A STUDY OF DIGITAL SIGNATURE BASED ON ELLIPTIC CURVE CRYPTOSYSTEM

劉作屏、陳澤雄

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

ABSTRACT

THE FOCUSES OF THE RESEARCH CONTAIN TWO PARTS: ONE IS THE DIGITAL SIGNATURE, AND THE OTH -ER IS THE PROXY DIGITAL SIGNATURE. FOR THE PART OF DIGITAL SIGNATURE, THE CURRENT RELATE -D SCHEMES ARE ESTABLISHED UNDER THE PUBLIC-KEY CRYPTOSYSTEM, IN WHICH EACH SIGNER IS PROV -IDED WITH A SECRET KEY AND A PUBLIC KEY. FROM THE VIEW OF SECURITY, SUCH A KIND OF CONST -RUCT FOR A SCHEME IS INSUFFICIENT FOR THE WEAK PROTECTION OF THE SECRET KEY. THEREFORE, A NEW SCHEME IS PROPOSED TO PROVIDE EACH SIGNER WITH TWO SECRET KEYS AND ONE PUBLIC KEY FOR THE OPERATION OF DIGITAL SIGNATURE. UNLESS AN ATTACKER CAN FORCE TO DERIVE THESE TWO SECR -ET KEYS AT THE SAME TIME, HE DISABLES TO INVADE THE CRYPTOSYSTEM ONLY BY ONE SECRET KEY S -O THE SECURITY OF THE SCHEME STILL CAN BE GUARANTEED. THE PROPOSED SCHEME CAN BE APPLIED TO THE PRESENT RELATED SCHEMES FOR THE DIGITAL SIGNATURE AND SUCCEEDS IN THE PROMOTION OF BOTH SECURITY AND EFFICIENCY IN PERFORMANCE. AS TO THE PART OF PROXY DIGITAL SIGNATURE, A SECURE MANNER IS REQUIRED FOR THE COMMUNICATI -ON BETWEEN THE ORIGINAL AND THE PROXY SIGNERS TO DELIVER THE DELEGATION PARAMETERS FOR THE PURPOSE OF DELEGATION PROXY IN THE PREVIOUS PROXY DIGITAL SIGNATURE SCHEMES.AIM AT THE AVO -IDANCE OF THE SECURE MANNER, AN INTERACTIVE COMMUNICATION OF PROXY DIGITAL SIGNATURE SCHE -ME IS PROPOSED BY ZHANG.THE SO-CALLED INTERACTIVE COMMUNICATION MEANS THE TO AND FRO EXCH -ANGE OF THE PARAMETERS BETWEEN THE ORIGINAL AND THE PROXY SIGNERS.SUCH A KIND OF DELEGATI -ON OBVIOUSLY CONSUMES WITH THE BANDWIDTH AND BECOMES INEFFICIENT.THUS,A NEW PROXY DIGITAL SIGNATURE SCHEME DIFFERENT FROM THAT BY ZHANG IS PROPOSED TO ACHIEVE THE PURPOSE OF DELEGAT ION PROXY WITHOUT A SECURE MANNER. IN THE RECENT YEARS, THE ELLIPTIC CURVE CRYPTOSYSTEM (ECC) IS WIDELY APPROVED OF THE APP -LICATION IN BOTH SECURITY AND EFFICIENCY FOR THE DESIGN OF THE CRYPTO-SCHEME.ITS POTENTIA -L FUTURE FOR VARIOUS APPLICATIONS INCLINES THE ELLIPTIC CURVE CRYPTOSYSTEM TO REPLACE THE CURRENT RSA OR DSS CRYPTOSYSTEM IN SOME SPECIFIC CONDITION.CONSEQUENTLY,THERE DEVELOPS A NE -W TENDENCY TO THE RELATED RESEARCH.USING A SHORTER PRIVATE KEY THAN THAT OF THE RSA OR DSA ,THE ECC CAN ACHIEVE THE EQUAL LEVEL OF SECURITY UNDER A LOWER COMPUTATIONAL OVERHEADS (HOW MUCH COMPUTATION IS REQUIRED TO PERFORM THE PUBLIC KEY AND PRIVATE KEY TRANSFORMATIONS) AN -D KEY SIZE (HOW MANY BITS ARE REQUIRED TO STORE THE KEY PAIRS AND ANY SYSTEM PARAMETERS). GENERALLY SPEAKING, WHEN THE LENGTH OF Q REACHES 160-BIT IN THE ECC OVER Q-BIT DOMAIN,WHOS -E SECURITY IS EQUIVALENT TO THE 1024-BIT MODULUS IN THE RSA.A SHORTER PRIVATE KEY MEANS TH -E SHORTER BANDWIDTH REQUIRED AND STORAGE SPACE. FOR THE APPLICATION OF COMPUTER SCIENCE, SUCH A CHARACTERISTIC IS A CRITICAL KEY TO DEVELOP THE NETWORK. OWING TO THE SUPERIORITY, THE RESEARCH IS PUT INTO THE ECC TO CONSTRUCT A NEW DIGITAL SIGN -ATURE CRYPTOSYSTEM WITH HIGHER EFFICIENCY THAN THE TRADITIONAL ONES.

Keywords : DIGITAL SIGNATURE, PROXY SIGNATURE, INFORMATION SECURITY, CRYPTOGRAPHY, AND ELLIPTIC CURVE CRYPTOSYSTEM

Table of Contents

REFERENCES

[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.