AN EFFICIENT AND SECURE ELECTRONIC SUBSCRIPTION SYSTEM WITH USER AUTHENTICATION

邱信富、曹偉駿

E-mail: 9019980@mail.dyu.edu.tw

ABSTRACT

WE ANTICIPATE THE PUBLISHING WAY IN THE FUTURE WILL BE THAT THE LITHOGRAPHIC BOOK AND THE ELECTRONIC ONE COEXIST. BASED ON THE PRINCIPLE OF "USAGE-BASED PAYMENT", THE THESIS DEVELOPS AN ELECTRONIC SUBSCRIPTION SYSTEM PERMITTING USERS TO PAY FOR THE RIGHTS OF READING PART OF ELECTRONIC PERIODICALS ACCORDING TO HIS/HER NEED OR INTEREST. IN THE THESIS WE INTEGRATE THE SECURITY OF ACCESS CONTROL, ELLIPTIC CURVE CRYPTOSYSTEMS AND SELF-CERTIFIED PUBLIC KEY CRYPTOSYSTEMS WITH THE FAIR EXCHANGE PROTOCOL TO CONSTRUCT A SECURE ELECTRONIC SUBSCRIPTION ENVIRONMENT. THE ELECTRONIC SUBSCRIPTION SYSTEM PROPOSED IN THIS THESIS POSSESSES THE FOLLOWING ADVANTAGES: 1. A USER AND THE PUBLISHER CAN AUTHENTICATE EACH OTHER WITHOUT VERIFYING SIGNATURE SIGNED BY TTP (TRUSTED THIRD PARTY) IN THEIR DIGITAL CERTIFICATES. 2. BASED ON THE SECURITY OF ELLIPTIC CURVE CRYPTOSYSTEMS, THE PROPOSED ELECTRONIC SUBSCRIPTION SYSTEM CAN POSSESS FEWER BITS ACHIEVING THE SAME SECURITY DEGREE AS OTHER PUBLIC KEY CRYPTOSYSTEMS. 3. ACCORDING TO THE APPROACH OF THE PROPOSED FAIR EXCHANGE PROTOCOL, THE ELECTRONIC SUBSCRIPTION SYSTEM CAN PREVENT A DISPUTE ABOUT THE TRANSACTION BETWEEN USERS AND THE PUBLISHER. 4. REGARDLESS OF USERS' SUBSCRIPTION PERIODS, THEY ALL KEEP ONLY A SECRET KEY, AND THE PUBLISHER CAN AUTHENTICATE THEIR READING PRIVILEGE EASILY. 5. WHEN A USER'S SUBSCRIPTING DATE HAS EXPIRED, THE FUNCTION OF HIS/HER SECRET KEY CAN BE TERMINATED AUTOMATICALLY. IN OTHER WORD, HIS/HER SECRET KEY HAS NO READING RIGHTS ANYMORE. 6. THE PROPOSED ELECTRONIC SUBSCRIPTION SYSTEM CAN PREVENT IMPERSONATION ATTACK AND THE REPLAY ATTACK.

Keywords : ELLIPTIC CURVE CRYPTOSYSTEMS, SELF-CERTIFIED PUBLIC KEY CRYPTOSYSTEMS, FAIR EXCHANGE PROTOCOL, ACCESS CONTROL, USER AUTHENTICATION

Table of Contents

REFERENCES

[1] 余千智，「電子商務總論」，智勝出版社，民國88年4月。

[2] 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) [3] 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。

[4] 鍾振華，「使用身分基礎之自我驗證公開金鑰的金鑰分配及會議金鑰分配技術」，台灣科技大學 資訊管理研究所碩士論文，民國88年。(指導教授:吳宗成) [5] 黃裕峰，「應用密碼理論製作之電子刊物安全訂閱系統」，台灣工業技術學院管理技術研究所碩 士論文，民國86年。(指導教授:吳宗成) [6] 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。

[7] CCITT RECOMMENDATION X.509, "THE DIRECTORY: AUTHENTICATION FRAMEWORK," JAN 1997.

[8] V. S. MILLER, "USE OF ELLIPTIC CURVE IN CRYPTOGRAPHY," ADVANCES IN CRYPTOLOGY: CRYPTO'85, 1985, PP.

