Post-quantum encryption overview

Gaudiano Antonio mat. 744102

Introduction

With the advent of quantum computing, the security of current cryptographic systems that rely on the difficulty of certain mathematical problems is potentially compromised. The powerful computational capabilities of quantum computers can potentially attack and breach these cryptographic systems and compromise the confidentiality, integrity and authenticity of communications. Post-quantum cryptography is a branch of cryptography that aims to develop cryptographic systems that can resist attacks performed by quantum computers. These systems are designed based on mathematical problems that are considered difficult even for quantum computers. Many post-quantum cryptographic schemes have been proposed, including Lattice Based Cryptography, which exploits lattices with hundreds of dimensions as the encryption system of data, represented by the lattice points themselves. It has been found to be computationally very efficient when performed on "classical" computers, i.e., not quantum computers, a very important feature since even in the era of quantum computers they will not be the only ones to exist because of their very high cost and the complex operations that needs to be performed to make them work properly.

In this essay, the design and implementation of post quantum cryptography schemes are analysed. The objective is to provide a comprehensive study of existing post-quantum schemes.

First, it is necessary to specify the difference between quantum encryption and post-quantum encryption, as they are two similar terms sometimes used synonymously, but which have quite different meanings. The term quantum encryption refers to encryption techniques that exploit certain properties of quantum mechanics to protect data and communications. A well-known example of quantum cryptography is QKD, Quantum Key Distribution [1], which allows two parties to securely generate a shared secret key by transmitting quantum states over an optical fiber. QKD provides security by exploiting properties of quantum mechanics, such as the non-cloning theorem to detect the presence of an eavesdropper. On the other hand, the term post-quantum encryption refers to encryption methods considered secure against attacks by quantum computers. Unlike quantum encryption, post-quantum encryption does not use the properties of quantum mechanics to provide security. Instead, it relies on mathematical problems deemed "difficult" (i.e., computationally burdensome) to solve, both for "classical" computers, as well as for quantum computers. Both approaches aim to protect data from unauthorized access but are based on different principles. From now on, the branch concerning post-quantum cryptography will be discussed.

State of the art

Speaking of securing protocols and technologies those are some of the most promising post-quantum cryptographic approaches:

- Lattice-based cryptography: this approach is based on the difficulty of solving problems on lattices, such as the shortest vector problem (SVP) and the closest vector problem (CVP). Lattice-based cryptography has been extensively studied and has shown strong security against quantum algorithms.

- Code-based cryptography: this approach is based on the hardness of decoding random linear codes. The McEliece cryptosystem [2] is one of the best-known cryptographic code-based system.
- Multivariate cryptography: this approach is based on the difficulty of solving systems of multivariate polynomial equations over finite fields. The best-known cryptographic system based on multivariate equations is the Rainbow scheme [3].
- Hash-based cryptography: this approach is based on the difficulty of finding collisions in cryptographic hash functions. The best-known cryptographic system based on hashes is the SPHINCS scheme [4].
- Isogeny-based cryptography: this approach is based on the difficulty of calculating isogenies between elliptic curves. The best-known cryptographic system based on isogeny is the SIKE scheme [5].

The Lattice-Based family seems the most likely candidate for future implementations of asymmetric post-quantum cryptography due to its good properties in terms of efficiency.

For these reasons, the NIST (National Institute of Standards and Technology) has actively shown interest in seeking new standards for post-quantum cryptography by issuing a call for proposals in which various algorithms will be studied [6].

As of July 2024, the fourth round of submissions has been reached.

Threats

Grover's algorithm is a quantum algorithm developed by Lov Grover in 1996. Given a generic function, the algorithm can find (with high probability) the unique input that produces the given output. Because of these properties, it is considered an algorithm for inverting function. The function is treated as a blackbox, so any function can be inverted, even one-way functions and hash functions. In the original 1996 article "A fast quantum mechanical algorithm for database search" [7], the problem was presented as a search on an unstructured database, thus lacking any sorting to facilitate the operation.

Shor's algorithm [8] is a quantum algorithm developed by Peter Shor in 1994. It succeeds in finding the prime factors of an integer N. Without going into the specifics of the mathematical operations involved, the algorithm makes it possible to solve the factorization problem very quickly by reducing the problem to computing the period of a function. Many tries are still required, but thanks to the quantistic property of the superposition they can be generated almost instantaneously.

