Slide attack is an attack against block ciphers which have all rounds the same. The success and the complexity of the attack is independent on the number of rounds. The original slide attack was mainly used on a Feistel structure, but very rarely on SPN networks, because in general, SPN networks have the last round diferent. This property does not allow to use normal slide attack. In the paper New slide attacks on almost self-similar ciphers by Orr Dunkelman, Nathan Keller, Noam Lasry, and Adi Shamir are introduced new slide attacks (four of them) which focus on SPN networks and they overcome a problem of the last round.

In this thesis we explain main idea of the original slide attack and the main idea of two new slide attacks – a slid sets attack and a slide attack using a hypercube of slid pairs. In both these attacks we create and use special structures of plaintexts and ciphertexts to get more pairs of plaintexts which we call slid pairs. Moreover, we explain some selected parts of two new slide attacks and we compute the complexity.