# Bridging Classical and Quantum Cryptography: Evaluating BB84 and the Role of Entanglement in Secure Communication

Vidarth Anbu

## Abstract

In the modern digital era, cryptographic protocols form the foundation of secure communication, from safeguarding messages to protecting national infrastructure. For years classical encryption techniques served the role of protecting our information; however, due to technological advancements not only in the engineering field but also in the field of physics classical encryption no longer provides reliable and safe security [2][3][4][7]. Quantum communication has introduced a fundamentally new paradigm in secure communication, most notably through the BB84 protocol [1]. This protocol uses a fundamentally different approach to security that offers unbreakable encryption [10]. The advances of the field not only offer protection but also open the possiblity to different approaches to attack [11][15]. However, despite its clear advantages, the widespread adoption of the BB84 protocol in everyday communication remains limited by technological and physical barriers [11][15]. These challenges include photon loss in transmission, limited key generation rates, short coherence of quantum states, and difficulty integrating these complex systems with existing classical infrastructures [14][17]. Furthermore, achieving scalability to support large, complex networks introduces new constraints [14]. While these systems can enable fast and long distance transmission, these technologies still remain developmental as well. This paper argues that an overlooked challenge in integrating quantum systems with classical infrastructure is the absence of entanglement in the BB84 protocol, which forces a reliance on classical components that introduce interference and instability [14][18][10]. Although the benefits of entanglement–based protocols are recognized in the literature [8][10] [19] the consequences of the BB84's non entangled design remains underexplored [14][17][13].

## Introduction

Cryptography is the science and mathematics of protecting information from unauthorized access by encoding messages into an unreadable cryptic format [5][6]. It plays a fundamental role in ensuring the confidentiality and authenticity of communications from private conversations to financial transactions to military intelligence [6][7]. Specifically, classical cryptography, developed long before modern computing, relies upon mathematical transformations and substitutions to convert plaintext into ciphertext [6]. These methods include algorithms such as the Caesar cipher and the Vigenere Cipher cipher [5][6]. These methods were designed under the assumption that unauthorized decryption is computationally unfeasible without the correct key [6].

The strength of these ciphers lay in the size of the keyspaces and the transformation rules. However, as computational power has increased over the years, and with the rise in quantum computing, the security once promised by these systems has now become a thing of the past.

Quantum computers harness and leverage principles of quantum physics –specifically superposition and entanglement – to perform many calculations that are difficult for classical computers. This includes scenarios such as optimization or search algorithms where many computations can be performed in parallel [2], giving rise to quantum algorithms that can solve certain problems far more efficiently. For example, Grover's Algorithm reduces the time needed to search an unsorted keyspace $N$ from $O(N)$ to $O(\sqrt{N}\ )$ [4],[1] making it exponentially faster for large keyspaces and significantly weakening the security of classical encryption methods that rely on long keys alone.

As a result, the limitations of key length based security have led researchers to explore fundamentally different approaches to cryptography [1][2][10]. One such direction is quantum cryptographic protocols that leverage not computational difficulty but rather derive from the physical principles of quantum mechanics. The most well known of these is the BB84 protocol, proposed in 1984 by Charles Bennett and Giles Brassard [1]. The protocol enables two parties, Alice and Bob, to establish a shared secret key using qubits - quantum bits that can exist in superposition and cannot be copied due to the no-cloning theorem [2][9]. The protocol involves transmitting qubits encoded in either Z basis which is a set of orthonormal basis states $|0>$ and $|1>$ or the X basis which is a set of diagonal basis states $|+>\ and\ |->$ and measuring them with randomly chosen bases. After measuring, the parties compare their basis choices, and discard the non matching bits from a sifted key. Specifically, in order to protect from eavesdropping, the Quantum Bit Error Rate (QBER) is used to detect any third parties and if it remains below a certain threshold the key is deemed to be secure for communications [10][11].

To better understand how quantum protocols like BB84 differ from classical methods, it is useful to first examine a few widely known classical encryption techniques. One of the simplest and most historically significant techniques is the Caesar cipher, also alternatively known as the shift cipher. An example of this technique is that with a shift of 3, and A would shift to the letter D, B shifts to E and so on and so forth. A mathematical representation of this cipher can be represented by this encryption function:

$$e(x)\ =\ x(numerical\ value)\ +\ k(shift\ value)\ mod\ 26$$

The modulus of 26 ensures that the final encryption remains inside the alphabet [5][6].
The decryption function on the other hand the shift value k is subtracted from the encrypted letters in the equation:

$$d(x)\ =\ x\ -\ k\ mod 26$$

Secondly, the Vigenere cipher is a method of encrypting text by using a repeating keyword to shift each letter of the text by a variable element, essentially creating a form of polyalphabetic

