JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Evaluating Quantum Key Distribution Protocols: Strengths, Limitations, and Future Directions in the Era of Quantum Computing

Kabir Bahl
Student
Vasant Valley School, New Delhi, India

Abstract

The rise of quantum computers poses a huge risk to current encryption methods and security protocols. The paper discusses whether Quantum Key Distribution (QKD) can be a useful tool in strengthening the current and existing cryptography methods and provide more robust security against both classical and quantum computers.

The research was conducted by analyzing the functioning of a quantum computer and the existing methods of encryption that are currently in use. An in-depth study looking at the strengths and weaknesses of three different QKD protocols- BB84, B92 and E91 was conducted. A python program was created to simulate the three QKD protocols and their efficiency in different noise environments.

The analysis shows how QKD methods have significantly evolved over the years and provide strong and comprehensive security systems and methods of encryption that are immune to quantum computers. QKD will be a key component in developing and strengthening encryption methods that are currently used by a vast majority of people.

The rise of quantum computers poses a significant threat to current encryption methods. By implementing QKD protocols, encryption and security will be greatly boosted, safeguarding sensitive data and maintaining users' privacy.

Although QKD has many advantages and great potential to strengthen encryption, there are many obstacles that are yet to be overcome such as hardware constraints, high quantum costs, and vulnerability to certain attacks. The study also touches upon the need for improvement =s in scalable quantum hardware, error correction, and noise reduction. Additionally, the study looks at the potential of hybrid solutions that combine classical and quantum encryption techniques which may provide the most practical and easy to implement way to keep personal information secure in the quantum age.

INTRODUCTION

Quantum computers utilize principles of quantum mechanics to function and perform tasks which are impossible at the hand of regular computers. Quantum computers use qubits, which unlike bits in classical computers, can simultaneously exist in the states of 0 and 1 due to the principle of superposition. Furthermore, these qubits are entangled, resulting in qubits directly affecting and impacting other qubits, which allows for information to be transferred quickly and enables fast processing speeds.

Current methods of data encryption such as asymmetric Key Encryption (which includes RSA and ECC), Advanced Encryption Standard, Data Encryption Standard and TripleDES are vulnerable to quantum attacks. These encryption methods can be easily broken by quantum algorithms such as Shor's and Grover's algorithm. As quantum computers continue to get more and more advanced, they pose a greater threat to the privacy and personal data of countless individuals.

By looking at the data regarding the efficiency and use of the different QKD protocols the study arrives at definite conclusions regarding the efficiency of the three protocols on the basis of three criteria, noise, quantum cost and raw key efficiency. It also talks about the future development and scope for Quantum Key Distribution

QUANTUM KEY DISTRIBUTION

Quantum Key Distribution allows for information to be securely exchanged between two individuals over a public channel. Governed by the principles of quantum physics such as quantum entanglement and superposition, QKD guarantees secure

transmission of data by making it easy to detect any signs of an eavesdropper. It has been proven mathematically that QKD can guarantee safe communication even against the most advanced computers.

Over the last few years, there has been a significant increase in the popularity of different Quantum Key Distribution protocols, allowing for the creation of protocols such as BB84 and E91. Due to its increasing vitality, these protocols have been the subject of extensive research, analyzing their effectiveness, security, and applicability to real-world communications networks.

HEISENBERG UNCERTINTY PRINCIPLE

The Heisenberg uncertainty principle is based on the concepts of wave-particle duality of quantum objects and is a key component of quantum cryptography. ‘’It states that certain pairs of physical properties of a particle or system cannot be precisely measured simultaneously.’’ This entails that any form of eavesdropping and efforts to intercept a quantum system carrying a secret key will be readily visible and detectable. This allows for any parties using quantum encryption methods to detect a disturbance in the signal, allowing them to be aware of-and prevent eavesdropping.

NO CLONING THEOREM

According to the no cloning theorem "it is impossible to create identical copies of an unknown quantum state," This inevitably makes it simple to identify eavesdroppers and enables us to determine whether anyone intercepted the communication while it was being transmitted.

RAW KEY EFFICIENCY

Raw key efficiency (RKE) is “the ratio between the number of qubits transmitted and the length of the raw key received.” Suppose Alice and Bob are two individuals trying to communicate with each other. Alice sends Bob n qubits. Of those n qubits, if they determine that m qubits were accurately measured and agree with one another- they will have a key length of m The ratio of accurately measured qubits (m) to all qubits supplied (n) is known as raw key efficiency.

