# EMPLOYING QUANTUM MECHANICS FOR QUANTUM CRYPTOGRAPHY

Rasika Abhang
*School of Professional Studies*
*Clark University*
Worcester, MA, USA
rabhang@clarku.edu

Naveen Anugu
*School of Professional Studies*
*Clark University*
Worcester, MA, USA
nanugu@clarku.edu

Sowmya Bale
*School of Professional Studies*
*Clark University*
Worcester, MA, USA
sbale@clarku.edu

Geethanjali Beeram
*School of Professional Studies*
*Clark University*
Worcester, MA, USA
gbeeram@clarku.edu

Zurendra Sai Raj Bhattu
*School of Professional Studies*
*Clark University*
Worcester, MA, USA
zbhattu@clarku.edu

Mohammed Mahmoud
*Department of Computer Science*
*University of Jamestown*
Jamestown, ND, USA
prof.mahmoud@uj.edu

2023 International Conference on Computational Science and Computational Intelligence (CSCI) | 979-8-3503-6151-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSCI62032.2023.00149

***Abstract*—Quantum cryptography is a field of study that explores the use of quantum mechanics to create new cryptographic techniques that are more secure than traditional cryptography. With the advancement of quantum computing technology, the security of many commonly used encryption algorithms is at risk. Quantum cryptography offers a potential solution to this problem by providing a method for secure communication based on the principles of quantum mechanics. In this paper, we will provide an overview of the fundamental concepts of quantum mechanics, their relevance to cryptography, and the most widely used quantum cryptography protocol, Quantum Key Distribution. The paper also examines the security and limitations of Quantum Key Distribution. The paper concludes with a summary of findings and implications for the future of cryptography and information security.**

***Keywords—Quantum cryptography, quantum mechanics, quantum computing, encryption algorithms, Quantum Key Distribution (QKD).***

## I. Introduction

Quantum cryptography has been gaining attention and investment from governments and businesses worldwide. This cutting-edge technology offers a new approach to secure communications that promises to overcome some of the limitations of traditional cryptosystems. Despite the effectiveness of modern cryptosystems, designed to be intractable and resistant to attacks, they still rely on mathematical algorithms that could be broken by advanced computing power [3]. Quantum cryptography, on the other hand, is based on the principles of quantum mechanics and uses the properties of photons to create unbreakable encryption keys.

This technology has the prospect of providing a level of security that is unprecedented in the field of cryptography. It offers protection against impossible attacks with classical methods, such as eavesdropping on data transmission without being detected.

Governments, businesses, and other institutions recognize the importance of secure communications as a critical success factor in maintaining a competitive advantage and protecting sensitive information. This has led to significant investments in quantum cryptography research and development and the implementation of quantum cryptography solutions by companies such as MagiQ Technologies and ID Quantique. As the threat landscape continues to grow and become more sophisticated, it is becoming increasingly clear that more than traditional cryptosystems may be needed to ensure the security of sensitive information. Quantum cryptography represents a new frontier in secure communications, and the investments in this technology are a testament to its potential to revolutionize the field of cryptography.

## II. Limitations of Modern Cryptosystems

Due to its slower speed, public key cryptography is more often used for key sharing than for the encryption of huge quantities of data [14]. Symmetric keys are distributed among distant participants using well-known key bargaining techniques like Rivest-Shamir-Adleman (RSA) and Diffie-Hellman. Many organizations favor a mixed strategy that incorporates the efficiency of a shared key system and the security of a public key system. Public key cryptosystems like RSA and Diffie-Hellman are not founded on precise mathematical justifications, but rather on years of public examination. Public key cryptosystems might be rendered immediately useless by developments in computer processing, such as quantum computing.

The Data Encryption Standard (DES) algorithm is no longer regarded as safe because technological developments have made it easy to circumvent. As a result, the Advanced Encryption Standard was created. Public key cryptography is susceptible to advancements in computer processing technology, and it's unclear whether a theorem will be created in time to factor large numbers into their primes, potentially posing a risk to sensitive areas of national security and intellectual property. Modern encryption is susceptible to increases in processing power and mathematical complexity, and organizations that are impacted may need to invest a lot of money in assessing the risk of harm and possibly rapidly deploying a new, expensive cryptography system.

