Quantum Computing and Security

Lee Zong Yang
Faculty of Science, Engineering and Technology
Swinburne University of Technology
Hawthorn, Australia-3122
100073484@student.swin.edu.au

***Abstract*—This paper aims to discuss the consequences of quantum computing in cybersecurity, the threats and opportunities it brings. The background section introduces the basic knowledge of quantum physic and present cryptographic schemes. In the threat section, there are discussions on how asymmetric and symmetric cryptography are affected, the possibility of retrospective data decryption, and the potential threat to cybercurrency. In the opportunities section, quantum key distribution with a brief discussion on BB84 protocol, post-quantum cryptography, quantum random number generator, and quantum machine learning are discussed.**

Keywords—quantum computing, symmetric cryptography, asymmetric cryptography, quantum key distribution, post-quantum cryptography

I. Introduction

As the development of quantum computer progress, there come threats and opportunities for the cybersecurity industry. Quantum computer leverages the law of quantum physics, such as superposition, quantum entanglement, and quantum teleportation to achieve better performance than a classical computer in certain tasks. It is important to note that quantum computer does not outperform classical computer totally, but only in a specific task, such as solving factorisation problem and discrete logarithm problem [1].

Although quantum computing will bring an end to current popular cryptography which relies on the difficulty of discrete logarithm problem and factorising large prime numbers, there is post-quantum cryptography that could run on a classical computer and resilient to quantum computing attack [2]. Moreover, there are quantum random number generator which could provide enhancement to classical cryptography and quantum key distribution which based on the law of quantum physic to defend against eavesdropping [3][4].

II. Background

A. Heisenberg Uncertainty Principle

In quantum physic, each system is described by wave function, which leads to the Heisenberg Uncertainty principle. Heisenberg Uncertainty principle states that the more precisely the momentum is known the more uncertain the position is and vice versa [5].

B. Superposition

Quantum superposition is a phenomenon when a system could exist in one of the possible states and described by the combination of the wave functions of the possible states. However, the measurement will cause changes and the wave function will collapse into a specific state [6]. For example, candy in a box could be red candy or blue candy before the opening of the box, so its state is both red candy and blue candy, but will be determined as red candy or blue candy after the opening of the box.

C. Quantum Entanglement

Scientists observe that two particles could be correlated even when the particles are far away from each other. At the start, a pair of entangled particles are in a superposition state, but measurement of one particle will determine the state of the other particle instantly even though they were separated [7]. Although this phenomenon contradicts classical physics which states that there must be time passed between causes and effects, it is supported by a lot of experiments [8].

D. Quantum Teleportation

It is the transferring of information instead of the particle as depicts in science fiction. Although the no-cloning theorem states that it is impossible to clone the particle in a superposition state, there is a workaround by using an extra pair of entangled particles as shown in figure 1 [9], [10].

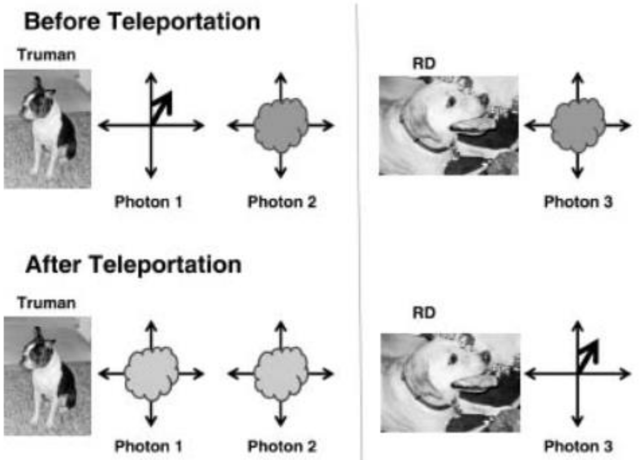

Fig 1. Before and after quantum teleportation (adapted from [10]).

Assume that RD wants to clone the state of photon 1 of Alice. There is an extra pair of entangled photons 2 and 3, which Truman will have the photon 2 and Bob will have the photon 3. Truman then measures both photon 1 and 2 as one system, which will cause changes in photon 3 too.

