智慧型安全電子付款系統之研究

廖仁億、曹偉駿

E-mail: 9023854@mail.dyu.edu.tw

摘 要

目前電子付款系統在實務的設計上，多採數位憑證為基礎的方式來處理相關的安全付款事宜，但是此作法有一個很重要的先決條件，那就是系統認證中心須是誠實的且必須保護金鑰目錄，另外還需額外耗費驗證系統憑證中心之簽章的時間。 在現實的環境中，其實我們並不能絕對認定系統憑證中心一定是誠實的，或者我們應該說，系統憑證中心也是有機會被駭客入侵的，故發展自我認證(SELF-CERTIFIED)的機制確有其必要性。所謂的自我認證是指交談的雙方僅需要靠雙方傳送一些公開的資訊，即可達成雙方身分的確認，而不需透過公正的第三者來作保證或協調。本論文所探討的是智慧型安全電子付款技術，故除了安全層級的顧慮外，還必須兼顧安全機制運算上的便捷與效率。因橢圓曲線公開金鑰密碼系統的運算較現存的其它公開金鑰密碼系統更快速，且以較少之位元數達到相同的安全度。因此，本論文發展出一套以橢圓曲線密碼系統為基礎的具自我認證公開金鑰密碼系統，並以此自我認證公開金鑰密碼系統發展出交談金鑰、數位簽章及盲簽章等安全機制，且將這些技術實際應用在較具傳統方式的電子現金型付款系統，藉以提升這類付款機制的安全與效率，使即時性的安全電子付款成為可行的方案。總之，本論文目的在於發展出有效率之自我認證為基礎的安全機制，藉此可使電子商務交易之安全付款機制更臻完備且更切實際，以提昇使用者對使用電子商務付款服務的信心。

關鍵詞 : 電子付款系統、橢圓曲線密碼系統、自我認證公開金鑰密碼系統、盲簽章

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，1998年8月。

[2]吳琮璠、謝清佳，資訊管理，智勝文化事業公司，1998年8月。

[3]邱筱雅，電子商務的付款機制:研究文獻回顧與評述，交通大學資訊管理研究所碩士論文， 民國85年。(指導教授:黃景彰) [4]段正明、李鎮樟，電子付款的分析與探討，CCL TECHNICAL JOURNAL，1996年12月。

[5]邵敏華，SET使用的密碼學技巧:優缺點之評估，CCL TECHNICAL JOURNAL，1999年12月。

[6]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) [7]夏雲浩，網路錢潮-談數位貨幣，翔威國際有限公司，1998年七月。

[8]林祝興、李正隆，"ELLIPTIC-CURVE UNDENIABLE SIGNATURE SCHEMES," 第十一屆全國資訊安全 會議，2001年5月。

[9]BELLART, M., GARAY, J.A., HAUSER, R., HERZBERG, A., KRAWCZYK, H., STEINER, M., TSUDIK, G., AND WAIDNER, M., "IKP -- A FAMILY OF SECURE ELECTRONIC PAYMENT PROTOCOLS," PROC -EEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, NEW YORK, JULY 1995.

[10]BLHAM, E., AND SHAMIR, A., "DIFFERENTIAL CRYPTANALYSIS OF THE DATA ENCRYPTION STAND -ARD," SPRINGER VERLAG, BERLIN, 1993.

[11]BOLY, J.P., BOSSELAERS, A., CRAMER, R., MICHELSEN, R., MJOLSNES, S., MULLER, F., PEDERSEN, T., PFITZMANN, B., ROOIJ P., SCHOENMAKERS, B., SCHUNTER, M., VALLEE, L., AND WAIDNER, M., "THE ESPRIT PROJECT CAFE:HIGH SECURITY DIGITAL PAYMENT SYSTEMS," ESORICS 94(THE THIRD EUROPEAN SYPOSIUM ON RESEARCH IN COMPUTER SECURITY, LNCS 875, SPRINGER VERLAG, BERLIN 1994, PP. 217-230.

[12]CAMP, L.J., SIRBU, M., AND TYGAR, J.D., "TOKEN AND NOTATIONAL MONEY IN ELECTRONIC COMMERCE," PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, NEW YORK, JULY 1995.