Quantum computers can probably violate any encryption algorithm whose security is based on the integer factorization problem, the discrete logarithm problem, discrete elliptic curve problem or any other closely correlated ones. The following common cryptography schemes and applications are found to be vulnerable:

- RSA.
- Diffie-Hellman (classical key exchange).
- Digital Signature Algorithm (DSA).
- Elliptic curve-based cryptography.
- HTTPS/TLS.
- VPN (Virtual Private Network).
- Random Number Generators.
- All other applications and protocols that use any of the abovementioned algorithms.

Considering simply HTTPS/TLS, it follows that most of the security of the Internet turns out to be breached. Not all encryption is compromised, but evaluating everyday use cases almost all applications would no longer be secure to use.

Solutions

Not all cryptography is vulnerable to quantum computers. Schemes that are not susceptible are called quantum resistant, quantum safe, or post quantum. The three terms have the same meaning and are equivalent. The following is a list of some quantum safe algorithms and protocols:

- Symmetric encryption schemes such as AES, doubling the length of the key.
- SHA-2, SHA-3, etc.
- Lattice-based schemes.
- Multivariate-based schemes.
- Code-based Schemes.
- Quantum-based ciphers.
- All other applications and protocols that rely on symmetric ciphers, doubling the key length.

Modern digital cryptography normally handles large bit sizes of protection that make classic brute-force attacks completely ineffective. In fact, there is not enough computational power to force the encryption keys used by modern algorithms. This remains true even taking exploiting the efficiency and speed of quantum computers (even using Grover's algorithm) and the properties of quantum mechanics.

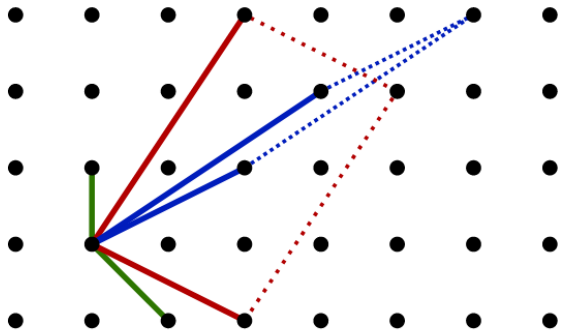
For example, just because a quantum computer can use superposition to generate every possible answer at once, it does not mean that it can choose the right solution. There must be a way to choose the correct answer from the infinite possible ones that a quantum computer can generate. These algorithms use quantum properties to reduce the pure mathematical steps and allowing us to find the answer we seek with fewer attempts. Shor's algorithm helps quantum computers factor large numbers of primes because it uses mathematical operations that allow solutions to be found much faster than a brute-force attack. One of the reasons why quantum computers can break most of the cryptographic traditional public key is that the mathematics on which it is based has a "weakness" that quantum computers and algorithms can exploit. The potential of Shor lies in the fact that he was able to create a faster mathematical solution that could only be realized by quantum computers.

However, not all problems have characteristics such that they are overly susceptible to quantum solutions. This is the case with traditional symmetric ciphers. Grover's algorithm uses a time reduction to halve the protection of symmetric ciphers. This is a significant reduction, but it is not fatal (as it would be if the time reduction were polynomial, quadratic or factorial). Any quantum computer that attacks these types of encryptions can be much faster than classical computers, but the number of bits in the key is still so large that the "much faster" does not significantly weaken the protection power of these ciphers or hashes. In addition, Grover's algorithm helps in inverting the hash function but not in finding collisions between hashes, for these reasons symmetric ciphers and hash functions are considered quantum safe. In general, doubling the size of symmetric keys and hash functions hashes will allow them to remain quantum safe for the foreseeable future. So, from a theoretical point of view, moving from AES-128 and SHA-256 to AES-256 and SHA-512 is considered a long-term solution.

Lattice-based cryptography

A lattice is a set of points in an n-dimensional space with periodic structure. A lattice can be generated from all linear combinations of n linear independent vectors said to be the lattice's base.

The same lattice can be expressed by multiple bases. For example, the two-dimensional lattice in Figure 1 can be expressed by the green vectors as a basis, as well as by the blue vectors. The red vectors, on the other hand, do not constitute a valid basis, since the parallelogram formed by the vectors contains some lattice points, which cannot be represented as a linear combination of the basis. In general, the parallelogram must not contain lattice points other than vertices to make the base valid. Blue vectors are a basis, since they satisfy this property.