QUANTUM COST

Quantum Cost is another method of comparing QKD protocols. Quantum cost metrics are a means of approximating and comparing the resources required to construct quantum circuits. These measures allocate a gate or a weight cost to each different type of gate. The overall quantum cost of a circuit is thus equal to the sum of its gate costs.

BB84

Developed by Bennett and Brassard, the BB84 protocol selects at random one of the four quantum states to encode each bit of the key. These states are selected from two distinct bases: diagonal (45° and 135°) and rectilinear (0° and 90°). Alice uses the quantum channel to send Bob the photons that represent these states after they have been encoded. Bob measures each photon using a randomly selected basis, not knowing the basis Alice used. Alice and Bob communicate on a classical channel following the broadcast in order to compare the bases they used. They are left with a series of bits that make up the raw key after discarding the results where their bases don't match. They can find out whether there was any eavesdropping by carrying out an error-checking process since any interception would cause the quantum states to change and introduce faults that may be detected. To ensure the security of the final key, Alice and Bob can also shorten the key using a process called privacy amplification. This eliminates any partial information that an eavesdropper could have gained. To further improve the key and get rid of any discrepancies, they could additionally employ error correcting techniques.

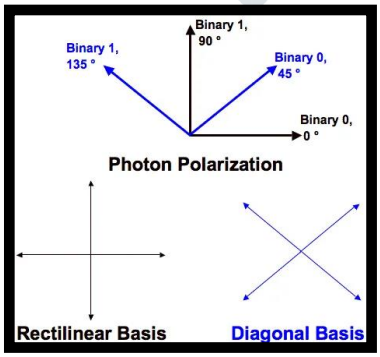

Fig 1: Photon polarization in BB84 protocol

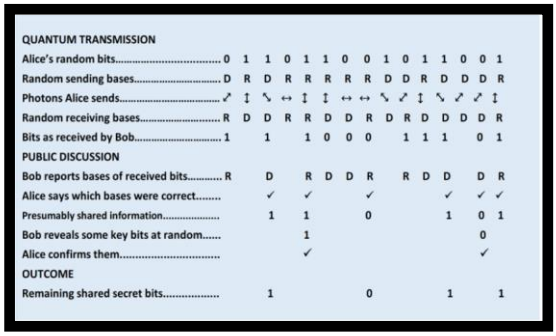

Fig 2: Possible outcomes of BB84 protocol

B92

Charles Bennett created the B92 protocol in 1992 as a simplified version of the BB84 protocol, which uses just two states to encode bits in photons. Alice uses the 45° state to represent a binary 1 or the 0° state to represent a binary 0 when she transmits a photon. Bob then uses a randomly chosen basis to measure each photon. if Bob selects the incorrect basis, he won't get any measurements since the states are non-orthogonal. Bob can tell he used the incorrect basis if there is no measurement, but if there is, the measurement result shows the right basis was employed. By communicating over a classical channel, Bob and Alice eliminate all the cases in which Bob failed to detect a photon. This guarantees that the final key contains just the bits that were measured correctly. Furthermore, because it is inherently difficult for an eavesdropper to obtain valuable information without being discovered, the B92 protocol benefits from an increased security mechanism. Because there are only two states utilized, it is more difficult for an attacker to obtain any valuable information and the protocol is less prone to errors during transmission.

E91

Arthur Eckert's E91 protocol adopts an alternative methodology. Alice and Bob use entangled particles known as Bell pairs to establish a secure key. No matter how far apart two particles are, entanglement guarantees that the state of one can always be instantly determined from the state of the other. Bob and Alice measure their particles separately during the process, using parameters that are chosen at random. When their results are compared, they will exhibit strong correlations because of the entanglement. These relationships, however, are only noticeable provided specific guidelines are followed when putting up the measurement. Alice and Bob use a classical channel to compare a subset of their measurements to create the final key. Any differences would be indicative of eavesdropping. The remaining measurements are utilized to generate a shared secret key since they are strongly correlated. Based on the fundamental ideas of quantum physics, E91's utilization of entanglement ensures security. To provide an additional layer of security, E91 can make use of Bell's theorem, which states that no theory based on local hidden variables can replicate the predictions of quantum physics. This ensures that the correlations between entangled particles cannot be explained by classical means. The protocol also allows for the possibility of using quantum teleportation in future implementations, further enhancing its security and potential applications in quantum communications.

