Cryptology ePrint Archive: Report 2011/361

The Exact Security of a Stateful IBE and New Compact Stateful PKE Schemes

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

Abstract: Recently, Baek et al. proposed a stateful identity based encryption scheme with compact ciphertext and commented that the security of the scheme can be reduced to the Computational Bilinear Diffie Hellman (CBDH) problem. In this paper, we formally prove that the security of the stateful identity based encryption scheme by Baek et al. cannot be reduced to the CBDH problem. In fact, we show that the challenger will confront the Y-Computational problem while providing the decryption oracle access to the adversary. We provide the exact and formal security proof for the scheme, assuming the hardness of the Gap Bilinear Diffie Hellman (GBDH) problem. We also propose two new stateful public key encryption scheme with ciphertext verifiability. Our schemes offer more compact ciphertext when compared to all existing stateful public key encryption schemes with ciphertext verifiability. We have proved all the schemes in the random oracle model.

Category / Keywords: Stateful Identity Based Encryption, Adaptive Chosen Ciphertext (CCA), Provable Security, Compact Ciphertext with/without Ciphertext Verification, Random Oracle model.

Date: received 4 Jul 2011, last revised 20 Mar 2012

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

Available formats: PDF | BibTeX Citation

Note: The previous draft had some subtle defects and it was pointed out by Dr. Gregory M. Zaverucha. We thank him for pointing out the defect in the previous draft, which helped us to improve the result.

Version: 20120320:060920 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]