Abstract

Algebraic attacks represent the type of cryptanalysis that consists inpresenting a cipher as a system of equations and then solving that system. Unfortunately, such attacks are effective only for ciphers with simple algebraic structures, i.e. with a low algebraic degree of the round function. In the case of a well-designed cipher, it is difficult to find low-degree equations, and the complexity of the algorithms currently applied in algebraic attacks decreases when the system is overdefined. Despite this, these algorithms cannot perform an attack in a time shorter than a brute force attack. Therefore, in this thesis, the idea of algebraic attacks was used, but instead of constructing overdefined systems, the focus was put on creating a system of equations that would allow obtaining the smallest possible target problem in the form of QUBO, solved with the use of quantum annealing. The main purpose of this dissertation was to adapt the known model of transformation of the system of equations to the form of an optimization problem, solved by quantum annealing, to use it in algebraic attacks on block ciphers. The implementation of the process of solving optimization problems using a D-Wave quantum computer, which was selected as a tool to perform algebraic attacks was also taken into consideration in this thesis.

In the research, it was possible to find equations systems that give the smallest possible size of the QUBO problem for algorithms of the three most popular types of block cipher structures (SPN, ARX, and Feistel). For the AES standard, the focus was put on the non-linear layer. An effective system describing the Sbox was found, which allowed to obtain 70% fewer binary variables in the final QUBO problem, compared to the results published so far. Two different methods of constructing the system of equations over $\mathbb{Z}_{2^n}$ have been presented for the Speck cipher, focusing on the execution way of the cipher operations in $\mathbb{Z}_{2^n}$ and the order in which they are performed. Since the matrix of the obtained optimization problem was denser than in the case of the AES algorithm, the method of constructing the equations system over $\mathbb{F}_2$ was presented for the same Speck cipher. By analyzing various algebraic structures over which equations describing a given block cipher were determined, it was shown that the matrix structure of the final optimization problem also affects the speed of obtaining a solution using the D-Wave quantum computer. For the Simon cipher, due to the linearity of operations in the round keys generation algorithm, two ways of constructing the system of equations are presented, depending on the way of representing round key bits. Additionally, for small instances of the analyzed block ciphers, the practical attack on the

available resources of the D-Wave quantum computer was performed. The dissertation also presents the estimated complexity of the proposed attack for various variants and parameters of the considered block ciphers. As a result, for some variants, estimated complexities were lower than for the best currently known classical attacks on these ciphers.