Method

A python program was created which modeled the efficiency of the three QKD protocols in varying noise levels from 0-100. To introduce random fluctuations in noise levels as seen in real life, a stochastic noise function was added which adds gaussian noise with a configurable standard deviation.

The efficiency of the E91 protocol was modeled with the help of a logistic delay function for different noise levels. It also includes a purification factor in order to account for entanglement purification.

The efficiency of the BB84 protocols was modeled using a piecewise function with 2 regions based on a noise threshold of 0.4. Detection loss and quantum bit error rates were also added to make the simulation more realistic.

The efficiency of the B92 protocol was modeled with detection loss and quantum bit error rates as well as cubic dependence on noise. In order to show diminishing returns at higher noise levels it includes logarithmic scaling.

The efficiency was calculated for the three protocols across all noise levels and then represented on a graph with the help of a line plot.

The program works on a few assumptions while modeling the efficiency of the three protocols in different noise levels. A logistic decay function was used to model the decrease in E91 protocol efficiency with increasing noise, based on the assumption that entanglement fidelity declines sharply beyond a certain threshold. The efficiency of the BB84 protocol was modeled as a piecewise function, assuming distinct behaviors below and above a noise threshold of 0.4. To reflect realistic experiment conditions for BB84 and B92, a constant detection loss of 20% and QBER of 5% was taken. Stochastic noise was introduced as Gaussian noise with a standard deviation of 0.02 to 0.03 to simulate random experimental variations. Noise was assumed to have a uniform impact, and specific noise sources were not modeled separately.

Previous work that analyzed Quantum cost and raw key efficiency of the three protocols was also taken into consideration- allowing for more factors to be considered while evaluating the three protocols.

ANALYSIS OF EXISTING QKD PROTOCOLS

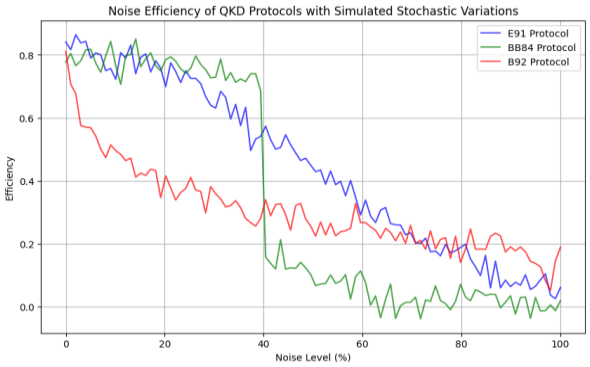

Fig 3: Graph depicting efficiency of BB84, B92 and E91 protocol at different noise levels

The graph shows the variation in efficiency of the three QKD protocols in varying noise levels. All three protocols show a downward trend as noise levels increase. The E91 protocol seems to be overall the most efficient across noise levels. The E91 protocol tends to decrease in efficiency with an increase in noise levels due to the entanglement of the quantum bits. The BB84 protocol shows a steep drop at a noise level of around 40% and is the least efficient of the three at higher noise levels. The B92 protocol is the least efficient of the three at low noise levels but tends to have a less steep drop than the other 2 protocols and is shown to be the most efficient at higher noise levels.

