The assurance of security of electronic voting through the use of secrets sharing schemes and benaloh electronic voting scheme

Alexandru-Mihnea SPIRIDONICĂ, Marius PISLARU - Technical University "Gheorghe Asachi" of Iasi

Information security, in the context of using computers to perform electronic operations, electronic voting, electronic voting, electronic payment, electronic auctions, taken on major importance. There is only one way to ensure information security in such situations, through implementation of a proper software. Mainly, such a software is based directly on cryptographic primitives. In this paper we will make a general description of secrets sharing schemes and then we will concentrate at one of the most important electronic vote scheme, namely Benaloh scheme based on homomorphic secrets compose. The schemes are presented in a uniform manner, in order to highlight the differences between then. The operation mode of the schemes that assure a protection and a good functioning of the electronic voting is materialized through the exemplification of implementation of the Benaloh electronic voting scheme.