節 拍賣會議的安全分析 35 第三節 安全線上拍賣之時間複雜度分析 37 第五章 結論 41

參考文獻

[1]李重君，論證券拍賣制度，東海大學企業管理研究所碩士論文，民國85年。

[2]梁高榮，農產品的電子拍賣，新世紀電子商務技術與實務學術研討會論文集，玄奘人文社會學院資 訊處／資訊管理學系，民國89年。

[3]黃博仁，植基於內插多項式之會議金鑰分配系統與多層次資料安全存取控制技術，台灣工業技術學 院管理技術研究所資訊管理學程碩士論文，民國84年。

[4]樊國楨，電子商務高階安全防護 : 公開金鑰密碼資訊系統安全原理，資策會，民國86年。

[5]盧文慧，競爭式網路拍賣協定之研究，銘傳大學資訊管理研究所碩士論文，民國88年。

[6]賴溪松，韓亮，張真誠，近代密碼學及其應用，松崗圖書資料公司，1998年8月。

[7]鍾振華，使用身分基礎之自我驗證的金鑰分配及會議金鑰分配技術，台灣科技大學管理研究所資訊 管理學程碩士論文，民國87年。

[8]BIERMAN, H.S., AND FERNANDEZ, L., GAME THEORY WITH ECONOMIC APPLICATIONS, ADDISON WESL -EY, 1993.

[9]BOTES, J.J., AND PENZHORN, W.T., "PUBLIC-KEY CRYPTOSYSTEMS BASED ON ELLIPTIC CURVES," PROCEEDINGS OF THE 1993 IEEE SOUTH AFRICAN SYMPOSIUM ON COMMUNICATIONS AND SIGNAL, OCT -OBER 1993, PP.1-5.

[10]CHANG, C.C., AND LIN, C.H., "HOW TO CONVERSE SECURELY IN A CONFERENCE," PROCEEDINGS OF 30TH ANNUAL 1996 INTERNATIONAL CARNAHAN CONFERENCE, 1996, PP.42-45.

[11]CHANG, Y.S., WU, T.C., AND HUANG, S.C., "ELGAMAL-LIKE DIGITAL SIGNATURE AND MULTISIGNA -TURE SCHEMES USING SELF-CERTIFIED PUBLIC KEYS," THE JOURNAL OF SYSTEMS AND SOFTWARE, 2000, PP.99-105.

[12]CHIKAZAWA T., AND YAMAGISHI A., " AN IMPROVED IDENTITY-BASED ONE-WAY CONFERENCE KEY SH -ARING SYSTEM," SINGAPORE ICCS/ISITA '92. 'COMMUNICATIONS ON THE MOVE', VOL. 1, 1990, PP.270-273.

[13]CHIOU, G.H., AND CHEN, W.T., " SECURE BROADCASTING USING THE SECURE LOCK," IEEE TRANSA -CTIONS ON SOFTWARE ENGINEERING, VOL. 15, NO. 8, AUGUST 1989, PP. 929-934.

