值基於橢圓曲線密碼系統的代理簽章機制之研究

鍾玉芳、陳澤雄 ; 余心淳

E-mail: 9225033@mail.dyu.edu.tw

摘 要

網路通訊技術的發展日新月異，造就線上交易與通信愈形普遍化的情形，可以想見電子商務將是未來資訊社會中商業活動的主流，因此也更加突顯資訊安全的重要性。在現行的網路安全研究領域上，公開金鑰密碼系統是接受度相當高的研究方向之一，該密碼系統運作中最關鍵的一環又非數位簽章機制莫屬，由於數位簽章技術的成熟與否對數位認證系統而言，具有決定性的指標意義，同時也是公開金鑰基礎建設研究中最重要的組成部分，其應用面之廣，也包含本論文的研究題目一代理簽章。 代理簽章技術及特性得以解決一般數位簽章在應用上的盲點，是非常值得著力的研究。所謂代理簽章，指的是具有權限的原始簽署者，以授權的方式委託代理人代為簽署文件，賦予文件合法的文件效力；授權後，代理簽署者再持授權資訊產生一個有效的代理簽章，對文件進行簽署；至於接收方驗證時，除了驗證簽章的有效性，同時還必須驗證授權資訊的合法性。所以當原始簽署者因故不克出席行使其簽章之權力與義務時，則可透過代理簽章機制授權所委託之代理者代為決行，以避免因時間點之延誤所導致的損失，進而提升執行程序之效能。代理簽章的相關應用還包括可移動代理、自我代理、電子現金、匿名投票系統等。 本論文的研究重點主要以安全性為經，執行效能為緯，透過對代理簽章研究系統化的歸納，深入探討相關文獻應用之理論，提出兩個因應不同應用需要的代理簽章機制，其一是不具代理保護的多重代理簽章機制，另一則為具代理保護的多重代理簽章機制，並且應用橢圓曲線密碼系統低運算量與短金鑰的特色，在滿足代理簽章機制所需的安全特性之餘，同時也具備一定的實用性，適用於網際網路資源有限之特殊環境，發展網路資訊科技。

關鍵詞 : 密碼系統 ; 數位簽章 ; 代理簽章 ; 電子商務安全

目錄

參考文獻

References [1] B. C. Neuman, Proxy-based Authorization and Accounting for Distributed Systems, “ Proc. 13th International Conference on Distributed Systems, ” 1993, pp.283-29157.

[2] M. Mambo, K. Usuda, and E. Okamoto, Proxy Signatures for Delegation Signing Operation, “ Proc. Third ACM Conf. on Computer and Communications Security, ” 1996, pp.48-57.

[3] M. Mambo, K. Usuda, and E. Okamoto, Proxy Signatures: Delegation of the Power to Sign Messages, “ IEICE Trans. Fundamentals, ” Vol.E79-A, No.9, Sep. 1996, pp.1338-1353.

[4] S. Kim, S. Park, and D. Won, Proxy Signatures, Revisited, “ ICICS'97, Lecture Notes in Computer Science 1334, ” Springer-Verlag, 1997, pp.223-232.

[5] N. Y. Lee, T. Hwang, and C. H. Wang, On Zhang ’ s Nonrepudiable Proxy Signature Schemes, “ Third Australasian Conference of ACISP ’ 98, ” 1998, pp.415-422.

[6] H. M. Sun, On Proxy (Multi-) Signature Schemes, “ Proceedings of the International Computer Symposium, ” 2000, pp.65-72.

[7] H. M. Sun and B. T. Hsieh, Remarks on two Nonrepudiable Proxy Signature Schemes, “ Ninth National Conference on Information Security, ” Taiwan, 1999, pp.241-246.

[8] H. M. Sun, N. Y. Lee, and T. Hwang, Threshold Proxy Signatures, “ IEE Proceedings—Computers and Digital Techniques, ” Vol.146, No.5, 1999, pp.259-263.

[9] S. M. Yen, C. P. Hung, and Y. Y. Lee, Remarks on Some Proxy Signature Schemes, “ Proceedings of the International Computer Symposium, ” 2000, pp.54-59.

