Journal of IoT and Intelligent Solutions
Available online: http://jiotis.com

Vol 1, No. 1, June 2023, pp. 64 - 67

Quantum decryption: Exploring the potential risk of data security

[1*]Omar Sallam and [1]Reda Ali Deeb

[1]Faculty of Computer Engineering ,
Halic University,
Istanbul,Turkey
**Corresponding Author*: 22092090098@ogr.halic.edu.net

Article Info

Article history:

Article received on 24 04 2023

Received in revised form 24 04 2023

Keywords:

Encrypted; Intercepted; Quantum computers; SNDL

ABSTRACT: Governments and individuals are intercepting and storing encrypted data, including sensitive information like passwords and military intelligence, which they believe they will be able to decrypt in the future using quantum computers. This technique, known as "save now decrypt later," is based on the assumption that certain types of data will remain valuable for many years. While there are currently no massive quantum computers capable of breaking encryption, the threat of this technology has prompted major corporations to develop quantum-resistant encryption. This is necessary because a powerful enough quantum computer would be able to crack all commonly used public key algorithms, according to the US National Security Agency.

1. INTRODUCTION

Prior to the 1970s, confidential information could only be exchanged through physical meetings with the exchange of a secret key, which is known as a symmetric key algorithm. But with the advent of remote communication, secure exchange of information became difficult. This led to the development of RSA, a breakthrough encryption technique developed by Ron Rivest, Adi Shamir, and Leonardo Adelman. RSA uses two large prime numbers that are multiplied together to get an even larger number, which is made public. When someone wants to send a private message, they use the recipient's public number to encrypt the message. Decoding the message without knowing the two prime factors of the public number is virtually impossible, making it easy for the intended recipient to decode. Current encryption employs prime factors that are around 313 digits long, which even with supercomputers would take around 16 million years to factor, but not with quantum computers.

2. PROBLEM STATEMENT

With the rise of quantum computing technology, there is growing concern that current encryption methods, like RSA encryption, may be vulnerable to attacks from quantum computers. Quantum computers can process information in several states at once due to the principles of quantum physics, making many widely-used encryption schemes susceptible to unauthorized access. To address this issue, academics and professionals are researching the creation of encryption methods that can resist quantum attacks. Studies on quantum teleportation, quantum-inspired classical algorithms, and quantum parameter estimation could potentially lead to the development of quantum-resistant encryption. To protect sensitive data, governments and businesses are investing in quantum-resistant encryption development, but more research is needed as this technology is still in its early stages.

3. LITRETURE REVIEW

[Niu et al., 2018] report a measurement-device-independent quantum secure direct communication protocol using Einstein-Podolsky-Rosen pairs[1]. [Nejatollahi et al., 2019] survey trends in lattice-based cryptographic schemes, some recent fundamental proposals for the use of lattices in computer security, challenges for their implementation in software and hardware, and emerging needs for their adoption[3]. [Kumar et al., 2019] propose to improve data security by increasing the key size shared between parties involved in quantum cryptography[4]. [Pirandola et al., 2019] provide a general introduction and a state-of-the-art description of recent advances in the field of quantum cryptography[5]. In contrast, [Jaques et al., 2019] introduce techniques that reduce the oracle depth, even if it requires more qubits[6], while [Falco et al., 2019] show perfect secrecy cryptography in classical optical channels[7]. Other influential works include [Khan et al., 2018][8], [Kumar et al., 2019][9], and [Moody et al., 2020][10].

4. METHODOLOGY

This research used a qualitative research design to investigate the potential danger of data security due to the development of quantum computers. The research question was to explore the impact of quantum computers on data security. Data was collected through a literature review of relevant articles and books and analyzed using a qualitative data analysis approach. Ethical considerations were taken into account during the research process, and the sources used in this research were properly cited to ensure academic integrity. The limitations of the research included the lack of primary data collection and potential bias in the selected articles and books. However, the research provided a thorough overview of the potential danger of data security because of quantum computers, and the methodology section outlined the research design, data collection and analysis methods, ethical considerations, and limitations and strengths of the research.

5. RESULTS

Quantum Computers: In traditional computers, a bit can only be in one of two states: 0 or 1. However, a pair of two bits can have four potential states, including 00, 01, 10, or 11. These bits can represent various information, including numerical data, but only one state at a time can be used for mathematical operations. Quantum computers use qubits, which also have two states, 0 or 1, but they can be in a superposition state that is a combination of the two states.

