行動電子商務環境下安全協定之研究

陳宗保、曹偉駿

E-mail: 9020048@mail.dyu.edu.tw

摘 要

目前有線電子商務的安全機制，均使用以憑證為基礎的公開金鑰密碼系統來解決相關的安全需求。然而，行動電子商務之無線的環境與前述有線的環境有顯著的差異性存在，如：較小的頻寬、傳輸時有較大延遲的現象、連線品質不佳比較容易斷線、無線的個人裝置運算能力與電力較低等諸多限制存在。因此，需要較多運算量的憑證基礎公開金鑰密碼系統並不適用於無線的環境，相當有必要對無線電子商務環境設計一個合適的安全基礎機制，我們稱之為無線公開金鑰安全基礎(Wireless Public Key Infrastructure)，以保障交易雙方的安全性。本論文將以較具效率之橢圓曲線密碼系統為基礎，設計出一個基於身分為考量的自我驗證公開金鑰密碼系統，並配合無線應用協定(Wireless Application Protocol；WAP)的相關標準，來打造出一個適合行動電子商務的安全基礎環境。本論文所提出之方法具有下列優點： (1) 相較於憑證基礎的方法，本方法驗證公鑰時，可免除額外的時間來對憑證作驗證簽章的動作； (2) 單一個邏輯步驟中同時完成簽章與加密的動作； (3) 分配交談金鑰及驗證公鑰的有效性可同時達成； (4) 驗證訊息簽章及驗證公鑰的有效性可同時達成； (5) 執行加解密及驗證公鑰的有效性可同時達成； (6) 因為本論文有結合身分為基礎的公開金鑰密碼系統，故可減少運算成本。 總之，基於上述優點，所使用的金鑰大小可以降低、可減少運算的複雜度及降低傳輸成本，故非常適合運用在具較小的記憶體與運算能力的裝置上，如智慧卡、手機與個人數位助理(PDA)等。此外，橢圓曲線密碼系統160位元金鑰長度的安全性，同等於RSA公開金鑰密碼系統的1024位元金鑰長度，而且本論文所使用的方法中，由於沒有金鑰目錄管理的問題，因此系統維護管理的成本也大大地降低。

關鍵詞 : 橢圓曲線密碼系統、無線公開金鑰安全基礎、自我驗證公開金鑰密碼系統、無線應用協定、橢圓曲線離散對數問題、鑑別加密法、行動電子商務

目錄

參考文獻

[1]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，民國88年8月。

[2]高銘智，「使用在WAP協定中的橢圓曲線密碼系統」，電腦與通訊 第85期，第45-48頁，民國88年 12月。

[3]鍾振華，「使用身分基礎之自我驗證公鑰的金鑰分配及會議金鑰分配技術」，台灣科技大學 資訊管理系碩士班碩士論文，民國88年。(指導教授:吳宗成) [4]胡國新，「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」，大葉大學 資訊管理 研究所碩士論文，民國89年。(指導教授:曹偉駿) [5]張瑗玲，「捍衛網際網路的商機」，松崗圖書資料公司，民國86年4月。

[6]余千智，「電子商務總論」，智勝出版社，民國88年4月。

[7]李澄興、林祺政，「電子商務概要」，美商麥格羅．希爾，民國89年10月。

[8]何淑君， "THE DEVELOPMENT OF MOBILE INTERNET TECHNOLOGY," 樹德科技大學-校園無線電子 商務研討會 論文集，第203-210頁，民國88年11月。

[9]林祝興、李正隆，"ELLIPTIC-CURVE UNDENIABLE SIGNATURE SCHEMES," 第11屆全國資訊安全會議，第331-338頁，民國90年5月。

[10]R. BAKALOV, "INTRODUCTION TO WAP'S WIRELESS TRANSPORT LAYER SECURITY," INFORMATION SECURTIY TECHNICAL REPORT, VOL. 5, NO. 3, ELSEVIER, 2000, PP. 15-22.

[11]E. BLHAM, AND A. SHAMIR, "DIFFERENTIAL CRYPTANALYSIS OF THE DATA ENCRYPTION STANDARD ," SPRINGER VERLAG, BERLIN, 1993.

