Cryptology ePrint Archive: Report 2011/494

Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting

Carmit Hazay and Gert Læssøe Mikkelsen and Tal Rabin and Tomas Toft

Abstract: The problem of generating an RSA composite in a distributed manner without leaking its factorization is particularly challenging and useful in many cryptographic protocols. Our first contribution is the first non-generic fully simulatable protocol for distributively generating an RSA composite with security against malicious behavior. Our second contribution is complete Paillier [Pai99] threshold encryption scheme in the two-party setting with security against malicious behavior. Furthermore, we describe how to extend our protocols to the multiparty setting with dishonest majority.

Our RSA key generation is comprised of the following: (i) a distributed protocol for generation of an RSA composite, and (ii) a biprimality test for verifying the validity of the generated composite. Our Paillier threshold encryption scheme uses the RSA composite as public key and is comprised of: (i) a distributed generation of the corresponding secret-key shares and, (ii) a distributed decryption protocol for decrypting according to Paillier.

Category / Keywords: cryptographic protocols / Secure Two-Party Computation, RSA Generation, Threshold Encryption Scheme, Paillier

Publication Info: CT-RSA

Date: received 12 Sep 2011, last revised 27 Feb 2012

Contact author: gert l mikkelsen at alexandra dk