The International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2022)
DOI: 10.54254/2753-8818/2/20220098

Comparative Study of RSA Encryption and Quantum Encryption

Chenbo Sun

Ningbo Huamao International School, Ningbo, China, 315000

Oliver.Sun@nbhis.com

Abstract. Encryption is an important factor during online communication. It is useful to protect users' privacy and prevent eavesdroppers listening. RSA encryption and quantum encryption are two mainstream encryption methods applied nowadays. This paper focuses on the evaluation and comparison between these two encryptions. It adopts the basic theory of RSA encryption and quantum encryption and provides an analysis of the benefits and shortcomings of these encryptions. It can be concluded that RSA (a type of mathematical encryption) is more popular than quantum encryption (a kind of physical encryption), but is less secure.

1. Introduction

Safety is one of factors concerned in daily online conversation. Eavesdroppers may join the conversation secretly to get some information illegally. To solve this problem, people have developed some encryption methods to protect the online message. They use encryption to lock the message, and receivers need to use the key to open the lock. However, the eavesdroppers are still able to break the lock or get the key. Then, developers create various locks to prevent the hackers.

RSA encryption and quantum encryption are two mainstream methods of encryption nowadays. However, they are not a perfect way to protect message, which means they still have some drawbacks and they cannot be applied in all situations. Therefore, it is important to study about the advantages and disadvantages of these two encryptions and to find out the best way of using them.

2. Comparative analysis of RSA encryption and quantum encryption

Encryption has been developed for many years, and various ways of encryption have been invented. Symmetric encryption and asymmetric encryption are two main data encryption methods nowadays [1]. RSA is an asymmetric key encryption. In contrast to symmetric key encryption, in public key encryption, the message sender and receiver do not publish all keys. When person A is sending a message to person B with symmetric key encryption, A must use a public key to encrypt and B needs to use the same public key to decrypt.[2] This encryption is dangerous and easy to break down because an attacker can easily get the public key. While using public key encryption, A is holding a public key from B and B is holding a private key by himself. When A sends a message to B, A uses B's public to encrypt the message. If B want to decrypt the message, he must use the private key which is owned by himself only. This method is more secure because an attacker cannot easily obtain the private key.

RSA is one of the most reliable encryptions using the public key method. It follows the public key encryption method in those steps: [3]

Step 1: Select prime numbers p and q.

© 2023 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-8818/2/20220098

$$P = 3,\ q = 7$$

Step 2: Compute public modulus n = p x q

$$\varphi(N) = (p\text{-}1) \text{ x } (q\text{-}1) = 2 \text{ x } 10 = 20$$

Step 3: Computing euler function $\varphi(N) = (p\text{-}1) \text{ x } (q\text{-}1)$

$$\varphi(N) = (p\text{-}1) \text{ x } (q\text{-}1) = 2 \text{ x } 10 = 20$$

Step 4: Computing public Key e

$$1< e < \varphi(N),\ 1< e < 20$$

E must be interchangeable with φ(N), so the range of e (3,7,9,11,13,17,19)

Pick number e = 7

Step 5: Compute the private key

$$e * d \% \varphi(N) = 1$$
$$7 * d \% 20 = 1$$
$$7 \text{ x } 3 = 21$$
$$d = 3$$

Step 6: Encryption

Assume that the number of encrypted packets is 6, the plaintext is A, and the ciphertext is B

$$B = A\text{^}e \% N = 6 \text{ ^ } 7 \% 33 = 279936 \% 33 = 30$$

Step 7: Decryption

$$A = B\text{^}d \% N = 30 \text{ ^ } 3 \% 33 = 27000 \% 33 = 6$$

Step 8: Homomorphic encryption

The ciphertext of plaintext A1 and A2 is B1 and B2

B1 times B2 is A1 to the e times A2 to the e, so it satisfies the multiplicative homomorphism.

It is basically using the factorization method with prime numbers to provide a key. Prime numbers are unpredictable using traditional computing methods, so it is relatively safe compared to traditional encryptions.

However, the RSA algorithm can be attacked in the following ways: [4]

Brute-force attack: This method attempts to exhaustive all possible private keys;

Mathematical attacks: There are a variety of mathematical attacks that essentially attempt to decompose the product of two prime numbers.

Timing attack: This attack method analyses the running time of encryption to try to decrypt.

Attack based on hardware fault: this method applies to the processor failure in the process of generating signatures;

Select ciphertext attack: use the properties of RSA algorithm;

Common modulus attack: As the speed of generating large prime numbers is still relatively slow at present, some people choose the same large prime numbers, that is, the same modulus, but different keys, in order to speed up the algorithm. It speeds up the process, but it also brings security risks to RSA algorithms.

Quantum computer can break RSA encryption.

That is why people are still developing on the safety of RSA with studying more about it.

Quantum encryption is an entirely different system. “Quantum cryptography uses the laws of quantum physics to transmit private information in a way that makes undetected eavesdropping impossible.” [5] Traditional encryption methods are based on mathematics, but quantum encryption is based on the laws of quantum which is a part of physics. The principle of quantum encryption can be summarized as following method. [6]

When the photon propagates forward, it will vibrate in the direction of up and down or left and right, that is, the direction of vibration is perpendicular to the direction of advance. At this time, if a baffle with a small gap is set in the direction of advance of the photon, so that when the polarization direction is consistent with the direction of advance, the light beam can pass through, and vice versa will be blocked.

DOI: 10.54254/2753-8818/2/20220098

Figure 1. Light beam pass through the gap.

