Quantum Computing and the Threat to Modern-Day Security

Pulkit Pannu
Student ID: 104093910
Swinburne University of Technology
Melbourne, Australia
104093910@student.swin.edu.au

***Abstract*—Store Now, Decrypt Later is a threat to modern-day security as attackers from around the world are storing encrypted data, such as bank account details, sensitive messages, email, etc. in the hopes of a quantum computer being available to the public which can be used to decrypt this sensitive data for their own benefits.**

In this report we look cryptography and how it's used in security, quantum computing and the threats on public key cryptosystems caused by using the Shor's algorithm on a large enough quantum computer to break the ciphers, quantum safe cryptosystems based on the mathematics of lattices and using the Learning with Errors problem to ensure unbreakable cryptographic algorithms.

I. Introduction

The world we live in today can be represented by numbers. To be precise, it can be represented by two very specific numbers, '0' and '1'. These are the binary digits that all the data to be ever documented on this planet boils down to. The mere existence of the technology that makes this world work are because of these 0s and 1s. High and low. On and off. This is what we call digital. The digital age, or the "Information Age", began with the development of transistors in 1947 at Bell Labs, New Jersey, USA [1]. Also known as the "Third Industrial Revolution", the rapid shift from traditional industries to entire economies centred on information technology [1] was met with mixed feelings but eventually it burst open the wide array of use cases of digital technologies and provided a significant impact on the way information is processed and transmitted today [1].

II. Cryptography as Security

With the rise of the internet, came threats to all the assets associated with it. The security for information technology is about risk management and using different methods and tools to defend an organization's digital assets [2].

Among the vast array of security techniques available today, cryptography is one of the most vital methods for providing confidentiality and integrity for the user data and communication channels, ensuring privacy and keeping sensitive information discrete.

"Cryptography is the practice of developing and using coded algorithms to protect and obscure transmitted information so that it may only be read by those with the permission and ability to decrypt it" [3]. Cryptography is at the core of keeping communications secret over the internet, providing means for valid and secure authentication, maintaining the integrity of sensitive information and keeping documents and messages private.

In general, there are two types of cryptosystems based on which key is used to encrypt and decrypt data. Symmetric key cryptography uses the same secret key to encrypt and decrypt electronic data [4] among all the devices communicating. Whereas, asymmetric key cryptography utilises a unique key-pair for each devices that wishes to communicate with another device. It encrypts the data using the public key of the receiver and the receiver decrypts it by using its own private key. As the name suggests, the public key is readily available to the general masses whereas the private key is kept secret and is never transmitted over an insecure channel.

Feature	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key Usage	Same key for encryption and decryption	Public key for encryption, private key for decryption
Speed	Faster	Slower
Security	Less secure due to key distribution issues	More secure due to separate public and private keys
Key Management	Key must be securely shared between parties	Public key can be shared openly
Common Algorithms	AES, DES, Triple DES	RSA, ECC
Ideal use case	Encrypting large amounts of data	Secure key exchange, digital signatures
Computational Overhead	Lower	Higher
Example	Disk encryption, secure file transfer	SSL/TLS, email encryption

Figure 1 Difference between symmetric and asymmetric key cryptography

Although, symmetric key cryptography is faster and more efficient than asymmetric cryptography, the biggest hurdle for it to pass is to safely exchange the secret key over an unsecure channel. Whereas, the major advantage of asymmetric cryptography is that it is *computationally* impossible to derive the private key from the public key. But due to its large key size, it is very slow to be used for encrypting and decrypting considerable amount of data. Hence, using the best of both worlds, we use asymmetric key cryptography to securely exchange and set up symmetric session keys. Moreover, asymmetric key cryptography is also used in digital signatures to verify the identity and authenticity of an individual or an organisation.

Hence, it is imperative for asymmetric or public key cryptosystems to be computationally impossible to be broken via brute force attacks. To achieve this, these cryptosystems use two number theory problems which have been widely studied but can't be solved, for specific cases, in polynomial-time with the provided computational power of the modern-day computers. These are the Prime Factorisation and the Discrete Logarithm problems used in the two of the most widely used public key cryptosystems, RSA and Elliptic Curves Cryptography (ECC) respectively.