Afterwards, Truman will use a classical channel to transmit the result of the measurement to RD, and RD could use the information to apply an operation on photon 3, so it will have the same state as photon 1 before the measurement. Since time is required to transmit information through the classical channel, the theory of relativity is not violated [9], [10].

E. *Symmetric Cryptography*

In symmetric cryptography, there is only one key for both encryption and decryption purpose, and thus it must be kept secret by both parties. The agreement on the secret key before the transmission of confidential information could be achieved by the manual installation or key exchange with asymmetric cryptography [11].

F. *Asymmetric Cryptography*

A revolutionary idea introduced by Diffie and Hellman in the 1970s, which uses two unique but mathematically related keys – a private key and a public key. Both the public key and private key could be used for encryption or decryption, but the private key must be kept secret while the public key could be known to the public [12].

Whether it is the public or private key for the encryption function depends on the scenario. If encrypt the message with the public key then only the holder of the private key can decrypt the message, and thus achieves confidentiality. If encrypt the message with the private key then can prove the identity of the sender as the public key can only decrypt the message encrypted with the right private key [13].

III. Threats

A. *Attack on Asymmetric Cryptography*

Peter Shor, a mathematician, proved that a quantum computer would significantly reduce the difficulties in factorizing large integers in his paper "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" [14]. Therefore, the present asymmetric cryptography will be deemed obsolete since all of it are based on discrete logarithm problem or large prime integer factorization. Digital signature or internet protocols like HTTPS that use asymmetric cryptography will be become invalid too.

The difference between a classical computer and a quantum could be illustrated using the example of finding the prime factors of number 15. Since the binary for 15 is 1111, we will use a 4-bit register for the classical computer and a 4-qubit register for the quantum computer and carry out the factorization through Shor's algorithm [15].

Shor's algorithm:

1. n is equal to the number we want to factorize, which is 15.
2. choose a random number x within the range of $1 < x < n - 1$.
3. For every possible number that could be formed using 4 binaries, x is raised to its power and then divided by n. The remainder will then be stored in another register.

At the 3rd step, we can see that the quantum computer could perform the calculation for every possible number in one operation, but the classical computer requires one operation for each possible number, which will be significant differences in time required when n becomes larger. Using $x = 2$, the result of the 3rd step using a 4-qubit register is shown in Table I. We can use $f = 4$ since there exists a repeating sequence of 4 numbers (1, 2, 4, 8), and find a possible factor with the equation: possible factor = $x^{f/2} - 1$. Different f values could be used when the result is not a prime number.

B. *Attack on Symmetric Cryptography*

Lov Grover invented an algorithm that could speed up the search of a specific record in an unsorted database using a quantum computer [16]. A classical computer requires O(N/2) time complexity but a quantum computer could reduce the time complexity to $O(\sqrt{N})$ by using Grover's algorithm.

Symmetric cryptography is safe from quantum computing attack if the key length is long enough. Currently, Grover's algorithm is the only algorithm that could reduce the O(N/2) time complexity to $O(\sqrt{N})$ time complexity i.e. $O(2^{n-1})$ to $O(2^{n/2})$ for n-bit cipher, so 128-bit key length will provide 64-bit security level. With current technology progression, 80-bit security level is sufficient, and thus Advanced Encryption Standard (AES) with at least 192-bit key length is safe from quantum computing attack. A summary of the security level for popular cryptography algorithms is presented in Table II [15].

Although symmetric cryptography is quantum resilient, it is still vulnerable if asymmetric cryptography (e.g., Diffie Hellman) is used to establish a secret key on two parties as the attacker could break Diffie Hellman and figure out the secret key.

C. *Attack on Hash Function*

A hash function, especially a cryptographic hash function, should have a minimal chance of hash collision to deter the attacker from carrying out the collision attack. If there is a legit transaction message "Alice will pay Eve 100 dollars." with the digital signature of Alice, then attacker Eve could try to find another message "Alice will pay Eve 1000 dollars." with the same hash output as the legit transaction message and submitting it with the digital signature of Alice will cause Alice to lose 1000 dollars [17].