Superposition notation example: $0.42\,|0\rangle + 0.91|1\rangle$

Quantum computers can complete calculations faster than traditional computers by using qubits in a superposition of states. With two pairs of qubits existing in each of the four potential states, calculations can be executed simultaneously. Adding more qubits increases the number of possible states, with 20 qubits allowing for over 1,048,576 states. However, reading all the states is impossible since measuring a state results in only one random number, with the others lost. Quantum computers have limited use in solving specific problems like public key cryptography. To harness their power, a way to convert a superposition of states into useful information is needed, but this is a challenging task, rendering quantum computers useless in many applications. Decryption algorithm: If N is a number with two prime factors p and q, For the purposes of this example, let's assume N to be 77. The two prime factors are now obvious, but when working with huge numbers, it wouldn't be. By repeatedly multiplying a random number g that does not have any factors in common with N, the result will eventually reach a multiple of N + 1. in other words, there always some exponent r, So that g r = mN + 1. Setting g = 8 to see how it works, this number does not share a factor with 77. It would also be extremely unusual to obtain a number that shares a factor with N if this were done with large prime numbers. now repeatedly multiply 8 by itself, then divide the result by 77 to get 1 in the remaining fraction.

g^r	Results	g^r / N	Remainder
8^1	8	0	8
8^2	64	0	64
8^3	512	6	50
8^4	4096	53	15
8^5	32768	425	43
8^6	262144	3404	36
8^7	2097152	27235	57
8^8	16777216	217885	71
8^9	134217728	1743087	29
8^{10}	1073741824	13944690	1

Figure 1: Algorithm table

With the identification of the exponent r (10) that fulfills the equation g r = mN + 1, the equation is reorganized

to g r - 1 = mN , (gr / 2 + 1) (gr / 2 - 1) = mN. In this form, as long as r is even, we have an integer times integer equals a multiple of N (p and q). Since r is 10, the two numbers are (85 +1) and (85 -1), which are, respectively, 32,769 and 32,767. these two numbers and N have a common factor. Euclid's algorithm can be applied to find the largest common factor of two numbers, such as 32,769 and 77, by dividing the larger number by the smaller one and recording the remainder. So 32,769/77 = 425 R44, then dividing the denominator over the remainder, 77/44 = 1 R33, 44/33 = 1 R11, 33/11 = 3 R0. When the remainder is 0 the divisor is indeed the greatest factor. Dividing 77 by 11 is 7, which is the other prime factor. In conclusion the algorithm is:

- Make a guess, g < N that shares no factors with N
- Find r such that.

$$g^r = \mathrm{mN} + 1 \qquad (1)$$

- If r is even, calculate

$$(\frac{g^r}{2} + 1)\,(\frac{g^r}{2} - 1) = \mathrm{mN} \qquad (2)$$

Use Euclid's algorithm to find the greatest common factor.

NO quantum computer is needed to run any one of these steps, yet it takes a long time on a classical computer. The second step, determining the exponent, is the crucial process that a quantum computer accelerates. If the step 2 calculation were to continue beyond 8 10, where the remainder is 1, the remainders would cycle

g^r	Results	g^r / N	Remainder
8^{11}	8589934592	111557592	8
8^{12}	6871947636	892460736	64
8^{13}	549755813888	7139685894	50
8^{14}	4398046511104	57117487157	15
8^{15}	35184372088832	456939897257	43
8^{16}	281474976710656	36555519178060	36
8^{17}	225179981368524	29244153424483	57
8^{18}	1801439850948198 4	233953227395806	71
8^{19}	1441151880758587 2	187162581916695 9	29
8^{20}	1152921504606846976	149730006553335676	1

Figure 2: Algorithm table

The exponent that yields 1 once more is 20, which is exactly 10 more than the exponent that yields 1 for the first time, which is 10. Any recurring remainders will likewise be separated by 10.

