Post Quantum Cryptography: Comparison between RSA and McEliece

Conference Paper · August 2022

DOI: 10.1109/ICISS55894.2022.9915232

I Putu Agus Eka Pratama
Udayana University
94 PUBLICATIONS **481** CITATIONS
SEE PROFILE

Agung Krisna
Udayana University
1 PUBLICATION **7** CITATIONS
SEE PROFILE

Post Quantum Cryptography: Comparison between RSA and McEliece

1st Pratama, I Putu Agus Eka
Department of Information Technology, Faculty of Engineering
Udayana University
Jimbaran, Indonesia
eka.pratama@unud.ac.id

2nd Adhitya, I Gusti Ngurah Agung Krisna
Department of Information Technology, Faculty of Engineering
Udayana University
Jimbaran, Indonesia
agungkrisna200@gmail.com

***Abstract*—Cryptography is one of the techniques used to secure the process of communication in the presence of an adversarial party. Public key cryptosystem allows the process of encryption and decryption to use two different keys. The current de-facto algorithm for public key cryptosystem is the RSA. However, this cryptosystem is now considered insecure in the presence of quantum computing. The insecurity of this cryptosystem comes from an algorithm that can efficiently solve the Integer Factorization Problem, which has been the strength of RSA cryptosystem. Shor's algorithm can factor composite integers into its prime factors using a quantum computer in polynomial time. This research will give an insight on an alternative public key cryptosystem that is quantum resistant. The result of this research shows that while the RSA has better average time than the McEliece cryptosystem, McEliece cryptosystem has better cryptographic strength when compared to RSA.**

Keywords—post quantum, cryptography, RSA, McEliece, code-based cryptography

I. Introduction

The ability of quantum computers to solve the Integer Factorization Problem has become a serious threat to the security of conventional public key cryptosystems such as RSA and ElGamal. The security of the RSA cryptosystem lies in the difficulty to factor a composite integer into its prime factors, which currently no known algorithm can solve the problem using a classical computer. Shor [1] created an algorithm that can solve the integer factorization problem in polynomial time using a quantum computer. Shor's algorithm has space complexity of $O(log\, n)$ and time complexity of $O((log\, n)^3)$ [2]. This algorithm will efficiently break cryptosystems that rely on integer factorization problems and discrete logarithms. By using a post quantum public key cryptosystem, the security of messages that are being sent can remain unbreakable, even when an adversarial party has access to quantum computers. There are a few post quantum cryptosystems that have been published and nominated as finalists in NIST's contest for standardization of post quantum cryptosystems [3]. One of the cryptosystems that are nominated as a finalist in the Classic McEliece. This cryptosystem is not a newly discovered one, and some research analyzes the security of this cryptosystem [4], [5]. Those research concluded that this cryptosystem remains secure, even when subjected to attacks using quantum computers.

II. Research Methodology

A. Research Questions

In order to keep the essence of the literature review that will be undertaken, we defined some problems that will be researched in this paper, including:

1) *Q1: Why RSA Cryptosystem is breakable by quantum computers?*

2) *Q2: What is the alternative cryptosystem that has no known efficient algorithm that can break the cryptosystem, even when using a quantum computer?*

3) *Q3: How does the alternative cryptosystem compare to the RSA in terms of the effectiveness of the cryptosystem?*

B. State of the Art

There is a lot of research focusing on the conventional public key cryptosystem and the post quantum cryptosystem. However, there was no published research focuses on comparing the conventional public key cryptosystem and post quantum cryptosystem, specifically the McEliece cryptosystem and the RSA cryptosystem in terms of cryptographic strength, computational complexity, and the effectiveness of the cryptosystem. Hence, this research was created to facilitate the process of understanding the differences between RSA and McEliece cryptosystem. The tabular representation below will illustrate some papers that become the present state-of-the-art.