[13]CARMENISCH, J.L., PIVETEAU, J.M., AND SRADLER, M.A., "BLIND SIGNATURES BASED ON THE DISCRETE LOGARITHM

PROBLEM," RUMP SESSION OF EUROCRYPT'94, PERGIA, ITALY, 1994.
[14]CHANG, Y.S., WU, T.C., AND HUANG, S.C., "ELGAMAL-LIKE DIGITAL SIGNATURE AND MULTISI -GNATURE SCHEMES USING SELF-CERTIFIED PUBLIC KEYS," THE JOURNAL OF SYSTEMS AND SOFT WARE, 2000, PP. 99-105.
[15]CHAUM, D., "BLIND SIGNATURE FOR UNTRACEABLE PAYMENTS," ADVANCES IN CRYPTOLOGY: CRYPTO' 82, 1983, PP. 199-203.
[16]CHAUM, D., FIAT, A., AND NAOR, M., "UNTRACEABLE ELECTRONIC CASH," ADVANCES IN CRYPT OLOGY: CRYPTO'88, 1988, PP. 319-327.
[17]COX, B., TYGAR, J.D., AND SIRBU, M., "NETBILL SECURITY AND TRANSACTION PROTOCOL," PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, NEW YORK, JULY 1995.
[18]CYBERCASH WEB SITE, URL: HTTP://WWW.CYBERCASH.COM.
[19]DAVIS, R.M., "THE DATA ENCRYPTION STANDARD IN PERSPECTIVE," COMPUTER SECURITY AND THE DATA ENCRYPTION STANDARD, NATIONAL BUREAU OF STANDARDS, SPECAL PUBLICATION, FEB. 1978.
[20]DIFFIE, W., AND HELLMAN, M.E., "NEW DIRECTIONS IN CRYPTOGRAPHY," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, 1976, PP. 644-654.
[21]ELGAMAL, T., "A PUBLIC KEY CRYPTOSYSTEM AND A SIGNATURE SCHEME BASED ON DISCRETE LOGARITHMS," IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, 1985, PP. 469-472.
[22]FERREIRA, L., DAHAB, R., "A SCHEME FOR ANALYZING ELECTRONIC PAYMENT SYSTEMS," COM -PUTER SECURITY APPLICATIONS CONFERENCE, 1998, PP. 137 -146.
[23]FRIER, A., KARLTON, P., AND KOCHER, P., "THE SSL 3.0 PROTOCOL," NETSCAPE COMMUNICA -TIONS CORP., 18 NOV. 1996. (URL: HTTP://HOME.NETSCAPE.COM/ENG/SSL3/DRAFT302.TXT) [24]GIRAULT, M., "SELF-CERTIFIED PUBLIC KEYS," LNCS 547, ADVANCES IN CRYPTOLOGY: PROC. EUROCRYPT'91, SPRINGER, 1992, PP. 490-497.
[25]GLOBE ID WEB SITE, URL: HTTP://WWW.GLOBEID.COM.
[26]HARN, L., "CRYPTANALYSIS OF THE BLIND SIGNATURES BASED ON THE DISCRETE LOGARITHM PROBLEM," ELECTRONICS LETTERS, VOL. 31, NO.14, 1995.
[27]JURISIC, A., AND MENEZES, A.J., "ELLIPTIC CURVES AND CRYPTOGRAPHY," DR. DOBB'S JOU -RNAL, 1997, PP. 26-35.
[28]JURISIC, A., AND MENEZES, A.J., "ECC WHITEPAPER:ELLIPTIC CURVES AND CRYPTOGRAPHY," URL: HTTP://WWW.CERTICOM.COM/RESEARCH/WECCRYPT.HTML [29]KALISKI, B.S., "AN OVERVIEW OF THE PKCS STANDARDS," RSA LABORATORIES, NOV. 1993.
[30]KOBLITZ, N., "ELLIPTIC CURVE CRYPTOSYSTEMS," MATHEMATICS OF COMPUTATION, VOL. 48, NO. 17, 1987, PP. 203-209.
[31]LAI, X., AND MASSEY, J., "A PROPOSAL FOR A NEW BLOCK ENCRYPTION STANDARD," PROCEED -INGS OF EUROCRYPT'90, SPRINGER VERLAG, BERLIN, 1991, PP. 389-404.
[32]MANASSE, M.S., "THE MILLICENT PROTOCOLS FOR ELECTRONIC COMMERCE," PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, NEW YORK, JULY 1995.
[33]MASTERCARD AND VISA, SECURE ELECTRONIC TRANSACTION (SET) SPECIFICATION, JUNE 1996.
[34]MEDVINSKY, G., AND NEUMAN, B.C., "NETCASH: A DESIGN FOR PRACTICAL ELECTRONIC CURRENCY ON THE INTERNET," PROCEEDINGS OF 1ST THE ACM CONFERENCE ON COMPUTER AND COMMUNICATION SECURITY, NOV. 1993.
[35]MILLER, V.S., "USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY," ADVANCES IN CRYPTOLOGY: CRYPTO'85, 1985, PP. 417-426.
[36]MOHAMMED, E., EMARAH, A.E., AND EL-SHENNAWY, K.H., "A BLIND SIGNATURE SCHEME BASED ON ELGAMAL SIGNATURE," SEVENTEENTH NATIONAL RADIO SCIENCE CONFERENCE, FEB. 2000, PP. 22-24.
[37]NEUMAN, C., AND MEDVINSKY, G., "REQUIREMENTS FOR NETWORK PAYMENT: THE NETCHEQUE PER -SPECTIVE," PROCEEDINGS OF IEEE COMPCON'95, MARCH 1995.
[38]NGUYEN, K.Q., MU, Y., AND VARADHARAJAN, V., "MICRO-DIGITAL MONEY FOR ELECTRONIC COMMERCE," COMPUTER SECURITY APPLICATIONS CONFERENCE, 1997, PP. 2-8.
[39]PEIRCE, M., AND O'MAHONY, D., "SCALEABLE, SECURE CASH PAYMENT FOR WWW RESOURCES WITH THE PAYME PROTOCOL SET," 4TH INTERNATIONAL WORLD WIDE WEB CONFERENCE, DEC. 11-14, 1995.
[40]PETERSEN, H., AND POUPARD, G., "EFFICIENT SCALABLE FAIR CASH WITH OFF-LINE EXTORTION PREVENTION," TECHNICAL REPORT LIENS-97-7, ECOLE NORMALE SUPERIEURE, MAY 1997.
[41]PETERSEN, H., AND HORSTER, P., "SELF-CERTIFIED KEYS-CONCEPTS AND APPLICATIONS," PROC -EEDINGS OF COMMUNICATIONS AND MULTIMEDIA SECURITY'97, 1997, PP. 102-116.
[42]PFITZMANN, B., SCHUNTER, M., AND WAIDNER, M., "HOW TO BREAK ANOTHER "PROVABLY SECURE" PAYMENT

