Post Quantum Counting on Cryptography

Zihao Ye

Ulink College of Shanghai, 559 South Laiting Road, Jiuting Town, Songjiang District, Shanghai, 201615, China
Corresponding Author: Zihao Ye, Email: 3254738740@qq.com

Abstract

With the rapid development of technologies in computer science, cryptography, a field regarding how to secure data, has been widely used in a variety of daily lives. Meanwhile, quantum computing is rapidly developing, where there exist some quantum algorithms such as Shor's Algorithm which can destroy the most common cryptography schema, i.e., the RSA cryptosystem. Consequently, the existing cryptography is facing severe challenges from the quantum computer. To overcome the threat of quantum computing on cryptography, this paper studies the post-quantum computing algorithms, which are robust to the attack by quantum computers, analyzes the existing post quantum computing algorithms and suggests the most promising one along with its future forecasting.

Keywords

Cryptography; RSA cryptosystem; Shor's algorithm; Post quantum cryptographies

Introduction

With the fast development of technologies, people pay more attention to protecting data from being stolen by third parties, which may result in severe damage and devastate modern life [1,2]. Cryptography, a field regarding how to secure data, dedicates to investigating the ways to protect data. It acts as a significant role in the development of data security in different areas. Consequently, the operation of modern society highly relies on reliable cryptography to maintain regularity.

RSA (Rivest–Shamir–Adleman) cryptosystem [3] is one of the most successful and frequently used cryptography schemas in human civilization. It secures communication and information with the "factorizing problem" that allows someone to receive certain intended information and not anyone else. If this cryptosystem suspends its functionality, modern life would come to a halt. For example, Internet traffic and cell phones would not operate normally, bank transactions would come to a standstill, and private information of people would be leaked to anyone. Therefore, encrypting sensitive data with the RSA cryptosystem is a vital way of inhibiting all that

Citation:Zihao Ye. (2022) Post Quantum Counting on Cryptography. The Journal of Young Researchers 4(39): e20220930

Copyright: © 2022 Zihao Ye. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Received on May 7, 2022; Accepted on July 10, 2022; Published on September 30, 2022

from happening.

On the other hand, quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics. Quantum computer has been demonstrated to solve problems costly problems for classical computers. For example, for the large number factorization problem, Shor's algorithm can solve it exponentially faster than the classical computer[4]. As a result, by using a mature quantum computer, Shor's algoritm has significant potential to decrypt the RSA cryptosystem which highly depends on the factorization of the problem in the near future.

The collapse of the RSA cryptosystem triggers further investigations in cryptography[5] to defend attacks from quantum computers. Therefore, this paper answer this open problem by discussing a branch of cryptography that is robust under algorithms of quantum computing. In general, the paper studies the histories and operations of the RSA cryptosystem and Shor's algorithm, explains the exact mathematical reason why Shor's algorithm can break the RSA cryptosystem [5], and list the known great achievements in post quantum cryptography[19, 20,23,26]. In addition, this paper provides an analysis on the pros and cons of different branches of post quantum cryptographies and based on that, suggests a promising path for post quantum cryptography to remain robust even under the rapid developments in quantum counting.

The paper is organized by starting with an introduction section to describe cryptography and quantum computing. Then a literature section is provided to present all necessary background knowledge required for the whole paper. Next, the paper comprehensively discusses how a quantum computer may destroy the existing cryptography system and reviews the algorithms which are robust for quantum computers along with analysis and future forecasting.

Literature Review

The literature review section will introduce the necessary concepts and knowledge used throughout the whole paper, mainly including RSA cryptosystem and Shor's algorithm. In particular, RSA cryptosystem is a powerful method to encrypt data during the process of data transmission among different classic computers based on the difficulty of factorizing large prime numbers. Its history, operation, and the availability of security will be analyzed in the section. Shor's algorithm aims to effectively solve large number factorization by applying technologies in quantum computers to transform the problem of factorizing to order finding, which dramatically reduces the time complexity of the RSA cryptosystem. As a consequence, Shor's algorithm consumes exponentially fewer amount of time to decrypt encryption methods based on "factorizing problem", which can be a severe problem of data security. In the subsection of Shor's algorithm, the history of its birth, the operation, and the underlying mechanisms will mainly be presented.

RSA Cryptosystem

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem widely used for secure data transmission. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977 [3]. An equivalent system was developed secretly in 1973 at GCHQ (the British signals intelligence agency) by the English mathematician Clifford Cocks [6]. That system was declassified in 1997. RSA cryptosystem utilized NP hard problem (hardness of factorizing large numbers), which will take a very long time even decrypting on the fastest computer on earth as the classic fundamental computer system does not enable classic computers to calculate that amount of data in a proper time.

