Comparative Analysis of Quantum Key Distribution Protocols: BB84 and B92 in the Context of Hybrid Quantum-Classical Networks

Yifeng Zheng

Computer Information Systems Department, Berkeley city college, Berkeley, 94709, USA

30039407@cc.peralta.edu

Abstract. As the internet continues to expand, demands for efficient multi-data transmission and heightened security grow ever stronger. However, traditional point-to-point systems fall short in meeting the increasing requirements for secure links among multiple users. This is where the hybrid Quantum-classical network, a practical and economically viable solution, steps in to serve a larger user base within a limited resource framework. This paper delves into two mature protocols, namely BB84 and B92, which underpin the functionality of these hybrid networks. An examination and comparison of these protocols, based on their underlying logic and transmission simulations, will lay a solid foundation for the creation of the hybrid Quantum-classical network. The concept of the hybrid Quantum-classical network will be elaborated upon, primarily focusing on its performance in optical fiber to simulate real-life data transmission. The intention is to offer perceptive recommendations on the establishment of a Quantum-classical hybrid network, bearing in mind the distinct differences between the BB84 and B92 protocols. In effect, this paper aims to be a valuable resource in the journey towards meeting the future demands of data transmission and security through quantum-classical hybrid networks. It underscores the transition from theory to practice, turning quantum protocols into a tangible reality in our daily digital interactions.

Keywords: Quantum optics, Quantum Key Distribution, BB84 protocols, B92 protocols

1 Introduction

As the Internet continues to grow, the demand for data transmission escalates at a rapid pace. This growth gives rise to challenges, including inadequate network transmission and the threat of eavesdroppers. Quantum Key Distribution (QKD), known for its efficiency and high security, has become a global research focus and a solution to these aforementioned issues. However, the point-to-point characteristic of QKD hinders the establishment of secure links among multiple users [1]. In an effort to serve more users with limited resources, building a quantum-classical hybrid option network emerges as an economical and practical choice. Nevertheless, the main

P. Kar et al. (eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)*, Advances in Computer Science Research 108,
https://doi.org/10.2991/978-94-6463-300-9_56

challenge during the construction of an actual quantum-classical hybrid network is the selection of suitable protocols.

This article will examine the differences between the BB84 and B92 protocols, demonstrated through basic logic and transmission simulation. Further discussion will encompass the performance of these protocols in real-world situations, such as varying numbers of users, the presence of eavesdroppers, and more. The objective here is to provide a reference for resolving issues related to the quantum-classical hybrid option network [2].

2 The Introduction of QKD in General

As methods of cracking cryptographic keys advance over time, classical cryptography is increasingly unable to serve as an impervious barrier to eavesdroppers. Consequently, attention has shifted towards a revolutionary approach for secure communication known as Quantum Key Distribution (QKD). This technique enables the generation of a random and secure key between two parties, referred to as Alice and Bob. They can use this key to encrypt and decrypt messages. A significant feature of QKD is its capacity to detect eavesdroppers [3]. Should a third-party attempt to intercept the communication, the process of measuring the qubits results in loss of information and the collapse to a single state. This action reveals the presence of the eavesdropper, thereby ensuring the security of the transmission.

According to Nandal, the QKD process can be segmented into three distinct phases: Raw Key Exchange, Key Sifting, and Key Distillation (p.246). The Raw Key Exchange represents the initiation of Quantum Key Distribution (QKD) and is unique in its requirement of a quantum channel. During this phase, multiple quantum states are shared between Alice and Bob. These states subsequently undergo sifting and error correction processes to produce the final secret key. Following this stage, the majority of QKD protocols transition from the quantum channel, opting instead for a classical channel in subsequent stages of QKD. This shift towards utilizing a classical channel is known as 'Classical post-processing'.

Key Sifting comprises the second part of the QKD process. Here, using the classical channel, Alice and Bob decide which measurements will be integrated into the final secret key and which ones will be disregarded. The logic behind this decision-making process varies (or might remain consistent) depending on the specific QKD protocols. Any measurements where Alice and Bob are not in agreement are discarded, resulting in what is termed the 'sifted key'. The final part of the QKD process is Key Distillation. This phase detects whether the transmission loss exceeds the error rate to counteract the errors induced by transmission channel losses [4].

3 Comparation of BB84 and B92 in Basic Logic

3.1 Implementation of BB84

In the first phase, known as the sending phase, Alice randomly selects bits from the set {0, 1} and bases from Z (0 and 1 basis) and X (- and + basis). This results in four possible combinations. If Alice chooses 0 and Z, the corresponding qubit state is |0>. For 1 and Z, the state is |1>. Similarly, 0 and X correspond to |+>, and 1 and X correspond to |->. Alice repeatedly then sends one of these four possible qubits to Bob.