TABLE I. State of the Art

Ref	Summary
[6]	McEliece cryptosystem is a quantum resistant cryptosystem due to the difficulty of decoding a random linear code.
[7]	Although breaking the RSA cryptosystem is hard in general, there are some implementation errors that allow attackers to break RSA even using a classical computer.
[8]	Neiderreiter and McEliece cryptosystems can both be used as an alternative public key cryptosystems, however, the McEliece cryptosystem has a probabilistic characteristic as opposed to the deterministic characteristic in the Neiderreiter cryptosystem.
[9]	McEliece cryptosystem cannot be broken using Quantum Fourier Sampling, the technique that can break most of the conventional public key cryptosystem that is based on integer factorization and discrete logarithm.

C. Literature Review

1) Quantum Computers

Quantum computers are a type of computer that exploits the principles of quantum mechanics in order to process information in a way that is impossible to replicate on a classical computer. Quantum computers have the ability to represent "0" and "1" bit at the same time by exploiting the superposition property in quantum mechanics.

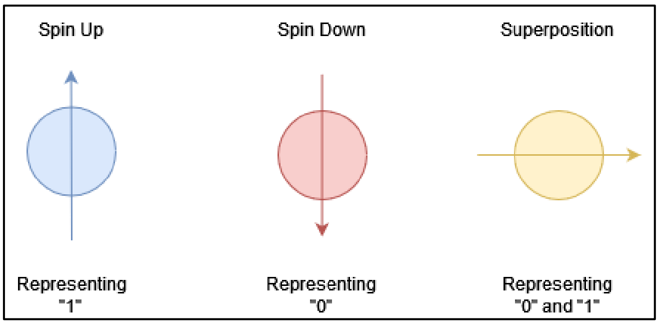

Fig. 1. Superposition in quantum computing

Quantum computer bits (qubits) can hold and process much more information than their classical counterpart, for example, 1000 qubits can hold information up to 2^{1000} ($\approx 10^{300}$) and manipulate that information in parallel at the same time. However, out of 10^{300} information, it will only pick one result at random during the process of reading their final state and all other information will disappear [10]. This is one of the main limitations in quantum computing, but there is a technique to gain the desired result by using a phenomenon called destructive interference. Shor's algorithm is able to use this phenomenon and able to factor large integers in polynomial time [1].

2) *Finite Field*

A finite field is a field with a finite number of elements and has the capacity to perform multiplication and addition. The definition of a field can be formally defined [6], as:

Definition 2.1: A field is a nonempty set F of elements with two operations '+' (addition) and '·' (multiplication), which satisfies the following for all a, b, and c ∈ F:

a) Closure with respect to addition and multiplication: a + b ∈ F and a · b ∈ F.

b) Commutative with respect to addition and multiplication: a + b = b + a and a · b = b · a.

c) Associative with respect to addition and multiplication: (a + b) + c = a + (b + c) and (a · b) · c = a · (b · c).

d) Distributivity holds on addition over multiplication: (a + b) · c = a · c + b · c.

e) a + 0 = a, ∀a ∈ F

f) $a \cdot 1 = a$ and $a \cdot 0 = 0, \forall a \in F$

g) $\forall a \neq 0 \in F, \exists a^{-1}: a \cdot a^{-1} = 1$

In order for a field to be finite, it can only have prime number of elements. In this research, the type of finite field that is in use is the binary finite field (F_2^n) which only has two elements, $\{0, 1\}$. A more thorough explanation with regard to finite field can be seen at [11].