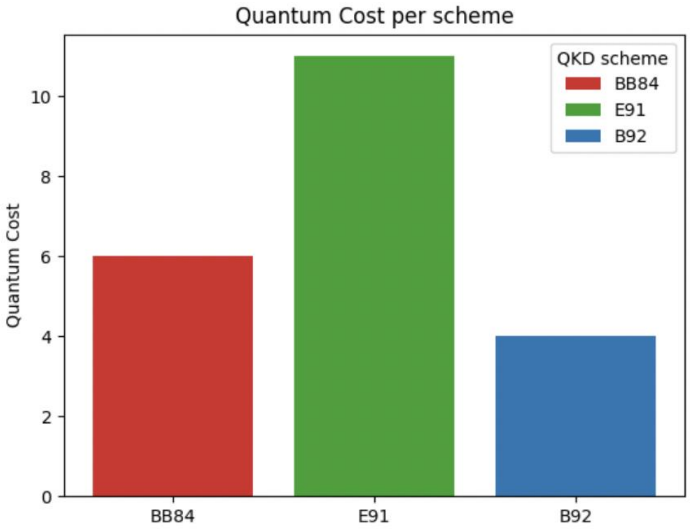

Fig 4: Quantum cost of BB84, B92 and E91 protocol

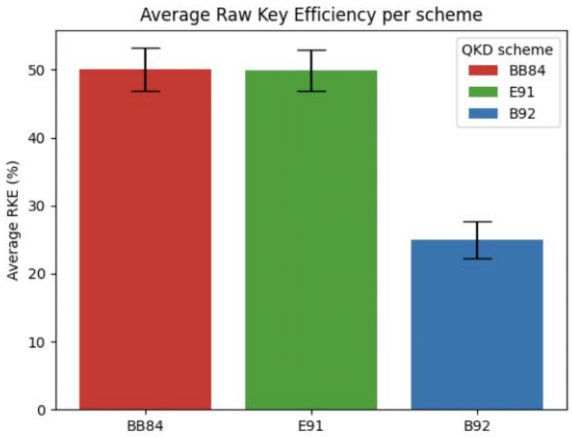

Fig 5: Raw key efficiency of BB84, B92 and E91 protocol

Even though the B92 system has the lowest quantum cost, it is clearly the least effective in terms of Raw Key Efficiency. The efficiency of the other two methods, BB84 and E91, is double that of B92, but their quantum costs are greater. The price difference between E91 and BB84 is substantial. E91 is about twice as expensive as BB84, however RKE does not profit from this higher cost because both schemes have efficiency levels of about 50%. Therefore, it appears that there is no advantage to picking E91 when choosing a QKD scheme with high RKE. Even though the plan makes use of several qubits and sophisticated quantum features like entanglement, it appears that this will simply drive-up costs since the far more straightforward BB84 obtains comparable results. B92 may be a suitable scheme to choose for minimal quantum cost, provided that RKE is not required. Still, there isn't much of a pricing difference between BB84 and B92. Selecting B92 instead of BB84 would save 33% in cost but result in a 50% reduction in RKE. As a result, BB84 is probably the most economical scheme overall, and its somewhat higher cost is justified by its better performance. To summarize, BB84 is the optimal choice in terms of both cost-efficiency and return on knowledge (RKE), whereas B92 could be a reasonable minimum-cost alternative. E91 is not a cost-justifiable option.

BB84

BB84 requires an ideal single photon source, which is unattainable with present technology. Currently available single photon sources are often bulky, costly, and inefficient. Instead, the highly attenuated lasers that use weak coherent pulses are largely exploited by QKD implementations. There is still a chance that a phase-randomized weak coherent pulse will include two or more photons as the photon number of such a pulse follows the Poisson distribution. The eavesdropper may initiate the PNS assault by taking advantage of the multiple-photon pulses. In this assault, the eavesdropper uses quantum non-demolition measurement to determine the photon number, block the single photon pulse and divides the single photon pulse into two for multiple-photon pulse. She then sends the receiver the other half of the multiple-photon pulse after keeping the first portion for herself. She can thereafter obtain the key value during the basis-reconciliation procedure. In this instance, the sender and receiver are unable to know of Eve's existence.

B92

In the B92 protocol, there is no way to tell the difference between the eavesdropping and the noise. There are three possible causes for the qubit error rate BER: Alice to Bob, Alice to Eve, and Eve to Bob. The qubit error rate in the original B92 protocol simply comes from the eavesdropping. Alice and Bob thus believe that there is an eavesdropper if there is a bit mistake. However, noise might also be the source of the bit error and it may not necessarily be due to eavesdropping. This means that in a noisy environment, the original B92 protocol cannot be utilized. The problem stems from the fact that the B92 protocol does not differentiate between the types of errors; instead, it uses the error rates between Alice and Bob to detect errors. In real-world situations when environmental noise and other disruptions are common, the BER might be influenced by factors unrelated to eavesdropping. As a result, the security of the protocol is compromised in such contexts, which might result in a reduction in overall resilience in real-world applications and unreliable detection of eavesdropping.