[1] Here, O(N) is a standard way of describing how an algorithm's runtime scales with input size. In this case, it means that a classical computer must try each of the N possible keys one by one.

substitution cipher that is more secure and reliable than simple Caesar shifts [5][7]. For example, an A in the alphabet can equal to 0 and B can be equal to 1 and so on and so forth. The specific mathematical equation used to represent this polyalphabetic substitution is:

$$c_i = (p_i(plaintext\ letter) + k_i(key\ letter))\ mod\ 26$$

In order to decrypt the text, we subtract the key values. In this case, the equation changes to:

$$p_i = (c_i - k_i + 26)\ mod\ 26$$

The addition of the 26 before taking the modulus avoids the negative numbers. In this situation the Vigenere cipher would appear stronger and more effective than its counterpart due to its modular arithmetic ability to shift each letter.

The BB84 Protocol initiates a secret key between two individuals. The protocol is developed through this process. Alice generates a random bit sequence of encoding bases- either the computational Z basis or the diagonal X basis. The Z basis is a set of orthonormal states $|0> and\ |1>$ the matrix being $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, and the other matrix $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ respectively, while the X basis is the superposition of these basis states [1][2][9].

These bits are then sent to Bob, who will randomly select measurement bases. After the transmission, the parties will compare their basis choices and will discard the bits that do not match. The matching states form a sifted key through the QBER. This method provides information on how many qubits are incorrect in comparison to each other. If the QBER is low and the rate at which it can produce is acceptable then the key can be used for secure communication between parties [1][2][9].

**Methods/Results**

In order to compare and evaluate the security of different key generation and distribution methods, we designed tests in order to discover how effectively each method protects the secrecy of the key in the presence of classical and quantum eavesdroppers. This paper will use classical key methods such as Caesar and Vigenere as well as the BB84 for a direct comparison.

Although classical programs are typically classified as encryption methods, they also rely heavily on secret keys shared between Alice and Bob. These key sharing approaches are more agreed upon and assumed rather than secured making them vulnerable to attacks by Eve. By contrast, the BB84 is a protocol designed to securely establish a shared secret key despite being in the presence of attacks by Eve.

To assess the strength of each key method, we used these 3 tests:

Resistance to brute force quantum attacks: We assessed the vulnerability of each method to quantum computational attacks targeting the secret key.

Resilience to brute-force guessing: We modeled brute force attacks on each key method to understand how much computational effort Eve would require to guess the correct key.
Detection of key interception: Finally, we examined whether the method offered a way to detect if a key has been compromised during transmission. This feature is uniquely specific only to the BB84 through its QBER, whereas the classical method has no such mechanism like this.

To validate each of these evaluations we used a comparative key analysis framework, which calculates how secure each key method is based on the size of its keyspace and its breakability to quantum search algorithms.

The keyspace size $N$ was calculated for each cipher:

Caesar Cipher: The Caesar cipher involves 25 possible shifts given a keyspace of $N$ = 25 [5].
Vigenere Cipher: For a fixed key length $L$, each key character can be any of the letters in the alphabet [6]. Therefore the total keyspace is $N = 26^L$. In this study we used $L = 5$, resulting in 881,376.
Columnar Transposition Cipher: The number of possible permutations for a key length $L = 6$ is $N = 6!$ = 720 [6].

***Caesar cipher vs Grover***

When $N = 25$, the search time is 25, with grover it is 5 [4]. Let's explore an example of a ciphertext. Take the text Khoor Zruog, for the attacker using the classical method. It would use each of the 25 s›hifts until it revealed the text Hello World with a key of 3 (shift of 3) [5]. The grover algorithm instead represents all 25 keys at once in quantum state. After this the programmer will define an oracle function $f(k)$ that returns 1 if a key is decrypted and the ciphertext can be decoded into a plaintext. Once the correct key is found the sign is flipped. Once the amplitude increases and the algorithm searches, the key of 3 is found in a time period of 5 [4].

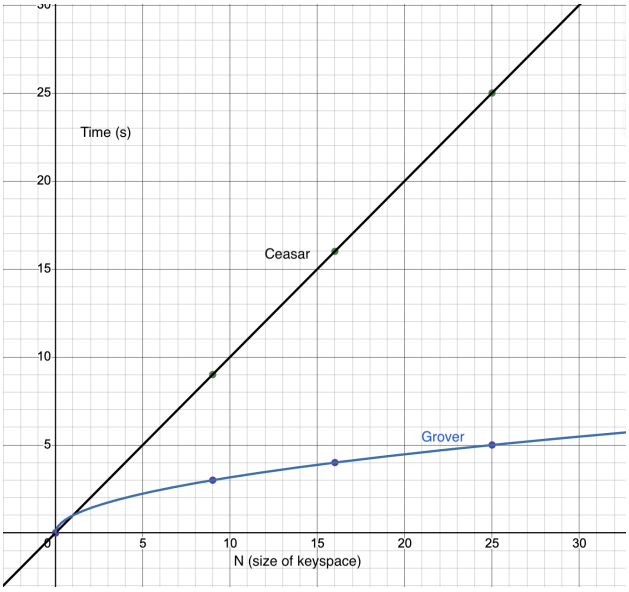


**Figure 1: Comparison of the typical number of steps needed to decipher a message encoded with a Vigenere cipher with a typical classical algorithm vs. Grover's search.**

