Quantum-resistant cryptography

Background:

In quantum computers, states are represented as vectors in a Hilbert space. Quantum gates act on the space and allow us to manipulate quantum states with combination of gates[1]. The size of the corresponding Hilbert space becomes exponentially larger as the amount of data grows. Parameterizing quantum states with classical computers costs a lot of computational resources. However, by using quantum computers, it becomes possible for us to solve some computationally hard problems efficiently. Algorithms proposed by Peter Shor[2] solve the integer factoring problem and the discrete logarithm problem quite efficiently, and thereby crack RSA-based cryptosystems and Diffie-Hellman key exchange. Another algorithm proposed by Lov Grover[3] also gives a method to perform unstructural search in square root of time, and thus endangers the symmetric cryptosystems. Quantum algorithms are so powerful that they have been seen as a worth-digging subject.

We first plan to study the strategies and techniques used on quantum algorithms to solve different problems, and to find out relations between different computational problems including how they are formulated into problems solvable by quantum algorithms. Then, we research on how to design quantum resistant cryptosystems. For instance, Grover algorithm performs multiple iterations. During each iteration, we first perform the phase inversion operation to mark the search target, perform inversion about the mean to amplify the marked component, and eventually find the target.

In the theory of computation, some problems are related to one another, and solving one may consequently solve another. Shor's algorithm transforms the integer factoring problem into the period finding problem, and uses quantum Fourier transform to extract the period of a given function. The hidden subgroup problems (HSP) are related to some computationally hard problems; for instance, HSP for some non-abelian groups are related to the graph isomorphism problem and the shortest vector problem on lattice. Shor's discrete logarithm algorithm transforms the discrete logarithm problem into the HSP for finite abelian groups as well.

This project is targeted at five mainstream topics in community of quantum-resistant cryptography (also called post quantum cryptography[4]): lattice-based cryptography,

multivariate-based cryptography, isogeny-based cryptography, hash-based cryptography, and code-based cryptography.

1. Lattice-based cryptography

In 1996, Ajtai and Dwork[5] raised the first lattice-based public-key cryptosystem. NTRU encryption algorithm was proposed in 1996 by Hoffstein, Pipher and Silverman[6] and GGH cryptosystem was published by Goldreih, Goldwasser and Halevi[7] in 1997. In 2009, Gentry introduced the first fully homomorphic encryption algorithm[8]. These cryptosystems are based on hardness of lattice problems like the shortest vector problem or the closest vector problem and they are resistant to attack by quantum computers.

2.Multivariate-based cryptography

In 1988, Matsumoto and Imai presented the first multivariate-based C* scheme[9], which inspired many new multivariate-based cryptosystems. The “Hidden Field Equations” and “Oil and Vinegar” were developed by Jacques Patarin[10][11] in 1996 and in 1997. The security of these cryptosystem are based on the hardness to find solutions on multivariate polynormials over a finite field or its extension field. Solving systems of multivariate polynomial equations is proven to be NP-hard and so the cryptosystems based on it are considered as good candidates for quantum-resistant cryptography.

3.Isogeny-based cryptography

Ordinary isogeny Diffie-Hellman key exchange(OIDH) was first proposed by Rostovsev and Stolbunov[12] in 2006. Childs, Jao, Soukharev[13] gave a quantum subexponential algorithm to break OIDH. Supersingular isogeny Diffie-Hellman key exchange(SIDH) was then raised by De Feo, Jao, Plut[14] in 2011. SIDH is based on the difficulty of finding isogenies between supersigular elliptic curves. The main technical idea is to transmit the images of torsion bases under the isogeny in order to allow the parties to construct a shared commutative square despite the noncommutativity of the endormorphism ring. Out of all quantum-resistant key exchanges, SIDH uses the smallest keys. SIDH uses 2688-bit public keys at a 128-bit quantum security level.

4.Hash-based cryptography

Hash-based cryptography was used for Lamport one-time signature scheme in the early 1970s. Since a one-time signature scheme key can only sign a single message securely, in the late 1970s, Ralph Merkle proposed the Merkle signature scheme[15],

which is a digital signature scheme based on hash tree (also called Merkle tree) and Lamport one-time signature scheme. Also, it is an alternative to traditional digital signatures such as RSA digital signature scheme. The Merkle signature scheme depends on the security of hash functions and it is believed to be resistant against quantum computer algorithms[16][17].

5.Code-based cryptography

The McEliece cryptosystem is a public-key encryption algorithm raised by Robert McEliece[18][19] in 1978. The algorithm is based on the hardness of decoding a general linear code, which is known as NP-hard. An error-correcting code C (Goppa code is suggested.) with kxn generator matrix G is selected to correct t errors. G is perturbated by two randomly selected invertible kxk binary matrix S and nxn permutation matrix P. Here public key is (G', t) with G'=SGP while private key is (S, G, P). For resiliency against quantum computers, size of n=6960, k=5413, t=119 with Goppa code were proposed, giving the size of public key of 8,373,911 bits.

The Niederreiter cryptosystem[20] is a variation of the McEliece cryptosystem developed by Harald Nidereiter in 1986. The encryption of it is about ten times faster than that of McEliece cryptosystem. It can be used to construct a digital signature scheme.

References

[1] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, ISBN 0-521-63503-9. OCLC 174527496, 2000.

[2] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th Ann. Symp. on Foundations of Computer Science (FOCS '94) pages 124-134, 1994.

[3] L. Grover. A fast quantum mechanical algorithm for database search. In Proc. 28th Ann. ACM Symp. on Theory of Computing, pages 212-219, 1996.

[4] D. Bernstein. Introduction to post-quantum cryptography. (Introduction chapter to book "Post-quantum cryptography"), Springer, 2009.

[5] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In STOC '97, pages 284-293. ACM, New York, 1999.

[6] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring-based public key cryptosystem. In Algorithmic Number Theory, volume 1423 of Lecture Notes in Comput. Sci., pages 267-288. Springer, Berlin, 1998.

[7] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In Advances in Cryptology-CRYPTO ’97, volume 1294 of Lecture Notes in Comput. Sci., pages 112-131. Springer, Berlin, 1997.
[8] C. Gantry. Fully homomorphic Encryption Scheme (Thesis). Stanford University, 2009.
[9] T. Matsumoto, and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. EUROCRYPT ’88, 1988.
[10] J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. CRYPTO'95, 1995.
[11] J. Patarin. Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms (extended version), Eurocrypt '96, 1996
[12] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006.
[13] A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology, 8(1), pages 1-29, 2014.
[14] L. De Feo, D. Jao, and J. Plut. Towards quantum resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), pages 209-247, 2014.
[15] Ralph Merkle. "Secrecy, authentication and public key systems / A certified digital signature". Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.
[16] G. Becker. "Merkle signature schemes, Merkle trees and their cryptanalysis", seminar 'Post Quantum Cryptology' at the Ruhr-University Bochum, Germany, 2008.
[17] T. Lange. "Hash-based signatures". Encyclopedia of Cryptography and Security, Springer US, 2011.
[18] R. McEliece. Public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 44, pages 114-116, 1978.
[19] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, 24(3), pages 384-386, 1978.
[20] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory. Problemy Upravlenija i Teorli Informacii. 15, pages 159-166, 1986.