Research on Post-Quantum Cryptosystem Based on IoT Devices

Song Wang
School of Computer Science, Wuhan Donghu University, Wuhan, Hubei, 430212, China
Email: ws@wdu.edu.cn

Abstract: With the emergence of quantum computers, public-key cryptographic algorithms commonly used in classical computers are no longer secure. However, the current post-quantum cryptographic algorithms are mainly concentrated on the desktop CPU of Intel and AMD. For the Internet of Things, which is increasingly widely used, the research on post-quantum cryptographic algorithms is still scarce. Based on the research of post-quantum cryptosystem, this paper explores the post-quantum key algorithm based on Internet of Things devices.

1. Preface
At present, on the basis of the Internet, the Internet of Things is connected to a large number of devices, connecting the physical world and the digital world, and bringing great convenience to people's lives. However, a large number of device nodes have brought great security problems for building a secure and credible Internet of Things ecosystem. The main security problems faced by the Internet of Things include: physical security, data transmission security, identity authentication, data security and privacy. At present, the security of Internet of Things is mainly based on PKI technology, that is, public key infrastructure.

In the security protocols and applications commonly used on classical computers, the public-key cryptographic algorithms are basically used as the most basic cryptography primitives. Most public-key cryptographic algorithms are mainly based on several famous mathematical problems, for example, RSA encryption and digital signature algorithms are based on the unidirectional Euler function and the mathematical principle of large prime number decomposition; Elliptic curve algorithm is to calculate the point group on elliptic curve in discrete logarithm problem. However, with the emergence of quantum computer, its highly efficient quantum algorithms can solve the mathematical problems that most public-key cryptographic algorithm security now depend on, which makes these public-key cryptographic algorithms no longer secure. For example, the Shor Quantum Algorithm proposed by Peter Williston Shor in 1994 threatens public-key cryptographic algorithms, and Grover Quantum Algorithm proposed by Grover in 1996 can search quickly and exhaustively, thus threatening symmetric cryptographic algorithms.

2. Classification of post-quantum cryptography
After the emergence of quantum computers, most public-key cryptographic algorithms can be broken by quantum computers. Post-quantum cryptography is a cryptographic algorithm that can resist this attack in quantum computing and later times. The National Institute of Standards and Technology...
(NIST) of the United States started the research on post-quantum cryptography in 2012, and started the worldwide collection of post-quantum cryptography standards in 2016. Among the collected algorithms, there are mainly four mathematical methods: lattice-based cryptosystem; hash-based digital signature; code-based cryptosystem; multivariate-based cryptosystem. When the parameters are appropriately selected, by far there are no classical or quantum algorithms that can solve these problems quickly.

Lattice-based cryptosystem has simple algorithm and high parallelism. Lattice is a vector set generated by \( m \) \((m \leq n)\) linearly independent vectors in \( n \)-dimensional linear space, and its structure is shown in Figure 1. In Figure 1, the lattice cryptography is based on \( b_1 \) and \( b_2 \) and all points in the space can be expressed linearly by \( b_1 \) and \( b_2 \). The main mathematical basis of lattice cryptography is the shortest vector problem (SVP) and the closest vector problem (CVP). The SVP is to find the non-zero vectors with the minimum distance between two points in the lattice generated in the basis for a given set of bases. The CVP is to find the vector nearest to the given vector in the lattice with a given lattice and any vector. Lattice-based algorithms can realize encryption, digital signature, key exchange and other existing cryptographic constructions, and their security is based on the difficulty of solving lattice problems.

Hash-based signature algorithm is evolved from one-time signature scheme and it uses Merkle Hash Tree authentication mechanism. The method is to change from one-time signature to multiple signatures. The root of the tree is the public key, the one-time authentication key is the leaf node of the tree, and the bottom layer of the tree is the data block connected to each corresponding hash node. During authentication, the hash values of adjacent small data blocks are spliced together to form a new string, and then the hash of this new string is calculated and pushed up layer by layer, finally forming an upside-down tree. Its structure is shown in Figure 2. The security of hash-based signature algorithm depends on the anti-collision of hash function. Multiple signatures are used in Merkle Hash Tree authentication mechanism, and there is no effective quantum algorithm that can quickly find the collision of hash function. If the output is long enough, the signature algorithm based on Merkle Hash Tree can resist quantum computer attacks. Moreover, the security of the algorithm does not depend on a specific hash function, and some hash functions were broken in actual use, so a safer hash function can be used to directly replace the broken hash function.

![Figure 1. Lattice](image)
CIBDA 2021
Journal of Physics: Conference Series
1883 (2021) 012082
doi:10.1088/1742-6596/1883/1/012082

Figure 2. Merkle Trees

Coding-based cryptosystem uses error-correcting codes to encode information, and adds enough random error information, so that the transmitted information cannot be deciphered by attackers, while the legitimate receiver corrects errors through the private key to recover the original information. The representative algorithms of coding-based cryptosystem include McEliece cryptosystem and Niederreiter’s dual version of McEliece’s cryptosystem. McEliece cryptosystem uses Goppa codes, and the key is randomly generated $k \times n$ order matrix $G$ with length $n$ and dimension $k$. $k \times k$ order random nonsingular invertible matrix $S$ is generated. $n \times n$ order binary random permutation matrix $P$ is generated. $G$ left multiplies the random nonsingular reversible matrix $S$ and right multiplies the binary random permutation matrix $P$, and the obtained matrix $G^{\text{pub}} (G^{\text{pub}} = SGP)$ is the public key. The receiver decrypts the encrypted information by using its own private key. Yet in reality, because the storage space for keys is too large, this cryptosystem is not widely used.

