Code-based Post-Quantum Cryptography

Jong-Seon No
(joint work with Wijik Lee)

It is known that in the quantum computer, Shor's algorithm can solve the problem of arithmetic decomposition and discrete logarithm in the polynomial-time. Thus, most of the conventional public key cryptosystems such as RSA cryptosystem, elliptic curve cryptosystem, and so on, can be broken by quantum computer. There have been many researches on cryptosystems robust to the attack by quantum computers, which are referred to as post-quantum cryptosystems (PQCs). The most popular PQCs are the code-based and the lattice-based cryptosystems. In this talk, we will focus on the code-based post-quantum cryptosystems and then several attacks against code-based cryptosystems will be introduced. The code-based cryptosystem is firstly introduced by McEliece in 1978. Later, Niederreiter cryptosystem is proposed, which is proved to be equivalent to the McEliece cryptosystem. The McEliece cryptosystem is known to be secure from the quantum computer attack because attacking the McEliece cryptosystem is NP-hard problem. In general, NP-hard problem is difficult to attack with quantum computer. The code-based cryptosystem has advantages of fast encryption and decryption. However, it requires very large public and private key sizes. Thus, there have been many works to reduce the key sizes of the McEliece cryptosystems. One approach to reduce the key sizes is to use other error correcting codes instead of the Goppa codes. For example, generalized Reed-Solomon (GRS) code, Gabidulin code, and Reed-Muller code have been adopted for the McEliece cryptosystem. However, these codes have structural characteristics and thus they are vulnerable to various attacks by their code structures. In the case of Reed-Muller code based cryptosystem, there are Minder-Shokrollahi attack and Chizhov-Borodin attack. We proposed puncturing and insertion techniques to overcome the vulnerability by complicating the code structure. Another approach to reduce the key sizes is to use quasi-cyclic (QC) codes, that is, a cryptosystem using quasi-cyclic medium-density parity-check (QC-MDPC) codes has been proposed to reduce the public key size to 4,800 bits with 80-bit security. The most basic attack against the code-based PQCs is information set decoding. Information set decoding attack is inefficient, but the attack algorithms have evolved gradually. If the computational complexity of information set decoding is larger than , it is regarded as a secure cryptosystem. Similar attack is finding minimum weight codeword, which is introduced by Stern and later developed into the Canteaut-Chabaud algorithm. The above two attacks are used as a measure of the security of the code-based cryptosystems. There are also message resend attack and partially known plaintext attack. To overcome these attacks, the semantically secure McEliece cryptosystem has been studied, which is called as CCA2-secure (security against adaptive chosen ciphertext attack). Recently, CCA-2 becomes the important

measure of security for the cryptosystems and thus, many cryptosystems are supplemented to satisfy CCA2-security.