417-426.
[9] B. S. KALISKI, "AN OVERVIEW OF THE PKCS STANDARDS," RSA LABORATORIES, NOV. 1993. 10] C. GUNTHER, "AN IDENTITY-BASED KEY-EXCHANGE PROTOCOL," ADVANCES IN CRYPTOLOGY EUROCRYPT '91, LECTURE NOTES IN COMPUTER SCIENCE, VOL. 547, SPRINGER-VERLAG, 1991, PP.29-37.
[11] C. P. SCHNORR, "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS," ADVANCES IN CRYPTOLOGY: CRYPTO'89, 1989, PP.339-351.
[12] E. BLHAM AND A. SHAMIR, "DIFFERENTIAL CRYPTANALYSIS OF THE DATA ENCRYPTION STANDARD, " SPRINGER-VERLAG, BERLIN, 1993.
[13] F. BAO, R. DENG, AND W. MAO, "EFFICIENT AND PRACTICAL FAIR EXCHANGE PROTOCOLS WITH OFF-LINE TTP," PROCEEDINGS OF THE IEEE SYMP. ON SECURITY AND PRIVACY, OAKLAND, CA, MAY 3-6, 1998, PP. 77-85.
[14] H. PETERSEN, AND P. HORSTER, "SELF-CERTIFIED KEYS CONCEPTS AND APPLICATIONS," PROC -EEDINGS OF COMMUNICATIONS AND MULTIMEDIA SECURITY'97, 1997, PP. 102-116.
[15] JURISIC AND A. J. MENEZES, "ELLIPTIC CURVES AND CRYPTOGRAPHY," DR. DOBB'S JOURNAL, 1997, PP. 26-35.
[16] C. H. LIN, "DYNAMIC KEY MANAGEMENT SCHEMES FOR ACCESS CONTROL IN A HIERARCHY," COMP -UTER COMMUNICATIONS, VOL.20, DEC 15, 1997, PP.1381-1385.
[17] M. GIRAULT, "SELF-CERTIFIED PUBLIC KEYS," ADVANCES IN CRYPTOLOGY: EUROCRYPT'91, LECTURE NOTES IN COMPUTER SCIENCE, VOL. 547, SPRINGER-VERLAG, 1991,4 PP. 491-497.
[18] M. K. FRANKLIN AND M. K. REITER, "FAIR EXCHANGE WITH A SEMI-TRUSTED THIRD PARTY, " PROCEEDINGS OF THE 4TH ACM CONFERENCES ON COMPUTER AND COMMUNICATIONS SECURITY, APRIL 1-4, 1997,PP. 1-5.
[19] M. STADLER, "PUBLICLY VERIFIABLE SECRET SHARING", PROCEEDINGS OF EUROCRYPTO'96, LNCS 1070, SPRINGER-VERLAG, 1996, PP. 190-199.
[20] MASTERCARD AND VISA, "SECURE ELECTRONIC TRANSACTION SPECIFICATION," JUNE 1996.
[21] N. ASOKAN, M. SCHUNTER AND M. WAIDNER, "OPTIMISTIC PROTOCOLS FOR FAIR EXCHANGE," PRO -CEEDINGS OF THE 4TH ACM CONFERENCES ON COMPUTER AND COMMUNICATIONS SECURITY, APRIL 1997, PP. 6-17.
[22] N. ASOKAN, V. SHOUP AND M. WAIDNER, "ASYNCHRONOUS PROTOCOLS FOR OPTIMISTIC FAIR EX -CHANGE," PROCEEDINGS OF THE IEEE SYMP. ON SECURITY AND PRIVACY, OAKLAND, CA, MAY 3-6, 1998, PP. 86-100.
[23] N. KOBLITZ, "ELLIPTIC CURVE CRYPTOSYSTEMS," MATHEMATICS OF COMPUTATION, VOL. 48, NO. 17, 1987, PP. 203-209.
[24] N. ZHANG, Q. SHI AND M. MERABTI, "A FLEXIBLE APPROACH TO SECURE AND FAIR DOCUMENT EXCHANGE," THE COMPUTER JOURNAL, VOL.42, NO 7, 1999, PP. 569-581.
[25] "PROPOSED FEDERAL INFORMATION PROCESSING STANDARD FOR DIGITAL SIGNATURE STANDARD," FEDERAL REGISTER, VOL. 56, NO.169, AUG.30, 1991, PP. 42980-42982.
[26] R. RIVEST, "THE MD5 MESSAGE DIGEST ALGORITHM," RFC 1321, 1992.
[27] 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, FEB. 1978, PP. 120-126.
[28] 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.
[29] S. SAEEDNIA, "IDENTITY-BASED AND SELF-CERTIFIED KEY-EXCHANGE PROTOCOLS," INFORMATION SECURITY AND PRIVACY: ACISP'97, 1997, PP. 303-313.
[30] S. VANSTONE, "ELLIPTIC CURVE CRYPTOSYSTEM-THE ANSWER TO STRONG, FAST PUBLIC-KEY CRYP -TOGRAPHY FOR SECURING CONSTRAINED ENVIRONMENTS," INFORMATION SECURITY TECHNICAL RE -PORT, VOL. 2, NO. 2, 1997, PP. 78-87.
[31] SHAMIR, "IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES," ADVANCES IN CRYPTOLOGY: CRYPTO'84, 1984, PP. 47-53.
[32] T. ELGAMAL, "A PUBLIC KEY CRYPTOSYSTEM AND A SIGNATURE SCHEME BASED ON DISCRETE LOG -ARITHMS, "IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, 1985, PP. 469 -472.
[33] T. C. WU, Y.S. CHANG, AND T.Y. LIN, "IMPROVEMENT OF SAEEDNIA'S SELF-CERTIFIED KEY EXCHANGE PROTOCOLS, "IEE ELECTRONIC LETTERS, VOL 34, NO 11, MAY 1998, PP. 1094-1095.
[34] T. C. WU, "DIGITAL SIGNATURE/MULTISIGNATURE SCHEMES GIVING PUBLIC KEY VERIFICATION AND MESSAGE RECOVERY SIMULTANEOUSLY," TO APPEAR IN COMPUTER SYSTEMS SCIENCE AND ENG -INEERING, 2001.
[35] "THE DIGITAL SIGNATURE STANDARD PROPOSED BY NIST," COMMUN. ACM, VOL.35, NO7, JULY 1992, PP. 41-54.
[36] H. M. TSAI AND C. C. CHANG, "A CRYPTOGRAPHIC IMPLEMENTATION FOR DYNAMIC ACCESS CON -TROL IN A USER HIERARCHY," COMPUTER AND SECURITY, VOL. 14,NO. 2, 1995, PP.159-166.

