A Study on Secure and Efficient Schemes for Electronic Procurement of Governments

李廣凱、曹偉駿

E-mail: 9222445@mail.dyu.edu.tw

ABSTRACT

Since Taiwan entered into the World Trade Organization in 2002, government procurement issues are in the spotlight around the world. As we know, there were many problems under the government procurement operations before, such as the difficulty of obtaining the procurement information, the complicated procurement process, the inconvenience of the bidding, the corruption of personal procurement, etc. If the government procurement operations can be done through the Internet, then it can not only save huge manpower, but also prevent personal corruption. Therefore, online government procurement can greatly improve our government image. As the Internet is a public environment, the security of the procurement information is very important to us. If we cannot take some security schemes to protect the procurement information, people can change or delete data easily and further influence the fairness of procurement. Thus, in this thesis we adopt Elliptic Curve Cryptosystems that can use few bits to reach the same security level as other public key cryptosystems, and also get a better efficiency during message transmission. On the other hand, using self-certified public key cryptosystems can verify efficiently the validity of public keys. Hence, in this thesis we first combine Elliptic Curve Cryptosystems with self-certified public key cryptosystems to develop a mutual authentication scheme, signcryption scheme, multi-signcryption scheme, blind signature scheme and fair document exchange scheme. Then, in the procedure of electronic procurement we can increase the security level, reduce the storage cost, and improve the efficiency of data transmission based on the schemes proposed above. Additionally, this thesis is to concentrate the study on the validity of bid bond and electronic contracting which had never been discussed before. The government organizations and bidders can process all procurement procedure by employing our proposed schemes to implement a complete electronic system. Therefore, this thesis is to provide a secure and efficient environment of government procurement.

Keywords : Elliptic Curve Cryptosystems, Self-certified Public key System, Information Security, Sealed-bid in Network, Government Procurement Law.

Table of Contents

REFERENCES

[1] 共同供應契約網站: http://sucon.pcc.gov.tw [2] 美國聯邦採購規則網站: http://www.arnet.gov/far [3] 財團法人資訊工業策進會電子商務應用推廣中心網站: http://www.find.org.tw/0105/home_new.asp [4] 採購公告系統網站: http://web.pcc.gov.tw [5] 國家資通安全應變中心網站: http://www.ncert.nat.gov.tw/infosec [6] 電子化網站評比網站: http://www.gov.tw/activity/honor200210/index.htm [7] 電子型錄及詢報價系統網站: http://gecs.pcc.gov.tw [8] 電子領投標系統網站: http://www.geps.gov.tw [9] 新加坡政府採購資訊網站: http://160.96.179.95/gitis/regime.html [10] 審計部相關法令網站: http://www.audit.gov.tw [11] CAL-Buy網站: http://www.pd.dgs.ca.gov/calbuy/default.htm [12] 王曉峰及洪國寶, 「利用智慧卡來建構一個遠端使用者認證系統」, Proceedings of 2000 Taiwan Area Network Conference, October, 2000, pp.32-39. (國科會研究計畫編號:NSC89-2213-E-005-036)。

[13] 何煒華, 「簽密法之設計」, 台灣科技大學資訊管理研究所博士論文, 民國八十九年(指導教授:吳宗成博士)。

[14] 李廣凱, 「顧客關係管理的運用-以金融服務業為例」, 逢甲大學電子商務經營管理研討會, 民國九十一年。

[15] 林祝興及李正隆, "Elliptic-curve undeniable signature schemes,"第11屆全國資訊安全會議, 第331-338頁, 民國九十年五月。

[16] 胡國新, 「在線上電子拍賣環境下設計植基於自我驗證公開金鑰系統之安全機制」, 大葉大學資訊管理研究所碩士論文, 民國八十九年(指導教授:曹偉駿博士)。

[17] 行政院公共工程委員會, 「政府採購法令彙編」, 三民書局, 民國九十二年。

[18] 陳宗保, 「行動電子商務環境下安全協定之研究」, 大葉大學資訊管理研究所碩士論文, 民國九十年(指導教授:曹偉駿博士)。

[19] 陳金鈴, 「一種前瞻性網路競標協定」, 國立中興大學應用數學研究所碩士論文, 民國八十八年(指導教授:詹進科博士)。

[20] 陳俊良, 「網際網路上的工程競標:應用密碼學理論建立一個安全且公平的商業機制」, 國立交通大學資訊管理研究所碩士論文, 民國八十七年(指導教授:黃景彰博士)。

[21] 陳振聲, 「網際網路投開標安全機制之研究」, 國防管理學院國防資訊研究所碩士論文, 民國八十九年(指導教授:陳正鎔博士)。

[22] 廖耕億, 「電子商務環境中網路拍賣系統之研究」, 國立交通大學資訊管理研究所博士論文, 民國九十年(指導教授:黃景彰博士)。

[23] 賴溪松、韓亮及張真誠, 「近代密碼學及其應用」, 松崗電腦圖書資料股份有限公司, 民國九十年。

[24] 賴居正、郭建邦及賴溪松, 「我國電子採購系統之規劃與探討」, 第十二屆全國資訊安全會議, 民國九十一年。

[25] L.M. Applegate, "Electronic commerce: Building blocks of new business opportunity", Journal of Organizational Computing and Electronic Commerce, Vol.6, No.1, 1996, pp. 1-10.

[26] F. Bao, R.H. Deng and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP," Security and Privacy, Proceedings 1998 IEEE Symposium on 1998, 1998, pp.77-85.

[27] M. Ben-Or, O. Goldreich, S. Micali and R. Rivest, "A fair protocol for signing contracts," IEEE Transactions on Information Theory, Vol.36, No.1, 1990, pp. 40-46.