[10] L. Yi, G. Bi and G. Xiao, Proxy Multi-signature Scheme: A New Type of Proxy Signature, “ Electronics Letters, ” 2000, Vol.36, No.6, pp.527-528.

[11] K. Zhang, Threshold Proxy Signature Schemes, “ 1997 Information Security Workshop, ” Japan, Sep. 1997, pp.191-199.

[12] Sun, H. M., Lee, N. Y., and Hwang T., Nonrepudiable Threshold Proxy Signatures, “ Proceedings of the Ninth National Conference on Information Security, ” 1999, pp. 254-261.

[13] Sun, H. M., An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers, “ Computer Communications, ” Vol.22, No.8, 1999, pp.717-722.

[14] Hsu C. L., Wu T. S., and Wu T. C., New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers, “ Journal of Systems and Software, ” 2001, Vol.58, No.2, pp.119-124.

[15] Hsu C. L., Wu T. S., and Wu T. C., Improvement of Threshold Proxy Signature Scheme, accepted by “ Applied Mathematics and Computation, ” 2001.

[16] Hsu C. L., Wu T. S., and Wu T. C., Efficient Proxy Signature Schemes Using Self-certified Public Keys, submitted to “ IEE Proceedings —Computers and Techniques, ” 2001.

[17] Okamoto T., Tada M., and Okamoto E., Extended Proxy Signatures for Smart Cards, “ Workshop on Information Security ISW'99, Springer-Verlag, ” 1999, pp.247-258.

[18] Sun H. M., Convertible Proxy Signature Scheme, “ National Computer Symposium, ” 1999, pp.186-189.

[19] Viswanathan K., Boyd C., and Dawson E., Publicly Verifiable Key Escrow with Limited Time Span, “ Proceedings of the Fourth Australasian Conference on Information Security and Privacy ACISP ’ 99, ” Springer-Verlag, pp.36-50.

[20] Hsu C. L., Wu T. S., He W. H., and Wu T. C., Efficient Proxy Multisignature Schemes, submitted to “ Computer Systems Science and Engineering, ” 2000.

[21] Itakura K. and Nakamura K., A Public-key Cryptosystem Suitable for Digital Multisignatures, “ NEC Research and Development, ” Vol.71, 1983, pp.1- 8.

[22] Boyd C., Digital Multisignature, “ Proceedings of Conference on Coding and Cryptography, ” 1986, pp. 15-17.

[23] Okamoto T., A Digital Multisignature Scheme Using Bijective Public-key Cryptosystem, “ ACM Transactions on Computer Systems, ” Vol.6, No.8, 1988, pp.432-441.

[24] Harn L. and Kiesler T., New Scheme for Digital Multisignature, “ Electronics Letters, ” Vol.25, No.15, 1989, pp.1002-1003.

[25] Boyd C., Multisignatures based on Zero-knowledge Schemes, “ Electronics Letters, ” Vol.27, No.22, 1991, pp.2002-2004.

[26] Ohta K. and Okamoto T., A Digital Multisignature Scheme based on the Fiat-Shamir Scheme, “ Advances in Cryptology —ASIACRYPT'91, ” Springer-Verlag, pp.139-148.

[27] Harn L., Group-oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature, “ IEE Proceedings—Computer and Digital Techniques, ” Vol.141, No.5, 1994, pp.307-313.

[28] Park S., Kim K., and Won D., Two Efficient RSA Multisignature Schemes, “ Proceedings of the First International Conference on Information and Communications Security ICICS'97, ” 1997, pp.217-222.

[29] Chang C. C., Leu J. J., Haung P. C., and Lee W. B., A Scheme for Obtaining a Message from the Digital Multisignature, “ Workshop on Practice and Theory in Public Key Cryptography PKC ’ 98, ” Springer-Verlag, 1998, pp.154-163.

[30] Harn L., Digital Multisignature with Distinguished Signing Authorities, “ Electronics Letters, ” Vol.35, No.4, 1999, pp.294-295.