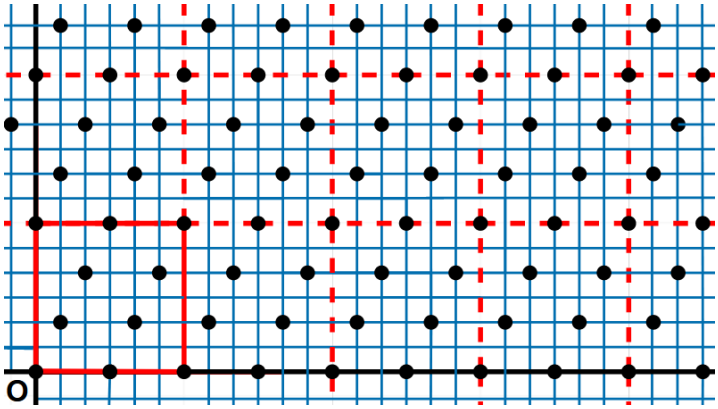
1 Bases example

It is worth noting that a valid basis can be either composed of short vectors and nearly orthogonal, as well as by long and asymmetrical vectors.

The basis of a lattice can also be expressed compactly by a matrix. The determinant of a lattice is the modulus of the determinant of its basis, and represents the "sparsity", i.e. how much the points of the lattice are scattered.

So far, real lattices have been considered, that is, lattices generated from a matrix base composed of vectors of real numbers. In cryptography, such lattices are of little use, because real numbers are not representable with infinite precision within a finite number of bits. For this reason, integer lattices, generated from a matrix base of integers and composed of vectors of integers, are more interesting. One class of integer lattices that has been shown to have good efficiency properties in cryptography are q-ary lattices. A q-ary lattice is an integer lattice that contains (also) vectors whose coordinates are multiples of q.

Figure 2 shows a two-dimensional 6-ary lattice. The blue lines represent integers, the black lines the axes, and the black dots the lattice elements. We note that all points whose coordinates are multiples of 6 are within the lattice. Moreover, the lattice repeats through square patterns of side 6 starting from the origin. Every integer lattice is q-ary for some large enough q; in cryptography, however, we are interested in q-ary lattices with small values of q, if they are large enough for lattice problems to be difficult to solve. In general, q has no special structure. For example, it does not have to be prime. The value of q is chosen to meet the efficiency requirements. A realistic value is q = 257, used in the parameterization of the SWIFFT hash function [9].



