Certificateless Aggregate Signcryption Schemes

Ziba Eslami [*] Nasrollah Pakniat

Department of Computer Science, Shahid Beheshti University, G.C.,Tehran, Iran

Abstract

The concept of an aggregate signcryption scheme was first introduced in 2009 by Selvi S.S.D. et. al. in the identity-based setting. The aggregation process of these schemes reduces the amount of exchanged information and is particularly useful in low-bandwidth communication networks and computationally-restricted environments. In this paper, we define a suitable security model for certificateless aggregate signcryption schemes and propose an example which we prove is secure in the random oracle model under the gap Bilinear Diffie-Hellman and computational Diffie-Helman intractability assumptions.

Key words: Certificateless cryptography, Identity based, Aggregate signcryption, Random oracle model, Bilinear pairing

[*] Corresponding author. Tel.: +982129903005; fax: +982122431655
Email addresses: z_eslami@sbu.ac.ir (Ziba Eslami), n.pakniat@sbu.ac.ir (Nasrollah Pakniat).