E91

The E91 protocol has the highest quantum cost out of any of the 3 protocols. This is because it requires the qubits to be entangled. It also requires a quantum channel to transit entangled photons unlike B92 and BB84, which over long distances can result in errors due to decoherence. E91 demands highly complex single photon detectors which can detect the photons in its entangled states. Due to the entanglement requirement, E91 requires extremely sophisticated single-photon detectors that have a high degree of precision when detecting photons in their entangled states. The difficult part of the process is keeping the entangled states coherent over potentially long distances and through noisy environments. However, since E91 uses entangled photons, it is resistant to photon number splitting (PNS) attacks, which are a frequent weakness in quantum key distribution protocols that depend on weak coherent pulses. Even though the use of entanglement in E91 presents technological challenges and comes at a high quantum cost, it offers a fundamental security benefit by utilizing the intrinsic qualities of quantum entanglement to guarantee safe communication.

WEAKNESSES IN CURRENT PROTOCOLS

Quantum cryptography is completely safe because no assumptions are made on Eve's inability to solve difficult mathematical problems, but rather about the fact that Eve can’t break the principles and laws that govern quantum mechanics. However, if Eve impersonates Bob or Alice, these protocols might be compromised by a man-in-the-middle attack. These kinds of attacks cannot be stopped unless Alice and Bob first authenticate one another. These protocols must be implemented carefully to avoid vulnerabilities. For example, physical layer attacks, including side-channel attacks, can enable Eve to obtain the key through unintended emissions or defects and faults in the hardware. These attacks take advantage of the physical properties of the devices used in quantum cryptography, which may allow information to leak in ways not anticipated by the protocol's design. Furthermore, using quantum cryptography in a loud environment or with malfunctioning equipment might result in bit-flip, phase errors, or measurement mistakes, making it less secure. discrepancies in the quantum states can be introduced by external noise or malfunctions in the equipment, which can result in increased error rates and possible weaknesses. In order to overcome these challenges, it is necessary to use strong error correction methods, cautious equipment calibration, and extensive testing under many

circumstances. Even though quantum cryptography is theoretically secure, in practice it must take these factors into account to make sure the system is secure in real-world situations.

FUTURE OF QUANTUM KEY DISTRIBUTION

Future developments in quantum Key distribution methods will guarantee strong security and have the potential to revolutionize cryptography. The development of quantum computers presents a significant danger to existing encryption methods, which in turn calls for the requirement of stronger and more robust encryption methods such as QKD. To provide a highly secure method of transmitting signals and data, quantum key distribution makes use of photon polarization and the ideas of quantum physics. This protects users against attacks by both classical and quantum computers.

As current QKD systems are developed over the next few years, increasing their scalability, practicality, and efficiency will be a key priority. QKD protocols, like BB84 and E91, have demonstrated encouraging outcomes thus far; nonetheless, they encounter difficulties when it comes to delivering data or sending signals over long distances or in noisy situations. Current research aims to increase the overall efficiency of the QKD system by lowering quantum bit error rates and improving the performance of single-photon sources and detectors. These developments will enable widespread use of QKD protocols and their integration into current communication infrastructures.

Another promising approach is to combine QKD with cryptographic systems and classical encryption techniques to create hybrid solutions. These hybrid solutions will enable quantum-resistant communications without requiring a whole redesign or replacement of the available technology. This strategy might significantly improve data transmission security, particularly in industries that require sensitive data and information, like banking, healthcare, and national security.

The threat posed by man-in-the-middle attacks and the necessity for secure data transmission in noisy situations are two key issues that require attention. Strong authentication techniques must be developed for QKD systems to stop these kinds of attacks and data leaks. Furthermore, advancements in error correction techniques as well as noise mitigation strategies will enhance the practical usability of QKD, especially in the real-world scenarios where ideal conditions are barely met.

There is also the possibility of using QKD in space. A growing number of people are interested in quantum communication satellites, in which QKD could potentially play a pivotal role by enabling secure satellite-based communication networks. These networks have the potential to offer worldwide coverage, facilitating safe communication in isolated, rural, and unreachable locations. China launched its own quantum communication satellite, Micius, demonstrating the viability of space based QKD and opening the door for further developments in this field.

In conclusion, there is a great deal of promise for the practical applications of QKD, provided that research and development efforts are directed towards surmounting specific obstacles and difficulties. QKD will probably play a significant role in international communication as quantum technology develops, offering consumers secure data transfer in opposition to the expanding danger of quantum computing.

