植基於橢圓曲線密碼系統的數之研究

劉作屏、陳澤雄

E-mail: 9127189@mail.dyu.edu.tw

摘 要

本篇論文研究的主題包含有數位簽章及代理簽章兩個部分。其中有關數位簽章的部分，目前的數位簽 章機制都是建立在公開金鑰密碼系統上，也就是說每位簽章者都只能擁有一把密鑰及一把公鑰。從安全 性來看，這樣的機制是不夠安全的，因為這把密鑰一但被攻擊者破解出來，其後果是不堪設想的。因此 ，我們提出了一種新的機制，使得每位簽章者可以同時用兩把密鑰及一把公鑰來做數位簽章的動作。此 時的攻擊者除非能同時破解出這兩把密鑰，否則只有破解出其中一把密鑰時，而本機制仍然是安全的。 這樣的機制，可以應用到數位簽章的機制上，以提高其安全性。 至於代理簽章的部分，在許多已提出的代理簽章機制中，原始簽章者與代理簽章者之間通常需要一個安 全的管道來傳遞授權參數，以達到授權代理的目的。為了必免安全管道的需求，學者 ZHANG 提出了一 個採用交談式的代理簽章機制。所謂交談式是指原始簽章者與代理簽章者之間有一些參數的往返，這樣 的授權方式明顯較浪費頻寬且沒有效率。因此，我們提出了一種有別於ZHANG且不需安全管道就能達到 授權代理目的之代理簽章機制。 此外，本研究還採用了橢圓曲線密碼系統作為數位簽章機制的架構，橢圓曲線密碼系統的相關研究近 年來相當為人矚目。從安全性及有效性來看，這種密碼系統有著重要的應用前景，是一種可能在近期內 某些方面取代RSA或DSS等現存的密碼系統，現已逐漸形成了研究的重點。這種密碼系統的誘人之處在於 安全性相同的前提下，可使用較短的密鑰金鑰，一般認為，在Q位元域上的橢圓曲線密碼系統，當Q的長 度為160位元時，其安全性卻相當於RSA使用1024位元模數，密鑰金鑰較短意味著所需要電腦網路的頻寬 和記憶體較小，這在電腦網路應用中有時候是個決定性的關鍵。 因此藉由橢圓曲線密碼系統短金匙特性的應用，本研究提出新的數位簽章系統，用以提昇安全機制的 效能。

關鍵詞 : 數位簽章、代理簽章、資訊安全、密碼學、橢圓曲線密碼系統

目錄

參考文獻

[1]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, 1985, PP. 417-426.
[2]N. KOBLITZ, ELLIPTIC CURVE CRYPTOSYSTEMS, "MATHEMATICS OF COMPUTATION," VOL. 48, 1987, PP. 203-209.
[3]N. KOBLITZ, "A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY," NEW YORK,NY: SPRINGER-VERLAG, SECOND EDITION, 1994.

