IIM > Vol.1 No.3, December 2009

OPEN ACCESS

Secure Signature Protocol

PDF (Size:214KB) PP. 174-179 DOI: 10.4236/iim.2009.13026

Author(s)

Shundong LI, Daoshun WANG, Yiqi DAI

ABSTRACT

This paper studies how to take advantage of other's computing ability to sign a message with one's private key without disclosing the private key. A protocol to this problem is presented, and it is proven, by well known simulation paradigm, that this protocol is private.

KEYWORDS

cryptography, secure computation, signature, service, protocol

Cite this paper

S. LI, D. WANG and Y. DAI, "Secure Signature Protocol," *Intelligent Information Management*, Vol. 1 No. 3, 2009, pp. 174-179. doi: 10.4236/iim.2009.13026.

References

[1] J. Feigenbaum, "Can you take advantage of someone without having to trust him," LNCS, Vol. 218, Springer- verlag, N.Y., pp. 477–488, 1986.

[2] R. Cramer and I. Damgaard, "Introduction to secure multi-party computations," In: Contemporary Cryptology, pp. 41–87, Advanced Courses in Mathematics CRM Barcelona, Birkhauser, at: http://homepages.cwi.nl/ cramer/, 2005.

[3] O. Goldreich, "Foundations of cryptography: Basic applications," Cambridge University Press, London, 2004.

[4] W. L. Du and M. J. Atallah, "Secure multi-party computaion problems and their applications: A review and open problems." In: Proceedings of New Security Paradigms Workshop, ACM Press, New York, pp. 13–22, 2001.

[5] S. Goldwasser, "Multi-party computations: Past and present [C]," In Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing (Santa Barbara, CA, August, 1997), ACM Press, New York, pp. 21–24, 1997.

[6] S. D. Li, D. S. Wang, Y. Q. Dai, and P. Luo, "Symmetric cryptographic solution to Yao's millionaires' problem and an evaluation of secure multiparty computations," Information Sciences, Vol. 178, pp. 244–255, 2008.