A photon vibrating vertically up and down represents 0, and a photon vibrating left and right represents 1, which can be called plan A. Users can also rotate the polarized light 45 degrees, so that the 45 degree polarized light represents 0 and the 135 degree photon represents 1, and it can be called plan B. At this point, users can emit values like 0 or 1 through two different plans, A and B. Of course, the receiver can also use A, and B two sets of plans for measurement. One photon sent is a qubit as a unit.

Table 1. Directions of light beam vibration.

Basis	0	1
+	↑	→
×	↗	↘

Here is an example. There is a sender Alice, a receiver Bob and an eavesdroppers Eve.

Alice generates a sequence randomly, 011010101 for example, and then she randomly selects a transmitting photon in plan A and B, namely Qubits, for each value of the sequence. Alice just has to remember the random sequence and the plan she used to send each number.

Bob uses two plans A and B randomly to detect photons and record whether the optical information is 0 or 1.

After all the quantum bits are transmitted, Alice and Bob talk on the phone in an open way. Bob tells Alice the measurement method of each quantum bit in turn without specifying the specific measurement value. Alice only needs to tell Bob which method of measuring quantum bits is correct.

Eventually, Bob knows which qubits are correct, and Alice knows which ones Bob has correctly measured, so the two can use the information as a password for each other.

In addition, Bob and Alice know someone is eavesdropping when they notice a change in the image of the photons on the screen. Eve eavesdrops on the photon transport, which is equivalent to adding detectors in front of the double slits in a two-slit interference experiment, and the streaks of light and dark on the screen disappear.

Since Bob randomly chooses plan A and plan B to measure the data sent by Alice, the probability of Bob choosing a wrong plan is 1/2. Depending on the nature of the light's polarization, a left-right or up-down photon can actually pass through a gap of 45 degrees or 135 degrees, but which angle it passes through is completely random. Then the photon sent by plan A, measured by plan B, has a half chance of being wrong. All told, Bob should be wrong about one-fourth of the time and right about 3/4 of the time. If Eve eavesdrops on the channel, the message becomes 9/16 of its original value. So as long as Bob and Alice check some of the data to see if it's correct less than 3/4 of the time, they can determine whether someone is listening.

The quantum encryption method is unbreakable because it is encrypted physically. Also, if any eavesdroppers join, it will be known. The future of quantum encryption is very promising. Quantum mechanics is the only proven way to produce random number, and it is what mathematic methods cannot achieve [7]. Nevertheless, it has a limitation: two people in communication must confirm that none of them is a pretended eavesdropper. Also, as quantum encryption is a new technology, it is still experience to build a quantum computer. “Such systems are expensive to implement, with the most common

DOI: 10.54254/2753-8818/2/20220098

polarization-based protocol, known as BB84, requiring four single-photon detectors, costing US$5,000 to $20,000 each, the NIST said." [8]

Both these two encryption methods have their own advantages and disadvantages. The reason people like to use quantum encryption is: physical method is more reliable; RSA can be attacked by a plenty of mathematic methods; RSA algorithm occupies much computing resources because the regular encryption length of the RSA algorithm is 2048 bits. The server consumes a lot of data, and the computing speed is slow and the efficiency is low.

Quantum encryption still has some problems, so people are still using the RSA method. The reason is: RSA is a popular algorithm. It is applied in many areas and systems and this technology is experienced; Quantum is still in a developing process; The quantum system is way more expensive than traditional encryption methods.

3. Conclusion

This paper is focusing on the comparison research between RSA and quantum encryption. It provides some theories about these two encryptions and advantages and disadvantages of using them respectively.

RSA is more popular encryption method because of its cheapness. Many people use this method to protect their information and messages. It is also a comparatively safe encryption method as traditional symmetric encryption is backward. However, the time required for encryption with RSA is pretty long, so eavesdropper may have enough time to hack the information. Furthermore, because RSA is based on mathematical method to encrypt, the safety of RSA is not wonderful comparing to quantum encryption.

The benefit of using quantum encryption is obvious: it is physical encryption method. However, it is also a disadvantage of this encryption, because quantum encryption device cost a lot and most firms are not able to afford the device. As quantum encryption is not a proven technology, not many people are using it.

These benefits and drawbacks of the two encryption methods are mostly considered for encryption choosing.

As this essay research is not studied from practice, it is not detailed enough. Future study with more practical research can find out more solutions of RSA attack and design a more detailed quantum encryption device.

References

[1] Daniel, Brett. "Symmetric vs. Asymmetric Encryption: What's the Difference?" Trenton Systems, 4 May 2021, https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption. Accessed 15 March 2022

[2] Brush, Kate. "Asymmetric Cryptography (Public Key Cryptography)." Tech Target, https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography. Accessed 14 March 2022.

[3] Kaliski, Burt. "The Mathematics of the RSA Public-Key Cryptosystem." Accessed 15 March 2022.

[4] Boneh, Dan. "Twenty Years of Attacks on the RSA Cryptosystem." Accessed 18 March 2022.

[5] Caltech's Faculty. "How Will Quantum Technologies Change Cryptography?" Caltech, https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography. Accessed 20 March 2022.

[6] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, and Jun Shen. "Quantum Cryptography for the Future Internet and the Security Analysis." Hindawi, https://www.hindawi.com/journals/scn/2018/8214619/. Accessed 21 March 2022.

[7] Mandich, Denis. "Quantum Encryption: The Basics." Info Security, 14 Feb. 2022, https://www.infosecurity-magazine.com/opinions/quantum-encryption-the-basics/. Accessed 19 March 2022.

DOI: 10.54254/2753-8818/2/20220098

[8] Broersma, Matthew. “Discovery slashes quantum cryptography cost.” PC World, 4 June 2008,https://www.pcworld.idg.com.au/article/223238/discovery_slashes_quantum_cryptography_costs/. Accessed 22 march 2022.