2769-5654/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCI62032.2023.00149

## III. Quantum Cryptography in Theory

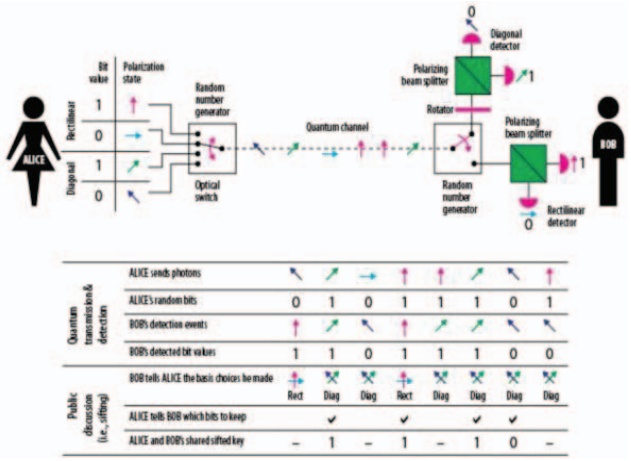


Fig. 1. Quantum cryptography.

The Heisenberg Uncertainty Principle, in general, and the photon polarization Principle are the foundations of quantum encryption. According to the Heisenberg Uncertainty principle, no system's quantum condition can be observed without causing some sort of disturbance [5]. According to the concept of photon polarization, light photons can be polarized or directed orientations and are only detectable by photon filters with the appropriate polarization. These ideas work together to make quantum encryption a compelling choice for protecting data privacy and thwarting prying eyes.

Quantum cryptography was created by Charles H. Bennet and Gilles Brassard to produce encryption passwords based on photon activity. This makes it possible to transmit keys securely without having to make inferences about the processing capacity of an adversary or work out challenging mathematical issues. Quantum cryptography is a trustworthy answer to the uncertainty issue in contemporary cryptography because it is founded on the laws of physics and is totally autonomous of the computational capacity of modern computing systems.

Quantum cryptography is a type of encryption method that uses the principles of quantum mechanics to secure data. It relies on the fact that no information can be copied without being detected. This means that if a hacker attempts to intercept a message, they will be unable to do so without leaving a trace. Quantum cryptography is considered theoretically unbreakable, as it relies on the laws of physics rather than mathematical algorithms.

The main benefit of quantum cryptography is that it provides an incredibly secure form of communication. It is also highly resistant to hacking and eavesdropping, as any attempt to intercept the data will be detected. This makes it ideal for sensitive communications, such as those between government agencies or businesses. As quantum cryptography becomes more widely available, it could revolutionize how we protect our data.

## IV. A Quantum Key Distribution Example

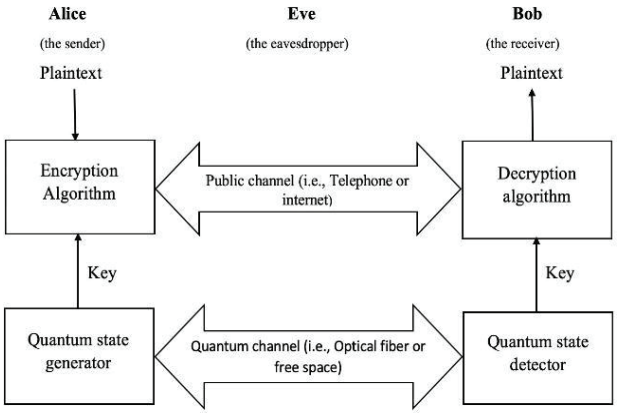


Fig. 2. Quantum Key Distribution.

The example given is about how quantum cryptography can be used to securely distribute keys between a sender, Alice, and a receiver, Bob, in the presence of a malicious eavesdropper, Eve. Alice sends a stream of randomly polarized photons to Bob using a photon gun. Bob randomly chooses a filter to measure the polarization of each photon and keeps a log of the correct measurements.

A predetermined portion of the stream of photons is used to build a key sequence for a one-time pad. Bob informs Alice about the type of measurement made and which measurements were of the correct type using an out-of-band communication system [2]. The correctly measured photons are translated into bits to form the basis of a one- time pad for sending encrypted information. The key is the product of both their random choices, which means neither Alice nor Bob can determine what the key will be in advance. Thus, quantum cryptography enables the secure distribution of a one-time key.

In the second paragraph, the scenario is presented where a malicious attacker, Eve, attempts to infiltrate the cryptosystem and defeat the Quantum Key Distribution mechanisms. If Eve tries to eavesdrop, she too must randomly select either a rectilinear or diagonal filter to measure each of Alice's photons. Eve will have an equal chance of selecting the right and wrong filter and will not be able to confirm with Alice the type of filter used. Even if Eve can successfully eavesdrop while Bob confirms with Alice the photons he received, this information will be of little use to Eve unless she knows the correct polarization of each particular photon. As a result, Eve will not correctly interpret the photons that form the final key and will not be able to render a meaningful key, thus thwarting her endeavors.