III. What is Quantum Computing?

Well, what is quantum? In physics, a quantum is the minimum amount of any physical entity involved in an interaction [5]. Then what is quantum mechanics? Quantum mechanics is a fundamental theory in physics that describes the behaviour of nature at and below the scale of atoms [6]. A quantum computer is a computer that exploits quantum mechanical phenomena where physical matter on small scales exhibit properties of both particles and waves [7]. This provides it a huge advantage over classical computers and modern supercomputers because, in theory, quantum computers can solve exponential time complex equations in polynomial time.

Like the classical two-bit digital infrastructure, quantum computers have what are known as quantum bits, or qubits, which can exist in a superposition of the two bits, 0 and 1. Basically this means that a qubit can be either 0 or 1 or a coefficient sum of both.

$$|\Psi\rangle = C_0|0\rangle + C_1|1\rangle \qquad [12]$$

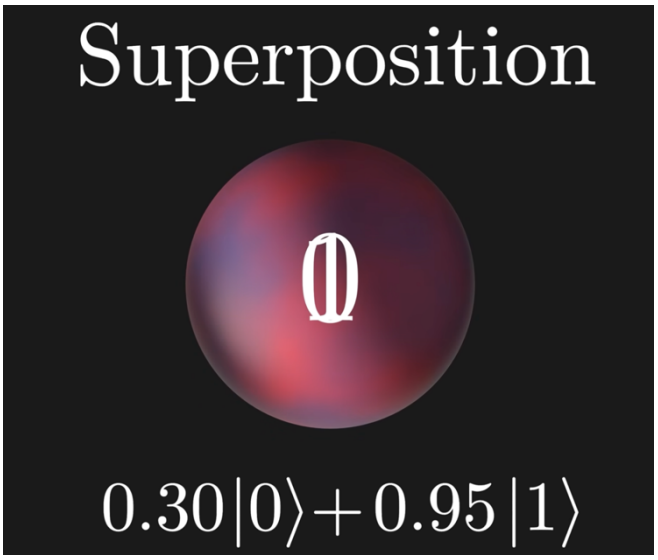

Figure 2 A single qubit representing the superposition of two states [23]

If there are two qubits then a quantum computer calculates the superposition of the four possible states at once.

$$|\Psi\rangle = C_0|00\rangle + C_1|01\rangle + C_2|10\rangle + C_3|11\rangle$$

Therefore, for "n" qubits, a quantum computer will calculate 2^n superpositions at the same time. This can be represented as parallel calculations unlike the classical computer where all the calculations and method calls are done one after the other in series. Hence, this behaviour of quantum computers provides it an edge over supercomputers and classical computers.

IV. Treats of Quantum Computing

" A quantum computer of sufficient size and sophistication - also known as a cryptanalytically relevant quantum computer - will be capable of breaking much of the public-key cryptography used on digital systems across the United States and the world" [8]. This threat to the modern digital systems by quantum computing became relevant when an American Mathematician named Peter Shor devised the Shor's algorithm, a quantum algorithm for factoring exponentially faster than the best currently-known algorithm running on a classical computer [9]. So in theory, on a quantum computer with sufficient qubits, one can run Shor's algorithm to break the prime factorisation and discrete logarithm problems which are the basis of the widely used public key cryptosystems [10].

On a quantum computer, Shor's algorithm can factor an integer N in polynomial time which is significantly faster than the most efficient known classical factoring algorithm, the General Number Field Sieve (GNFS), which works in sub-exponential time [11]. Shor's algorithm uses the Quantum Fourier Transform (QFT) [13], which is the quantum analogy of the Discrete Fourier transform, to derive the desired result from the superposition of outputs that a quantum computer provides.

V. Quantum Safe Cryptography

On July 5, 2022 the National Institute of Standards and Technology (NIST) announced the first group of winners from its six-year long competition for developing quantum-resistant cryptographic algorithms [14]. Three of the four winning algorithms were based on lattice-based cryptography.