RSA Code Operation

RSA cryptosystem has been developing with developments in other fields of cryptography and nowadays there are various applications of it is not only cryptography on transferring data on classic computers. Here the simplified version operation of a commonly used RSA cryptosystem in data tele-transmission is mentioned for delving into its key idea of it in a concise way.

A basic principle behind RSA is the "factoring problem" that it is hard to find three very large positive integers *e*, *d*, and *n*, such that with modular exponentiation for all integers *m* (with $0 \leq m < n$):

$$m^{ed} \equiv m(modn)$$

and that knowing *e* and *n*, or even *m*, it can be extremely difficult to find *d*.

The generation of a simplified version of the RSA code is conducted as below

Procedure 1: choose 2 distinct prime numbers p and q

Procedure 2: compute the product of p and q, name it N

Procedure 3: compute the product of (p-1) and (q-1)

Procedure 4: choose public key-- an integer e coprime to (p-1)(q-1)

Procedure 5: make public e and N (while keep others secret)

During the encrypting process, the sender first turns plaintext (content that will be displayed to the receiver after all processes of RSA cryptosystem) into an integer m, such that $0 \leq$ m < n by using an agreed-upon reversible protocol known as a padding scheme. The sender then computes the one ciphertext c, using the public key e, corresponding to

$$c \equiv m^e(modn)$$

The message encrypted by RSA code (namely cipher text) is then transmitted to the receiver with public key N and e. The receiver can recover m from c by using her private key exponent d by computing

$$c^d = (m^e)\hat{}d \equiv m(mod\ n)$$

Given m, the receiver can recover the ciphertexts c by reversing the padding scheme.

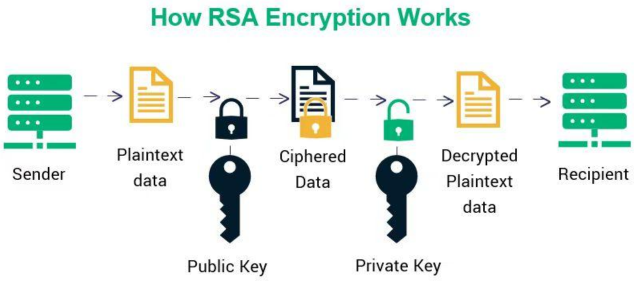

Figure 1. The operation of RSA cryptosystem[31]

An Example of the Process of RSA Cryptosystem on Data Transmission

This example is changed from "A concise introduction to pure mathematics" [7].

Choose two large prime numbers p and q, and multiply them together to get *N = pq*. Then find *(p−1)(q−1)* and choose a large number *e* which is coprime to *(p−1)(q−1)*. Next make public the numbers N and e, but keep the values of *p* and *q* secret.

Values of these numbers are such that

$$\begin{aligned} p = 37, q = 61, N = pq \\ = 2257, (p-1)(q-1) \\ = 2160, e = 11 \end{aligned}$$

(In practice, to ensure the security of the code, one uses primes with around 200 digits, but these primes will serve for illustrative purposes.) The pair (*N,e*) is called the public key of the code. Anyone who wants to send us a message can use the numbers N and e in the following way. First, they convert their message into a string of numbers by some process such as the one given above (01 for A, etc.). They then break up this string into a sequence of numbers with fewer digits than N. For example, with p,q

as above, substitute 01 for an A, 02 for a B, 03 for a C, and so on until we get to 26 for a Z. Then the message "SMALLBRAINISTHECULPRIT" can be transformed into plaintext:
1913011212021801091409192008050321121
which would be broken up as the sequence
191,301,121,202,180,109,140,919,200,805,032

So the message now is a sequence of numbers; call it $m_1, m_2, ..., m_k$. The next step is to encode this message. To do this, the sender calculates, for $1 \leq i \leq k$, the value of n_i, where $n_i \equiv m_i^e\ (modN)$ The encoded message is the new list of numbers $n_1, n_2, ..., n_k$, and this is the message that is sent to the receiver. In the example above,
m_1= 191, N = 2257 and e = 11,
and using the method of successive squares, we have

$$191^2 \equiv 369(mod2257), 191^4 \equiv 741(mod2257), 191^8 \equiv 630(mod2257)$$

and hence

$$191^{11} \equiv 191^{8+2+1} \equiv 630 \cdot 369 \cdot 191 \equiv 2066(mod2257)$$

Hence $n_1 = 2066$. Similarly, we find that $n_2 = 483, n_3 = 914, n_4 = 1808$, and so on. So the encoded message is

$$2066,483,914,1808, ...$$

Once we have received the message, we have to decode it. In other words, given the received list of numbers $n_1, n_2, ..., n_k$, we need to find the original numbers $m_1, m_2, ..., m_k$, where $n_i \equiv m_i^e\ (modN)$. since e has been chosen to be coprime to (p − 1)(q − 1), we can use the Euclidean algorithm to find a positive integer d such that $de \equiv 1(mod(p-1)(q-1))$ Then the solution to the congruence equation $x^e \equiv n_i modN$ is $x \equiv n_i^d modN$. This solution must be the original number m_i, and hence we recover the original message $m_1, m_2, ..., m_k$ as desired.

