Cryptology ePrint Archive: Report 2013/114

Public Key Exchange Using Matrices Over Group Rings

Delaram Kahrobaei and Charalambos Koupparis and Vladimir Shpilrain

Abstract: We offer a public key exchange protocol in the spirit of Diffie-Hellman, but we use (small) matrices over a group ring of a (small) symmetric group as the platform. This ``nested structure'' of the platform makes computation very efficient for legitimate parties. We discuss security of this scheme by addressing the Decision Diffie-Hellman (DDH) and Computational Diffie-Hellman (CDH) problems for our platform.

Category / Keywords: public-key cryptography / public key exchange

Date: received 26 Feb 2013

Contact author: shpil at groups sci ccny cuny edu