[37] W. CAELLI, E. DAWSON, AND S. REA, "PKI, ELLIPTIC CURVE CRYPTOGRAPHY AND DIGITAL SI -GNATURES," COMPUTER AND SECURITY, VOL. 18, NO. 1, 1999, PP. 47-66.
[38] W. DIFFIE AND M. E. HELLMAN, "NEW DIRECTIONS IN CRYPTOGRAPHY, "IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, 1976, PP. 644-654.
[39] Y. S. CHANG, T. C. WU, AND S. C. HUANG, "ELGAMAL-LIKE DIGITAL SIGNATURE AND MULTISI -GNATURE SCHEMES USING SELF-CERTIFIED PUBLIC KEYS," THE JOURNAL OF SYSTEM AND SOFTWA -RE, 2000, PP. 99-105.
[40] HTTP://WWW.EHANISM.COM.TW/ [41] HTTP://WWW.SILKBOOK.NET/ [42] HTTP://WWW.ZDNET.COM/ [43] HTTP://WWW.ROCKETBOOK.COM/ [44] HTTP://WWW.SOFTBOOK.COM/ [45] HTTP://WWW.BOOKINSIGHT.COM.TW/ [46] HTTP://WWW.DIGIEBOOKS.COM/ [47] D. B. JOHNSON AND A. J. MENEZES, "ECDSA: AN ENHANCED DSA", HTTP://WWW.CERTICOM.COM