3) *Goppa Code*

Goppa code is a family of linear code that is used to perform error correction alongside decoding messages using McEliece cryptosystem. Goppa code is the recommended family of linear code for McEliece cryptosystem because of the suitable properties for cryptographical use, this recommendation was given by the creator of the cryptosystem himself [12]. Goppa code can be formally defined as:

Definition 2.2: Goppa polynomial can be defined as a polynomial in $\mathrm{F}(\mathrm{p}^{\mathrm{m}})$*, where:*

$$g(x) = g_0 + g_1 x + \cdots + g_t x^t = \sum_{i=0}^{t} g_i x^i \tag{1}$$

The syndrome of vector c ∈ $\mathrm{F}_{\mathrm{n}}^{2}$ *can be defined as:*

$$S_c(x) = \sum_{i=0}^{n-1} \frac{c_i}{x - a_i} \tag{2}$$

A binary goppa code is a c ∈ $\mathrm{F}_{\mathrm{n}}^{2}$ which has the identity of $\mathrm{S}_{\mathrm{c}}(\mathrm{x}) = 0$. To check whether *c* is a part of C, Goppa code has the parity check matrix H with the dimension of t × n.

Goppa code can correct up to t errors. To decode messages using this family of linear code, use Patterson's algorithm in order to have the most optimum rate of efficacy.

4) *RSA Cryptosystem*

RSA cryptosystem is a public key cryptosystem that leverages the difficulty of integer factorization as the security of their cryptosystem. This cryptosystem has two distinct keys, namely the public key and the private key. Public key is utilized to encrypt messages and the private key is utilized to decrypt messages. In using public key cryptosystem, there are three main processes that must be done in order to exchange information between two parties, namely the key generation, message encryption, and message decryption [13].

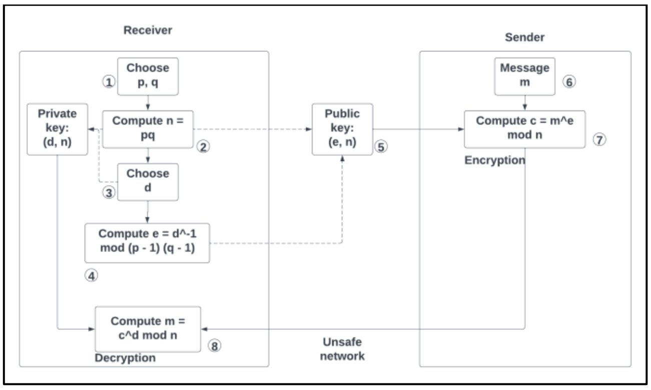

Fig. 2. Communication scheme using RSA cryptosystem

Key generation process starts with choosing two prime numbers, p and q. Compute the value of n where n is the product of p and q ($n = pq$).

Choose a large integer d at random, where the greatest common divisor of d and $(p-1)(q-1)$ is equal to 1.

Compute the value of e by finding the multiplicative inverse of d: $e = d^{-1} \bmod (p-1)(q-1)$. The value of e and d are related. The relation between the two keys can be expressed as:

$$ed = 1 \bmod (p-1) \cdot (q-1) \tag{3}$$

The RSA public keys are comprised of the value of n and e, and the private keys are comprised of d and e.

To encrypt a message, the sender must first convert the alphanumerical message m into sits numerical value where $m \in Z$. Message encryption is done by computing the modular exponentiation between m and e with the modulus of n.

$$c = m^e \bmod n \quad (4)$$

To decrypt a message, the receiver needs to compute the value of modular exponentiation between c and d with the modulus of n.

$$m = c^d \; mod \; n \quad (5)$$

Although this cryptosystem is the de-facto standard for public key cryptosystem, there exists a method to efficiently break the security of RSA using Shor's algorithm. This research [14] successfully implemented Shor's algorithm on IBM Q quantum computer and has succeeded in factoring n with the value of $n = 15$ and $n = 21$ with just 16 qubits.

5) McEliece Cryptosystem

McEliece cryptosystem is a public key cryptosystem that leverages the difficulty of decoding a random linear code. Due to the fact that this is a public key cryptosystem, it has two distinct keys, namely the public key and the private key.

