Cryptology ePrint Archive: Report 2011/684

Identification Based Encryption with RSA-OAEP. Using SEM and Without

Rkia Aouinatou, Mostafa Belkasmi

Abstract: In this article we show how we can integrate the RSA (RSA-OAEP) into the IBE. Our prove can be make with either Standard Model or Random Oracle. We firstly develop the basic ideas made in this direction, so that to create a novel scheme with which we can signs and crypt at the same time. Then we give our new approach which conserves properly the syntax of the RSA classic. Additionally we compare our authentication with the signature of Shamir. More than that, in the RSA-IBE there is the problem of relating the exponent with an identity. Even if, there was some proposals in this direction, but they operate only with the Random Oracle. And in this article we will response to question of Xuhua Ding and Gene Tsudik, in order to propose an efficient exponent for an RSA-IBE. In the end of the article we give a useful appendix.

Category / Keywords: public-key cryptography / IBE, mRSA, SEM, RSA-IBE, Classic RSA, OAEP, CPA, CCA2, authentication, Shamir signature....

Date: received 16 Dec 2011

Contact author: rkiaaouinatou at yahoo fr

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20111223:120845 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]