In this work, we deal with cryptosystems which are provably secure even if we encrypt a key-dependent message. These cryptosystems are called KDM-secure.

First, we define KDM-security and discuss its relationship with other kinds of security, especially IND-CPA-security. Thereafter, we construct the public-key and the symmetric-key encryption scheme of Applebaum et al. (CRYPTO 2009) and we prove KDM-security of these cryprosystems with respect to the set of affine functions.

The security of our cryptosystems is based on the LWE problem and the LPN problem as its special case. We study these problems and their variants. Moreover, we give a brief introduction to lattices and hard lattice problems because there exist reductions from hard lattice problems to LWE.