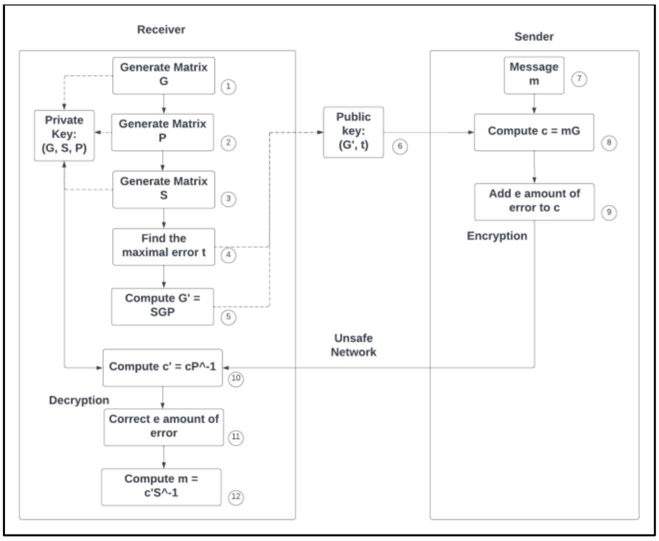

Fig. 3. Communication scheme using McEliece cryptosystem

There are three important processes that must be done in order to be able to exchange information between two parties. Those processes are key generation, message encryption, and message decryption.

Private keys consist of a generator matrix G from the goppa polynomial $g(z)$ with the degree of t, a scrambler matrix S, and a permutator matrix P.

Public keys consist of a matrix G' whose value is derived from the product of matrix multiplication between S, G, and P. The maximum amount of error t is also included in the public key.

$$G' = SGP \quad (6)$$

Encryption is done by multiplying G' with message bits m, and then adding random error e with an amount lesser than t.

$$c = mG' + e \quad (7)$$

To decrypt a message, the receiver must compute the value of c' by multiplying c with the multiplicative inverse of permutator matrix P.

$$c' = c \cdot P^{-1} \quad (8)$$

After acquiring the value of c', the receiver must correct e amount of error by using Goppa Code G to acquire the value of m'.

Because the value of m' is still in a scrambled form, multiply the value of m' and the multiplicative inverse of scrambler matrix S in order to find the original message m.

$$m = m' \cdot S^{-1} \quad (9)$$

This algorithm is considered to be able to resist the attack of quantum computers. This is caused by the fact that there is no available algorithm that can efficiently decode a random linear code [5]. The complexity of this problem has been classified as NP-Hard [15].

III. Research Result

In this research, we will measure the quantitative performance of each cryptosystem in order to answer the research questions.

- Lenovo Legion 5 Pro
- Processor: AMD Ryzen 7 5800H
- Memory: DDR4 16 GB
- Storage: SSD 1 TB

The list above is the specification of the device that was used to measure the performance of each cryptosystem.

The software that were used in measuring the performance can be seen in the list below.

- Debian-based Operating System (Elementary OS 6.1)
- C compiler (gcc version 9.4.0)
- C++ compiler (gcc version 9.4.0)
- Git version 2.25.1 (Version Control System)

The program that was used to measure the performance of the RSA cryptosystem was acquired from the Github code repository and was created by Shane Tully [16]. The program that was used to measure the performance of the McEliece cryptosystem was acquired from the Github code repository and was created by a user with the username of Varad0621 [17].

Each cryptosystem will be tested ten times in order to reduce the likelihood of random error when measuring its efficiency.

The parameters that were used in the McEliece cryptosystem come from the recommendation of the creator of the cryptosystem himself [12] and the latest recommendation from NIST [18]. Those parameters are presented in tabular form as follows in the table below.

TABLE II. PARAMETERS FOR MCELIECE CRYPTOSYSTEM

Parameter	Value
n_0	2

t	20
w	45
P	1000

The parameters that were used in order to measure the efficiency of RSA cryptosystem come from the recommendation of NIST [19]. Those parameters are presented in tabular form as follows in the table below.