Upon receiving the qubit, Bob selects bases on the Z and X in a randomized manner. In the scenario where Bob opts for the Z basis, and Alice's transmitted qubit assumes the state |0>, Bob's measurement outcome will yield a classical bit value of 0. Conversely, if Alice's qubit is |1>, Bob will observe a measurement outcome of 1. In the case of |+> and |-> qubit states, Bob's measurements will yield a probabilistic distribution, entailing a 50% probability of obtaining 0 and an equivalent 50% probability of obtaining 1. Conversely, should Bob select the X basis, the measurement outcomes for |0> and |1> qubit states will yield an equal probability of 0 and 1 (50% each), while the |+> state will result in a measurement outcome of 0, and the |-> state will yield a measurement outcome of 1. Considering the eight conceivable outcomes arising from the combination of basis selections and qubit measurements, there exist four scenarios wherein Bob's measured bit aligns with Alice's original bit, leading to an overall match rate of 50%. To provide an illustrative example, consider a scenario involving the transmission of 500 qubits: approximately 250 of these qubits will align, forming the key generated by the BB84 protocol [5].

3.2 Implementation of B92

B92, proposed by Charles H Bennett, is a variant of the BB84 protocol. It adheres to a similar triphasic structure as BB84. However, a slight divergence occurs during the initial sending phase. In contrast to BB84, where both bases and bits are selected, Alice, in the B92 protocol, only selects bits, denoted as Alice_bits, ranging from 0 to 1. This gives rise to only two potential qubits: |0> represented by 0, and |+> represented by 1. Alice proceeds by transmitting the selected qubit (either |0> or |+>) to Bob [2].

In the receiving phase, Bob independently selects a list of integers, termed Bob_bases, drawn uniformly from the set [0, 1]. This protocol aligns with the standard BB84 convention, where 0 corresponds to the Z basis, and 1 signifies the X basis. If Bob selects the Z basis, and Alice transmits the qubit state |0>, Bob's resulting measurement will invariably yield 0. If Alice, however, sends the qubit state |+> and Bob uses the Z basis for his measurement, the outcome will be equally likely to be 0 or 1. In cases where Bob utilizes the X basis, the measurement result will be either 0 or 1 with a probability of 50% when Alice transmits |0>. Meanwhile, when Alice sends the qubit state |+>, Bob's measurement will always yield 0 [6].

The key generation process discards all instances where Bob decodes 0, retaining only those where he decodes 1. The indices of these instances are compiled into a list named Bob_one_indices. Alice then reverts to the bases used in phase one, Alice_bits, and flips the bits (0 to 1 and vice versa) corresponding to the indices in Bob_one_indices. It is observed that the outcome aligns with the bits in Bob_bases that Bob later decodes as 1: Flipped (Alice_bits [Bob_one_indices[i]]) = Bob_bases [Bob_one_indices[i]]. Based on the above analysis, it can be inferred that approximately half the time, the bits in Bob_bases and Alice_bits will correspond, since both parties are randomly selecting between 0 and 1. Conversely, the remaining half of the bits in Bob_bases and Alice_bits will not match. Within these instances, about half the time, Bob will measure a 0, while during the other half, he will measure a 1. This suggests that roughly ¼ of the decoded bits retrieved by Bob will be 1. Consequently, the length of the key produced in this process will be about ¼ of the length of the original bits generated by Alice. This is in contrast to the ½ key length yielded through the BB84 protocol [7].

4 BB84 and B92: The Difference

4.1 Encoding and Measurement Bases

During BB84, Alice uses two bases, the rectilinear and diagonal bases, to encode her qubits. Consequently, there exist four potential outcomes for each qubit. Through subsequent processing and analysis, only half of the original bit string transmitted by Alice will ultimately contribute to the final secret key.

In B92, however, Alice only uses two possible states, rectilinear and diagonal, to encode her qubits. Consequently, there exist two potential outcomes for each qubit. Through subsequent processing and analysis, only one-fourth of the original bit string transmitted by Alice will ultimately contribute to the final secret key.