Finding hash collision is like searching an unsorted database, and thus Grover's algorithm could be employed to speed up the process. Moreover, Brassard et al. [21] described a way to combine the birthday paradox with Grover's algorithm to further increase the efficiency of searching, which made a lot of the present hash functions obsolete. Luckily, both SHA-3 and SHA-2 are still safe by having a longer output [15].

D. *Retrospective Decryption of Data*

Although the organization could change to use post-quantum cryptography now or employ quantum key distribution in the future, quantum computing still poses significant threats to the security of data encrypted with present cryptography. There are illegal organisations or governments' secret services collecting encrypted data to decrypt it in the future [18]. It is worthy to mention that data encrypted with an algorithm with short key length is susceptible to the increasing computing power of classical computer too.

TABLE I. REMAINDERS STORED IN THE 4-QUBIT REGISTER 2 FOR EACH POSSIBLE STATE IN REGISTER 1 (ADAPTED FROM [15])

Register 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Register 2	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

TABLE II. SUMMARY OF THE SECURITY LEVEL FOR POPULAR CRYPTOGRAPHY ALGORITHMS. (ADAPTED FROM [15])

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
AES-256	256	256	128
AES-128	128	128	64
RSA-2048	2048	112	0
RSA-1024	1024	80	0
ECC-384	384	256	0
ECC-256	256	128	0

E. Attack on cybercurrency

The attack on cybercurrency could be studied using Bitcoin as an example [19]. The address of a Bitcoin user is generated using a public key and a private key. To perform a transaction of Bitcoin from one address to another, the digital signature (sign with private key) of the sender is required to authorize the transaction. At this point, we can see that quantum computing allows the falsification of digital signature, results in the spending of anyone's Bitcoins without authorization.

Pay-to-public-key (p2pk) and pay-to-public-key-hash (p2pkh) are the two main types of Bitcoin address. As the name suggests, the public key could be obtained directly from the address of pay-to-public-key (p2pk) type while only the hash of the public key could be obtained from the address of pay-to-public-key-hash (p2pkh) type. However, the public key of the address of pay-to-public-key-hash (p2pkh) type will be revealed when a transaction is initiated by the address owner.

We can conclude that addresses of pay-to-public-key (p2pk) type and pay-to-public-key-hash (p2pkh) type that had initiate transaction of Bitcoin are susceptible to quantum computing attack. However, addresses of pay-to public-key-hash (p2pkh) without any transaction initiated are relatively safe as hash function is a one-way function and it is difficult to figure out the public key with only the hash value.

IV. Opportunities

A. Quantum Key Distribution

As discussed above, symmetric cryptography is quantum resilient if the key length is long enough, but the establishment of secret key requires the use of asymmetric cryptography, which will be obsolete in the age of quantum computing.

Fortunately, quantum key distribution, a method that leverages the law of quantum physic, could allow the exchange of key over an untrusted channel securely. Quantum key distribution was known to the world when the first quantum key distribution protocol, BB84 protocol was developed by Charles Bennett and Gilles Brassard in 1984 [4], [20]. Quantum key distribution relies fully on the law of quantum mechanics (Heisenberg Uncertainty principle and quantum entanglement) and thus unaffected by the threat of increasing computational power.

If there is an eavesdropper, the act will change the quantum state, allowing the detection of the eavesdropper. If there are two parties (Alice and Bob) who want to communicate securely, Alice could produce pair of entangled objects and send Bob the counterparts, result in the same state for each pair of entangled objects when one side made the measurement, which could be used to construct the secret key.

There are a lot of different quantum key distribution protocols, namely BB84 [4], [20], BBM [21], E91 [22], and SARG04 [23], [24] but we will only discuss BB84 in this paper. Mayers points out that BB84 is secure, and a secret key could be generated if the error rate is less than 7% [25], [26]. Two different bases are defined in BB84, base 1 have the polarized 0° equal to 0 and polarized 90° equal to 1 while base 2 have the polarized 45° equal to 1 and polarized 135° equal to 0, and thus measuring in different bases will yield a different result.