Firstly, the Heisenberg Uncertainty Principle states that information about photons cannot be duplicated since photons are destroyed when measured or interfered with. Secondly, Alice and Bob must calculate the number of photons required to construct the encryption key ahead of time so that the length of the one-time pad corresponds to the length of the message.

Furthermore, if Bob's photon count deviates from the predetermined fixed number, he can be certain that

communication is being sniffed or that something is wrong with the system. Since Eve is unable to duplicate an unknown quantum state, if she sees a photon, it will no longer exist for Bob to detect. If Eve attempts to make and transmit a photon to Bob, she will have to choose its orientation at random and be mistaken roughly half of the time - a high enough error rate to reveal her presence [11].

## V. Desirable QKD Attributes

QKD is a method of secure communication that uses the principles of quantum mechanics to generate and distribute secure cryptographic keys.

### A. Confidentiality of Keys

Confidentiality of keys in quantum cryptography refers to the fact that the transmission of a key between two parties is secure and secret. This means the key is protected from being intercepted or decrypted by any third party. This is possible due to the laws of quantum mechanics, which ensure that any attempt to eavesdrop on the transmission of a key will be detectable [7]. Additionally, quantum cryptography utilizes techniques such as quantum teleportation and entanglement to ensure the key is entirely secure.

The security of the key is ensured by the fact that any attempt to intercept the photons or modify the key will cause the photons to become uncorrelated, resulting in the key becoming unusable. In addition, the photons used in Quantum Key Distribution are almost impossible to replicate, making it impossible to create a duplicate key.

Overall, QKD is a highly secure method of exchanging sensitive data between two users. The system's security is ensured by the laws of quantum mechanics, which make it impossible for a third party to intercept or modify the key. In addition, the use of post-processing techniques make it even more secure. As such, QKD is an excellent way to ensure the confidentiality of data [19].

### B. Authentication

Authentication is based on the principles of quantum mechanics, which state that information cannot be copied or observed without changing it. Authentication in quantum cryptography is accomplished by using a quantum key, which is a string of randomly generated bits that can only be read by the two parties involved in the communication session [16]. The quantum key is then used to encrypt and decrypt messages, ensuring that only the intended recipient can access the transmitted data.

### C. Rapid Key Delivery

Rapid Key Delivery (RKD) is based on the principles of QKD, which utilizes the principles of quantum mechanics to create a secure communication link between two parties. Unlike conventional cryptography, which relies on complex mathematical algorithms to encode and decode messages, QKD relies on the fundamental laws of physics to make sure that the key exchange is secure. RKD is a variation of QKD that is designed to be faster and more efficient than other methods of secure key exchange. The protocol works by having two parties (Alice and Bob) generate a key using a secure quantum random number generator. The key is then exchanged between both parties in a secure, encrypted format.

### D. Robustness

Robustness in quantum cryptography refers to the ability of a quantum cryptographic system to withstand attacks from adversaries. This form of cryptography is much more secure than traditional cryptographic systems because it is impossible to intercept or tamper with the data without being detected. Robustness in quantum cryptography ensures that the data is kept secure even when faced with several attempts to crack it.

The robustness of QKD can also be improved using hardware-based security measures. For example, hardware-based random number generators can ensure that the key is truly random, thus making it more difficult to guess. Additionally, using trusted hardware can help ensure that the key is not intercepted or manipulated by an adversary.

Finally, robustness in QKD can be further improved by using post-processing techniques. Post- processing techniques can be used to detect errors in the transmission of the key and to detect any tampering that may have occurred [9]. Post-processing techniques can also detect any attempts to eavesdrop on the key.

### E. Prevention of the Analysis of Traffic Patterns

The prevention of the analysis of traffic patterns in quantum cryptography is achieved by using QKD. This method ensures that the communication is secure by preventing an eavesdropper from intercepting or analyzing the traffic patterns.

This is done by using a quantum-mechanically entangled system, where the particles used to encode the key are randomly generated and the communication is done using single photons. Entanglement ensures that any attempt to intercept the communication will be detected, making it virtually impossible to analyze the traffic patterns.

QKD also uses a “quantum state monitor,” which is a device that measures the state of the quantum channel at each point of transmission. The monitor constantly checks for any irregularities in the quantum state and will automatically discard any data that does not meet the required security standards.

QKD utilizes an “authentication protocol,” which verifies the identity of both parties before data is sent. This means that any attempts at traffic analysis must first be authenticated by both parties before any data is exchanged, making it much more challenging to perform traffic analysis. QKD also utilizes a “quantum channel,” a secure channel for exchanging data protected from any outside interference. Any traffic analysis attempts are rendered moot, as the data remains secure from interception throughout its transmission.