So the receiver can decode the ciphertext as below
191,301,121,202,180,109,140,919,200,805,032,112,161
and then by the original substitutions, 01 for A, 02 for B, etc., you finally translate this into the urgent message: SMALLBRAINISTHECULPRIT

Shor's Algorithm

Until now, "factoring problem" is the basis of encryption for data transmission in classic computers. Whereas with the rapid developments of technology in quantum computers, by using hundreds of atoms, essentially in parallel, it seems that with the special physical properties of quantum gates which can save much time in solving "factoring problem", current encryption methods to protect security of our telecommunication will lose their functions.

In classical computing, numbers are represented by either 0s or 1s. These 0s and 1s are manipulated by an algorithm on a classic computer in order to produce an output based on an input. Quantum computing, on the other hand, utilizes atomic-scale units, also known as "qubits," which may be simultaneously 0 and 1 - a state known as a superposition. A qubit can perform two separate streams of calculations in parallel in this state, making computations faster than a traditional computer.

In 1994, Peter Shor, the Morss Professor of Applied Mathematics at MIT, came up with a quantum algorithm that calculates the prime factors of a large number, vastly more efficiently than a classical computer [4]. However, the algorithm's success depends on a computer with a large number of quantum bits. Although any integer number can be decomposed into a product of primes (proved by the fundamental theorem of algebra, also known as unique factorization theorem [8]), finding the prime factors is considered to be a difficult problem. Essentially, our online transactions are secure because factoring integers with many digits isn't practically possible. It was challenged in 1995 when Peter Shor proposed the Shor's algorithm [4], which may be the most dramatic example of how quantum computing changed our perception of what problems are tractable.

Quantum Fourier Transformation

Before getting into how Shor's algorithm works to be applied as a key tool for quantum computers to accomplish decrypting encryption methods like RSA cryptosystem, explaining "Quantum Fourier Transformation" is necessary as it is the most important mathematical tool for Shor's algorithm to conduct its functions.

The Fourier transform occurs in many different versions throughout classical computing, in areas ranging from signal processing to data compression to complexity theory. The quantum Fourier transform (QFT) is the quantum implementation of the discrete Fourier transform over the amplitudes of a wave function. It is part of many quantum algorithms, most notably Shor's (factoring) algorithm and quantum phase estimation.

The discrete Fourier transform acts on a vector $(x_0, x_1, x_2, x_3 ... x_{N-1})$ and maps in a vector $(y_0 ... y_{N-1})$ by the formula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

Where $\omega_N^{jk} = e^{2\pi i \frac{jk}{N}}$

Similarly, the quantum Fourier transform acts on a quantum state $|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ and maps it to output the quantum state $|Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$ by the same formula

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

This can also be expressed as the unitary matrix:

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle\langle j|$$

The QFT (quantum Fourier transform is) a transformation between two bases, the computational (Z) basis and the Fourier basis. The H-gate is the single-qubit QFT, and it transforms between the Z-basis states $|0\rangle$ $|0\rangle$ and $|1\rangle$ $|1\rangle$ to the X-basis states $|+\rangle$ $|+\rangle$ and $|-\rangle$ $|-\rangle$. Furthermore, all multiqubit states in the computational basis also correspond to states in the Fourier basis [9].

Circuit Implementation on Quantum Fourier Transformation

The circuit that implements QFT utilizes two gates-- single-qubit Hadamard gate and the controlled phase gate R_m, here in terms of

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^m} \end{pmatrix}$$

With $e^{2\pi i/2^m} = \omega'_m = \omega_{(2^m)}$ the primitive 2^m th root of unity.