At the start, Alice randomly selects the base and the value for the photon to be sent to Bob. Bob will randomly choose the base for each received photon too. At the end of transmission of all photons, Alice and Bob will announce the base selected to each other and Bob will discard the photon with a different base, then both will get the states of the photons by measuring the photons. Afterwards, error checking with each other using a portion of the bits. If the error rate is less than a certain threshold, it can be concluded that there is no eavesdropper, and a secret key is generated using the state of the photons. The error rate is attributed to the process of exchanging bits for error checking, and thus the states of photons are still the same for Alice and Bob [26].

Since the eavesdropper does not know the exact base chosen by Alice, the photon received at Bob side will have an inconsistent state if the eavesdropper measured the photon using a different base as Alice, and thus increase the error rate. Due to the no-cloning theorem, it is impossible for the eavesdropper to first clone the photon in a superposition state and measure it after Alice announce the base she chooses while preserving the state of the original photon. Figure 2 illustrates the BB84 protocol.

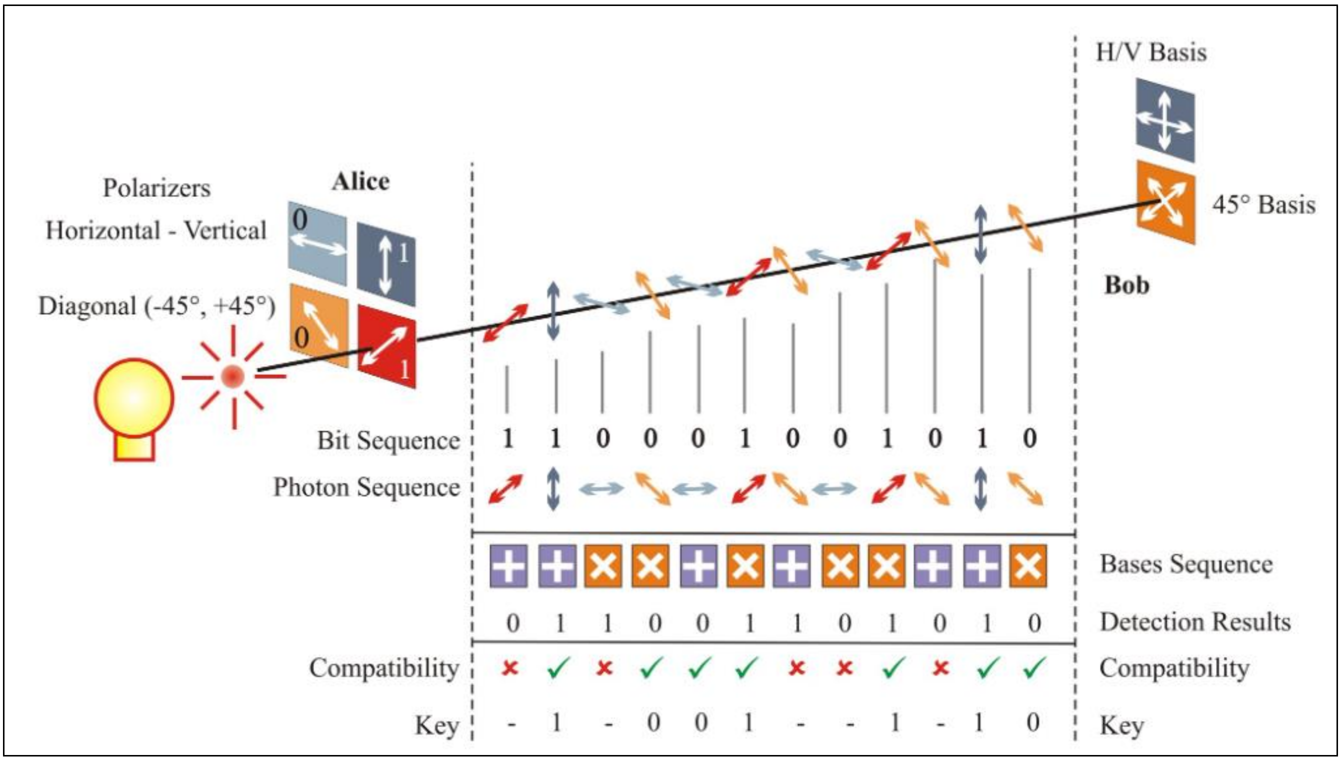
H/V Basis
45° Basis
Bob
Polarizers
Horizontal - Vertical
Alice
0
1
Diagonal (-45°, +45°)
0
1
Bit Sequence 1 1 0 0 0 1 0 0 1 0 1 0
Photon Sequence
Bases Sequence
0 1 1 0 0 1 1 0 1 0 1 0 Detection Results
Compatibility ✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓ Compatibility
Key - 1 - 0 0 1 - - 1 - 1 0 Key