TABLE III. PARAMETERS FOR RSA CRYPTOSYSTEM

Parameter	Value
N	2048 bit

A. *Why RSA Cryptosystem is breakable by quantum computers?*

RSA cryptosystem is now considered to be breakable by quantum computers because of Shor's algorithm. This algorithm consists of two parts, the first part is the reduction of integer factorization into an order-finding problem, and the second part is to utilize the power of quantum computing in order to solve the order-finding problem. Quantum Fourier Sampling is the algorithm that allows quantum speedup, allowing Shor's algorithm to run in polynomial time[9].

B. *What is the alternative cryptosystem that has no known efficient algorithm that can break the cryptosystem, even when using a quantum computer?*

McEliece is an alternative public key cryptosystem that resists quantum computing attacks by leveraging the difficulty of decoding a random linear code. This public key cryptosystem does not have the same weakness as the RSA, which has been considered broken due to the existence of an algorithm that can break the integer factorization problem.

The difficulty of factoring a large integer was the key of success in the RSA cryptosystem. Up until this point in time, there is no non-quantum integer factorization algorithm that can run in polynomial time using a classical computer. However, a quantum computer can solve the integer factorization problem by using Shor's algorithm. Shor's algorithm can break RSA cryptosystem in $O((\log n)^3)$, making it a very serious threat to the security of the messages that were encrypted using this cryptosystem.

Although the difficulty of decoding a random linear code has been classified as an NP-hard problem, there exists another method of attacking the McEliece cryptosystem called the information set decoding. This method of attack requires 2^{64} binary operations to break a linear code with the length of 1024 bits [20] and gets exponentially harder to break with longer message bits.

C. *How does the alternative cryptosystem compare to the RSA in terms of the effectiveness of the cryptosystem?*

The result from testing both of the cryptosystems will give an understanding of their performance in terms of the required time to generate a key, encrypt, and decrypt a message. The performance of the McEliece cryptosystem is presented in TABLE IV. and the performance of the RSA cryptosystem is presented in TABLE V.

TABLE IV. TIME REQUIRED FOR MCELIECE CRYPTOSYSTEM

Test trial	Key Generation (s)	Encryption (s)	Decryption (s)
1	4.8	0.03	0.03
2	5.2	0.03	0.03
3	5	0.04	0.03
4	4.6	0.04	0.03
5	4.7	0.04	0.03
6	4.8	0.03	0.03
7	4.8	0.03	0.03
8	4.8	0.03	0.03
9	4.9	0.03	0.03
10	5	0.03	0.03
Average	5	0.03	0.03

TABLE IV. shows that the average time for McEliece cryptosystem to generate a keypair is 5 seconds. Encryption took 0.03 seconds, and decryption took 0.03 seconds. This result shows that McEliece cryptosystem has quick encryption and decryption time however it's relatively slow to finish the key generation process.

TABLE V. TIME REQUIRED FOR RSA CRYPTOSYSTEM

Test Trial	Key Generation (s)	Encryption (s)	Decryption (s)
1	0.03	0.001	0.001
2	0.07	0.001	0.008
3	0.03	0.001	0.008
4	0.07	0.001	0.008
5	0.01	0.001	0.007
6	0.04	0.001	0.007
7	0.07	0.001	0.007
8	0.02	0.001	0.007
9	0.08	0.001	0.007
10	0.03	0.001	0.009
Average	0.04	0.001	0.007

TABLE V. shows that the average time for RSA cryptosystem has average of 0.04 seconds in order to generate a keypair. Encryption has an average time of 0.001 seconds, and decryption has an average time of 0.007 seconds. The current implementation of RSA cryptosystem has a significantly faster time in performing three important processes in the public key cryptosystem, namely the key generation, encryption, and decryption.

IV. CONCLUSIONS AND FURTHER WORK

Code-based cryptography that is implemented in the McEliece cryptosystem has a great potential in being an alternative to the conventional public key cryptosystem such as RSA. This is caused by the lack of availability of an efficient algorithm that can break the McEliece cryptosystem, even with the help of quantum computers. The tests that have been done in this research allow us to discover that the current implementation of the RSA cryptosystem has a significantly faster performance than the McEliece cryptosystem. However, due to the fact that an efficient algorithm with the capability to break RSA security exists, the need for having a post quantum cryptosystem has now increased more than ever.

