Cryptology ePrint Archive: Report 2011/695

Deterministic Identity Based Signature Scheme and its Application for Aggregate Signatures

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

Abstract: The revolutionary impact offered by identity based cryptography is phenomenal. This novel mechanism was first coined by Adi Shami 1984. Since then, several identity based signature schemes were reported. But surprisingly, none of the identity based signature scheme is having property of determinism and does rely on bilinear pairing. We think positively in answering this long standing question of realizing deterministic identity based signature in composite order groups and we succeed in developing a signature scheme based on RSA assumption and is determin It is indeed helpful in devising variants of signature primitive. Fully aggregateable identity based signature schemes without prior communication between the signing parties is an interesting issue in identity based cryptography. It is easy to see that deterministic identity based signature schen lead to full aggregation of signatures without the aforementioned overhead. The major contribution of this paper is a novel deterministic identity b signature scheme whose security relies on the strong RSA assumption and random oracles. Based on this newly proposed deterministic identity based signature scheme, we design an identity based aggregate signature scheme which achieves full aggregation in one round. We formally prov schemes to be existentially unforgeable under adaptive chosen message and identity attack.

Category / Keywords: public-key cryptography / Identity Based Deterministic Signature, Aggregate Signature, Full Aggregation, Random Ora Model, Provable Security

Date: received 21 Dec 2011

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