PROTECT

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 reflect the progress made in their performance and penetration. It is therefore possible that current public key encryption will be unable to provide secure 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 errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era) as a new cryptosystem that aims to satisfy the following conditions:

(1) Quantum-resistant: Must be difficult to break even by quantum computers
(2) Versatile: Must be applicable to browsers, databases, and many communication, transportation, and industrial systems.

“A base cryptosystem is added with functionality”

LOTUS is a lattice-based cryptosystem*1 based, in particular, on the LWE problem*2, 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.

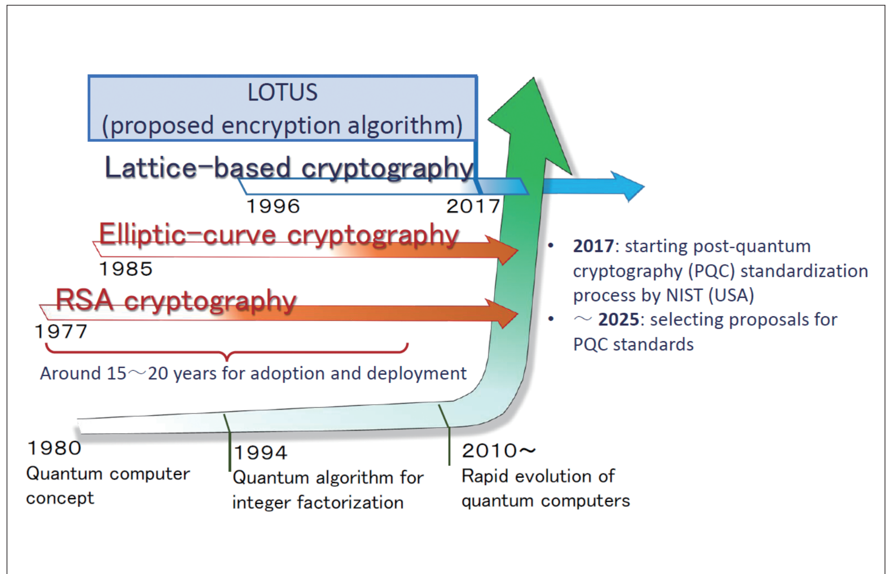


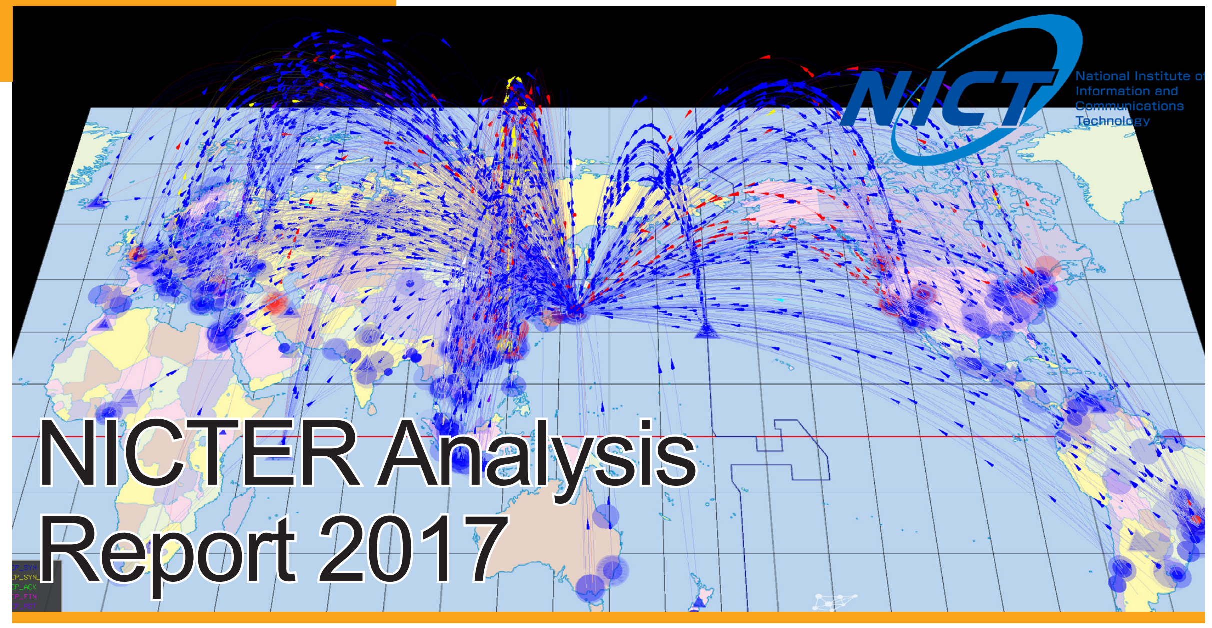
Fig.1 : Transition of public key encryption

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.

PROTECT



NICTER Analysis Report 2017

The NICT Cybersecurity Research Institute has been operating a large-scale cyberattack monitoring network (darknet monitoring) as part of the NICTER*1 project and has been monitoring cyberattack-related network packets*2 since 2005. The monitoring and analysis results of the NICTER project for 2017 (released in February 2018) are summarized below.

Cyberattack-related network packets observed in 2017 on the NICTER darknet monitoring network (about 300,000 IP addresses) rose to a total of 150.4 billion, which is about 560,000 packets per IP address per year (Fig.1).

The total number of packets per year represents only the number of packets arriving within the range of the darknet monitored by NICTER and should not be interpreted as the number of attacks mounted throughout Japan or against government institutions.

The total number of observed packets per IP address per year keeps increasing each year (Fig.2) and from 2016 to 2017, this number increased by 1,2 times.

Year	Total packets (billion)	# of darknet IP addresses	Packets received per IP address
2005	0.31	16,000	19,066
2006	0.81	100,000	17,231
2007	1.99	100,000	19,118
2008	2.29	120,000	22,710
2009	3.57	120,000	36,190
2010	5.65	120,000	50,128
2011	4.54	120,000	40,654
2012	7.78	190,000	53,085
2013	12.88	210,000	63,655
2014	25.66	240,000	115,323
2015	54.51	280,000	213,523
2016	128.1	300,000	469,104
2017	150.4	300,000	559,125

Fig.1 : NICTER darknet monitoring statistics

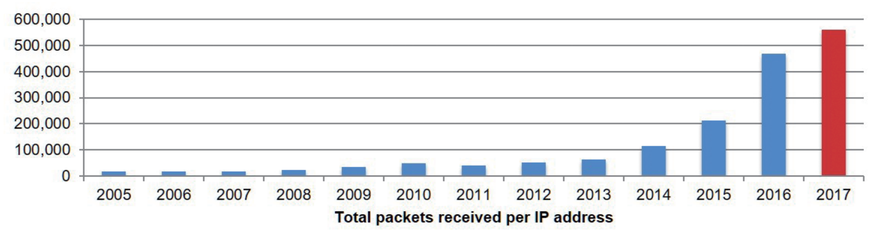


Fig.2 : Total number of observed packets per IP address per year

“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-