[28] D. Boneh and M. Franklin, "Identity- base encryption from the weil pairing," Advances in Cryptology Crypto'2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, , 2001, pp. 213-229.

[29] W. Caelli, E. Dawson and S. Rea, "PKI, Elliptic curve cryptography and digital signatures," Computer & Security, Vol. 18, No. 1, 1999, pp. 47-66.

[30] J. Camenisch, J. Piveteau and M. Stadler, "Blind signatures based on the discrete logarithm problem," Advances in cryptology-proc. Eurocrypt 94' LNCS 950, Springer-Verlag, 1994, pp. 428-432.

[31] C. K. Chan and L. M. Cheng "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, 2000. pp. 992-993.

[32] D. Chaum, "Blind signature for untraceable payments," Advances in Cryptology Crpto'82, Lecture Notes in Computer Science, Springer-Verlag, 1982, pp. 199-203.

[33] CCITT Recommendation X.509, "The directory: authentication framework," Jan 1997.

[34] M. Franklin and M. Reiter, "The design and implementation of a secure auction service," IEEE Transactions on Software Engineering, Vol. 22, No. 5, 1996, pp. 302-312.

[35] M. Franklin and M. Reiter, "Fair exchange with a semi-trusted third party," Proceedings of the 4th ACM Conferences on Computer and Communications Security, 1997, pp. 1-126.

[36] W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, pp. 644-654.

[37] T. ElGamal, "A public key cryptosystem and a signature scheme based on discreter logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, 1985, pp. 469-472.

[38] S. Even, O. Goldreich and A. Lempel, "A randomized protocol for signing contracts," Communications of the ACM, Vol. 28, No. 6, 1985, pp. 637-647.

[39] M. Girault, "Self-certified public keys", Advances in Cryptology: EuroCrypt '91, Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, 1991, pp. 491-497.

[40] D. Hirakiuchi and K. Sakurai, "English vs. Sealed bid in anonymous electronic auction protocols," Enabling Technologies: Infrastructure for collaborative Enterprises, 2001, WET ICE 2001 Proceedings, 10th IEEE International workshops on, 2001.

[41] M. N. Huhns and J. M. Vidal, "Online auctions," IEEE Internet Computing, Vol. 3, No. 3, 1999, pp. 103-105.

[42] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, 2000, pp. 28-30.

[43] J. K. Jan and C. C. Tai, "A secure electronic voting protocol with ic cards," The Journal of Systems and Software, U.S.A. Vol. 39, 1997, pp. 93-101.

[44] A. Jurisic and A. J. Menezes, "Elliptic curves and cryptography," Dr. Dobb's Journal, 1997, pp. 26-35.

[45] A. Jurisic, and A.J. Menezes, "ECC whitepapers: elliptic curves and cryptography, "Certicom corp., (http://www. certicom.com/research/weccrypt.html).

[46] B. S. Kaliski, "An overview of the PKCS standards," RSA Laboratories, Nov. 1993.

[47] H. Kikuchi, M. Harkavy and J. D. Tygar, "Multi-round anonymous auction schemes," IEEE Workshop on Dependable and Real-Time e-Commerce System, 1998, pp. 62-69.

[48] D. F. Knuth, "Seminumerical algorithms," The Art of Computer programming, Second Edition, Addison-Wesley, Reading, MA, Vol. 2, 1981, pp. 441-466.

[49] K. Kobayashi and H. Morita, "Efficient sealed-bid auction with quantitative competition using one-way functions," Technical Report of IEICE, ISEC 95-30, 1999, pp. 31-37.

[50] N. Koblitz, "Elliptic curve cryptosystems," Math. Computal., Vol. 48, 1987, pp. 203-209.

[51] S. Liu, C. Wang and Y. Wang, "A secure multi-round electronic auction scheme," Eurocomm 2000, Information Systems for Enhanced Public Safety and Security IEEE/AFCEA, 2000.

[52] V. S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology Crypto'85, LNCS 218, Springer-Verlag, 1986, pp. 417-426.

[53] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," In Proceedings of Conference on Computer and Communications Security -- CCS'93, ACM Press, 1993, pp. 58-61.

[54] F. J. Riggins and H. S. Rhee, "Toward a unified view of electronic commerce," Communications of the ACM Vol.41, No. 10, 1998, pp. 88-95.

[55] 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, 1978, pp. 120-126.

[56] C. P. Schnorr, "Efficient identification and signatures for smart cards," Advances in Cryptology: Crypto '89, Springer-Verlag, 1990, pp. 339-351.

[57] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology: crypto '84, Springer-Verlag, 1985, pp. 47-53.

[58] W. Stallings, "Cryptography and network security, principles and practice," Second edition, pp. 7.

[59] S. Vanstone, "Elliptic curve cryptosystem - the answer to strong, fast public-key cryptography for securing constrained environments," Information Security Technical Report, Vol. 2, No. 2, Elsevier, 1997, pp. 78-87.

[60] Y. Watanabe and H. Imai, "Reducing the round complexity of a sealed-bid auction protocol with an off-Line TTP," Proceeding of the 7th ACM conference on computer and communications security, 2000, pp. 80-86.

[61] S. M. Yen and C. S. Laih, "New digital signature scheme based on discrete logarithm," Electronics Letters, No. 12, 1993, pp. 1120-1121.

[62] F. Zhang, Q. Li and Y. Wang, "A new secure electronic auction scheme," Eurocumm 2000, Information System for Enhanced Public Safety and Security IEEE/AFCEA, 2000, pp. 54-56.

[63] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)," Advances in Cryptology - CRYPTO'97, Springer-Verlag, 1997, pp. 165-179.