Cryptology ePrint Archive: Report 2011/203

Key agreement based on homomorphisms of algebraic structures

Juha Partala

Abstract: We give a generalization of the Diffie-Hellman key agreement scheme that is based on the hardness of computing homomorphic images from an algebra to another. We formulate computational and decision versions of the homomorphic image problem and devise a key agreement protocol that is secure in the Canetti-Krawczyk model under the decision homomorphic image assumption. We also give an instantiation of the protocol using an additively homomorphic symmetric encryption scheme of Armknecht and Sadeghi. We prove that the instantiation is secure under the assumption that the encryption scheme is IND-CPA secure.

Category / Keywords: cryptographic protocols / public-key cryptography, key exchange, session key agreement, algebraic system, universal algebra

Date: received 21 Apr 2011

Contact author: juha partala at ee oulu fi