Cryptology ePrint Archive: Report 2011/319

Structure Preserving CCA Secure Encryption and Its Application to Oblivious Third Parties

Jan Camenisch and Kristiyan Haralambiev and Markulf Kohlweiss and Jorn Lapon and Vincent Naessens

Abstract: In this paper we present the first public key encryption scheme that is structure preserving, i.e., our encryption scheme uses only algebraic operations. In particular it does not use hash-functions or interpret group elements as bit-strings. This makes our scheme a perfect building block for cryptographic protocols where parties for instance want to prove, to each other, properties about ciphertexts or jointly compute ciphertexts. Our scheme is also very efficient and is secure against \dkg adaptive\blk{} chosen ciphertext attacks. We also provide a few example protocols for our scheme. For instance, a joint computation of a ciphertext\dkg, generated from two secret plaintexts from each party respectively\blk, where in the end, only one of the parties learns the ciphertext. This latter protocol serves as a building block for our second contribution which is a set of protocols that implement the concept of oblivious trusted third parties. This concept has been proposed before, but no concrete realization was known.

Category / Keywords: cryptographic protocols / public-key encryption, structure preserving, oblivious party

Date: received 16 Jun 2011

Contact author: markulf at microsoft com