## VI. Implementing Quantum Cryptography

Here, we talk about different systems that have successfully implemented quantum cryptography technologies.

### A. The DARPA Quantum Network

Virtual Private Network (VPN) cryptography is the DARPA security model. To achieve secrecy and authentication/integrity, traditional VPNs employ both public- key and symmetric cryptography [10]. Public-key techniques allow for key agreement or exchange and endpoint authentication. Traffic confidentiality and integrity are provided through symmetric techniques (like 3DES and SHA1). Since the public network linking the VPN sites is not trusted, VPN systems can provide confidentiality and authentication/integrity [12]. In DARPA research, keys provided by quantum cryptography are supplemented or entirely replaced by current VPN key agreement primitives.

### B. MagiQ Technologies

MagiQ Technologies, a technology start-up with its headquarters in New York City, is one of the businesses creating solutions based on quantum cryptography [8]. The financial services sector, together with academic and government labs, are among the target markets for MagiQ's solutions [4]. According to MagiQ's business strategy, current cryptography methods are supplemented by quantum cryptography rather than replacing existing encryption technologies like PKI to create a hybrid system that is more secure.

The Navajo QPN Security Gateway is the name of MagiQ's remedy. MagiQ asserts that the QKD hardware box is the first QKD system to be made commercially available. It costs roughly $50,000 and includes a 40-pound chassis that can be mounted in a regular 19-inch rack.

## VII. Quantum Key Distribution Protocol Implementation

Quantum cryptography involves several specialized protocols, including sifting, error correction, and privacy amplification. These protocols are designed to ensure the secure transmission of information between two parties, Alice and Bob, in the presence of an eavesdropper, Eve [13].

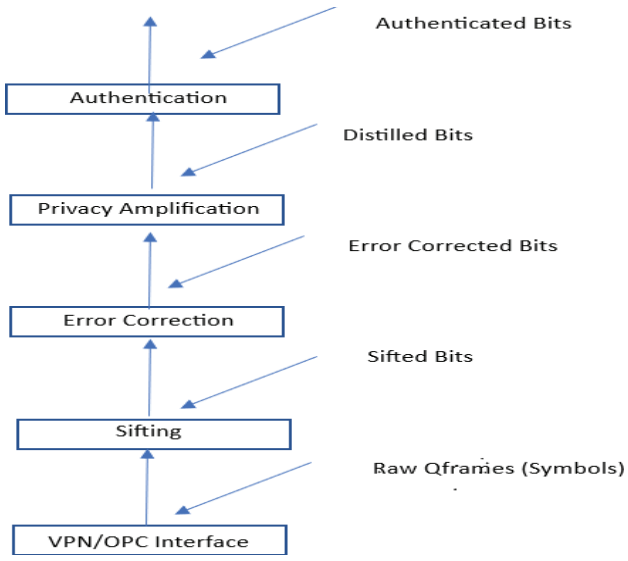


Fig. 3. The QKD protocol stack.

### A. Sifting

In quantum cryptography, sifting is the first step in the process of generating a secure, shared key between two parties, Alice and Bob. This step involves removing any failed qubits from the series of pulses transmitted by Alice to Bob. Failed qubits may result from several reasons, such as the laser not transmitting, detectors not working, or photons being lost in transmission [15]. Additionally, symbols where Alice chose one basis for transmission, but Bob chose the other for receiving are also discarded. These discarded symbols are referred to as the sifted keys.

After the sifting process, Alice and Bob eliminate the useless symbols from their internal storage and keep only those that Bob received, and his basis matches Alice's. This ensures that the remaining bits are error-free and suitable for use in the process's next step, error correction.

Sifting is a critical step in quantum cryptography, ensuring that only reliable bits are used for further processing. Removing failed qubits and incompatible basis symbols ensures that the remaining bits are suitable for use in the following steps. With sifting, the error rate would be significantly higher, leading to reliable key generation and communication. Additionally, sifting helps to reduce the amount of information that needs to be processed, making the overall process more efficient.

### B. Error Correction

In quantum cryptography, error correction is the second step in the process of generating a secure, shared key between two parties, Alice and Bob.

This step involves identifying and correcting all the error bits in their shared, sifted bits to have the same error-corrected bit sequence. Error bits result from noise or eavesdropping and must be assumed to be known to Eve, the potential eavesdropper, in error detection and correction codes [6].