Lattice-based cryptography is basically creating cryptographic algorithms that involves lattices which have proved to be resistant to attacks by both classical and quantum computers [15]. The initial work done in lattice-based cryptography was Short Integer Solutions (SIS) [16] in 1996, NTRU [17] in 1998 and Learning with Errors problem (LWE) [18] in 2005.

CRYSTALS-Kyber, **CRYSTALS-Dilithuim** and **Falcon** were part of the winning algorithms announced by NIST which were based on the mathematics of lattices and they incorporate a combination of SIS, NTRU or LWE for their own implementation of the algorithm. Hence, a general overview of lattice-based cryptography is provided below.

VI. Lattice-based Cryptography [24]

A lattice can be defined as an infinite set of points in the real coordinate space that can be generated by a set of initial basis vectors on that plane using vector addition or subtraction [19].

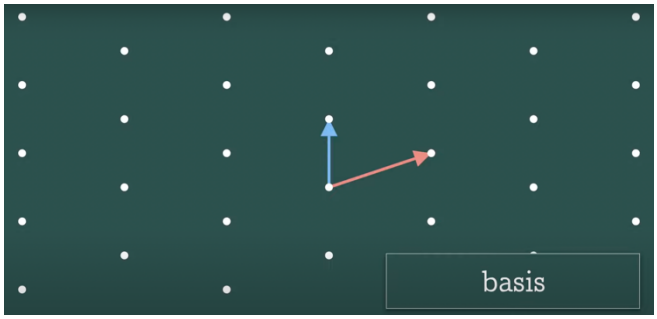

Figure 3 Initial vector basis used to generate a lattice [24]

A very useful and important property of lattice vectors is that two very different set of basis vectors can produce the same lattice plane.

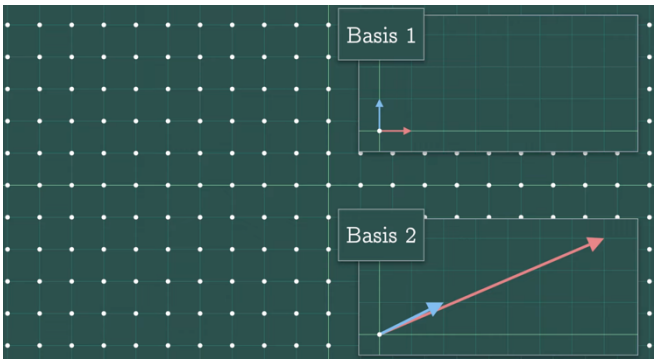

Figure 4 Two different basis vectors can generate the same lattice [24]

One of the mathematical problems used in lattice-based cryptography is known as the closest vector problem (CVP) [20] where, given a set of initial basis vectors, one needs to find the vector which is closest to a given point on the lattice by adding and subtracting the initial given basis vectors. If the basis vectors are almost orthogonal to each other then it is quite easy to solve CVP. But if the basis vectors are almost parallel to each other, then solving the CVP becomes much harder. Moreover, if we have "n" basis vectors then the lattice plane generated by these vectors will be n-dimensional, increasing the complexity of CVP exponentially such that even a quantum computer won't be able to solve it.

Therefore, the CVP makes a terrific mathematical basis for lattice-based cryptography. Basically, each device creates two different sets of basis vectors which generates the same lattice. The first basis has the vectors close to perpendicular to each other and is known as the good basis. Whereas, the other set of basis vectors are close to parallel and are known as the bad basis. Since, its comparatively easier to solve the CVP using the good basis than the bad basis, the good basis is the private key and the bad basis is the public key of the device.

