

The thesis aims to describe the [CLT15] scheme, which is based on the Diffie-Hellman scheme and uses multilinear maps over integers. This scheme enables an exchange of a key among several participants. The level κ scheme (using a κ -linear map) enables the exchange of a key among $\kappa + 1$ participants. The thesis introduces the basic terms, describes the needed theory, the base of which is the Chinese Remainder Theorem, and also the preparation and usage of the scheme. The correctness of the scheme is proved as well and the related requirements on the basic parameters are discussed.