[31] Lee N. Y., Hwang T., and Wang C. H., The security of two ID-based Multisignature Protocols for Sequential and Broadcasting Architectures, “ Information Processing Letters, ” Vol.70, No.2, 1999, pp.79-81.

[32] Harn L. and Yang S., Group-Oriented Undeniable Signature Schemes without the Assistance of a Mutually Trusted Party, “ Advances in Cryptology—AUSCRYPT ’ 92, ” Springer-Verlag, 1993, pp.133-142.

[33] Li C. M., Hwang T., and Lee N. Y., Remark on the Threshold RSA Signature Scheme, “ Advances in Cryptology—CRYPTO ’ 93, ” Springer-Verlag, 1993, pp.413-419.

[34] [LHL94] Li C. M., Hwang T., and Lee N. Y., Threshold-multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Shareholders, “ Advances in Cryptology—EUROCRYPT ’ 94, ” Springer-Verlag, 1994, pp.194-203.

[35] Langford S. K., Threshold DSS Signature without a Trusted Party, “ Advances in Cryptology—CRYPTO ’ 95, ” Springer-Verlag, 1995, pp.397-409.

[36] Gennaro R., Jarecki S., Krawczyk H., and Rabin T., Robust Threshold DSS Signatures, “ Advances in Cryptology—EUROCRYPT ’ 96, ” Springer-Verlag, 1996, pp.354-371.

[37] Park C. and Kurosawa K., New ElGamal Type Threshold Digital Signature Scheme, “ IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E79-A, No.1, 1996, pp.86-93.

[38] Wang C. T., Lin, C. H., and Chang C. C., Threshold Signature Schemes with Traceable Signers in Group Communications, “ Computer Communications, ” Vol.21, No.8, 1998, pp.771-776.

[39] Lee W. B. and Chang C. C., (t, n) threshold Digital Signature with Traceability Property, “ Journal of Information Science and Engineering, ” Vol.15, No.5, 1999, pp.669-678.

[40] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, “ Handbook of Applied Cryptography, ” CRC Press, Boca Raton, Florida, 1997.

[41] N. Koblitz, Elliptic Curve Cryptosystems, “ Mathematics of Computation, ” Vol.48, 1987, pp.203-209.

[42] V. S. Miller, Uses of Elliptic Curves in Cryptography, “ Advances in Cryptology—Crypto ’ 85: Lecture Notes in Compute Science, ” New York, Springer-Verlag, No.218, 1985, pp.417-426.

[43] N. Koblitz, “ A Course in Number Theory and Cryptography, ” New York, Springer-Verlag, Second edition, 1994.

[44] N. Koblitz, A. Menezes, and S. Vanstone, The State of Elliptic Curve Cryptography, “ Designs, Codes and Cryptography, ” Vol.19, 2000, pp.173-193.

[45] A. Menezes, T. Okamoto, and S. Vanstone, Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, “ IEEE Transactions on Information Theory, ” Vol.39, 1993, pp.1639-1646.

[46] N. Torii and K. Yokoyama, Elliptic Curve Cryptosystem, “ FUJITSU Sci. Tech. J., ” 36, 2, 2000, pp.140-146.

[47] J. Guajardo and C. Paar, Efficient Algorithms for Elliptic Curve Cryptosystems, “ Advances in Cryptology—Crypto'97: Lecture Notes in Compute Science, ” Springer-Verlag, No.1294, 1997, pp.342-356.

[48] G. Agnew, R. Mullin, and S. Vanstone, An Implementation of Elliptic Curve Cryptosystems over , “ IEEE Journal on Selected Areas in Communications, ” Vol.11, 1993, pp.804-813.

[49] J. Pollard, Monte Carlo Methods for Index Computation Mod p, “ Mathematics of Computation, ” Vol.32, 1978, pp.918-924.

[50] T. Satoh and K. Araki, Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves, “ Commentarii Mathematici Universitatis Sancti Pauli, ” Vol.47, 1998, pp.81-92.

[51] I. Semaev, Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p, “ Mathematics of Computation, ” Vol.67, 1998, pp.353-356.

[52] IEEE P1363: Standard Specifications For Public Key Cryptography, http://grouper.ieee.org/groups/1363/.