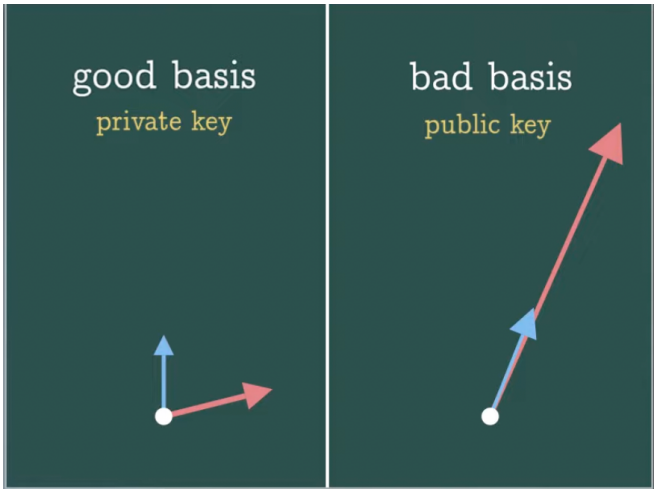

Figure 5 Describing the private and the public keys in lattice-based cryptography [24]

The sender uses the bad basis, or the public key, of the receiver to encode its message as a lattice point and sends a point which does not lie on the lattice and is closest to the generated lattice point as the encrypted message. The receiver with the good basis can easily find the closest vector point and decrypt the message but for anyone else eavesdropping the conversation, it's very hard to decrypt the message using the bad basis. This was the idea behind the GGH encryption scheme [21] published in 1997 but it was cryptanalyzed, or broken, in 1999 by Phong Q. Nguyen [22] where he showed that every ciphertext reveals information about the plaintext and that the problem of decryption could be turned into a special CVP which is much easier to solve than the general CVP [21].

To solve this problem with the encryption scheme, cryptographers used different variations of the Learning with Errors problem (LWE) [18] developed by Oded Regev in 2005.

VII. Learning with Errors [25]

Unlike stated before, to implement LWE in cryptography, the public key is actually a bunch of linear equations which can be solved by using the values of the private key vectors. The problem with this is that one can easily find the private variables from the public equations if the number of equations available is equal to the number of variables by using matrix multiplication.

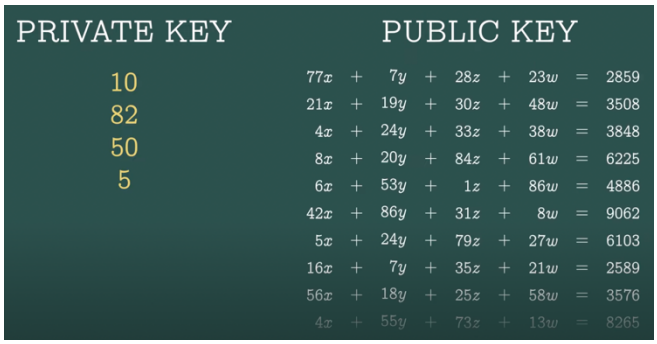

Figure 6 Public and Private key format in LWE problems [25]

Hence, to hop over this hurdle, we add a small noise or an error value, integers near 0, to the public equations. These error values are kept secret. This error filled system of linear equations almost always doesn't have a solution as it has more equations than variables, also known as an over-determined system, which are essentially straining the value of the variables. Since, the error values are not publicly available, therefore, it's impossible for an eavesdropper to deduce the private key. To add another layer of difficulty, all the RHS values of the equations are written modulo some number after adding the errors.

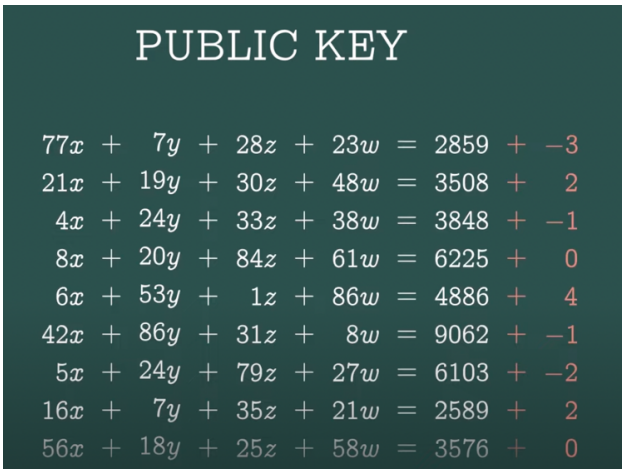

Figure 7 Adding errors or noise to the public key to make it indeterministic [25]