Although the current implementation of McEliece cryptosystem is not as fast as RSA cryptosystem, it is not unlikely that McEliece cryptosystem will have some improvements and optimization in order to reduce the time required to perform the three main processes in public key cryptosystem, namely the key generation, encryption, and decryption.

Regarding the implementation of McEliece cryptosystem, some additional analyzes can be useful in order to find the most efficient method in key generation, which has been the slowest process in this cryptosystem. Furthermore, more tests can be done in various computing devices in order to find the optimum and minimum amount of computational resource that is required for this cryptosystem.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring.," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Jun. 1994.

[2] P. Véron, "Code Based Cryptography and Steganography," Jun. 2013. doi: 10.1007/978-3-642-40663-8_5.

[3] NIST, "Post-Quantum Cryptography Standardization." Jun. 2017. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[4] A. S. Bhatia and A. Kumar, "McEliece Cryptosystem Based On Extended Golay Code," *ArXiv*, vol. abs/1811.06246, 2018.

[5] P. Z. Marek Repka, "Overview of the McEliece Cryptosystem and its Security," *Tatra Mountains Mathematical Publications*, vol. 60, 2014, [Online]. Available: https://www.researchgate.net/profile/Marek_Repka/publication/273902880_Overview_of_the_Mceliece_Cryptosystem_and_its_Security/links/5659c2a208ae1ef9297fb19e.pdf

[6] H. Singh, "Code based Cryptography: Classic McEliece," *arXiv*, Jun. 2019, doi: 10.48550/ARXIV.1907.12754.

[7] A. Abubakar *et al.*, "Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) Cryptosystem: Issues and Challenges," *Journal of Applied and Theoritical Information Technology*, vol. 61, pp. 1–7, Jun. 2014.

[8] N. Bardis, V. Kharchenko, O. Potii, and A. Vambol, "Post-Quantum Network Security: McEliece and Niederreiter Cryptosystems Analysis and Education Issues post-quantum cryptography," *WSEAS Transactions on Systems and Control*, vol. 15, pp. 627–634, Jun. 2020, doi: 10.37394/23203.2020.15.62.

[9] H. Dinh, C. Moore, and A. Russell, "The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks," *arXiv*, Jun. 2010.

[10] S. Aaronson, "The limits of quantum," *Sci Am*, vol. 298, no. 3, pp. 62–69, 2008.

[11] W. Stallings, *Cryptography and network security principles and practice*. Prentice Hall, 2011.

[12] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[13] E. Milanov, "The RSA algorithm," *RSA laboratories*, pp. 1–11, 2009.

[14] M. Amico, Z. H. Saleem, and M. Kumph, "Experimental study of Shors factoring algorithm using the IBM Q Experience," *Physical Review A*, vol. 100, no. 1, Jul. 2019, doi: 10.1103/physreva.100.012305.

[15] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems (Corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978, doi: 10.1109/TIT.1978.1055873.

[16] S. Tully, "Crypto-Example." [Online]. Available: https://github.com/shanet/Crypto-Example

[17] Varad0612, " The McEliece Cryptosystem." [Online]. Available: https://github.com/Varad0612/The-McEliece-Cryptosystem

[18] J.-P. T. Nicolas Sendrier, "QC-MDPC: A public-key code-based encryption scheme based on quasi-cyclic moderate density parity check codes." [Online]. Available: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session1-tillich-jean-pierre.pdf

[19] E. Barker, E. Barker, W. Burr, W. Polk, M. Smid, and others, *Recommendation for key management: Part 1: General*. National Institute of Standards and Technology, Technology Administration~…, 2006.

[20] N. K. Chaubey and B. B. Prajapati, *Quantum Cryptography and the Future of Cyber Security*. IGI Global, 2020.