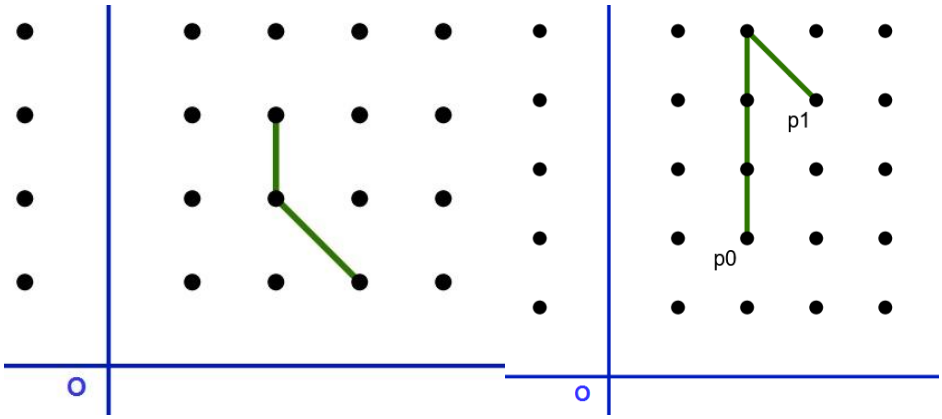
2 Q-ary lattice example

Shortest Vector Problem

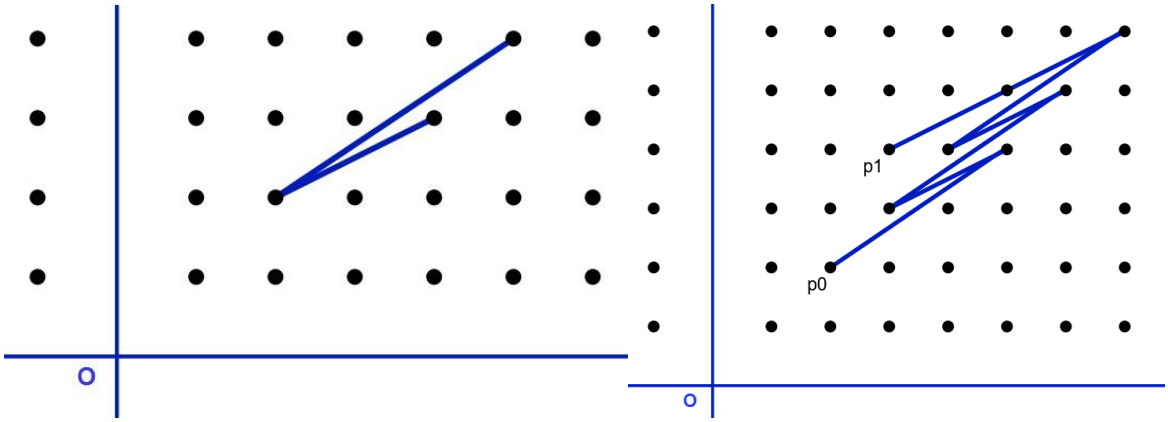
On lattices it is possible to define a class of problems considered difficult, the most fundamental of which is the Shortest Vector Problem (SVP). SVP aims to find the shortest non-zero vector of an input lattice given its basis. By "shortest" is typically meant in the Euclidean distance.

Intuitively, the difficulty of an SVP problem depends largely on the basis which the lattice is represented with. For example, if the lattice in Figure 1 is represented by the green basis, then SVP will be easy since the solution coincides with one of the basis vectors. On the other hand, if the lattice is represented by the blue basis, then SVP is considerably more difficult. In general, short and nearly orthogonal bases are "good bases" for SVP, while long and distorted bases are “bad” bases, i.e. difficult to be computed.

Figures 3 and 4 shows an example of good and "bad" basis, respectively (on the left the basis vectors, on the right the SVP example). In the first case it is easy to see that it is not particularly complex to reach the point p1 starting from p0, in the case of long, nonorthogonal vectors, on the other hand, this operation is immediately seen to be more complicated, requiring a greater number of steps that are also less intuitive (starting from p0 going straight and then going back).



3 Easy SVP example



4 Hard SVP example

It is worth noting that the examples of two-dimensional lattices shown so far are for illustrative purposes only and serve to understand the basic concepts. Lattice-based cryptography used in real-world applications employs lattices with hundreds of dimensions; in fact, computing SVPs with a few dimensions is always trivial, regardless of the basis.

Closely related to the shortest vector problem (SVP) and the closest vector problem (CVP) is the Learning With Errors (LWE) problem, whose first appearance was introduced by Oded Regev in 2005 [10]. The basic idea is to hide secrets by introducing noise into them. The reason why the LWE problem is so useful for constructing encryption schemes is its decision form proved to be equally complex to solve. The LWE decision problem is defined as follows: given a matrix A whose elements are chosen randomly, decide whether a given point y is:

- a point with noise addition (perturbed lattice point)
- a completely random point.

The goal is to distinguish between the first and second cases with a probability much higher than 50%.

In the most modern literature is also mentioned the RLWE (Learning With Errors over Rings) problem, which is a particular case of LWE problem dealing with rings, a particular mathematical structure that offers some useful properties that helps in calculating the solutions, making this approach even more suitable for implementations on non-quantum computers.

In conclusion, lattice-based cryptography, with its resistance to quantum attacks and robust mathematical foundations, represents a promising frontier in post-quantum encryption. By leveraging hard lattice problems, such schemes offer enhanced security against future quantum threats while maintaining practical efficiency for current applications. Continued research and development in this area are crucial for ensuring long-term data security in a quantum-enabled world.

References

[1] H.K. Lo, M. Curty and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics,* vol. 8, no. 8, pp. 595-604, 2014.

[2] “Classic McEliece,” [Online]. Available: https://classic.mceliece.org/.

[3] “Rainbow,” [Online]. Available: https://www.pqcrainbow.org/.

[4] “SPHINCS,” [Online]. Available: https://sphincs.org/.

[5] “SIKE,” [Online]. Available: https://sike.org/.

[6] “NIST Post-Quantum Cryptography,” [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.

[7] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996.

[8] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review,* vol. 41, no. 2, pp. 303-332, 1999.

[9] V. M. D. Lyubashevsky, C. Peikert and A. Rosen, “SWIFFT: A Modest Proposal for FFT Hashing,” in *Fast Software Encryption: 15th International Workshop*, Lausanne, 2008.

[10] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, New York, 2005.