In the thesis we study deniable encryption, as proposed by Canetti et al. (CRYPTO 1997). Standard encryption schemes guarantee good security level unless the adversary is able to force the sender and/or receiver to reveal her secret knowledge. Assuming that the adversary knows true ciphertext, the secret inputs usually commits the sender/receiver to the true plaintext. On the contrary, deniable scheme is equipped with algorithms that provide alternative secrets which makes the adversary believe that different plaintext was encrypted.

We recall the most important results in the area, in particular, the schemes of Canetti et al. (CRYPTO 1997), the scheme of Klonowski et al. (SOFSEM 2008) based on ElGamal encryption, schemes of O'Neill et al. (CRYPTO 2011), and schemes and impossibility result of Bendlin et al. (ASIACRYPT 2011). In addition to presenting known results in an unified environment, we deeply investigate simulatable-encryption based schemes. In particular, we construct a scheme that is bideniable, and both of its induced schemes are receiver-deniable (in the flexible/multi-distributional setting). We also disprove part of the results of Bendlin et al. (ASIACRYPT 2011) by showing that their construction of fully bideniable scheme is wrong. This result is verified using computer simulation. Therefore, construction of such scheme is an open problem again.