Title: Diffie and Hellman are exchanging matrices over group rings

Author: Romana Linkeová

Department: Department of Algebra

Supervisor: Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: The Diffie-Hellman key exchange protocol is not suitable for devices with limited computational power while computing over group $\mathbb{Z}_p^*$ (where p is at least a 300-digit number). This fact led to the research of other algebraic structures, which may help in reducing the computational and storage cost of the protocol. D. Kahrobaei et al. posted in 2013 a proposal for working over a structure of small matrices and claimed that this modification will not affect the security of the protocol. We will attempt to attack this modification of the Diffie-Hellman protocol with the help of the theory of symmetric group representations. Firstly, we mention the basics of the theory of representations together with both the classical and the modified Diffie-Hellman protocol. Next, we elaborate the attack step by step and complement some of the steps with examples. Then, we probed security of the modified protocol against the baby-step giant-step attack.

Keywords: public key cryptography, symmetric group representations,
Diffie-Hellman protocol