Cryptology ePrint Archive: Report 2011/217

Identity Based Deterministic Signature Scheme Without Forking-Lemma

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

Abstract: Since the discovery of identity based cryptography, a number of identity based signature schemes were reported in the literature. Although, a lot of identity based signature schemes were proposed, the only identity based deterministic signature scheme was given by Javier Herranz. This signature scheme uses Schnorr signature scheme for generating the private key of the users and uses BLS short signature scheme for generating users signature. The security of this scheme was proved in the random oracle model using forking lemma. In this paper, we introduce a new identity based deterministic signature scheme and prove the security of the scheme in the random oracle model, without the aid of forking lemma. Hence, our scheme offers tighter security reduction to the underlying hard problem than the existing identity based deterministic signature scheme.

Category / Keywords: public-key cryptography / Identity Based Cryptography, Deterministic, Signature, Tight Security, Random Oracle Model, Provable Security, Without Forking-Lemma.

Date: received 5 May 2011, last revised 12 Mar 2012

Contact author: sharmioshin at gmail com,ssreevivek@gmail com,prangan55@gmail com