Title: Proofs of security for digital signatures

Author: Anna Godušová

Department: Department of Algebra

Supervisor: Mgr. Štěpán Holub Ph.D.

Abstract: This paper deals with signature schemes that are used for digital signing of documents. More specifically it deals with the general signature schemes based on trapdoor permutation. In the beginning we prove the security of general scheme, further we quantify this security and we prove the security of signature scheme based on security of trapdoor permutation. Finally, we introduce modified scheme with probability hashing for better estimation of the security.

Keywords: digital signature, signature scheme, exact security, PSS