Cryptology ePrint Archive: Report 2011/664

On the Security of ID Based Signcryption Schemes

S. Sharmila Deva Selvi and S. Sree Vivek and Dhinakaran Vinayagamurthy and C. Pandu Rangan

Abstract: A signcryption scheme is secure only if it satisfies both the confidentiality and the unforgeability properties. All the ID based signcryption schemes presented in the standard model till now do not have either the confidentiality or the unforgeability or both of these properties. Cryptanalysis of some of the schemes have been proposed already. In this work, we present the security attacks on `Secure ID based signcryption in the standard model' proposed by Li-Takagi and `Further improvement of an identity-based signcryption scheme in the standard model' by Li et al. and the flaws in the proof of security of `Efficient ID based signcryption in the standard model' proposed by Li et al., which are the recently proposed ID based signcryption schemes in the standard model. We also present the cryptanalysis of `Construction of identity based signcryption schemes' proposed by Pandey-Barua and the cryptanalysis of `Identity-Based Signcryption from Identity-Based Cryptography' proposed by Lee-Seo-Lee. These schemes present the methods of constructing an ID based signcryption scheme in the random oracle model from an ID based signature scheme and an ID based encryption scheme. Since none of the existing schemes in the standard model are found to be provably secure, we analyse the security of signcryption schemes got by directly combining an ID based signature scheme and an ID based encryption scheme in the standard model.

Category / Keywords: public-key cryptography / cryptanalysis, provable security, ID-based signcryption

Date: received 8 Dec 2011, last revised 22 Sep 2012

Contact author: sharmioshin at gmail com