Fig 2. BB84 protocol (adapted from [27]).

Although BB84 is secure by the law of physic, the actual implementation may not be, as found out by Lydersen et al. in 2010 [28]. Through the blinding of the APD-based detector, the receiver failed to notice that the secret key has been inspected by an eavesdropper.

B. *Post Quantum Cryptography*

There is development of cryptographic algorithms running on a classical computer which are quantum resilient. Therefore, transition to post cryptographic algorithms could prevent retrospective decryption of data attack. There are lattices-based, isogenies-based, codes-based, and hash-based cryptographic algorithms. In this paper, only brief discussion on the lattices-based cryptographic algorithm is conducted since it is the most actively studied and most efficient and secure algorithm.

Assume there is a system of linear equations:

$$a_{0,0}x_0 + a_{0,1}x_1 + \ldots + a_{0,n}x_n = y_0$$
$$a_{1,0}x_0 + a_{1,1}x_1 + \ldots + a_{1,n}x_n = y_1$$
$$\vdots$$
$$a_{n,0}x_0 + a_{n,1}x_1 + \ldots + a_{n,n}x_n = y_n$$

Gaussian elimination could solve for the x quickly. Consider there is a function f(a) = $a_{0,0}x_0 + a_{0,1}x_1 + \ldots + a_{0,n}x_n$, for each vector *a* input, the result of the function is known but the vector *x* is kept secret. If the function could be executed multiple times with different input *a*, *x* could be figured out through approximation method i.e., machine learning. However, the method will fail if we add some noise to the function with an error term *e* and modulo arithmetic, f(a) = $a_{0,0}x_0 + a_{0,1}x_1 + \ldots + a_{0,n}x_n + e \bmod q$. It is mathematically proven that it is extremely difficult to learn this noisy function as the error term will increase exponentially [29]. Therefore, quantum computing poses little threat to it as the functions are dependent on each other and quantum computing could not solve it through one or few operations on superposition state.

C. *Quantum Random Number Generators*

A lot of cryptographic algorithms relies on randomness i.e., in challenge response authentication, the expected response for the same challenge issued should be different to prevent replay attack. This could be achieved by using an initialisation vector generated randomly and shared with both parties using Diffie Hellman key exchange algorithm.

However, it is difficult to harness true randomness in quantity through random events in the environment i.e., keystrokes of the user. Therefore, most of the random number generators are pseudo-random number generator, which generates numbers that seem random at the start but will eventually repeat the sequence, and the attacker may gain enough information to compromise the system after some duration. Hereby, a quantum random number generator could provide adequate random numbers and the cryptographic algorithms could use it to address the issue [3].

D. *Quantum Machine Learning*

Nowadays, machine learning has revolutionized a lot of fields, and cybersecurity is one of them. A new form of attack could be detected and blocked by learning on past data. However, the volumes of data grow exponentially as time passed or there is novel algorithm that requires more computational power. Quantum computing could provide extraordinary computing power to support present machine learning algorithms. Furthermore, the study of quantum physics allows the discovering of novel algorithm [30].