A corresponding graph of quantum circuit *Figure.2* can be helpful to illustrate the use of these gates in the during the process of quantum Fourier transformation

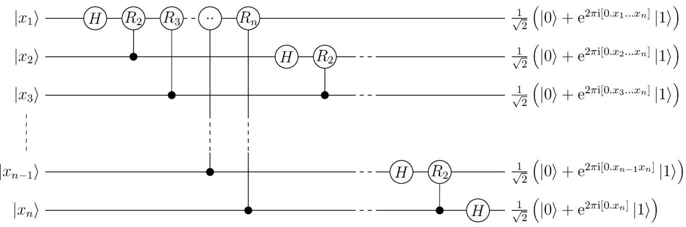
$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|x_{n-1}\rangle$
$|x_n\rangle$
H
R_2
R_3
R_n
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1...x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_2...x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_3...x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_{n-1}x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_n]}|1\rangle\right)$

Figure 2. The quantum circuit for quantum Fourier transformation [32]

The quantum gates labeled with represented Hadamard gates, while the gates labeled with represent phase gates that are used here as controlled gates (control qubit, as usual, indicated by a black dot and a connecting line to the target qubit; controlled phase). In the case of qubits, the quantum Fourier transform requires gates for the corresponding circuit as well as additional gates in order to bring the output qubits into the correct order $nO(n^2)O(n)$.

Additionally, as the QFT circuit becomes larger, an increasing amount of time is spent doing increasingly slight rotations. It turns out that rotations below a certain threshold can be ignored and decent results are still achieved, which is known as the approximate QFT that is important in physical implementations, as reducing the number of operations can greatly reduce decoherence and potential gate errors.

Operation of Shor's Algorithm

The problem that Shor's algorithm is trying to solve is that, given an integer N, find another integer p between 1 and N that divides N.

Shor's algorithm consists of two parts:

1. A reduction from the factoring problem to the problem of order-finding, which can be done on a classical computer.
2. A quantum algorithm to solve the order-finding problem.

Classical part

Pick a pseudo-random number a < N and then Compute Gcd(a, N). This may be done using the Euclidean algorithm. If Gcd(a, N) ≠ 1, then there is a nontrivial factor of N, so it is done. Otherwise, use the period-finding subroutine (below) to find r, the period of the following function:

$$f(x) = a^x (modN)$$

Calculate the smallest r such that $f(x + r) = f(x)$

If r is odd, go back to step 1. Otherwise, if $a^{r/2} \equiv -1(modN)$, go back to step 1. Otherwise then both $gcd\left(a^{r/2} + 1, N\right)$ or $gcd\left(a^{r/2} - 1, N\right)$ are nontrivial factors of N so the classical part is finished.

Quantum part: period-finding subroutine

1. Start with a pair of input and output qubit registers with log2N qubits each, and initialize them to
$$N^{-1/2}\Sigma_x|x\rangle|0\rangle$$
where x runs from 0 to N - 1.
2. Construct f(x) as a quantum function and apply it to the above state, to obtain
$$N^{-1/2}\sum_x |x\rangle|f(x)\rangle$$
3. Apply the quantum Fourier transform on the input register. The quantum Fourier transform on N points is defined by
$$U_{QFT}|x\rangle = N^{-1/2}\Sigma_y e^{2\pi ixy/N}|y\rangle$$
4. Perform a measurement. Some outcome y in the input register and f(x0) in the output register can be obtained. Since f is periodic. The probability to measure some y is given by
$$N^{-1}|\Sigma_x : f(x) = f(x_0)e^{2\pi ixy/N}|^2$$
$$= N^{-1}|\Sigma_b e^{2\pi i(x_0+rb)y/N}|^2$$
5. Turn y/N into an irreducible fraction, and extract the denominator r', which is a candidate for r.
6. Check if f(x) = f(x + r'). If so, the algorithm is done.
7. Otherwise, obtain more candidates for r by using values near y, or multiples of r. If any candidate works, the algorithm done.
8. Otherwise, go back to step 1 of the subroutine.

To summarize, the algorithm is composed of two parts. The first part of the algorithm turns the factoring problem into the problem of finding the period of a function, and may be implemented classically. The second part finds the period using the quantum Fourier transform, and is responsible for the quantum speedup.

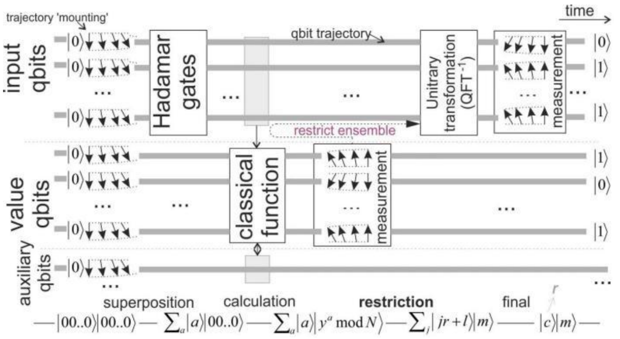

Figure 3. The operation of Shor’s algorithm in a quantum circuit [33]