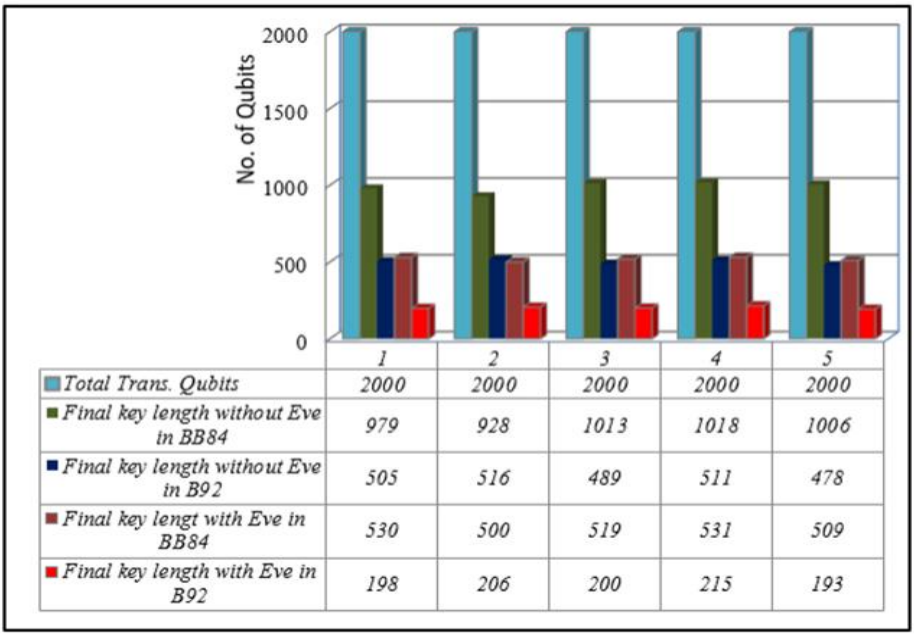
4.2 Theorem Involved

The BB84 protocol utilizes the no-cloning theorem as its underlying security principle. The no-cloning theorem, a fundamental concept in quantum mechanics, states that it is impossible to create an exact copy of an unknown quantum state. In the context of BB84, this theorem ensures that any attempt by an eavesdropper (referred to as Eve) to intercept and clone the qubits being transmitted by Alice will result in detectable errors. Since Eve cannot perfectly clone the qubits without being discovered, any eavesdropping attempt can be identified through the discrepancies observed by Alice and Bob during the key reconciliation process [8].

In contrast, the B92 protocol relies on the concept of quantum entanglement as its security theorem. Quantum entanglement refers to a phenomenon in which two or more particles become inherently correlated, regardless of the physical distance separating them [9]. B92 exploits this entanglement property by using pairs of entangled qubits to distribute the secure key. The security of the B92 protocol lies in

the fact that any attempt by Eve to measure or intercept the qubits during transmission will perturb the entanglement and lead to observable discrepancies between Alice and Bob's measurements. By comparing their measurement results and checking for inconsistencies, Alice and Bob can detect the presence of an eavesdropper [10].

4.3 Efficiency



	1	2	3	4	5
Total Trans. Qubits	2000	2000	2000	2000	2000
Final key length without Eve in BB84	979	928	1013	1018	1006
Final key length without Eve in B92	505	516	489	511	478
Final key lengt with Eve in BB84	530	500	519	531	509
Final key length with Eve in B92	198	206	200	215	193

Fig 1. Total transmitted qubits from Alice and successful received qubits from Bob without and with Eve existent versus number of attempts using both the BB84 and B92 protocols with (N=2000 qubits, error rate=2%.) [2]

According to the article "A Simulative Comparison of BB84 with B92 Quantum Cryptography Protocol" authored by Alsreeh, Alabeedy, and Kamal, experimental results illustrate key performance variances between the BB84 and B92 protocols under varying circumstances.

Based on the Fig 1, when there is no eavesdropper, the BB84 protocol showed roughly a 50% success rate in receiving transmitted bits, while the B92 protocol registered a success rate near 25%. When eavesdropping was introduced, these success rates fell markedly, reaching around 25% for BB84 and approximately 12.5% for B92. These outcomes suggest that BB84 operates at double the efficiency of B92 in terms of key generation rate.