[12]M. BORCHERDING, "MOBILE SECURITY - AN OVERVIEW OF GSM, SAT AND WAP," R. BAUMGART(ED.): CQRE'99, LNCS 1740, SPRINGER-VERLAG, 1999, PP. 133-141.
[13]W. CAELLI, E. DAWSON, AND S. REA, "PKI, ELLIPTIC CURVE CRYPTOGRAPHY AND DIGITAL SIGN -ATURES," COMPUTER & SECURITY, VOL. 18, NO. 1, 1999, PP. 47-66.
[14]CCITT RECOMMENDATION X.509, "THE DIRECTORY: AUTHENTICATION FRAMEWORK," JAN 1997.
[15]CERTICOM CORP., "SEC 1: ELLIPTIC CURVE CRYPTOGRAPHY," STANDARDS FOR EFFICIENT CRYPTO -GRAPHY GROUP, SEPTEMBER 2000. (URL: HTTP://WWW.SECG.ORG/).
[16]Y.S. CHANG, T.C. WU, AND S.C. HUANG, "ELGAMAL-LIKE DIGITAL SIGNATURE AND MULTISIGNAT -URE SCHEMES USING SELF-CERTIFIED PUBLIC KEYS," THE JOURNAL OF SYSTEM AND SOFTWARE, 2000, PP. 99-105.
[17]W. DIFFIE, AND M.E. HELLMAN, "NEW DIRECTIONS IN CRYPTOGRAPHY," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, 1976, PP. 644-654.
[18]T. DIERKS, C. ALLEN, "THE TLS PROTOCOL VERSION 1.0," IETF RFC 2246, JANUARY 1998. (URL: FTP://FTP.ISI.EDU/IN-NOTES/RFC2246.TXT) [19]DURLACHER RESEARCH, "MOBILE COMMERCE REPORT," 2000. (URL: HTTP://WWW.DURLACHER.COM/).
[20]T. ELGAMAL, "A PUBLIC KEY CRYPTOSYSTEM AND A SIGNATURE SCHEME BASED ON DISCRETE LOGA RITHMS," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, 1985, PP. 469-472.
[21]ETSI WEB SITE, (URL: HTTP://WWW.ETSI.ORG/).
[22]S. FARRELL, "THE WAP FORUM'S WIRELESS PUBLIC KEY INFRASTRUCTURE," INFORMATION SECUR -TIY TECHNICAL REPORT, VOL. 5, NO. 3, ELSEVIER, 2000, PP. 23-31.
[23]A. FRIER, P. KARLTON AND P. KOCHER, "THE SSL 3.0 PROTOCOL," (URL: HTTP://HOME.NETSCA -PE.COM/ENG/SSL3/DRAFT302.TXT), 18 NOVEMBER 1996, NETSCAPE COMMUNICATIONS CORP.
[24]M. GIRAULT, "SELF-CERTIFIED PUBLIC KEYS," ADVANCES IN CRYPTOLOGY: EUROCRYPT'91, LECT -URE NOTES IN COMPUTER SCIENCE, VOL. 547, SPRINGER-VERLAG, 1991, PP. 491-497.
[25]C. GUNTHER, "AN IDENTITY-BASED KEY-EXCHANGE PROTOCOL," ADVANCES IN CRYPTOLOGY EUROCR -YPT'91, LECTURE NOTES IN COMPUTER SCIENCE, VOL. 547, SPRINGER-VERLAG, 1991, PP.29-37.
[26]GSM WEB SITE, (URL: HTTP://WWW.GSM.ORG/).
[27]M. HOOGENBOOM AND P. STEEMERS, "SECURITY FOR REMOTE ACCESS AND MOBILE APPLICATION," COMPUTER & SECURITY, VOL. 19, NO. 2, 2000, PP. 149-163.
[28]P. HORSTER, M. MICHELS AND H. PETERSEN, "AUTHENTICATED ENCRYPTION SCHEMES WITH LOW COMMUNICATION COSTS," ELECTRONICS LETTERS, VOL.30, NO.15, 1994, PP. 1212-1213.
[29]IEEE P1363 WORKING GROUP, "IEEE P1363 STANDARD SPECIFICATIONS FOR PUBLIC KEY CRYPTO -GRAPHY," (URL:HTTP://GROUPER.IEEE.ORG/GROUPS/1363/).
[30]A. JURISIC, AND A.J. MENEZES, "ELLIPTIC CURVES AND CRYPTOGRAPHY," DR. DOBB'S JOURNAL, 1997, PP. 26-35.
[31]A. JURISIC, AND A.J. MENEZES, "ECC WHITEPAPERS: ELLIPTIC CURVES AND CRYPTOGRAPHY," CERTICOM CORP., (URL: HTTP://WWW.CERTICOM.COM/RESEARCH/WECCRYPT.HTML).
[32]B.S. KALISKI, "AN OVERVIEW OF THE PKCS STANDARDS," RSA LABORATORIES, NOV. 1993.
[33]S. KIM, S. OH, S. PARK, AND D. WON, "ON SAEEDNIA'S KEY-EXCHANGE PROTOCOLS," KICS (KO -REAN INSTITUTE OF COMMUNICATION SCIENCES) CONFERENCE, VOL. 17, NO. 2, KOREA, 1998, PP.1001-1004.
[34]N. KOBLITZ, "ELLIPTIC CURVE CRYPTOSYSTEMS," MATHEMATICS OF COMPUTATION, VOL. 48, NO. 17, 1987, PP. 203-209.
[35]X. LAI, AND J. MASSEY, "A PROPOSAL FOR A NEW BLOCK ENCRYPTION STANDARD," ADVANCES IN CRYPTOLOGY EUROCRYPT'90, SPRINGER-VERLAG, 1991, PP. 389-404.
[36]W.B. LEE AND C.C. CHANG, "AUTHENTICATED ENCRYPTION SCHEME WITHOUT USING A ONE WAY FUN -CTION," ELECTRONICS LETTERS, VOL.31, NO.19, 1995, PP. 1656-1657.
[37]A.J. MENEZES AND S.A. VANSTONE, "ELLIPTIC CURVE CRYPTOSYSTEM AND THEIR IMPLEMENTATION, " JOURNAL OF CRYPTOLOGY, VOL. 6, NO. 4, 1993, PP. 209-224.
[38]V.S. MILLER., "USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY," ADVANCES IN CRYPTOLOGY:CRYPTO '85, SPRINGER-VERLAG,1986, PP. 417-426.
[39]MASTERCARD AND VISA, "SECURE ELECTRONIC TRANSACTION (SET) SPECIFICATION," JUNE 1996.
[40]NATIONAL BUREAU OF STANDARDS, "DATA ENCRYPTION STANDARD," FEDERAL INFORMATION PROCES -SING STANDARDS PUBLICATION FIPS PUB 46 U.S. DEPARTMENT OF COMMERCE, 1977.
[41]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST FIPS PUB 180, "SECURE HASH STAN -DARD," U.S. DEPARTMENT OF COMMERCE, 1993.