CONCLUSION

Quantum computing poses a significant challenge to current encryption and cryptographic techniques, making QKD increasingly vital and important. It is clear from a detailed analysis of the three QKD protocols—BB84, E91, and B92—that QKD is an effective solution that can be applied to safely transfer data in the age of quantum computing. The protocols demonstrate the ability to improve security against both conventional and quantum computers, despite their respective strengths and drawbacks.

BB84 is an excellent and adaptable protocol for a wide range of applications due to its high efficiency and comparatively cheap quantum cost. Its use of weak coherent pulses and its potential for improvements in single-photon sources demonstrate that BB84 is an extraordinarily powerful QKD technique and will be an important model for further study. However, there are various challenges that also exist with BB84—it is vulnerable to Photon Number Splitting (PNS) attacks and demands improved hardware in order for it to truly reach its potential.

Both the B92 and E91 protocols have certain benefits, such as simplicity and immunity against certain types of attacks, but they also have a lot of drawbacks. In comparison to the other protocols, B92 is less efficient and finds it challenging to distinguish between eavesdropping and noise. Meanwhile, E91 is extremely complex and has a high quantum cost. Improvements in error correction, noise reduction, and effective quantum hardware systems are needed for both protocols. The practical implementation of these protocols requires addressing these challenges, especially in noisy environments or over long distances.

Looking ahead, hybrid models, which include aspects of both traditional and QKD systems, show the greatest promise. The importance of fusing quantum key distribution (QKD) with traditional encryption to create quantum-resistant communication systems is becoming more and more clear as quantum computing advances.

Strong authentication methods must also be developed to stop man-in-the-middle attacks, which continue to pose a serious danger to QKD systems. Improvements in single-photon sources and detectors, as well as the scalability and viability of these systems for broad use, will also be critical to the success of QKD in the future. With the advent of quantum communication satellites, QKD has great promise to transform international communication networks. These developments might make QKD a pillar of safe global communication by enabling secure connection in isolated and distant locations.

To summarize, the success of QKD protocol development and implementation is critical to the future of cryptography and encryption. The goal of current research is to explore new development paths and overcome existing limitations. As quantum computing poses ever-changing threats to sensitive data, QKD is set to become an essential part of secure communication

networks. Without a doubt, QKD systems will significantly alter the cryptography landscape and ensure that secure communication is still possible in an increasingly quantum environment.

WORKS CITED

Akter, Shapna. Quantum cryptography for Enhanced Network Security, June 2, 2023. https://arxiv.org/pdf/2306.09248.

Asif, MR. "Quantum Key Distribution and BB84 Protocol." Medium, May 10, 2022. https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5.

"China Launches Quantum-Enabled Satellite Micius." BBC News, August 16, 2016. https://www.bbc.com/news/world-asia-china-37091833.

Li, Leilei, Jian Li, Chaoyang Li, Hengji Li, Yuguang Yang, and Xiubo Chen. "The Security Analysis of Quantum B92 Protocol in Collective-Rotation Noise Channel." *International Journal of Theoretical Physics* 58, no. 4 (February 4, 2019): 1326–36. https://doi.org/10.1007/s10773-019-04025-7.

Lidbjörk, Erik, and Rasmus Söderström Nylander. Cost and efficiency comparison of Quantum Key Distribution schemes, June 10, 2023. https://www.diva-portal.org/smash/get/diva2:1779798/FULLTEXT01.pdf.

Ling, Alexander, Matt Peloso, Ivan Marcikic, Antía Lamas-Linares, and Christian Kurtsiefer. "Experimental E91 Quantum Key Distribution." *SPIE Proceedings*, February 7, 2008. https://doi.org/10.1117/12.778556.

M, SujayKumar Reddy, and Chandra Mohan B. "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol." Arxiv, December 9, 2023. https://arxiv.org/html/2312.05609v1#:~:text=The%20working%20principle%20of%20BB84,below%20with%20Alice%20and%20Bob.&text=for%20preceding%20element-,1.

Zhang, Qiang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. "Large Scale Quantum Key Distribution: Challenges and Solutions [Invited]."

Optics Express 26, no. 18 (August 31, 2018): 24260. https://doi.org/10.1364/oe.26.024260.