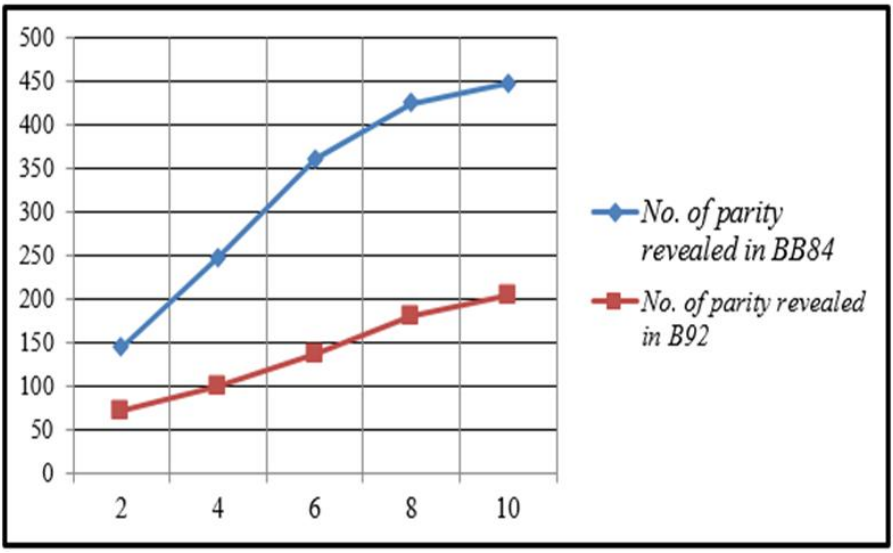


Fig 2. No. of parity revealed versus the actual error rate (N=2000). [2]

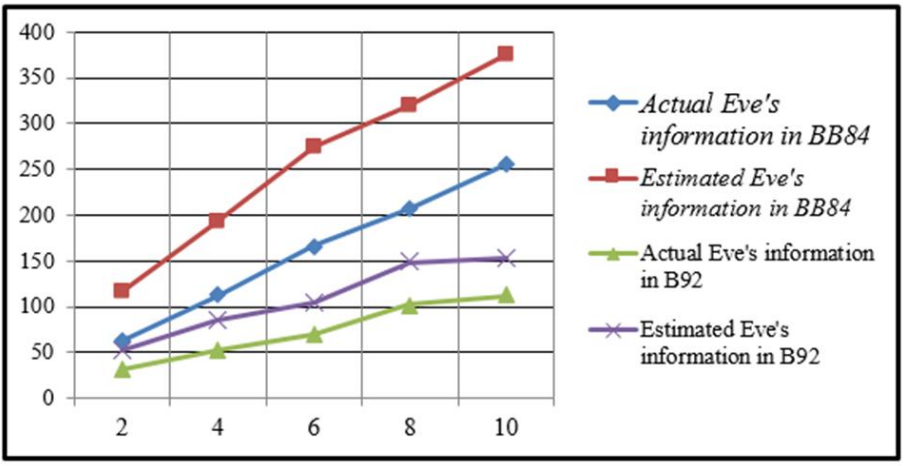


Fig 3. Expected and actual Eve's information on the sifted key versus actual bit error rate inputted to the program for both BB84 and B92 protocols (N=2000).[2]

Additionally, a closer examination of the second and third experimental charts in this study, as depicted in Fig 2 and 3, provides a more in-depth understanding of the disclosure of parity information and the expected versus actual information a potential eavesdropper could extract from the sifted key in each protocol, given a constant error rate. The results reveal that the B92 protocol discloses fewer parities than the BB84, predominantly because the length of the sifted keys in B92 is half that in BB84..

5 The Advantage of BB84

5.1 Security

BB84 provides a significant level of flexibility in terms of the number of encoding states and measurement bases utilized. By employing four distinct states and two measurement bases, BB84 enhances the information capacity and reinforces security against potential eavesdropping attempts.

5.2 Fault Tolerance

The BB84 protocol incorporates error detection mechanisms during the key reconciliation process. Alice and Bob compare the measurement bases used, enabling them to identify and discard qubits where the measurement bases do not align. This step minimizes the risk of utilizing compromised qubits for key generation and enhances the overall fault tolerance of the protocol.

5.3 Efficiency

In simulation, we can see the BB84 protocols is generally more efficient than the B92 in producing the key. BB84 utilizes four quantum states to encode information which is the reason it is more efficient compared to B92 utilizes two quantum states, allowing for the transmission of one bit of classical information per qubit.

6 The Advantage of B92

6.1 Stability and Simplicity

B92 stands out for its simplicity and the utilization of fewer physical qubits compared to BB84. This simplicity contributes to a lower probability of qubit pollution, ensuring higher stability in the protocol. The reduced number of physical qubits in B92 decreases the likelihood of interference and external perturbations, thereby enhancing the overall stability of the protocol.

6.2 The Proposal Based on the Difference of BB84 and B92 for the Quantum-classical Option Network Establishment

The transition towards quantum key distribution networks signifies a pivotal advancement in key distribution, especially for multi-user, high-speed, and long-range applications in the future. Enhancing the confidentiality and security of communications, these point-to-point key distribution protocols are critical [5]. In broad terms, quantum key distribution networks can be classified into trusted relay key distribution networks, passive optical device key distribution networks, and

quantum entanglement key distribution networks, each type reflecting different deployment strategies. Among these, the most feasible strategy given present technological capabilities involves the integration of the passive optical network (WDM-PON) to establish a quantum-classical hybrid optical network [7].

