

兼具使用者認證之有效率的電子訂閱系統

邱信富、曹偉駿

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

摘要

預期日後的出版型態，將是平面與電子版本同時發行的局面，基於「使用者付費」的原則，本論文提出一電子訂閱系統，使得使用者可依其需要或興趣，付費購買部分電子刊物的閱讀權利。本論文整合存取控制機制、橢圓曲線密碼系統與自我認證公開金鑰密碼系統的安全特性，並結合公平交換協定，來建構一個安全的電子訂閱環境。本論文所提出的電子訂閱系統具有下列優點：1. 使用者和出版商之間可以不必依靠公正的第三單位所簽發的數位憑證以驗證彼此的身分。2. 植基於橢圓曲線密碼系統的安全特性，以更少的位元數來達到相同的安全等級。3. 運用公平交換的原理，處理使用者訂閱的相關資訊，以維護雙方權益。4. 不論訂閱期限的長短，訂閱者只需保有一把秘密金鑰，系統即能判別所有訂閱期之刊物的使用權限。5. 當訂閱者的訂閱期限到期時，秘密金鑰即自動失效，換言之逾期的秘密金鑰會失去閱讀刊物的權利。6. 本電子訂閱系統能夠防止攻擊者的偽冒及重送攻擊。

關鍵詞：橢圓曲線密碼系統、自我認證公開金鑰密碼系統、公平交換協定、存取控制、使用者認證

目錄

第一章 緒論--P1 1.1 研究背景與動機--P1 1.2 研究目的--P3 1.3 研究架構--P4 1.4 論文架構--P6 第二章 文獻探討--P7 2.1 電子商務安全需求--P7 2.2 電子書--P11 2.3 密碼學背景--P14 2.4 公開金鑰密碼系統--P17 2.4.1 憑證為基礎的公開金鑰密碼系統--P18 2.4.2 身份為基礎的公開金鑰密碼系統--P18 2.4.3 自我認證公開金鑰密碼系統--P20 2.4.4 橢圓曲線公開金鑰密碼系統--P24 2.5 公平交換協定--P29 2.5.1 On-line TTP--P29 2.5.2 Off-line TTP--P31 2.6 存取控制機制--P33 第三章 兼具使用者認證之電子訂閱系統--P36 3.1 植基於自我認證公開金鑰密碼系統的公平交換協定CEMBS--P36 3.2 安全電子訂閱系統之設計--P40 第四章 安全及複雜度分析--P45 4.1 安全性分析--P45 4.2 計算複雜度分析--P48 4.3 資料傳輸量分析--P52 第五章 結論與建議--P55 參考文獻--P57 附錄一：PEDLDLL憑證--P62

參考文獻

- [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. W AidNER, "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. W AidNER, "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/](http://www.ehanism.com.tw/) [41] [HTTP://WWW.SILKBOOK.NET/](http://www.silkbook.net/) [42] [HTTP://WWW.ZDNET.COM/](http://www.zdnet.com/) [43] [HTTP://WWW.ROCKETBOOK.COM/](http://www.rocketbook.com/) [44] [HTTP://WWW.SOFTBOOK.COM/](http://www.softbook.com/) [45] [HTTP://WWW.BOOKINSIGHT.COM.TW/](http://www.bookinsight.com.tw/) [46] [HTTP://WWW.DIGIEBOOKS.COM/](http://www.digiebooks.com/) [47] D. B. JOHNSON AND A. J. MENEZES, "ECDSA: AN ENHANCED DSA", [HTTP://WWW.CERTICOM.COM](http://www.certicom.com)