Cryptology ePrint Archive: Report 2011/224

Cryptanalysis and Improvement of an Efficient CCA Secure PKE Scheme

Xu An Wang and Liqiang Wu and Xiaoyuan Yang and Huaqun Wang

Abstract: Recently in Chinese Journal of Computers, Kang et al. [12] proposed an efficient CCA secure public key encryption (PKE) scheme, and claimed that it is more efficient in the public/private keys than the famous CS98 and BMW05 CCA secure public key encryption scheme. However, in this paper we will show that their proposal is not secure at all. Furthermore, we improve their scheme to be a secure one and prove its security.

Category / Keywords: public-key cryptography /

Date: received 7 May 2011, last revised 7 May 2011

Contact author: wangxahq at yahoo com cn

Available formats: PDF | BibTeX Citation

Version: 20110511:104746 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]