[42]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST FIPS PUB 186, "DIGITAL SIGNATURE STANDARD," U.S. DEPARTMENT OF COMMERCE, 1994.
[43]H. PETERSEN, AND P. HORSTER, "SELF-CERTIFIED KEYS CONCEPTS AND APPLICATIONS," PROCEED -INGS OF COMMUNICATIONS AND MULTIMEDIA SECURITY'97, 1997, PP. 102-116.
[44]R. RIVEST, A. SHAMIR, AND L. ADLEMAN, "A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS," COMMUNICATIONS OF THE ACM, VOL. 21, NO. 2, 1978, PP. 120- 126.
[45]R. RIVEST, "THE MD5 MESSAGE DIGEST ALGORITHM," RFC 1321, 1992.
[46]S. SAEEDNIA, "IDENTITY-BASED AND SELF-CERTIFIED KEY-EXCHANGE PROTOCOLS," INFORMATION SECURITY AND PRIVACY: ACISP'97, 1997, PP. 303-313.
[47]C.P. SCHNORR, "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS," ADVANCES IN CRYPTOLOGY: CRYPTO'89, SPRINGER-VERLAG, 1990, PP.339-351.
[48]R.M. SCHNORR, "THE DATA ENCRYPTION STANDARD IN PERSPECTIVE," COMPUTER SECURITY AND THE DATA ENCRYPTION STANDARD, NATIONAL BUREAU OF STANDARDS, FEB 1978.
[49]A. SHAMIR, "IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES," ADVANCES IN CRYPTOLO GY: CRYPTO'84, SPRINGER-VERLAG, 1985, PP. 47-53.
[50]S. VANSTONE, "ELLIPTIC CURVE CRYPTOSYSTEM - THE ANSWER TO STRONG, FAST PUBLIC-KEY CR -YPTOGRAPHY FOR SECURING CONSTRAINED ENVIRONMENTS," INFORMATION SECURITY TECHNICAL REPORT, VOL. 2, NO. 2, ELSEVIER, 1997, PP. 78-87.
[51]T.C. WU, Y.S. CHANG AND T.Y. LIN, "IMPROVEMENT OF SAEEDNIA'S SELF-CERTIFIED KEY EXC -HANGE PROTOCOLS," IEE ELECTRONIC LETTERS,VOL 34, NO 11, MAY 1998, PP. 1094-1095.
[52]T.C. WU, "DIGITAL SIGNATURE/MULTISIGNATURE SCHEMES GIVING PUBLIC KEY VERIFICATION AND MESSAGE RECOVERY SIMULTANEOUSLY," TO APPEAR IN COMPUTER SYSTEMS SCIENCE AND ENGINEE -RING, 2001.
[53]WAP FORUM, (URL: HTTP://WWW.WAPFORUM.ORG/).
[54]WAP FORUM, "WAP ARCHITETURE SPECIFICATION," 30 APRIL 1998, (URL: HTTP://WWW.WAPFORUM. ORG/).
[55]WAP FORUM, "WIRELESS TRANSPORT LAYER SECURITY SPECIFICATION," 18 FEBRUARY 2000, (URL: HTTP://WWW.WAPFORUM.ORG/).