Cryptology ePrint Archive: Report 2013/093

On the security of a certificateless aggregate signature scheme

Lin Cheng and Qiaoyan Wen and Zhengping Jin and Hua Zhang and Liming Zhou

Abstract: Aggregate signature can combinensignatures on nmessages fromnusers into a single short signature, and the resulting signature can convince the verifier that thenusers indeed signed the ncorresponding messages. This feature makes aggregate signature very useful especially in environments with low bandwidth communication, low storage and low computability since it greatly reduces the total signature length and verification cost. Recently, Xiong et al. presented an efficient certificateless aggregate signature scheme. They proved that their scheme is secure in a strengthened security model, where the “malicious-but-passive” KGC attack was considered. In this paper, we show that Xiong et al.’s certificateless aggregate signature scheme is not secure even in a weaker security model called “honest-but-curious” KGC attack model.

Category / Keywords: public-key cryptography / cryptanalysis

Date: received 20 Feb 2013

Contact author: stonewoods302 at 163 com