The error correction process involves using quantum error-correcting codes to detect and correct errors in quantum bits or qubits [18]. These codes are based on the principles of quantum mechanics and involve encoding the original message into a more extensive set of qubits. The encoded qubits are transmitted through the quantum channel, and any errors introduced during transmission are detected and corrected using the error-correcting code.

Once the error correction process is complete, Alice and Bob will have identical error-corrected bit sequences. However, Eve may have gained some knowledge of the shared bits during the error correction process. Privacy amplification is crucial to reduce Eve's knowledge of the shared bits to an acceptable level.

### C. Privacy Amplification

This technique reduces Eve's knowledge of the shared bits to an acceptable level. Privacy amplification is also known as advantage distillation. To initiate privacy amplification, the side that initiates the process chooses a linear hash function over the Galois Field GF[2n]. N is the number of bits as input rounded up to a multiple of 32.

Four pieces of information are then transmitted to the other end, which includes the number of bits m of the shortened result, the sparse primitive polynomial of the Galois field, a multiplier that is n bits long, and an m-bit polynomial to add, which is a bit string to exclusive-or with the product. Both sides then perform the corresponding hash and truncate the result to m bits for privacy amplification.

### D. Authentication

Authentication is a crucial aspect of quantum cryptography that enables Alice and Bob to ensure that an attacker does not intercept their communication. In particular, authentication is necessary to guard against "man-in-the-middle attacks," where an attacker intercepts and alters the communication between Alice and Bob.

Alice and Bob must continuously authenticate all critical management traffic to authenticate their communication [1]. They typically use universal families of hash functions, introduced by Wegman and Carter [20], to generate an authentication hash of the public correspondence between them. These hash functions are designed to be efficient and secure, allowing Alice and Bob to authenticate their communication in real time.

However, it is essential to note that the secret key bits used for this approach can only be reused without compromising security. In other words, if Alice and Bob were to reuse the secret critical bits for authentication, they would be vulnerable to attacks from an attacker who has intercepted their communication.

Therefore, using new secret key bits for each authentication session is critical. Alice and Bob can use a complete authenticated conversation to generate new secret vital bits from QKD to validate new, shared secret bits. A few of these new secret key bits may replenish the pool of secret critical bits used for authentication.

Finally, it is worth noting that applying authentication techniques to authenticate the QKD protocols and the VPN data traffic is crucial. This helps to ensure that the communication between Alice and Bob remains secure, even in the presence of an attacker who may attempt to intercept or alter their communication.

## VIII. Results

In this paper, we provide a summary of the key ideas in quantum physics and their application to cryptography. In addition, we examined QKD's security and restrictions as well as the risks and challenges facing quantum cryptography.

According to our results, QKD offers a secure way to exchange encryption keys that is based on the laws of quantum physics. It does have certain drawbacks, though, like the poor speed of transmission and requirement for a secure channel for exchange of data [17]. We also discussed how different quantum cryptography protocols might offer additional privacy options.

## IX. Conclusion

An innovative method for secure communications, quantum cryptography is a promising technology. It is becoming progressively more obvious that more sophisticated safety precautions are required as the threat posed by quantum computing to conventional cryptosystems grows. Through providing an alternative for secure communication based on the concepts of quantum mechanics, quantum cryptography offers a potential answer to this situation.

Despite progress in quantum cryptography, there are still a lot of significant challenges to be solved. It may take some time before quantum cryptography solutions are widely used since they demand considerable infrastructure and resource investments. Furthermore, quantum cryptography techniques still may be vulnerable, which needs to be addressed.

## X. Future Work

The threat to conventional cryptosystems will increase as quantum computing technology progresses. Therefore, it is crucial to conduct additional research and development in the area of quantum cryptography. The next phase of research should concentrate on developing new quantum cryptography protocols, enhancing the performance of existing ones, and investigating quantum cryptography's potential applications beyond communication security.

The development of post-quantum encryption solutions that can withstand attacks from quantum computers is another subject for future research. Therefore, to maintain the long-term security of critical data, researchers should keep looking towards post-quantum cryptography solutions.

## References


[1] C. Bennett and G. Brassard, “Quantum Cryptography:Public Key Distribution and Coin Tossing,” International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for

Quantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. 7. Salkever, Alex. "A Quantum Leap in Cryptography." BusinessWeek Online. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, “Building the quantum network,” New J. Phys. 4 (July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." Quantum Communication, Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical Review Letters 85.2 (2000): 441.

[14] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.

[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society for Optics and Photonics, 2002.

[16] Barnum, Howard, et al. "Authentication of quantum messages." Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.

[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003.

[18] Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67.5 (2003): 052303.

[19] Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.

[20] Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." Physical Review A 59.5 (1999): 3301.