A Verifiable Identity-based RSA Multisignature Scheme for Mobile Communications

Ya-Fen Chang*, Po-Chun Chen, and Tse-Hsiang Chen

Department of Computer Science and Information Engineering

National Taichung Institute of Technology

Taichung 404, Taiwan, R.O.C.

cyf@cs.ccu.edu.tw, jc7003@hotmail.com, q204227@hotmail.com

Received 15 July 2009; Revised 15 August 2009; Accepted 10 September 2009

Abstract. Digital signature provides origination, integrity and non-repudiation. Multisignature is a special type of digital signature, where multiple users cooperate to sign one message. On the other hand, RSA is a popular cryptosystem, and using identities to be public keys is a convenient approach for identification. So, Harm and Ren proposed an identity-based RSA multisignature scheme which combines Shamir's identity-based signature scheme in 2008. Later, Chang et al. indicated that Harm and Ren's scheme suffers from some drawbacks in 2009. In this manuscript, we will propose a secure identity-based RSA multisignature scheme to improve Harm and Ren's scheme. Moreover, identity-based public keys will not place extra burden on users because users do not need to verify certificates in advance. The proposed multisignature scheme can be applied for mobile communications.

Keywords: RSA, identity-based, multisignature, signature.

References

[1] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the Association for Computing Machinery*, Vol. 21, No. 2, pp. 120-126, 1978.

[2] Y. Desmedt, "Society and Group Oriented Cryptography: A New Concept," *Advances in cryptology - Crypto'87: Lecture Notes in Computer Science*, Vol. 293, Berlin, Springer-Verlag, pp.120-127, 1987.

[3] C. C. Chang and H. C. Lee, "A New Generalized Group Oriented Cryptoscheme without Trusted Centers," *IEEE journal on Selected Areas in Communications*, Vol. 11, No. 5, pp.725-729, 1993.

[4] D. Chaum and E. van Heyst, "Group Signatures," *Advances in cryptology – EuroCrypt'91: Lecture Notes in Computer Science*, Vol. 547, Berlin, Springer-Verlag, pp.257-265, 1991.

[5] A. Shamir, "Identiby-based Cryptosystem and Signature Schemes," *Advances in cryptology - Crypto'84: Lecture Notes in Computer Science*, Vol. 196, Berlin, Springer-Verlag, pp. 47-53, 1985.

[6] M. Bellare, C. Nameprempre, G. Neven, "Security Proofs for Identity-based Identification and Signature Schemes," *Advances in cryptology - EurcoCrypt'04: Lecture Notes in Computer Science*, Vol. 3027, Berlin, Springer-Verlag, pp. 268-286, 2004.

[7] L. Harn and J. Ren, "Efficient Identity-based RSA Multisignatures," *Computers & Security*, Vol. 27, pp.12-15, 2008.

[8] Y. F. Chang, Y. C. Lai, M. Y. Chen, "Further Remarks on Identity-based RSA Multisignature," *NTIT technical report*, 2009.

* Correspondence author