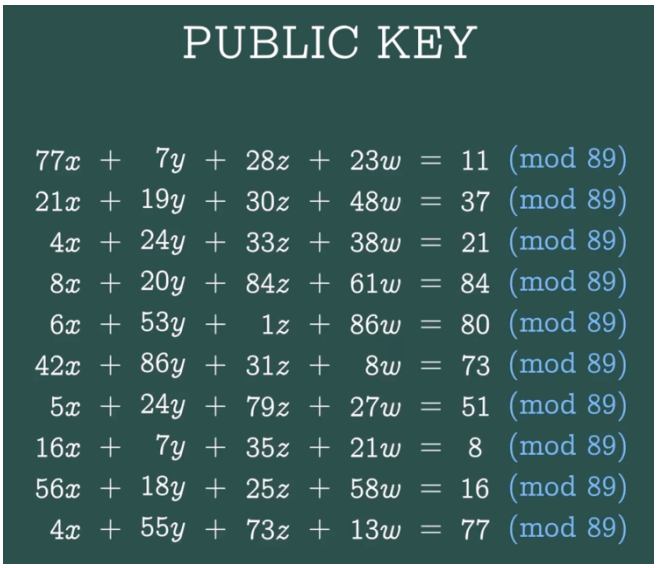

Figure 8 Doing modulus of the RHS of the public equations to increase complexity [25]

Now, to use this system, lets assume that the sender wants to encrypt a bit, a "0" or a "1". To do this, he takes some random number of equations from the public key of the receiver and adds them to produce a new equation.

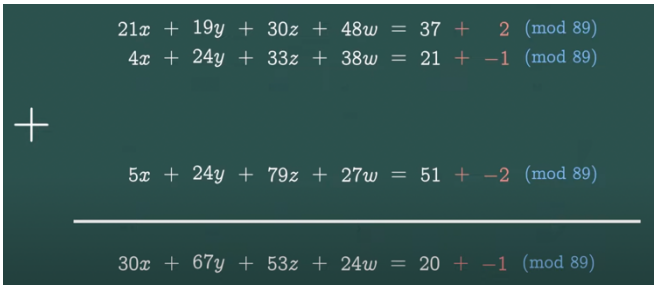

Figure 9 Adding a random number of public equations for encrypting a bit [25]

To encrypt a 0, the sender just sends the added equation as it is to the receiver, whereas, if he wants to encrypt a 1, then he would add to the RHS, the half of the number that was used to do the modulus of the RHS value initially.

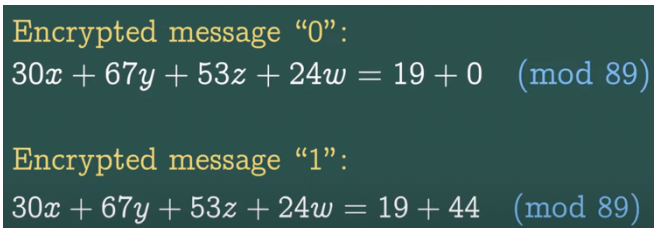

Figure 10 Encrypting a 0 or a 1 [25]

This is done because, when the receiver uses the private key to solve the encrypted message, he can deduce the error by subtracting the actual value, produced from the LHS, from the RHS. If the error value is near 0, then the encrypted message was a 0, whereas, if the error value is near the half of the number used as the modulus, then the encrypted message was a 1.

This LWE problem can be modified in various ways and used in lattice-based cryptography by using the RHS of the equations as a lattice point and when the error is added, the receiver essentially needs to solve the CVP and decrypt the message. As a matter of fact, CRYSTALS-Kyber, used for key establishment purposes, and CRYSTALS-Dilithium, used for digital signature purposes, use different modules of LWE in their algorithms.

