Fair and Practical Electronic Transaction Scheme for Privacy-Protection Policy without Trusted Third Party based on Random Oracle Model

Hong-Feng Zhu[1, *], Tian-Hua Liu[1], and Jeng-Shyang Pan[2]

[1] Software College,

Shenyang Normal University,

No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034, China

zhuhongfeng1978@163.com, liutianhua@sina.com

[2] Department of Electrical Engineering,

National Kaohsiung University of Applied Sciences,

Kaohsiung 807, Taiwan, ROC

jspan@cc.kuas.edu.tw

Received 15 October 2011; Revised 15 January 2012; Accepted 30 January 2012

Abstract. Many applications of E-business need to solve the following problems of privacy and fairness for counter parties: without loss of generality for two traders, how to assure their clandestine trade with satisfying both sides, or protect rights when either of traders has a dispute? In this paper we develop a novel scheme, called FKESS, to settle the aforementioned typical problem. Its main idea is to judiciously choose a proof (called a keystone) during both sides agree on a session key. We give a full specification of this scheme, including how to realize specific properties by analyzing cryptography tools, how to define the complete fairness and design the scheme, and how to prove the scheme based on random oracle model. A primary advantage of the scheme is that it can be adopted among any traders in private without the trusted third party involved, but when the keystone will be published any one can become the arbiter. We contrast with typical related literature to evaluate the scheme, and show the significant performance improvements on the existing scheme.

Keywords: security protocol, key exchange, fair signature, E-business

Acknowledgement

This research was supported by Liaoning Provincial Natural Science Foundation of China (Grant No. 20102202, 201102201), Foundation of Liaoning Educational Committee in China (No. 2009A665) and Liaoning Baiqianwan Talents Program.

References

[1] D. Boneh and M. Naor, "Timed Commitments," in *Proceeding of Advances in Cryptology - CRYPTO 2000*, Santa Barbara, California, USA, Vol. 1880, pp. 236-254, 2000.

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

[3] O. Goldreich, "A Simple Protocol for Signing Contracts," in *Proceeding of Advances in Cryptology - CRYPTO 1983*, Santa Barbara, California, USA, pp. 133-136, 1983.

[4] F. Bao, "Colluding Attacks to a Payment Protocol and Two Signature Exchange Schemes," in *Proceeding of Advances in Cryptology - ASIACRYPT 2004*, Jeju Island, Korea, Vol. 3329, pp. 417-429, 2004.

*Correspondence author

[5] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proceeding of Advances in Cryptology - EUROCRYPT 2003*, Warsaw, Poland, Vol. 2656, pp. 416-432, 2003.

[6] Y. Dodis and L. Reyzin, "Breaking and Repairing Optimistic Fair Exchange from PODC 2003," in *Proceedings of the 3rd ACM workshop on Digital rights management*, Washington, DC, USA, pp. 47-54, 2003.

[7] J. M. Park, E. K. P. Chong, H. J. Siegel, "Constructing Fair-exchange Protocols for E-Commerce via Distributed Computation of RSA Signatures," in *Proceedings of the 22th annual symposium on Principles of distributed computing*, Boston, Massachusetts, USA, pp. 172-181, 2003.

[8] J. Zhou, R. Deng, F. Bao, "Some Remarks on a Fair Exchange Protocol," in *Proceedings of the 3rd International Workshop on Practice and Theory in Public Key Cryptosystem*, Melbourne, Victoria, Australia, pp. 46-57, 2000.

[9] N. Asokan, V. Shoup, M. Waidner, "Optimistic Fair Exchange of Digital Signatures," in *Proceeding of Advances in Cryptology - EUROCRYPT 1998*, Espoo, Finland, Vol. 1403, pp. 591-606, 1998.

[10] F. Bao, R. H. Deng, W.B. Mao, "Efficient and Practical Fair Exchange Protocols with Off-line TTP," in *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 77-85, 1998.

[11] A. Nenadic, N. Zhang, B. M. G. Cheetham, C. A. Goble, "RSA-based Certified Delivery of E-Goods Using Verifiable and Recoverable Signature Encryption," *Journal of Universal Computer Sciences*, Vol. 11, No. 1, pp. 175-192, 2005.

[12] L. Chen, C. Kudla, K. G. Paterson, "Concurrent Signature," in *Proceeding of Advances in Cryptology - EUROCRYPT 2004*, Interlaken, Switzerland, Vol. 3027, pp. 287-305, 2004.

[13] R. L. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret," in *Proceeding of Advances in Cryptology - ASIACRYPT 2001*, Gold Coast, Australia, Vol. 2248, pp. 552-565, 2001.

[14] M. Abe, M. Ohkubo, K. Suzuki, "1-out-of-n Signatures from a Variety of Keys," in *Proceeding of Advances in Cryptology - ASIACRYPT 2002*, Queenstown , New Zealand, Vol. 2501, pp. 415-432, 2002.

[15] G. Wang, F. Bao, J.Y. Zhou, "The Fairness of Perfect Concurrent Signature," in *Proceeding of the 8th International Conference on information and Communications Security*, Raleigh, NC, USA, pp. 435-451, 2006.

[16] S.H. Seo, K.Y. Choi, J.Y. Hwang, S.J. Kim, "Efficient Certificateless Proxy Signature Scheme with Provable Security," *Information Sciences*, Vol. 188, pp. 322-337, 2012.