V. Conclusion

In the modern day, information is valuable and thus confidential data must be protected. Quantum computing poses a significant threat to present cryptographic schemes. Nevertheless, there are new opportunities gain from the advancement of quantum computing to enhance the protection of data too. Quantum key distribution and post-quantum cryptography are the answers to the threats in the age of quantum computing. Additionally, quantum random number generator allows the enhancement of present cryptography while quantum machine learning allows the deployment of a better precision algorithm.

VI. References

[1] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information.” American Association of Physics Teachers, p. 201, 2002.

[2] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography,* Springer, 2009, pp. 1–14.

[3] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” *Rev. Mod. Phys.*, vol. 89, no. 1, p. 15004, 2017.

[4] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.

[5] P. Busch, T. Heinonen, and P. Lahti, “Heisenberg’s uncertainty principle,” *Phys. Rep.*, vol. 452, no. 6, pp. 155–176, 2007.

[6] P. A. M. Dirac, “The principle of superposition,” in *The principles of quantum mechanics*, no. 27, Oxford university press, 1981, p. 12.

[7] R. Horodecki and M. H. K. Horodecki Pawełand Horodecki, “Quantum entanglement,” *Rev. Mod. Phys.*, vol. 81, no. 2, p. 865, 2009.

[8] J. Yin *et al.*, “Bounding the speed of spooky action at a distance’,” *arXiv Prepr. arXiv1303.0614*, 2013.

[9] V. Bužek and M. Hillery, “Quantum copying: Beyond the no-cloning theorem,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 54, no. 3, pp. 1844–1852, Sep. 1996, doi: 10.1103/PhysRevA.54.1844.

[10] C. Orzel, “Beam me a photon: Quantum Teleportation,” in *How to teach quantum physics to your dog*, Simon and Schuster, 2010.

[11] S. Chandra, S. Bhattacharyya, S. Paira, and S. S. Alam, “A study and analysis on symmetric cryptography,” in *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 2014, pp. 1–8, doi: 10.1109/ICSEMR.2014.7043664.

[12] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, “Computer security: principles and practice,” Pearson Education Upper Saddle River, NJ, USA, 2012, p. 165.

[13] R. H. Arpaci-Dusseau and A. C. Arpaci-Dusseau, “Operating systems: Three easy pieces,” Arpaci-Dusseau Books LLC, 2018.

[14] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[15] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The impact of quantum computing on present cryptography,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 405–414, 2018, doi: 10.14569/IJACSA.2018.090354.

[16] L. K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” in *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, 1996, pp. 212–219.

[17] A. Sotirov *et al.*, “MD5 considered harmful today, creating a rogue CA certificate,” in *25th Annual Chaos Communication Congress*, 2008, no. CONF.

[18] T. Zerdick, L. Olejnik, and R. Riemann, “Quantum computing and cryptography,” *EDPS TechDispatch*, no. 2, 2020, doi: 10.2804/36404.

[19] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, “Quantum attacks on Bitcoin, and how to protect against them,” *arXiv Prepr. arXiv1710.10377*, 2017.

[20] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992, doi: 10.1007/BF00191318.

[21] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557, 1992.

[22] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[23] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Phys. Rev. Lett.*, vol. 92, no. 5, p. 57901, 2004.

[24] A. Acin, N. Gisin, and V. Scarani, “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks,” *Phys. Rev. A*, vol. 69, no. 1, p. 12309, 2004.

[25] D. Mayers, “Unconditional security in quantum cryptography,” *J. ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[26] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, “Security of two quantum cryptography protocols using the same four qubit states,” *Phys. Rev. A*, vol. 72, no. 3, p. 32301, 2005.

[27] V. Makarov, “Quantum cryptography and quantum cryptanalysis,” 2007.

[28] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nat. Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[29] O. Regev, “The learning with errors problem,” *Invit. Surv. CCC*, vol. 7, no. 30, p. 11, 2010.

[30] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.