The Time Complexity of Shor’s Algorithm

On a quantum computer, to factor an integer N, Shor's algorithm runs in polynomial time, meaning the time taken is polynomial in log N, which is almost the exponential acceleration of *e* for the most effective classical factorization algorithm known. It takes quantum gates of order $O((\log N)^2(\log\log N)(\log\log\log N))$ using fast multiplication thus demonstrating that the integer factorization problem can be efficiently solved on a quantum computer. This is almost exponentially faster than the most efficient known classical factoring algorithm which works in sub-exponential time: $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$. Such acceleration will break modern encryption mechanism such as RSA on a quantum computer [10].

Discussion

The discussion section discusses why and how Shor’s algorithm can destroy the RSA cryptosystem based on the knowledge in the literature review section and reveals the severe consequences in data security as well as in finance. To defend the cryptosystem against quantum computing, the section then introduces multiple categories of effective post quantum cryptography, which are designed to be robust under the attacks of quantum algorithms such as Shor’s algorithm. In particular, these post quantum cryptography algorithms include multivariate cryptography, code-based cryptography, lattice-based cryptography, and Hash-based cryptography. The main properties, applications, and development of these categories are next disussed. Furthermore, by analyzing the pros and cons of the above cryptographies, suggestions for the development of each are provided along with concluding a promising path for the post quantum cryptography.

The Collapse of RSA Cryptosystem in the Future

The security and robustness of RSA is based on the assumption that factorizing large integers into a product of prime numbers is computationally intractable. As far as known, this assumption is typically valid for classical (non-quantum) computers, which also means that the security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "NP hard problem"; no algorithms run on a classical computer is proved to be able to factor integers in polynomial time.

However, Shor's algorithm—a post quantum algorithm, theoretically succeeds solving this problem, which transforms the NP hard problem into an order-finding routine that is assessed on the quantum circuit as illustrated by the use of quantum Fourier transformation in the literature review section. As professor B.P.Lanyon and his colleagues indicates practicing a compiled version of Shor's algorithm in a photonic system using single photons and employing the non-linearity induced by measurement in 2007, which is the first time people demonstrate the core processes, coherent control, and resultant entangled states that are required in a full-scale implementation of Shor's algorithm [11] and consequently prove that by taking the Shor’s algorithm, it becomes possible to finally break the RSA cryptosystem by ultimately constructing a perfectly-designed quantum computer for Shor’s algorithm.

Severe Consequences of the Collapse of RSA Cryptosystem

The potential collapse of RSA cryptosystem due to the developing quantum technology will bring damaging impact on the daily lives of human being because RSA has widely essential applications in various industries. It indeed implies the fact that NP hard problem, which we used to consider as the most powerful mathematical tool to secure our data loses its time complexity because with a suitable quantum circuit, post quantum algorithms such as Shor’s algorithm can solve factorizing a huge prime number within seconds but it takes approximately thousands of years to factorize a 200-digit prime number on the most powerful classical computer by applying Euclidean algorithm; the key of the NP hard problem is the long-lasting time exploited in the process of prime number factorizing.

Data security an area where RSA plays an important role. RSA is one of the most important cipher suites used in TLS (Transport Layer Security), which is used by HTTPS (Hypertext Transfer Protocol), so RSA may be used in any connection to an https: URL (Uniform Resource Locator). In addition to security on transmission as explained in the section of literature review, Secrecy in storage is usually maintained by RSA cryptosystem where the user can provide the key (in this way RSA cryptosystem is transformed to use one key only) to the computer at the beginning of a session, and the system then takes care of encryption and decryption throughout the course of normal use. As an example, the data on disks of personal computers can be automatically encrypted with a variety of hardware devices. When the computer is turned on, the user ought to provide a key to the encryption hardware. The information cannot be read meaningfully without this key, so even if the disk is stolen, the information on it will not be useable [12].