VIII. Conclusion

To summarise, this report gives a brief overview of how the modern-day security can be affected by large enough quantum computers and the measures taken by NIST to encourage cryptographers from all over the world to develop quantum-safe cryptographic algorithms.

Moreover, we also take a look at lattice-based cryptography and how its implemented, as more than half of the algorithms chosen by NIST were based on lattices and presumably all of the future public key encryption could be made lattice based.

IX. References

[1] "Information Age", Wikipedia, https://en.wikipedia.org/wiki/Information_Age (accessed May 13, 2024)

[2] Madelyn Bacon, "security", TechTarget, https://www.techtarget.com/searchsecurity/definition/security

[3] "What is Cryptography?", IBM, https://www.ibm.com/topics/cryptography (accessed Jun 3, 2024)

[4] Peter Smirnoff and Dawn M. Turner, "Symmetric Key Encryption – why, where and how it's used in banking", Cryptomathic, https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking (accesse Jan 03, 2020)

[5] "Quantum", Wikipedia, https://en.wikipedia.org/wiki/Quantum (accessed Jun 4, 2024)

[6] "Quantum mechanics", Wikipedia, https://en.wikipedia.org/wiki/Quantum_mechanics (accessed Jun 04, 2024)

[7] "Quantum Computing", Wikipedia, https://en.wikipedia.org/wiki/Quantum_computing (accessed Jun 04, 2024)

[8] News, "President Biden signs memo to combat quantum computing threat", National Security Agency/Central Security Service, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-biden-signs-memo-to-combat-quantum-computing-threat/ (accessed May 04, 2022)

[9] "Peter Shor", Wikipedia, https://en.wikipedia.org/wiki/Peter_Shor (accessed Jun 04, 2024)

[10] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" , (accessed Jan 25, 1996)

[11] "Shor's Algorithm", Wikipedia, https://en.wikipedia.org/wiki/Shor%27s_algorithm (accessed Jun 04, 2024)

[12] "Quantum Superposition", Wikipedia, https://en.wikipedia.org/wiki/Quantum_superposition (accessed Jun 04, 2024)

[13] "Quantum Fourier Transform", Wikipedia, https://en.wikipedia.org/wiki/Quantum_Fourier_transform (accessed Jun 04, 2024)

[14] "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms", NIST, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed July 5, 2022)

[15] "Lattice-based Cryptography", Wikipedia, https://en.wikipedia.org/wiki/Lattice-based_cryptography (accessed Jun 04, 2024)

[16] "Short Integer Solutions Problem", Wikipedia, https://en.wikipedia.org/wiki/Short_integer_solution_problem (accessed Jun 04, 2024)

[17] "NTRUEncrypt", Wikipedia, https://en.wikipedia.org/wiki/NTRUEncrypt (accessed Jun 04, 2024)

[18] "Learning with errors" Wikipedia, https://en.wikipedia.org/wiki/Learning_with_errors (accessed Jun 04, 2024)

[19] "Lattice (group)", Wikipedia, https://en.wikipedia.org/wiki/Lattice_(group) (accessed Jun 04, 2024)

[20] "Lattice Problem", Wikipedia, https://en.wikipedia.org/wiki/Lattice_problem (accessed Jun 04, 2024)

[21] "GGH encryption scheme", Wikipedia, https://en.wikipedia.org/wiki/GGH_encryption_scheme (accessed Jun 04, 2024)

[22] Phong Nguyen, "Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto'97", 1999

[23] Veratasium, "How Quantum Computers Break The Internet… Starting Now", YouTube, 2023. [Online]. Available: https://www.youtube.com/watch?v=-UrdExQW0cs

[24] Chalk Talk, "Lattice-based cryptography: The tricky math of dots", YouTube, 2023. [Online]. Available: https://www.youtube.com/watch?v=QDdOoYdb748

[25] Chalk Talk, "Learning with errors: Encrypting with unsolvable equations", YouTube, 2023. [Online]. Available: https://youtu.be/K026C5YaB3A?si=7Ein2ommfs7F3ipJ