值基於橢圓曲線密碼系統的門檻簽章和鑑別加密機制之研究

黃國軒、陳澤雄 ; 余心淳

E-mail: 9225039@mail.dyu.edu.tw

摘 要

門檻(threshold)的概念在群體導向的簽章機制中被廣泛的應用。截至目前為止，有為數眾多的文章在不斷的探討及發展門檻簽章(threshold signature)。近幾年，門檻驗證(threshold verification)被提出後，也逐漸引起多方關注。考量二者之特性，本論文中將這兩種研究概念加以整合，並且提出一個可指定驗證者的群體導向門檻簽章機制。在該簽章機制中，不論是簽章的產生或驗證，其參與人數不要求全體成員的參與，但須達到一個特定的門檻值。此外，在驗證者的部分，只有被指定的驗證者才有資格進行簽章的驗證，這樣的限制在某些特定情況下將形成一定的效用與安全防範。 為了同時達到訊息傳遞的機密性(privacy)、完整性(integrity)及鑑別性(authenticity)，本文中尚提出一種低運算量及低通訊量的鑑別加密機制(authenticated encryption scheme)，其中並且包含門檻簽章(threshold signature)與門檻驗證(threshold verification)的特性。 此外，由於考慮所簽署文件的長度可能過大造成簽署者的工作負荷，文中也引入分工(division of labor)及訊息鏈結(message linkage)的概念，提出具有訊息鏈結的分工簽章之門檻鑑別加密機制。在有效減少各個簽署者對於訊息審核及簽章所需花費的時間的同時，也降低其工作負擔，提昇工作效率，並且根據訊息鏈結的特性，驗證者具有能力判別所收到的群體簽章區塊(group-signature block)是否遭人惡意打亂其次序或竄改其內容。 為了使所提的方法具有更佳的執行效率，本研究採用橢圓曲線密碼系統(elliptic curve cryptosystem)為應用平台，使所提方法的安全性構築於橢圓曲線離散對數問題(elliptic curve discrete logarithm problem)的困難度上。

關鍵詞 : 門檻簽章 ; 鑑別加密機制 ; 分工簽章 ; 訊息鏈結 ; 橢圓曲線密碼系統

目錄

參考文獻

[1] Desmedt, Y.,“ Society and group oriented cryptography, ” Advances in Cryptology — CRYPTO'87, Springer-Verlag, 1987, pp.120-127.

[2] 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.

[3] 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.

[4] 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.

[5] Langford, S.K.,“ Threshold DSS signature without a trusted party, ” Advances in Cryptology — CRYPTO'95, Springer-Verlag, 1995, pp.397-409.

[6] Gennaro, R., Jarecki, S., Krawczyk, H., and Rabin, T.,“ Robust threshold DSS signatures, ” Advances in Cryptology — EUROCRYPT'96, Springer-Verlag, 1996, pp.354-371.

[7] 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.

