Cryptology ePrint Archive: Report 2011/379

Cryptanalysis and improvement of a certificateless multi-proxy signature scheme

Miaomiao Tian and Wei Yang and Liusheng Huang

Abstract: Multi-proxy signature allows an original signer authorizing a proxy group as his proxy agent and only the cooperation of all proxy signers in the group can create a proxy signature on behalf of the original signer. Recently, Jin and Wen defined a formal model of certificateless multi-proxy signature and proposed a concrete scheme. They claimed that their scheme is provably secure in their security model. Unfortunately, by giving concrete attacks, we show that Jin-Wen's certificateless multi-proxy signature scheme is not secure according to their security model. Possible improvements of their scheme are also suggested to prevent these attacks.

Category / Keywords: Certificateless cryptography; Multi-proxy signature; Bilinear pairing; Cryptanalysis

Date: received 12 Jul 2011, last revised 12 Jul 2011

Contact author: miaotian at mail ustc edu cn

Available formats: PDF | BibTeX Citation

Version: 20110713:010607 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]