### *Vigenere cipher vs Grover*

The Vigenere cipher with a fixed key length of 5 and 26 alphabetic possibilities per key character has a key space of 26^5 = 11,881,376. Grover's algorithm, though again, takes the superposition of all 11.8 million possible keys and solves in about 3,447 iterations [4].

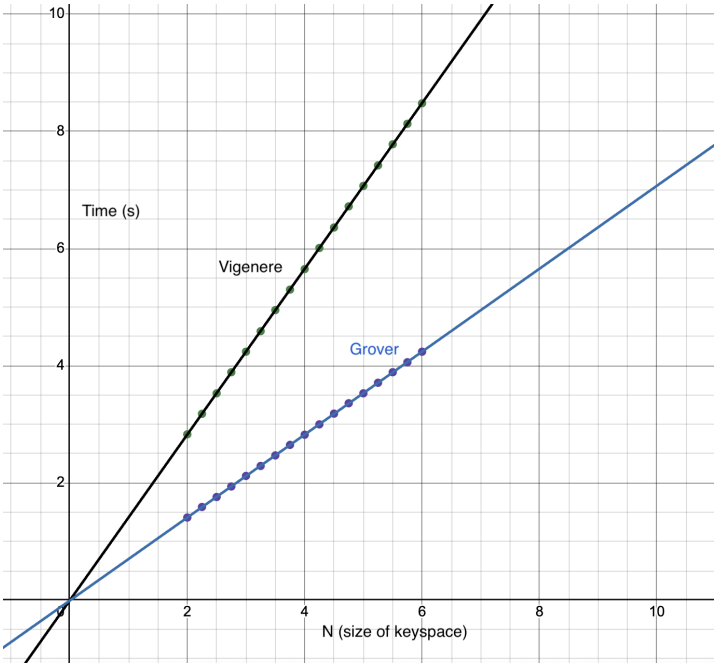


**Figure 2: Comparison of the typical number of steps needed to decipher a message encoded with a Caesar cipher with a typical classical algorithm vs. Grover's search.**

After evaluating the computational vulnerability of these classical ciphers under Grover's strength, it is evident that even minute increases in quantum capability can drastically reduce the time needed to break these systems [4]. While each classical cipher relies on hiding information within large keyspaces, quantum algorithms bypass its only strength on a fundamental level by reducing the time complexity.

However, the BB84 protocol is a demonstration that it is a key distribution method rather than an encryption in itself. Its strength lies not in encoding messages but rather in securely establishing a shared secret key between two parties, without the need to transmit the key through potentially insecure classical channels [1][10]. Because the BB84 protocol relies on the quantum measurement principle and the nocloning theorem [9], any attempt by Eve to measure by use of the Grover's Algorithm disturbs their state. This disturbance is detected by Alice and Bob via the measurement from the QBER, making extraction of the key impossible [10][16]. Nevertheless, once the key is established, it is typically used with a classical symmetric encryption algorithm such as a one-time pad or the Advanced Encryption Standard [2][7]. This means the final encryption is still subject to brute-force attacks. The distinction here is why the BB84 ensures the secure delivery of the key, not the immunity of the key to all future attacks.

To assess this distinction, we designed a test that evaluates the post security of a BB84-generated key. Specifically, we compared the difficulty Eve faces in trying to brute force a key obtained through BB84 with a purely classical key of the same length, while accounting for realistic noise, error correction, and privacy amplification. This Brute Force test captures how BB84 defends not by increasing key length, but by ensuring the attacker begins with virtually zero usable information [17][19].

To illustrate the resilience of the BB84 generated keys under the pressure of brute force guessing, we simulated a standard key exchange transmission and evaluated the number of secure bits that can be extracted and evaluated after accounting for disturbances and imperfections in the system.

Let's assume that Alice and Bob have successfully exchanged a total of:
$n_{raw} = 2,000,000$ qubits (Raw key length)
Quantum Bit Error Rate = 3% (a realistic value observed in fiber-based QKD experiments) [10][17]
Due to random basis mismatches during the transmission, only half the transmitted qubits are able to be used after being sifted:
Basis Sifting Factor: $q = 0.5$
So after sifting, Alice and Bob retain approximately:

$n_{sifted} = q * n_{raw} = 1,000,000$ bits

Errors in the raw key can originate from noise and Eve's interference. To find out how much information Eve gained, we use the binary entropy function.

