New cryptographic technology for the quantum computer age

Proposal of Public Key Encryption based on Lattices for International Standardization

It has been known that a quantum computer of sufficient performance is capable of breaking RSA and discrete logarithm problems, which are currently used to secure communications over the Internet. At the same time, the commercialization of quantum computers and their availability as a free-of-charge cloud service in recent years reflects the progress made in their performance and penetration. It is therefore possible that current public key encryption will be unable to provide security for communications sometime in the future (Fig.1).

To protect the communication of information in the age of quantum computers, the Cybersecurity Research Institute of NICT developed LOTUS (Learning with the Cybersecurity Research Institute of Mathematics in the age of quantum computers, future (Fig.1)).

To protect the communication of information in the age of quantum computers, the Cybersecurity Research Institute of NICT developed LOTUS (Learning with the Cybersecurity Research Institute of Mathematics in the age of quantum computers, future (Fig.1)).

“Base cryptography is added with functionality”

LOTUS is a lattice-based cryptosystem, which has been intensively studied of late. The LOTUS team at Security Fundamentals Laboratory explains the design rationale of LOTUS as follows: “It is achieved by first configuring a base cryptosystem and then adding functionality for checking the structure of ciphertext at the time of decryption.”

This cryptographic technology is a first-round candidate in the PQC standardization process held by the National Institute of Standards and Technology (NIST) of the United States. All submitted candidates, including LOTUS, are being analyzed by experts in this field for a period of three years or more that started at the end of 2017 to choose a new standard for the future.

Footnote

1. Lattice-based cryptosystem

A set of points arranged in a regular way in space is called a lattice and a cipher that ensures safety by using the mathematical properties of a lattice is called a lattice-based cryptosystem. Here, expressing the property of regular arrangement as a matrix enables encryption and decryption processing to be performed in parallel, ensuring efficient implementations.

2. LWE problem

Short for Learning with Errors problem. Given a set of simultaneous linear equations in which the number of equations is greater than the number of variables, this problem consists of finding an integer solution such that the difference between the left side and right side of each equation becomes small. It has been shown that this problem is as hard as the lattice shortest vector problem depending on parameters, which indicates that finding a solution would take an extremely large amount of time even for a quantum computer.

Footnote

1. LWE problem

Short for Learning with Errors problem. Given a set of simultaneous linear equations in which the number of equations is greater than the number of variables, this problem consists of finding an integer solution such that the difference between the left side and right side of each equation becomes small. It has been shown that this problem is as hard as the lattice shortest vector problem depending on parameters, which indicates that finding a solution would take an extremely large amount of time even for a quantum computer.

"We raise our awareness of the need for applying security measures to IoT devices too.”

Figure 3 shows the top 10 attack targets (destination port numbers) observed by NICTER in 2017. The blue portions of this pie chart, which constitute more than half of the total, corre-