The public key based on a multivariate-based cryptosystem is composed of a set of nonlinear polynomials with multiple variables in a finite field, as shown in Equation 1. There are $n$ variables in the finite field, which are composed of quadratic multivariate polynomial equations of $m$ polynomials. The security of the cryptosystem depends on the difficulty of solving the nonlinear equations.

$$
p^{(1)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}
$$

$$
p^{(2)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}
$$

$$
\vdots
$$

$$
p^{(m)}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}
$$

3. Exploration of post-quantum cryptosystem based on IoT devices

At present, the post-quantum cryptographic algorithms are mainly concentrated on the desktop CPU of Intel and AMD. For some new devices, such as ARM-based embedded devices and Internet of Things devices, optimized algorithms are rarely realized. Meanwhile, these platforms and devices are increasingly widely used, so it is of great value to implement fast and secure post-quantum algorithms on these devices.

Among the four types of post-quantum cryptosystems introduced above, the code-based McEliece cryptosystem needs to use a large matrix storing public keys and private keys, which will occupy a lot of resources, which is a constrain for devices with limited resources. Hash-based algorithms are mainly used to construct digital signatures. Lattice-based cryptosystem can be used to construct
various cryptographic algorithms and applications, but the current research is mainly based on desktop CPU. The multivariable-based algorithm system uses quadratic polynomial groups with multi-variables to construct encryption and signature algorithms. The algorithm is fast in calculation, but the size of public key is large, so it is very suitable for the cases where public key transmission is not frequently needed. 

The Internet of Things, as the global information infrastructure for connecting goods, has been developing very fast in recent years, but the security problems of the Internet of Things can not be ignored. In 2016, the National Institute of Standards and Technology (NIST) of the United States launched a worldwide collection of post-quantum cryptography standards, and in 2019, China issued the national standards of Internet of Things security technology. At present, the standard of post-quantum cryptography has not been determined, and the research on post-quantum cryptosystem for Internet of Things security is relatively few. From the basic business process of the Internet of Things, the application of post-quantum cryptography must be targeted. A basic business process in the Internet of Things industry is shown in Figure 3.

![Figure 3. Basic processes for the Internet of Things](image)

From the basic business flow chart of the Internet of Things industry, it can be seen that the security of the Internet of Things involves physical environment, communication network, management system and computing environment, etc. Meanwhile, the integration and diversification of IoT terminals and applications also brought more uncertainty to the security of the Internet of Things, and the ever-growing IoT connected devices also give attackers more extensive network attack entrances. The cloud server of Internet of Things can be built by quantum computer, which enables users to communicate data in an absolutely secure network. Cloud server and application layer can use lattice-based cryptosystem. Lattice-based algorithm has smaller size of public and private keys than the other three types of constructions, and its computing speed is faster. It can be used to construct a variety of cryptographic primitives, so it is more suitable for real-world applications. In recent years, the lattice cryptography construction based on LWE (Learning with Errors) and RLWE (Ring-LWE) has been developing rapidly and it is considered as one of the most promising technical routes to be standardized. At present, among the various algorithms collected by NIST, the lattice-based and code-based constructions are the most, and they are mainly used to construct public key encryption (key exchange) algorithms. Due to the limited resources of IoT terminal devices, it is unlikely to use a complex cryptosystem. For example, the RFID system widely uses the stream cipher system. After entering the quantum computer era, in order to ensure the data security of IoT devices, we can choose the multivariate-based algorithm system for post-quantum cryptosystem. Although its public key size...
is large, it is more practical for IoT terminal devices that do not need frequent public key transmission.

4. Conclusion
The good algorithms in post-quantum cryptography can directly replace the existing public key encryption, digital signature and key exchange algorithms, including RSA encryption/signature, Diffie-Hellman key exchange, elliptic curve encryption/signature, etc. At present, the standard of post-quantum cryptography has not been determined, and the research on post-quantum cryptography based on Internet of Things is still scarce. After analyzing several types of post-quantum cryptosystem collected by NIST, we find that we cannot draw a unified conclusion to the post-quantum cryptosystem based on the Internet of Things. We need to conduct targeted studies on different security issues in the Internet of Things to solve the threat that the future quantum computers may bring to IoT devices.

References
[1] Li Zhe, HAN Yiliang, LI Yu. (2020) An overview of code-based encryption schemes[J]. Journal of National University of Defense Technology 2020(4).
[2] Deng Longtao, Mao Xiangjie. (2018). The Application of Post-quantum Cryptography in Blockchain System. INFORMATION&COMMUNICATIONS, No.192(12), 59-61.
[3] Pan Feng. (2017). Analysis of the Application of Post-quantum Cryptosystem in Information Security Level Protection. China Computer&Communication, 000(018), 211-212.
[4] HAN Yiliang, WANG Zhong. (2019). Anti-quantum Cryptography Scheme Based on Multivariate and LRPC Codes. Netinfo Security, 2019, 19(8): 36-43.
[5] LI Zichen, XIE Ting, CAI Juliang, ZHANG Xiaowei. (2018). New post quantum authenticated key exchange protocol based on ring learning with errors problem. Journal of Computer Applications, 038(008), 2243-2248, 2273.
[6] Zhou Xiaoyi, Zhao Yongzhe, Li Yihong. (2018). Security research based on quantum cryptography for RFID system in Internet of things. Application Research of Computers, 35(10), 226-229.