Another important use of RSA cryptosystem is in economy. In the current financial system, the data stored in the servers such as the details of credits and debits of a multinational company apply the RSA cryptosystem or similar cryptography methods based on the NP hard problem for its high time complexity to avoid intentional attacks from the third party. In addition, Banks use encryption to secure sensitive information like credit card numbers or bank account information.This data is very crucial and if they are in the wrong hands it can ruin the banking system. Criminals may use this information to access customers’ bank accounts and withdraw or steal funds. Customers’ accounts can also be used as a medium of money laundering.To secure the customers’ data, encryption is used in which all the data is encoded before saving. In ideal cases, only higher management has the access to the encryption key but the collapse of encryption in bank system will lead to unauthentificated access to the data of banks so as to break the function of bank system. Another important use of it is in block chain, which is the basic principle of cryptocurrencies and the decentralization computations of digital assets in economy [13], a third party who would like to change or read the content of a single block, would have to essentially solve the RSA problem: finding the private key by solving the NP hard problem, which as mentioned, takes more than thousands of years on the classical computers. These damages

The collapse of RSA cryptography due to solving the NP hard problem will force the RSA-based encryption algorithms used in these important areas especially the finance to lose their functions, which means that the third-parties can easily read people's private information as they wish by operating Shor's algorithm on a quantum computer and fundamental data of servers can be easily read and changed by those people, thus leaving great potential threats to the developments in various areas.

Post Quantum Cryptography

As discussed in the previous content, the problem with many of currently popular crypto-algorithms is that their security relies on a hard mathematical problem: the factorization problem, which can be solved on a sufficiently powerful quantum computer running Shor's algorithm. Even though current, publicly known, experimental quantum computers lack processing power to break any real cryptographic algorithm [14], many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. The theory of constructing these algorithms are so called post quantum cryptography-- An area of cryptography that researches and advances the use of quantum-resistant primitives [15], with the goal of keeping existing public key infrastructure intact in a future era of quantum computing. Intended to be secure against both quantum and classical computers and deployable without drastic changes to existing communication protocols and networks.

Efficient Post Quantum Cryptosystems

Multivariate Cryptography

Multivariate cryptography is the generic term for asymmetric cryptographic primitives based on multivariate polynomials and solving systems of multivariate polynomial equations is proven to be NP-complete [16]. This includes cryptographic systems such as the Rainbow scheme which is based on the difficulty of solving systems of multivariate equations whose signature schemes like Rainbow can provide a unique building block for quantum secure digital signatures [17]. However, with long-lasting investigations in this post quantum encryption method, some drawbacks of it have been revealed and noted. As Adam Thomas Feldmann indicates in "A Survey of Attacks on Multivariate Cryptosystems" in 2005, Attacks using Gr¨obner bases, the XL algorithm and MinRank-base [18] can be useful in efficiently break this algorithm. In addition, due to the property of multivariate polynomials used in the multivariate cryptography, these attacks seem to be inevitable.

Code-based Cryptography

One of the few mathematical techniques allowing the construction of public-key cryptosystems that are secure against an adversary with a quantum computer is code-based cryptography [19]. This includes cryptographic systems which rely on error-correcting codes, such as the McEliece and Niederreiter encryption algorithms [20] and the related Courtois, Finiasz and Sendrier Signature scheme [21]. The main drawback of code-based schemes, including the popular proposals by McEliece and Niederreiter, are the large keys whose size is inherently determined by the underlying code, which is found to possibly be addressed by the use of rank instead of Hamming metric [22], but is not clear in the observable future.

Lattice-based Cryptography

Lattice-based cryptography is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. At the moment, lattice-based constructions are important candidates for post-quantum cryptography. Some lattice-based constructions seem to be resistant to attack by both classical and quantum computers, unlike some more widely used and known public-key schemes such as the RSA cryptosystem and many of them are considered to be secure under the assumption that some certain computational lattice problems [23] cannot be solved efficiently.

Hash-based Cryptography

Hash-based cryptography is the generic term for constructions of cryptographic primitives based on the security of hashing [24]. Hashing is a mathematical procedure that is easy to execute but is incredibly difficult to reverse. The difference between hash and encryption is that the encryption can be reversed or decrypted using a specific key. The most extensively used hash functions are MD5, SHA1, and SHA-256. Some hashing processes are considerably harder to crack than others [25]. A Lamport signature is an example of this cryptographic system [26]. A hash-based digital signature was invented in 1982 by Ralph Merkle [27] and has since been studied facinatingly as an alternative to number-theoretic digital signatures like RSA. The main drawbacks is that for any hash-based public key, there is a limit to the number of signatures that can be signed with the corresponding set of private keys, but compared to the drawbacks of some other known post quantum cryptograhies, it is not a severe problem because it will not affect its strong capability to resist attacks from quantum computers. Note that all the above schemes are one-time or bounded-time signatures, Moni Naor and Moti Yung invented UOWHF hashing in 1989 and designed a signature based on hashing (the Naor-Yung scheme) [28].

Future Directions of Post Quantum Cryptographies

The pros and cons of each of these efficient post quantum cryptographies are concluded in the last subsection. To survey the most promising path for the post quantum cryptographies, this subsection is going to give more details of each cryptography and compare their advantages as well disadvantages and give suggestions of which one is more promising in different applications.

