IIM > Vol.1 No.1, July 2009

OPEN ACCESS

Investigations on Simultaneously Secure IBE Scheme and Security Proofs under RO and Non-RO Model

PDF (Size:510KB) PP. 6-13 DOI: 10.4236/iim.2009.11002

Author(s)

Zhengtao JIANG, Yongbin WANG, Yong WANG, Yumin WANG

ABSTRACT

This paper analyses security mechanism and authentication, key agreement protocol of 3G system amply, puts forward a amelioration scheme. This scheme assures security communications without credible VLR. This paper analyses ameliorative protocol and resolves the security communications problem between MS and HLR.

KEYWORDS

3G Security, 3G Security Structure, 3G authentication and key agreement protocol Security arith- metic

Cite this paper

Z. JIANG, Y. WANG, Y. WANG and Y. WANG, "Investigations on Simultaneously Secure IBE Scheme and Security Proofs under RO and Non-RO Model," *Intelligent Information Management*, Vol. 1 No. 1, 2009, pp. 6-13. doi: 10.4236/iim.2009.11002.

References

[1] Wang Yu-Min, Liu Jian-Wei. Communication network security- Theory and technique. Xidian University Press, 2002, 5 (王育民, 劉建偉. 通信網的安全—理論與技術. 西安電子科技大學出版社, 2002, 5).

[2] PKI. http://www.pki-page.org/

[3] Shamir A.. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, LNCS 196, 1984, Berlin: Springer-Verlag, 47-53.

[4] Tanaka H.. A realization scheme for the identity-based crypto-system. Advances in Cryptology-Crypto'87, LNCS 293, 1987, Berlin: Springer-Verlag, 341-349.

[5] Hühnlein D., Jacobson, M. Weber D.. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders. Selected Areas in Cryptography, LNCS 2012, 2000, Berlin: Springer-Verlag, 275-287.

[6] Sakai R., Ohgishi K., Kasahara M.. Cryptosystems based on pairing. Symposium on Cryptography and Information Secu-rity-SCIS’00, 2000, Okinawa, Japan, 26-28.

[7] Ma Chun-Bo, Ao Jun, He Da-Ke. Multi-Signature and Group Signature Based on Bilinear Pairing. Chinese Journal of Com-puters, 2005, 28(9): 1558-1563 (in Chinese) (馬春波, 敖珺, 何大可. 基於雙線性映射的多重簽名與群簽名. 電腦學報, 2005, 28(9): 1558-1563).

[8] Boyen X., Waters B. Full-domain subgroup hiding and con-stant-size Group signatures. Advances in Cryptology-PKC'07, LNCS 4450, 2007, Berlin: Springer-Verlag, 1-15.

[9] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. Advances in Cryptology-Crypto'01, LNCS 2139, 2001, Berlin: Springer-Verlag, 213-22.

[10] Canetti R., Halevi S., Katz J. A forward-secure public-key en-cryption scheme. Advances in Cryptology-EUROCRYPT'03, LNCS 2656, 2003, Berlin: Springer-Verlag, 255-271.

- Open Special Issues
- Published Special Issues
- Special Issues Guideline

IIM Subscription

Most popular papers in IIM

About IIM News

Frequently Asked Questions

Recommend to Peers

Recommend to Library

Contact Us

[11] Canetti R., Halevi S., Katz J. Chosen-ciphertext security from identity-based encryption. Advances in Cryptology-EUROC RYPT'04, LNCS 3027, 2004, Berlin: Springer-Verlag, 207-22.

[12] Boneh D., Boyen X. Efficient selective-ID secure identity based encryption without random oracles. Advances in Cryptol-ogy-EUROCRYPT' 04, LNCS 3027, 2004, Berlin: Springer- Verlag, 223-238.

[13] Boneh D., Boyen X. Secure identity based encryption without random oracles. Advances in Cryptology-CRYPTO 2004, LNCS 3152, 2004, Berlin: Springer-Verlag, 443-59.

[14] Waters B. Efficient identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT'05, LNCS 3494, 2005, Berlin: Springer-Verlag, 114-127.

[15] Goyal V. Reducing Trust in the PKG in Identity Based Crypto-systems. Advances in Cryptology –CRYPTO'07, NCS 4622, Berlin: Springer, 2007, 430-447.

[16] Washington L. C.. Elliptic Curve Number Theory and Cryptog-raphy. New York, CRC Press, 2003.

[17] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. SIAM Journal of Computing, 2003, 32(3): 586-615.

[18] Ming Yang. Study and design of universal designated verifier signature schemes [Ph. D. dissertation]. Xi'an: Xidian University, 2007, 12 (in Chinese) ([明07] 明洋. 廣義指定驗證者簽名體制的研究和設計[博士論文]. 西安電子科技大學, 2007, 12).