[4]IEEE P1363: STANDARD SPECIFICATIONS FOR PUBLIC KEY CRYPTOGRAPHY, HTTP://GROUPER.IEEE.O -RG/GROUPS/1363/.
[5]R. SCHOOF, ELLIPTIC CURVE OVER FINITE FIELDS AND THE COMPUTATION OF SQUARE ROOTS MOD P, "MATHEMATIC OF COMPUTATION," VOL. 44, 1985, PP. 483-494.
[6]R. LERCIER, AND F. MORAIN, COUNTING THE NUMBER OF POINTS ON ELLIPTIC CURVES OVER FINIT -E FIELDS: STRATEGY AND PERFORMANCES, "ANN. SCI. ECOLE NORM. SUP.," VOL. 2, 1969, PP. 521-560.
[7]E. WATERHOUSE, ABELIAN VARIETIES OVER FINITE FIELDS, "MATHEMATIC OF COMPUTATION," VOL. 44, 1985, PP. 483-494.
[8]J. S. BRICKELL, AND K. S. MCCURELY, ECC: DO WE NEED TO COUNT?, "ADVANCES IN CRYPTOLOGY -ASIACRYPT'99, LECTURE NOTES IN COMPUTE SCIENCE, SPRINGER-VERLAG," NO. 1716, 1999, PP. 122-134.
[9]A. J. MENEZES, P. C. VAN OORSCHOT, AND S. A. VANSTONE, "HANDBOOK OF APPLIED CRYPTOGRAP -HY", CRC PRESS, BOCA RATON, FLORIDA, 1997.
[10]S. POHLIG, AND M. HELLMAN, AN IMPROVED ALGORITHM FOR COMPUTING LOGARITHMS OVER GF(P) A -ND ITS CRYPTOGRAPHIC SIGNIFICANCE, "IEEE TRANSACTIONS ON INFORMATION THEORY," VOL. 24 ,1978, PP. 106-110.
[11]A. J. MENEZES, T. OKAMOTO, AND S. A. VANSTONE, REDUCING ELLIPTIC CURVE LOGARITHMS TO L -OGARITHMS IN A FINITE FIELD, "IEEE TRANSACTIONS ON INFORMATION THEORY," VOL. 39,1993, PP. 1639-1646.
[12]C. P. PFLEEGER, "SECURITY IN COMPUTING," PRENTICE HALL, 1989, PP. 132-136.
[13]R. L. RIVEST, A. SHAMIR, AND L. ADELMAN, A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEM, "COMMUNICATION OF ACM," VOL. 21, NO. 2, 1978, PP. 120-126.
[14]T. ELGAMAL, A PUBLIC-KEY CRYPTOSYSTEM AND SIGNATURE SCHEME BASED ON DISCRETE LOGARITHM -S, "IEEE TRANSACTIONS ON INFORMATION THEORY," VOL. IT-31, 1985, PP. 469-472.
[15]PROPOSED FEDERAL INFORMATION PROCESSING STANDARD FOR DIGITAL SIGNATURE STANDARD (DSS), "IN FEDERAL REGISTER," VOL. 56, NO. 169, 30 AUG. 1991, PP. 42980-42982.
[16]SET SPECIFICATION, HTTP://WWW.VISA.COM/CGI-BIN/VEE/HT/ECOMM/ SET/DOWNLOADS.HTML SPECS.
[17]THE SECURE SOCKETS LAYER PROTOCOL, HTTP://WWW.NETSCAPE.COM/ INFO/SECURITY-DOC.HTML.
[18]CERTICOM CORPORATION, HTTP://WWW.CERTICOM.COM.
[19]S. M. YEN, C. S. LAIH, AND A. K. LENTRA, MULTI-EXPONENTIATION, "IEE PROCEEDINGS,COMPUT -ERS AND DIGITAL TECHNIQUES," VOL. 141, NO. 6, NOV. 1994, PP. 325-326.
[20]K. S. MCCURLEY, AN OPEN COMMENT LETTER FROM THE SANDIA NATIONAL LABORATORIES ON THE DS -A OF THE NIST," 7 NOV. 1991.
[21]S. GOLDWASSER, S. MICALI AND C. RACKOFF, THE KNOWLEDGE COMPLEXITY OF INTERACTIVE PROOF -S, "SIAM J. COMPUTER," VOL. 18, NO. 1, 1989, PP. 186-208.
[22]C. POPESCU, AN IDENTIFICATION SCHEME BASED ON THE ELLIPTIC CURVE DISCRETE LOGARITHM PR -OBLEM, "HIGH PERFORMANCE COMPUTING IN THE ASIA-PACIFIC REGION, 2000, PROCEEDINGS, THE FOURTH INTERNATIONAL CONFERENCE/EXHIBITION," VOL. 2, 2000, PP. 624-625.
[23]T. BETH, EFFICIENT ZERO-KNOWLEDGE IDENTIFICATION SCHEME FOR SMART CARDS, "PROCEEDINGS OF EUROCRYPT'88, LECTURE NOTES IN COMPUTE SCIENCE, SPRINGER-VERLAG," NO. 330, 1988,PP. 77-86.
[24]U. FEIGE, A. FIAT, AND A. SHAMIR, ZERO KNOWLEDGE PROOFS OF IDENTITY, "PROCEEDINGS OF S -TOC," 1987, PP. 210-217.
[25]A. FIAT, AND A. SHAMIR, HOW TO PROVE YOURSELF: PRACTICAL SOLUTIONS TO IDENTIFICATION A -ND SIGNATURE PROBLEMS, "PROCEEDINGS OF CRYPTO'86, LECTURE NOTES IN COMPUTE SCIENCE, S -PRINGER-VERLAG," NO. 263, 1987, PP. 186-194.
[26]K. OHTA, AND T. OKAMOTO, A MODIFICATION OF THE FIAT-SHAMIR SCHEME, "PROCEEDINGS OF CRY -PTO'88, LECTURE NOTES IN COMPUTE SCIENCE, SPRINGER-VERLAG," NO. 403, 1990, PP.232-243.
[27]T. OKAMOTO, PRACTICAL IDENTIFICATION SCHEMES AS SECURE THE DL AND RSA PROBLEMS, "SUBMI -TTED TO IEEE P1363: IDENTIFICATION SCHEMES, MARCH 1999. HTTP://GROUPER.IEEE.ORG/GROUP S/1363/ STUDYGROUP/IDENTIFICATION.HTML.
[28]D. NYANG, AND J. SONG, KNOWLEDGE-PROOF BASED VERSATILE SMART CARD VERIFICATION PROTOCO -L, "COMPUTER COMMUNICATION REVIEW, ACM SIGCOMM," VOL. 30, JULY 2000.
[29]D. JOHNSON, A. MENEZES, AND S. VANSTONE, THE ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITH -M (ECDSA), HTTP://WWW. CERTICOM.COM/PDFS/WHITEPAPERS.
[30]C. LIN, AND C. LEE, ELLIPTIC-CURVE UNDENIABLE SIGNATURE SCHEMES, "PROCEEDINGS OF THE E -LEVENTH NATIONAL CONFERENCE ON INFORMATION SECURITY," 2001, PP. 331-338.