Due to the inevitable attacks to Multivariate cryptography[18], it probably can not be considered independently as a mature base of cryptosystem resistant to attacks from quantum computers though it is proved efficient against certain attacks[18]. Its developments will also be restricted by the solvability of multivariate polynomial, which might be progressed with the development of quantum computers. Considering all these flaws, Multivariate cryptography should not develop as an individual field of cryptography when applying. Instead, it seems promising to utilize the features of multivariate polynomials in other maturer cryptosystems as a double ensuring of data security.

Code-based cryptography has exceptional mobility and plasticity[19], which may result in great advantage in the future because it means it can be conveniently transformed into other cryptosystems as a functional module. Though the large keys that can create large load on computer are not determined to be solvable (a potential solution is the use of rank instead of hamming metric).

Lattice-based cryptography is based on certain computational lattice problem such as shortest vector problem[23], which, like multivariate polynomials, may be solvable with the development of quantum computers[29]. But, currently there is no known efficient types of attack that can break it, which means, in the near future, it can act as temporary defense against high-load attacks[23].

Hash-based cryptography utilizes numerber theoretic principles- properties of Hash function which, like the use of factorzing problem in RSA cryptosystem, has high time complexity if cracked by classical algorithms. But Shor's algorithm can not crack it as well, which implies its high efficiency of defense against attacks from quantum computers. Its main drawback, as mentioned, the limit of the number of signatures that can be signed with the corresponding set of private keys, may lead to inconvenience in some practical uses but is not negative to its capability to resist attacks[30].

In general, based on the above, the future development of multivariate cryptography and code-based cryptography may be somewhat limited. Lattice-based cryptography is recommended as the main defense in the near future since the lattice computational problems are proved to hardly be solved. Furtermore, the Hash-based cryptography may serve as the main post quantum cryptography to act in cryptosystem, because it has also the mobility and plasticity for its mathematical properties and known threats to it is proved negligible to its main function to resist against attacks.

In addition, the Hash-based cryptography is proved efficient in practice because it has been used in finance. Except that its use in securing regular data such as bank accounts can be as powerful as RSA in face of attacks from official computers. In particular, When a company learns that the passwords of a network have been compromised, it typically means that hackers have obtained the password-representing hashes. Hackers then run the hashes of most used words and combinations of common words and numbers to decrypt some of the passwords that users have saved. The cybersecurity industry is now using the salting mechanism. Salting involves adding random data to the password before hashing it and storing the salt value with the hash. This process makes it more difficult for hackers to use the pre-computation techniques and crack the hashed data they have acquired. It also plays a important role in blockchain. Cryptographic hashing has long played a part in cyber defense and is poised to drive the coming wave of blockchain applications. Rather than other cryptographies listed which may only be very effectively functional in certain areas, Hash-based has other important uses in addition. For information-security applications, It can have notable usage in digital signatures, message authentication codes and fingerprinting etc.

Conclusion

To conclude, this paper explained the detailed operation and mathematical principles of the RSA cryptosystem and Shor's algorithm and, based on that, explained further the reason why cryptography in the past would lose its functionality to secure data dueto the maturity of quantum counting and the discovery of Shor's algorithm by comparing Shor's algorithm's complexity and analyzing the polynomial time of the operation of Shor's algorithm. To deal with the threats with the development of quantum counting, this paper studied four main branches of post quantum cryptography and analyzed their pros and cons. In addition, this work gave some suggestions and pointed out a path of developing for post quantum cryptography based on the analysis of existing branches post quantum cryptographies and their mathematical properties.

Conflict of Interests: the author has claimed that no conflict of interests exists.

References

[1] Katz, Jonathan, and Yehuda Lindell. 2014. Introduction to Modern Cryptography. 2nd ed. Chapman & Hall/CRC Cryptography and Network Security Series. Boca Raton, FL: CRC Press.

[2]Becket, B (1988). Introduction to Cryptology. Blackwell Scientific Publications. ISBN 978-0-632-01836-9. OCLC 16832704. Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems.

[3] Rivest, R., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM, 21, 120-126. http://dx.doi.org/10.1145/359340.359342

[4]Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-26.

[5]Tenzer, Theo (2021): SUPER SECRETO – The Third Epoch of Cryptography: Multiple, exponential, quantum-secure and above all, simple and practical Encryption for Everyone, Norderstedt, ISBN 9783755761174.