SYSTEM," EUROCRYPT '95, LNCS 921, SPRINGER VERLAG, BERLIN, 1995, PP. 121-132.
[43]PFITZMANN, B., AND WAIDNER, M., "STRONG LOSS TOLERANCE OF ELECTRONIC COIN SYSTEMS," ACM TRANSACTION ON COMPUTER SYSTEMS, VOL. 15, NO. 2, MAY 1997, PP. 194-213.
[44]POINTCHEVAL, D., AND STERN, J., "SECURITY ARGUMENTS FOR DIGITAL SIGNATURES AND BLIND SIGNATURES," JOURNAL OF CRYPTOLOGY, VOL. 13, 2000, PP. 361-396.
[45]RIVEST, R., "THE MD5 MESSAGE DIGEST ALGORITHM," RFC 1321, 1992.
[46]RIVEST, R., AND SHAMIR, A., "PAYWORD AND MICROMINT: TWO SIMPLE MICROPAYMENT SCHEMES," PROCEEDINGS OF RSA'96 CONFERENCE, 1996.
[47]RIVEST, R., SHAMIR, A., AND ADLEMAN, L., "A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS," COMMUNICATIONS OF THE ACM, VOL. 21, NO. 2, FEB. 1978, PP. 120-126.
[48]SAEEDNIA, S., "IDENTITY-BASED AND SELF-CERTIFIED KEY-EXCHANGE PROTOCOLS," INFORMATION SECURITY AND PRIVACY: ACISP'97, 1998, PP. 303-313.
[49]SCHNORR, C.P., "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS," ADVANCES IN CRYPTOLOGY: CRYPTO'89, 1990, PP. 339-351.
[50]SHAMIR, A., "IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES," ADVANCES IN CRYPTO -LOGY: CRYPTO'84, 1985, PP. 47-53.
[51]SCHOENMAKERS, B., "BASIC SECURITY OF THE ECASHTM PAYMENT SYSTEM," STATE OF THE ART IN APPLIED CRYPTOGRAPHY, COURSE ON COMPUTER SECURITY AND INDUSTRIAL CRYPTOGRAPHY, LEUVEN, BELGIUM, JUNE 3-6,1997, VOL. 1528 OF LECTURE NOTES IN COMPUTER SCIENCE, PP. 338-352.
[52]CCITT RECOMMENDATION X.509, "THE DIRECTORY: AUTHENTICATION FRAMEWORK," 1993.
[53]WRIGHT, M., "AUTHENTICATING ELECTRONIC CASH TRANSACTIONS," COMPUTER FRAUD & SECURITY, APR. 1997.
[54]WU, T.C., "DIGITAL SIGNATURE/MULTISIGNATURE SCHEMES GIVING PUBLIC KEY VERIFICATION AND MESSAGE RECOVERY SIMULTANEOUSLY," TO APPEAR IN COMPUTER SYSTEMS SCIENCE AND ENGI -NEERING, 2001.