In this discussion, the emphasis will be on this specific context. By examining the differences between the BB84 protocol and the B92 protocol concerning network performance, it is possible to define the influence of the classical signal as a constant and assume a user count of N. In this scenario, the cost of building the network can be given as: CBB84 = NCsend + NCreceive + Cnetwork. From the earlier analysis, it's seen that when transmitting a message of the same length, the BB84 requires twice the qubit length compared to B92. This implies that the cost of establishing a BB84 network is roughly twice that of a B92 network for a network of the same specifications. Reviewing the properties of BB84 and B92, it is possible to draw some conclusions exclusively between the BB84 protocol and B92 protocol. Given its high efficiency and cost, the BB84 is advantageous in small-scale networks, providing rapid message transmission over short distances at a reasonable cost. For medium-sized networks, B92 could be a more suitable choice due to its lower cost and ease of maintenance. As for larger networks, based on current quantum technology, it is deemed more reliable to opt for a non-quantum protocol as a practical plan in actual network deployment [4].

7 Conclusion

In conclusion, this research report offers an in-depth exploration of the Quantum Key Distribution protocol, incorporating a broad overview of its general methodology and mechanisms. Subsequently, the focus shifts to the specifics of two major QKD protocols: BB84 and B92. Detailed explanations are provided about the principles that govern their implementation. Moreover, this report presents a comprehensive analysis of the differences between these two protocols with respect to security, efficiency, stability, and fault tolerance. With the insights gleaned from this study, informed decisions can be made regarding the selection of either BB84 or B92, based on specific requirements and priorities. The BB84 protocol demonstrates significant strengths in the areas of security, fault tolerance, and efficiency. This makes it a solid choice for applications demanding high efficiency and rigorous security measures. In contrast, the B92 protocol forgoes efficiency in favor of simplicity and reduced resource requirements, making it a viable option especially in scenarios where resource limitations are a significant factor. Further in the report, a cost analysis of network deployment under similar circumstances for both the BB84 and B92 is undertaken. Utilizing specific formulae, it becomes evident that the BB84 protocol is well-suited to smaller network deployments due to its high efficiency, despite its higher cost. On the other hand, the B92 protocol emerges as a practical choice for medium-scale network deployments due to its cost-effectiveness and stability. However, for larger network deployments, neither the BB84 nor the B92 protocols prove to be reliable. As a result, this particular scenario is not addressed in the report.

References

1. Hwang, W. Y., Choi, S., & Gong, G. (2021). A comparative study of quantum key distribution protocols BB84 and B92 in the presence of loss. Quantum Information Processing, 20(4), 132.
2. Fahira, G., Hikmaturokhman, A., & Danisya, A. R. (2020). 5G NR Planning at mmWave Frequency: Study Case in Indonesia Industrial Area. In 2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE) (pp. 205-210). IEEE.
3. Ghosh, A., Kumar, V., & Bera, M. K. (2020). Comparison between BB84 and B92 quantum key distribution protocols using coherent and squeezed states. Optik-International Journal for Light and Electron Optics, 209, 164219.
4. Choi, S., & Hwang, W. Y. (2019). Comparison between decoy-state BB84 and B92 protocols under various channel losses. Quantum Information Processing, 18(11), 349.
5. Li, L., Meng, X., Xu, H., Luo, P., & Ma, W. (2019). Comparative study between BB84 and B92 quantum key distribution protocols based on mutually unbiased bases. Quantum Information Processing, 18(7), 207.
6. Bhowmick, A., Kundu, A., & Karmakar, K. (2018). Performance comparison of BB84 and B92 protocols in the presence of individual eavesdropping attacks. Optik-International Journal for Light and Electron Optics, 156, 242-252.
7. Rejeb, I., & el Allati, A. (2018). Comparative study of BB84 and B92 quantum key distribution protocols for satellite communication network. International Journal of Satellite Communications and Networking, 36(3), 191-196.
8. Ghosh, A., Kumar, V., & Bera, M. K. (2017). Comparative analysis of BB84 and B92 quantum key distribution protocols using squeezed states. Optical and Quantum Electronics, 49(10), 340.
9. Li, Q., Yang, L., Feng, X., & Xu, F. (2016). A comparative study of BB84 and B92 quantum key distribution protocols based on weak coherence states. The European Physical Journal D, 70(7), 140.
10. Thakur, G. S., & Rai, A. K. (2015). Performance comparison of BB84 and B92 quantum key distribution protocols under imperfect laser source. Optik-International Journal for Light and Electron Optics, 126(2), 166-169.