[31]A. JURISIC AND A. J. MENEZES, ELLIPTIC CURVES AND CRYPTOGRAPHY, HTTP://WWW.CERTICOM.CO -M [32]M. MAMBO, K. USUDA, AND E. OKAMOTO, PROXY SIGNATURES FOR DELEGATING SIGNING OPERATION, "PROCEEDING 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY," ACM PRESS, 19 -96, PP. 48-57.
[33]M. MAMBO, K. USUDA, AND E. OKAMOTO, PROXY SIGNATURES: DELEGATION OF THE POWER TO SIGN MESSAGES, "IEICE TRANSACTIONS FUNDAMENTALS," VOL. E79-A, NO. 9, SEP. 1996, PP. 1338-13 54.
[34]M. BLAZE, G. BLEUMER, AND M. STRAUSS, DIVERTIBLE PROTOCOLS AND ATOMIC PROXY CRYPTOGRAP -HY, "ADVANCES IN CRYPTOLOGY- EUROCRYPT'98, LECTURE NOTES IN COMPUTER SCIENCE, SPRINGE R-VERLAG," NO. 1403, 1998, PP. 127-144.
[35]S. KIM, S. PARK, AND D. WON, PROXY SIGNATURES, REVISITED, "ICICS'97, LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER- VERLAG," NO. 1334, 1997, PP. 223-232.
[36]L. YI, G. BAI, AND G. XIAO, PROXY MULTI-SIGNATURE SCHEME: A NEW TYPE OF PROXY SIGNATUR -E SCHEME, "ELECTRONICS LETTERS," VOL. 36, NO. 6, 2000, PP. 527-528.
[37]H. M. SUN, IMPROVED PROXY SIGNATURE SCHEMES, "PROCEEDINGS OF THE INTERNATIONAL COMPUTE -R SYMPOSIUM," 2000.
[38]H. M. SUN, ON PROXY MULTI-SIGNATURE SCHEMES, "PROCEEDINGS OF THE INTERNATIONAL COMPUTE -R SYMPOSIUM," 2000, PP. 65-72.
[39]L. HARN. GROUP-ORIENTED (T, N) THRESHOLD SIGNATURE AND MULTI SIGNATURE, "IEE PROCEEDIN -GS COMPUTERS AND DIGITAL TECHNIQUES," VOL. 141, NO. 5, SEP. 1994, PP. 307-313.
[40]L. HARN. ELLIPTIC-CURVE DIGITAL SIGNATURES AND ACCESSORIES, "ELECTRONICS LETTERS,"VOL. 35, NO. 4, FEB. 1999.
[41]L. HARN. BATCH VERIFYING MULTIPLE DSA-TYPE DIGITAL SIGNATURES, "ELECTRONICS LETTERS," VOL. 34, NO. 9, APRIL 1998, PP. 870-871.
[42]IEEE P1363/D4: STANDARD SPECIFICATIONS FOR PUBLIC KEY CRYPTOGRAPHY, "THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC." 16 JUNE, 1998.
[43]A CERTICOM WHITEPAPER, THE ELLIPTIC CURVE CRYPTOSYSTEM, JULY 2000, HTTP://WWW.CERTICOM .COM.
[44]H. M. SUN, AN EFFICIENT NONREPUDIABLE THRESHOLD PROXY SIGNATURE SCHEME WITH KNOWN SIGN -ERS, "COMPUTER COMMUNICATIONS," VOL. 22, 1999, PP. 717-722.
[45]C. L. HSU, T. S. WU, AND T. C. WU, NEW NONREPUDIABLE THRESHOLD PROXY SIGNATURE SCHEME WITH KNOWN SIGNERS, "THE JOURNAL OF SYSTEMS AND SOFTWARE," VOL. 58, 2001, PP. 119-124.
[46]K. ZHANG, THRESHOLD PROXY SIGNATURE SCHEMES, "1997 INFORMATION SECURITY WORKSHOP, JAPA N," SEP. 1997, PP. 191-197.
[47]N. Y. LEE, T. HWANG, AND C. H. WANG, ON ZHANG'S NONREPUDIABLE PROXY SIGNATURE SCHEMES, "ACISP'98, LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER-VERLAG," VOL.1438,1998, PP.415 -422.
[48]WILLIAM STALLINGS, "CRYPTOGRAPHY AND NETWORK SECURITY," SECOND EDITION, PUBLISHER BY ALAN APT.
[49]賴溪松、韓亮、張真誠, "近代密碼學及其應用," 松崗圖書, SEP. 1995.
[50]G. W. LO, AND C. S. LAIH, "THE STUDY AND IMPLEMENTATION ON ELLIPTIC CURVE DIGITAL SIGN -ATURE SCHEMES," JUNE 2000.
[51]C. H. SHI, AND S. J. HWANG, "PROXY SIGNATURE SCHEMES FOR INDIVIDUAL AND GROUP-ORIENTED PROXY SIGNERS," MAY 2000.