[6] Clifford Cocks CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security November 2013 Pages 463–474 https://doi.org/10.1145/2508859.2516672

[7] Martin Liebeck, "A concise introduction to pure mathematics" Pages 127-132 doi:http://dx.doi.org/10.1137/S0097539795293 172

[8]Maier H. (2008) Fundamental Theorem of Algebra. In: Floudas C., Pardalos P. (eds) Encyclopedia of Optimization. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-74759-0_193

[9]Chang, WL., Vasilakos, A.V. (2021). Quantum Fourier Transform and Its Applications. In: Fundamentals of Quantum Programming in IBM's Quantum Computers. Studies in Big Data, vol 81. https://doi.org/10.1007/978-3-030-63583-1_4

[10] Wikipedia https://en.wikipedia.org/wiki/Shor%27s_algorithm?msclkid=77bb5624ba7f11ecbd56bcc439b7f647

[11] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James*, A. Gilchrist, A. G. White Experimental demonstration of Shor's algorithm with quantum entanglement Physical Review Letters 99, 250505 (2007) https://doi.org/10.1103/PhysRevLett.99.250505

[12]Hegde, R. (2015). Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique.

[13]Vidal Attias, Luigi Vigneri, Vassil Dimitrov "On the Decentralized Generation of theRSA Moduli in Multi-Party Settings" https://doi.org/10.48550/arXiv.1912.11401

[14]Canadian Institute for Advanced Research "New qubit control bodes well for future of quantum computing". phys.org

[15]Atefeh Mashatan, Douglas Heintzman Communications of the ACM, September 2021, Vol. 64 No. 9, Pages 46-53 10.1145/3464905

[16] Garey, Michael R. (1979). Computers and intractability : a guide to the theory of NP-completeness. Johnson, David S., 1945-. San Francisco: W.H. Freeman. ISBN 0-7167-1044-7. OCLC 4195125.

[17]Ding, Jintai; Schmidt (7 June 2005). "Rainbow, a New Multivariable Polynomial Signature Scheme". In Ioannidis, John (ed.). *Third International Conference, ACNS 2005, New York, NY, USA, June 7–10, 2005. Proceedings*. Lecture Notes in Computer Science. Vol. 3531. pp. 64–175.

[18] Adam Feldmann (2005). A Survey of Attacks on Multivariate Cryptosystems. UWSpace. http://hdl.handle.net/10012/1032

[19]N. Sendrier, "Code-Based Cryptography: State of the Art and Perspectives," in IEEE Security & Privacy, vol. 15, no. 4, pp. 44-50, 2017, doi: 10.1109/MSP.2017.3151345

[20]Baldi, M. (2014). The McEliece and Niederreiter Cryptosystems. In: QC-LDPC Code-Based Cryptography. SpringerBriefs in

Electrical and Computer Engineering. https://doi.org/10.1007/978-3-319-02556-8_5

[21]Dallot, L. (2008). Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme. In: Lucks, S., Sadeghi, AR., Wolf, C. (eds) Research in Cryptology. WEWoRC 2007. Lecture Notes in Computer Science, vol 4945. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88353-1_6

[22]Heyse, S., von Maurich, I., Güneysu, T. (2013). Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices. In: Bertoni, G., Coron, JS. (eds) Cryptographic Hardware and Embedded Systems - CHES 2013. CHES 2013. Lecture Notes in Computer Science, vol 8086. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40349-1_16

[23]Micciancio D. (2011) Lattice-Based Cryptography. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_417

[24] Blanton M. (2018) Hash Functions. In: Liu L., Özsu M.T. (eds) Encyclopedia of Database Systems.. https://doi.org/10.1007/978-1-4614-8265-9_1482

[25] https://www.blockchain-council.org/blockchain/cryptographic-hashing-a-complete-overview/

[26] (2011) Lamport One-Time Signatures. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_1131

[27] Ralph C. Merkle, Secrecy, authentication, and public key systems (Computer science), UMI Research Press, 1982, ISBN 0-8357-1384-9.

[28]Moni Naor, Moti Yung: Universal One-Way Hash Functions and their Cryptographic Applications .STOC 1989: 33-43

[29]Richard J. Lipton; Kenneth W. Regan, "Shor's Algorithm," in Quantum Algorithms via Linear Algebra: A Primer , MIT Press, 2014, pp.97-108.

[30] Xiao, D., Liao, X., Deng, S. (2011). Chaos Based Hash Function. In: Kocarev, L., Lian, S. (eds) Chaos-Based Cryptography. Studies in Computational Intelligence, vol 354. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20542-2_5

[31] https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/

[32]https://en.wikipedia.org/wiki/Shor%27s_algorithm#/media/File:Shor's_algorithm.svg

[33]https://physics.stackexchange.com/questions/369590/shors-algorithm-why-doesnt-the-final-collapse-of-the-auxiliary-qubits-crippl