[8] 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.
[9] Li, Z.C., Zhang, J.M., Luo, J., Song, W., and Dai, Y.Q., " Group-oriented (t, n) threshold digital signature schemes with traceable signers, " ISEC 2001, LNCS 2040, 2001, pp.57-69.
[10] Harn, L., and Kiesler, T., " New scheme for digital multisignature, " Electronics Letters, Vol.25, No.15, 1989, pp.1002-1003.
[11] Boyd, C., " Multisignatures based on zero-knowledge schemes, " Electronics Letters, Vol.27, No.22, 1991, pp.2002-2004.
[12] Chang, Y.S., Wu, T.C., and Huang, S.C., " ElGamal-like digital signature and multisignature schemes using self-certified public keys, " The Journal of Systems and Software, Vol.50, 2000, pp.99-105.
[13] 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.
[14] De Soete, M., Quisquater, J.J., and Vedder, K., " A signature with shared verification scheme, " Advances in Cryptology — CRYPTO'89, Springer-Verlag, 1989, pp.253-262.
[15] Harn, L., " Digital signature with (t, n) shared verification based on discrete logarithms, " Electronics Letters, Vol.29, No.24, 1993, pp.2094-2095.
[16] Horster, P., Michels, M., and Petersen, H., " Comment: digital signature with (t, n) shared verification based on discrete logarithms, " Electronics Letters, Vol.31, No.14, 1995, pp.1137.
[17] Lee, W.B., and Chang, C.C., " Comment: digital signature with (t, n) shared verification based on discrete logarithms, " Electronics Letters, Vol.31, No.3, 1995, pp.176-177.
[18] Nyberg, K., and Rueppel, R.A., " A new signature scheme based on the DSA given message recovery, " Proceedings of the First ACM Conference on Computer and Communications Security, 1993, pp.58-61.
[19] Nyberg, K., and Rueppel, R.A., " Message recovery for signature schemes based on the discrete logarithm, " Advances in Cryptoloty-EUROCRYPT ' 94, Springer-Verlag, Berlin, 1994, pp.175-190.
[20] Piveteau, J.M., " New signature scheme with message recovery, " Electronic Letters, Vol.29, No.25, 1993, pp.2185-2186.
[21] Pinch, R.G.E., " Comment: new signature scheme with message recovery, " Electronics Letters, Vol.30, No.11, 1994, pp.852.
[22] Lin, C.C., and Laih, C.S., " Cryptanalysis of Nyberg-Ruppel ' s message recovery scheme, " IEEE Communication Letters, Vol.4, No.7, 2000, pp.231-232.
[23] Chen, K., " Signature with message recovery, " Electronics Letters, Vol.34, No.20, 1998, pp.1934.
[24] Mitchell, C.J., and Yeun, C.Y., " Comment: signature with message recovery, " Electronics Letters, Vol.35, No.3, 1999, pp.217.
[25] Horster, P., Michels, M., and Petersen, H., " Authenticated encryption schemes with low communication costs, " Electronics Letters, Vol.30, No.15, 1994, pp.1212-1213.
[26] Lee, W.B. and Chang, C.C., " Authenticated encryption scheme without using a one way function, " Electronics Letters, Vol.31, No.19, 1995, pp.1656-1657.
[27] Hsu, C.L. and Wu, T.C., " Authenticated encryption scheme with (t, n) shared verification, " IEE Proceedings — Computers and Digital Techniques, Vol.145, No.2, 1998, pp.117-120.
[28] Araki, S., Uehara, S., and Imamura, K., " The limited verifier signature and its application, " IEICE Trans. on Fundamentals, Vol.E82-A, No.1, 1999, pp.63-68.
[29] Yeun, C.Y., " Digital signature with message recovery and authenticated encryption(signcryption)-a comparison, " Crypto & Coding ' 99, LNCS 1746, 1999, pp.307-312.
[30] Wang, C.T., Chang, C.C., and Lin, C.H., " Generalization of threshold signature and authenticated encryption for group communications, " IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, Vol.E83-A, No.6, 2000, pp.1228-1237.
[31] Hsu, C.L., Wu, T.S., and Wu, T.C., " Improvements of generalization of threshold signature and authenticated encryption for group communications, " Information Processing Letters, Vol.81, No.1, 2002, pp.41-45.
[32] Tseng, Y.M., Jan, J.K., and Chien, H.Y., " On the security of generalization of threshold signature and authenticated encryption, " IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, Vol.E84-A, No.10, 2001, pp.2606-2609.
[33] Wu, T.S., and Hsu, C.L., " Convertible authenticated encryption scheme, " The Journal of Systems and Software, Vol.62, 2002, pp.205-209.
[34] Hwang, S.J., Chang, C.C., and Yang, W.P., " Authenticated encryption schemes with message linkage, " Information Processing Letters, Vol.58, 1996, pp.189-194.
[35] Lee, W.B. and Chang, C.C., " Authenticated encryption schemes with linkage between message blocks, " Information Processing Letters, Vol.63, No.5, 1997, pp.247-250.
[36] Tseng, Y.M., and Jan, J.K., " An efficient authenticated encryption scheme with message linkages and low communication costs, " Journal of Information Science and Engineering, Vol.18, No.1, 2002, pp.41-46.
[37] Huang, H.F., and Chang, C.C., " Enhancement of the authenticated encryption schemes with message linkages, " The Second International Workshop for Asian Public Key Infrastructures, 2002, Taiwan.
[38] Tseng, Y.M., Jan, J.K., and Chien, H.Y., " Authenticated encryption schemes with message linkages for message flows, " Computers and

Electrical Engineering, Vol.29, 2003, pp.101-109.
[39] Tseng, Y.M., Jan, J.K., and Chien, H.Y., “ Digital signature with message recovery using self-certified public keys and its variants, ” Applied Mathematics and Computation, Vol.136, 2003, pp.203-214.
[40] Koblitz, N., “ Elliptic curve cryptosystems, ” Mathematics of Computation, Vol.48, 1987, pp.203-209.
[41] Miller, V.S., “ Uses of elliptic curves in cryptography, ” Advances in Cryptology-Crypto'85, Proceedings, Lecture Notes in Compute Science, New York, NY: Springer-Verlag, No.218, 1985, pp.417-426.
[42] Koblitz, N., “ A course in number theory and cryptography, ” New York, NY: Springer-Verlag, Second edition, 1994.
[43] Koblitz, N., Menezes, A., and Vanstone, S., “ The state of elliptic curve cryptography, ” Designs, Codes and Cryptography, Vol.19, 2000, pp.173-193 [44] Menezes, A., Okamoto, T., and Vanstone, S., “ Reducing elliptic curve logarithms to logarithms in a finite field, ” IEEE Transactions on Information Theory, Vol. 39, 1993, pp. 1639-1646.
[45] Torii, N., and Yokoyama, K., “ Elliptic curve cryptosystem, ” FUJITSU Sci. Tech. J., 36,2, 2000, pp.140-146.
[46] Guajardo, J., and Paar, C., “ Efficient algorithms for elliptic curve cryptosystems, ” Advances in Cryptology-Crypto'97, Lecture Notes in Compute Science, Springer-Verlag, No.1294, 1997, pp.342-356.
[47] Agnew, G., Mullin, R., and Vanstone, S., “ An implementation of elliptic curve cryptosystems over , ” IEEE Journal on Selected Areas in Communications, Vol.11, 1993, pp.804-813.
[48] Shamir, A., “ How to share a secret, ” Commum. ACM, Vol.22, 1979, pp.612-613.
[49] Menezes, A.J., Van Oorschot, P.C., and Vanstone, S.A., “ Handbook of applied cryptography, ” CRC Press, 1996.