A Concurrent Signature Scheme with Anonymity and Identification

Shin-Jia Hwang* and Te-Yu Hsu

Department of Computer Science and Information Engineering,
TamKang University,
Tamsui, Taipei Hsien, 251, Taiwan
sjhwang@mail.tku.edu.tw

Received 20 September 2009; Revised 5 March 2010; Accepted 5 April 2010

Abstract. For the privacy protection, Nguyen first proposed an asymmetric concurrent signature scheme with signers' anonymity in 2005. Except correctness, unforgeability, and fairness, Nguyen's scheme satisfies two new properties: Anonymity and unlinkability. To satisfy the anonymity property, Nguyen's scheme has identification flaw that signers cannot identify each other during the exchange protocol. So an attacker makes use of this flaw to trick signers to exhaust signers' computation resources. However, the concurrent signature schemes with signers' ambiguity do not have this identification flaw. So the identification property is defined for the concurrent signature scheme with signers' anonymity. Then our asymmetric concurrent scheme is proposed to provide both anonymity and identification. Our improved scheme satisfies identification, anonymity, and unlinkability at the same time. With identification, anonymity, and unlinkability, the signers' privacy is protected well without flaws.

Keywords: concurrent signatures, anonymity, identification, privacy, signature schemes

References

[1] E.F. Brickell, D. Chaum, I.B. Damgård, J. V. D. Graaf, "Gradual and Verifiable Release of a Secret," *Advances in Cryptology-Crypto 1987*, LNCS 293, Springer-Verlag, New York, USA, pp.156-166, 1987.

[2] R. Cleve, "Controlled Gradual Disclosure Schemes for Random Bits and Their Applications," *Advances in Cryptology-CRYPTO 1989*, LNCS 435, Springer-Verlag, New York, USA, pp.573-588, 1990.

[3] I.B. Damgård, "Practical and Provably Secure Release of a Secret and Exchange of Signatures," *Advances in Cryptology-Eurocrypt 1993*, LNCS 765, Springer-Verlag, New York, USA, pp. 200-217, 1994.

[4] S. Even, O. Goldreich, A. Lempel, "A Randomized Protocol for Signing Contracts," *Communications of the ACM*, Vol. 28, No. 6, pp.637-647, 1985.

[5] O. Goldreich, "Sending Certified Mail Using Oblivious Transfer and a Threshold Scheme," *Technical Report*, Computer Science Department, Israel Institute of Technology, 1984.

[6] O. Goldreich, "A Simple Protocol for Signing Contracts," *Advances in Cryptology-CRYPTO 1983*, Springer-Verlag, New York, USA, pp.133-136, 1984.

[7] M. Abadi, N. Glew, B. Horne, B. Pinkas, "Certified E-mail with a Light On-line Trusted Third Party: Design and Implementation," *Proceedings of the 11th International World Wide Web Conference (WWW 2002)*, Honolulu, Hawaii, USA, pp. 387-395, 2002.

[8] M.K. Franlin and M.K. Reiter, "Fair Exchange with a Semi-Trusted Third Party," *Proceedings of the 4th ACM Conference on Computer and Communications Security*, Zurich, Switzerland, pp.1-5, 1997.

[9] M.K. Franlin and G. Tsudik, "Secure Group Barter: Multi-party Fair Exchange with Semi-trusted Neutral Parties," *Proceedings of Financial Cryptology- Eurocrypt 1998*, LNCS 1465, Springer-Verlag, New York, USA, pp.90-102,

* Correspondence author

1998.

[10] N. Asokan, V. Shoup, M. Waidner, "Optimistic Fair Exchange of Digital Signatures," *Advances in Cryptology-Eurocrypt 1998*, LNCS 1403, Springer-Verlag, New York, USA, pp.591-606, 1998.

[11] C. Cachin and J. Camenisch, "Optimistic Fair Secure Computation," *Advances in Cryptology-Crypto 2000*, LNCS. 1880, Springer-Verlag, New York, USA, pp.94-112, 2000.

[12] J.A. Garay, M. Jakobsson, P. MacKenzie, "Abuse-free Optimistic Contract Signing," *Advances in Cryptology-CRYPTO 1999*, LNCS 1666, Springer-Verlag, New York, USA, pp.449-466, 1999.

[13] B. Pfitzmann, M. Schunter, M. Waidner, "Optimal Efficiency of Optimistic Contract Signing," *Proceedings of the 7th Annual ACM Symposium on Principles of Distributed Computing*, New York, USA, pp.113-122, 1998.

[14] L. Chen, C. Kudla, K.G. Paterson, "Concurrent Signatures," *Advances in Cryptology- Eurocrypt 2004*, LNCS 3207, Springer-Verlag, New York, USA, pp. 287-305, 2004.

[15] M. Abe, M. Ohkubo, K. Suzuki, "1-out-of-n Signatures from a Variety of Keys," *Advances in Cryptology-Asiacrypt 2002*, LNCS 2501, Springer-Verlag, New York, USA, pp. 415-432, 2002.

[16] R.L. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret," Advances in Cryptology- *Asiacrypt* 2001, LNCS 2248, Springer-Verlag, New York, USA, pp.552-565, 2001.

[17] W. Susilo, Y. Mu, F. Zhang, "Perfect Concurrent Signature Schemes," *Proceedings of Information and Communications Security Conference (ICICS 2004)*, LNCS 3269, Springer-Verlag, New York, USA, pp. 14-26, 2004.

[18] G. Wang, F. Bao, J. Zhou, "The Fairness of Perfect Concurrent Signatures," *The 8th International Conference on Information and Communications Security (ICICS 2006)*, LNCS 4307, Springer-Verlag, New York, USA, pp. 435-451, 2006.

[19] K. Nguyen, "Asymmetric Concurrent Signatures," *Proceedings of Information and Communications Security Conference (ICICS 2004)*, LNCS 3783, Springer-Verlag, New York, USA, pp. 181-193, 2005.

[20] Y.C. Chen, "On the Research of Fair Exchange Protocols and Micropayment Schemes," *Master Thesis*, National Central University, Taiwan, ROC, 2006.

[21] C.P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Advances in Cryptology-Crypto 1989*, LNCS 435, Springer-Verlag, New York, USA, pp.239-252, 1990.

[22] G. Ateniese, "Efficient Verifiable Encryption (and Fair Exchange) of Digital Signature," *Proceedings of AMC Conference on Computer and Communications Security (CCS'99)*, New York, USA, pp. 138-146, 1999.