[14]DIFFIE, W., AND HELLMAN, M.E., "NEW DIRECTIONS IN CRYPTOGRAPHY," IEEE TRANSACTIONS ON INFORMATION

THEORY, VOL. IT-22, NO. 6, 1976, PP. 644-654.
[15]ELGAMAL, T., "A PUBLIC-KEY CRYPTOSYSTEM AND A SIGNATURE SCHEME BASED ON DISCRETE LOGAR -ITHMS," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, 1985, PP.469-472.
[16]FRANKLIN, M.K., AND REITER, M.K., "THE DESIGN AND IMPLEMENTATION OF A SECURE AUCTION SERVICE," PROCEEDINGS OF IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 1995, PP. 2-14.
[17]FRANKLIN, M.K., AND REITER, M.K., "THE DESIGN AND IMPLEMENTATION OF A SECURE AUCTION SERVICE," IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 22, NO. 5, MAY 1996, PP. 302-312.
[18]GIRAULT, M., "SELF-CERTIFIED PUBLIC KEYS," ADVANCES IN CRYPTOLOGY: EUROCRYPT '91, PP. 490-497.
[19]HUHNS, M.N., AND VIDAL, J.M., "ONLINE AUCTIONS," IEEE INTERNET COMPUTING, VOL. 3, NO. 3, MAY-JUNE 1999, PP.103-105.
[20]HWANG, T., AND CHEN, J.L., "IDENTITY-BASED CONFERENCE KEY BROADCAST SYSTEMS," IEE PROC -EEDINGS-COMPUTERS AND DIGITAL TECHNIQUES, VO.141, NO. 1, JANUARY 1994, PP.57-60.
[21]INGEMARSSON, I., TANG, D.T., AND WONG, C.K., "A CONFERENCE KEY DISTRIBUTION SYSTEM," IEEE TRANSACTIONS ON INFORMATION THEORY, IT-28, 1982, PP. 714-720.
[22]JURISIC, A., AND MENEZES, A.J., "ELLIPTIC CURVES AND CRYPTOGRAPHY," DR. DOBB'S JOURNAL ,1997, PP. 26-35.
[23]KNUTH, D.E., THE ART OF COMPUTER PROGRAMMING, VOLUME 2, SEMINUMERICAL ALGORITHMS, ADDI -SON-WESLEY, 1981.
[24]KOBLITZ, N., "CONSTRUCTING ELLIPTIC CURVE CRYPTOSYSTEMS IN CHARACTERISTIC 2," ADVANCE IN CRYPTOLOGY: CRYPTO'90, PP. 156-167.
[25]KOBLITZ, N., "ELLIPTIC CURVE CRYPTOSYSTEMS," MATHEMATICS OF COMPUTATION, VOL. 48, NO. 17, 1987, PP. 203-209.
[26]KOYAMA, K., AND OHTA, K., "IDENTITY-BASED CONFERENCE KEY DISTRIBUTION SYSTEMS," ADVANC -ES IN CRYPTOLOGY: CRYPTO' 87, PP. 175-184.
[27]KOYAMA, K., AND OHTA, K., "SECURITY OF IMPROVE IDENTITY-BASED CONFERENCE KEY DISTRIBUT -ION SYSTEMS," ADVANCES IN CRYPTOLOGY: EUROCRYPT'88, PP.11-19.
[28]LAIH, C.S., AND YEN S.M., "ON THE DESIGN OF CONFERENCE KEY DISTRIBUTION SYSTEMS FOR THE BROADCASTING NETWORKS," PROCEEDINGS OF TWELFTH ANNUAL JOINT CONFERENCE OF IEEE COMPUT -ER AND COMMUNICATION SOCIETIES, VOL. 3, 1993, PP. 1406-1413.
[29]LU, E.H., HWANG, W.Y., AND LEE, J.Y., "A CONFERENCE KEY DISTRIBUTION SYSTEM BASED ON T -HE LAGRANGE INTERPOLATING POLYNOMIAL," PROCEEDINGS OF SEVENTH ANNUAL JOINT CONFERENCE OF IEEE COMPUTER AND COMMUNICATIONS SOCIETIES, 1988, PP. 1092-1094.
[30]MENEZES, A.J., AND VANSTONE, S.A., "ELLIPTIC CURVES CRYPTOSYSTEMS AND THEIR IMPLEMENTA -TION," JOURNAL OF CRYPTOLOGY, VOL. 6, NO. 4, 1993, PP. 209-224.
[31]MILLER, V.S., "USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY," ADVANCES IN CRYPTOLOGY: CRYPTO '85, PP.417-426.
[32]PETERSEN, H., AND HORSTER, P., "SELF-CERTIFIED KEYS - CONCEPTS AND APPLICATIONS", PRO -CEEDINGS OF COMMUNICATIONS AND MULTIMEDIA SECURITY'97, 1997, PP.102-116.
[33]RIVEST, R., SHAMIR, A., AND ADLEMAN, L.," A METHOD FOR OBTAINING DIGITAL SIGNATURES AN -D PUBLIC-KEY CRYPTOSYSTEMS," COMMUNICATIONS OF THE ACM, VOL. 21, NO. 2, 1978, PP. 120 -126.
[34]ROBINSON, D.J.S., A COURSE IN LINEAR AIGEBRA WITH APPLICATION, WORLD SCIENTIFIC, NEW JERSEY, 1991.
[35]SAEEDNIA, S., "IDENTITY-BASED AND SELF-CERTIFIED KEY-EXCHANGE PROTOCOLS," INFORMATION SECURITY AND PRIVACY: ACISP '97, PP. 303-313.
[36]SCHNORR, C.P., "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS," ADVANCES IN CRYPTOLOGY: CRYPTO'89, PP.339-351.
[37]SHAMIR, A., "IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES," ADVANCES IN CRYPTOLO -GY: CRYPTO '84, PP.47-53.
[38]SHERIF, M.H., SERHROUCHNI, A., GAID, A.Y., AND FARAZMANDNIA, F., "SET AND SSL: ELECTRO -NIC PAYMENTS ON THE INTERNET," PROCEEDINGS OF THIRD IEEE SYMPOSIUM ON COMPUTER AND CO -MMUNICATION, 1998, PP.353-358.
[39]SLIVERMAN, J., THE ARITHMETIC OF ELLIPTIC CURVES, SPRINGER-VERLAG, NEW YORK, 1986.
[40]VICKREY, W., "COUNTERSPECULATION, AUCTIONS, AND COMPETITIVE SEALED TENDERS," JOURNAL OF FINANCE, VOL. 16, MARCH 1961, PP. 8-37.
[41]WU, T.C., "CONFERENCE KEY DISTRIBUTION SYSTEM WITH USE ANONYMITY BASED ON ALGEBRAIC AP -PROACH," IEE PROCEEDINGS- COMPUTERS AND DIGITAL TECHNIQUES, VOL. 144, NO. 2, MARCH 19 97, PP. 145-148.
[42]WU, T.C., CHANG, Y.S., AND LIN, T.Y., "IMPROVEMENT OF SAEEDNIA'S SELF-CERTIFIED KEY EX -CHANGE

PROTOCOLS" ELECTRONICS LETTERS, VOL. 34, NO. 11, 28 MAY 1998, PP. 1094-1095.
[43]YANG, H.K., CHOI, J.H., AND ANN, Y.H., "SELF-CERTIFIED IDENTITY INFORMATION USING THE MINIMUM KNOWLEDGE," IEEE TENCON., 1996, VOL. 2, PP. 641-647.
[44]HTTP://WWW2.BID.COM.TW/SAFE1.ASP~SAFE3.ASP [45]HTTP://WWW.P2P.COM.TW/SECURITY.HTML
[46]HTTP://WWW1.COOLBID.COM/VERISIGN.HTML [47]HTTP://WWW.HITRUST.COM.TW/128位元新聞稿.DOC
[48]HTTP://WWW.EBAY.COM [49]HTTP://WWW.ONLINEAUTHENTICS.COM/OA/DEFAULT.ASP?SID=1