Specialized Digital Signatures Based on the Paillier Cryptosystem

Zinkova, Valentyna (School: Technic Lyceum of NTUU "KPI")

Okamoto-Uchiyama encryption scheme is one of the Paillier cryptosystem's foundations. Unfortunately, its "twin" signature scheme, properties and specialized kinds of digital signatures are not well explored. The purpose of this project was an analysis of structure and security of specialized digital signatures based on the degree residues over composite modulo. Paillier signature scheme calculates a signature (s1, s2) for given message m. Paillier cryptosystem's and Okamoto-Uchiyama encryption's security is based on the complexity of integer factorization and properties of degree □ residues modulo □. In this work Okamoto-Uchiyama digital signature was proposed similarly to the Paillier signature. The randomization property also was proved for both digital signatures. Blind digital signatures have been constructed similarly to the blind signature based on the RSA cryptosystem. The aggregate digital signature construction (so-called "multisignature") for both cryptosystems has been studied. It turned out that the construction of such signature is impossible without losing the scheme's security due to peculiarities of generating individual and collective keys. In addition, existential forgeries were constructed and classified in 3 types according to the structure of the s1 component. As a result, Okamoto-Uchiyama digital signature was presented. Also randomization was proved for both cryptosystems. Blind signatures were constructed. It was shown that aggregate signatures' building is impossible without losing security parameters. In addition, existential forgeries on the signature schemes were constructed. Obtained results can be used for analysis of existing digital signature schemes, including current standards, and for development of new secure cryptosystems.