Bleichenbacher-type Attacks on Generalized El-Gamal Schemes

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

The El-Gamal digital signature scheme (or its modifications) is a core for many modern cryptographic standards, but most of known attacks do not consider generalizations of this scheme. The purpose of this project was to develop Bleichenbacher-type attacks on generalized El-Gamal signatures and to consider protection mechanisms. The El-Gamal scheme calculates a signature (r,s) for given message m. A generalized El-Gamal scheme is parameterized with A,B,C values, which are predefined functions of m,r,s. A goal of Bleichenbacher's attack is a forgery of the valid signature for an arbitrary message without knowing a private key. Four classes of generalized schemes were considered with A,B,C values taken from sets {±m,±r,±s}, {±mr,±s,D}, {±ms,±r,D} and {±rs,±m,D} (120 schemes in total), where D is some constant. Schemes from the first class turned out to be vulnerable to original Bleichenbacher's attack, but known countermeasures are also applicable for them. For every scheme from next three classes, a Bleichenbacher-type attack was developed with one of three possible ways of r-value modifications. It was revealed that the known security countermeasures are not applicable for some of considered schemes. As a result, Bleichenbacher-type attacks were developed for every of 120 implementations of a generalized El-Gamal scheme. For every implemented scheme, one must consider security against this type of attack; also, security mechanisms must be created for some schemes. The obtained results can be used for analysis of existing digital signature schemes, including current standards, and for development of new secure cryptosystems and protection mechanisms against cryptanalytic attacks.