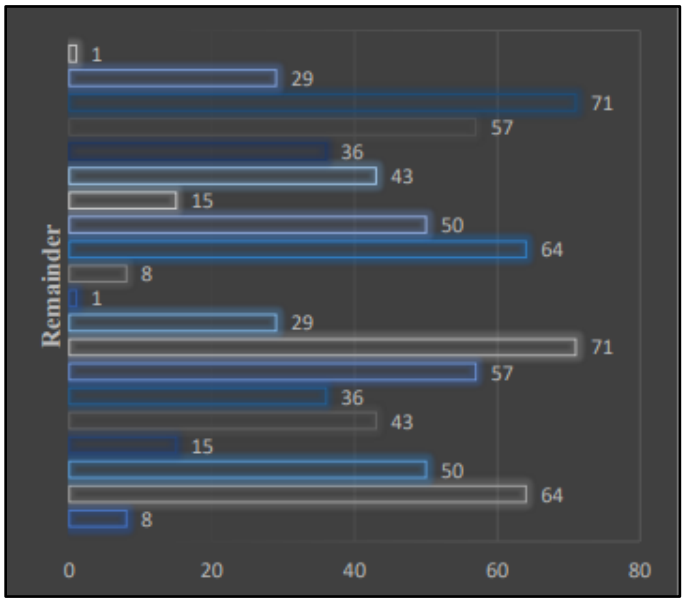

Figure 3: Periodic graph

It has a period of 10 and is periodic, as the graph demonstrates. The period would have changed if a different g had been selected, but there will always be a remainder of 1. that is because the pattern is repeatable and begins with the g0 , and any integer that is raised to 0 equals 1. Calculations for this step on quantum computers are performed using the quantum Fourier transform. Quantum Fourier transform: In 1944, Peter Shor and Don Coppersmith discovered how to use a quantum Fourier transform, which functions just like a regular Fourier transform and returns the frequencies that are in a signal when applied to a periodic signal. If there is a superposition of states that is periodic, meaning that the terms in the superposition are separated by a regular amount, quantum Fourier can be applied to get the states that contain the frequency of the signal so that this can be measured. A periodic superposition can have frequency information extracted from it via the quantum Fourier transform. Post-quantum cryptography: The national institute of standards and technology (NIST) launched a competition in 2016 to find new encryption algorithms. Cryptographers from around the world submitted 82 proposals; some of them passed rigorous testing but others failed. In 2022, NIST chose four of the algorithms to be included in their post-quantum cryptography standards. The mathematics of latices is the foundation for three of the algorithms. By using a set of vectors in a multiple dimensional lattice to reach a point that is on the grid, the different combination of these two vectors to achieve the point will act as the prime factors in the RSA encryption and the point to be reached is the public key or the product of the factors.

6. CONCLUSION

Only a few thousand perfect qubits are required for the decryption process, but flawed qubits necessitate the use

of additional qubits as redundant information. In 2012, a billion physical qubits were believed to be necessary for RSA encryption decryption, but that number reduced to 230 million five years later, and further technological advancements in 2019 reduced the estimate to only 20 million physical qubits. The current number of qubits available is nowhere near that number, although growth seems to be exponential. It is only a matter of time before every public key encryption presently in use can be broken, prompting researchers to seek effective methods of quantum-proof data encryption.

REFERENCES, *IEEE*

[1] X. Niu et al., "Measurement-device-independent quantum secure direct communication protocol using Einstein-Podolsky-Rosen pairs," Phys. Rev. A, vol. 97, no. 6, Jun. 2018, Art. no. 062317.

[2] S. Nejatollahi et al., "Lattice-Based Cryptography: Trends and Challenges," Cryptography, vol. 3, no. 2, Apr. 2019, Art. no. 17.

[3] P. Kumar et al., "Enhanced key size for secure data transmission using quantum cryptography," Int. J. Recent Technol. Eng., vol. 8, no. 4S3, Nov. 2019, pp. 537-540.

[4] S. Pirandola et al., "Advances in quantum cryptography," npj Quantum Inf., vol. 5, no. 1, Dec. 2019, Art. no. 103.

[5] M. Ott et al., "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility," NISTIR, vol. 8309, Nov. 2019.

[6] M. Jaques et al., "Quantum Speedups for Oracle Problems with Bus and Tree Structures," Phys. Rev. A, vol. 99, no. 1, Jan. 2019, Art. no. 012326.

[7] S. Falco et al., "Perfect secrecy cryptography in classical optical channels," arXiv:1904.12677, Apr. 2019

[8] M. Khan et al., "A review on quantum cryptography and its possible implementation," Int. J. Innov. Res. Comput. Commun. Eng., vol. 6, no. 9, Sep. 2018, pp. 223-232.

[9] P. Kumar et al., "A survey of quantum key distribution protocols," J. Netw. Comput. Appl., vol. 142, Dec. 2019, Art. no. 102405.

[10] K. Moody et al., "Quantum Cybersecurity: Challenges and Opportunities," J. Phys. A: Math. Theor., vol. 53, no. 1, Dec. 2020, Art. no. 013001.

[11] Joseph, D., et al. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237-243.

[12] Kotas, W. A. (2000). A brief history of cryptography. University of Tennessee.

[13] Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

[14] Kak, A. (2023). Lecture 12: Public-Key Cryptography and the RSA Algorithm.

[15] Coppersmith, D. (2002). An approximate Fourier transform useful in quantum factoring. arXiv preprint quant-ph/0201067.

[16] Asfaw, A. (2020). Shor's Algorithm Lecture Series, Qiskit Summer School.

[17] O'Gorman, J., & Campbell, E. T. (2017). Quantum computation with realistic magic-state factories. Physical Review A, 95(3), 032338.

[18] The IBM Quantum Development Roadmap, IBM.

[19] Thijs, L. (2015). Lattice cryptography and lattice cryptanalysis.