$h_2(Q) = -Qlog_2(Q) - (1-Q)log_2(1-Q)$

For Q= 0.03

$h_2(0.03) \simeq 0.1906$ ([17])

This means that for every sifted bit, up to 0.1906 bits of information could leak to Eve.

Then using the Shor-Preskill key rate formula, we can calculate the number of truly secure bits remain after accounting for Eve's interferences [16]:

$R = q(1-2h_2(Q))$

After the substitution.

This means that for every raw qubit that was sent between Alice and Bob, only 0.31 bits remained after calculation from Eve's intrusions.

So from 2,000,00 raw qubits:

$n_{key} = R * n_{raw}$ = 0.3094 * 2,000,000 = 618,800 bits

During the comparison, the information must be disclosed to synchronize and match Alice and Bob's keys [22]. The amount of information that is potentially leaked to Eve can be modeled as:

$leak_{ec} = f * n_{sifted} * h_2(Q)$

$f$ is the error correction efficiency factor, typically between 1.05 and 1.2 depending on the protocol's performance. In this case we assume $f$ = 1.1.

$leak_{ec} = 1.1 * 1,000,000 * 0.1906 \simeq$ 209,660 bits [17][19]

This means that Eve can gain information about 210k bits during the comparison period.

To eliminate Eve's potential knowledge, Alice and Bob can perform a function called privacy amplification. This function compresses the key to a shorter length that is provably secure [21]. The final key length is then given by this:

$n_{final} = n_{key} - leak_{ec}$

When substituted, the final key length is then 409,140 bits.

This number means that a classical adversary attacking a 409,140 bit key would face $2^{409,140}$ possible guesses [2][17][19]. A number so large that it is completely impossible to search even with quantum algorithms. While this key length reflects the BB84's strength, it's important to consider that these keys can be compressed using privacy amplification to more real lengths like 128 or 256 bits, which are important for classical encryption techniques. The advantage that

the BB84 has over classical is that Eve gains 0 information about these bits, guaranteeing their security after size reduction.

While brute-force guessing remains an option for an Eve after a properly executed BB84 key exchange, real-world adversaries are more likely to attempt active attacks during transmission to extract information before privacy amplification. To evaluate how these attacks impact the security of BB84, we modeled two common quantum attack strategies: the intercept-resend attack and the no-cloning attack. These simulate scenarios in which an eavesdropper, Eve, attempts to interfere with the quantum states exchanged between Alice and Bob. However, due to the fundamental quantum principle known as the no-cloning theorem, any such interference introduces errors, which are then captured and quantified through the observed QBER [13][14].

In order to analyze how quickly the BB84 protocol detects an intrusion, we can simulate how Alice sends 1,000 qubits encoded randomly in different basis states, and Bob measures those states. Eve's job is to intercept each qubit, measure, and resend it to Bob. But since she doesn't know Alice's basis, she has a 50% chance of choosing the wrong states therein introducing errors (Branciard et al., 2005). When the P(Bob is equivalent to Alice), it represents the probability that Bob used the same basis as Alice when measuring the qubit. Since bases are chosen randomly and independently, the chance of them aligning is 50% or 0.5 [13]:

$$P_{error} = P(wrong\ basis) * P(Bob = Alice) * P(Eve\ disturbs)$$

| % when Intercepted by Eve | % for Expected QBER |
|---|---|
| 0% | 0% |
| 10% | $0.1 * 0.25$ = 2.5% |
| 20% | $0.2 * 0.25$ = 5% |
| 30% | $0.3 * 0.25$ = 7.5% |
| 40% | $0.4 * 0.25$ = 10% |
| 50% | $0.5 * 0.25$ = 12.5% |
| 75% | $0.75 * 0.25$ = 18.75% |
| 100% | $1 * 0.25$ = 25% |

As we can see, the BB84 protocol offers a different test of security, where rather than relying on the computation difficulty of decryption. Studies by Lutkenhaus demonstrate that if Eve intercepts more than 20 to 30% of said message, the resulting QBER reaches detectable errors. Beyond this threshold, detection by the parties are certain, making it impossible for Eve to

intercept 40% or more of the qubits without being noticed. Moreover, Eve would also need to measure and resend the qubits fast enough to avoid introducing further anomalies. Rendering interception impossible for Eve therein strengthening the resilience of the BB84 protocol.

## Conclusion

While the theoretical security of the BB84 protocol has been widely acknowledged since its inception by Bennett and Brassard. However, the transition from theory to widespread practice remains riddled with challenges [14][13]. In controlled laboratory environments, the BB84 consistently demonstrates the theoretic security that surpasses classical cryptographic systems by leveraging the power of quantum mechanics. While integrating quantum components into classical systems is possible, the BB84's dependence on classical feedback loops and lack of entanglement make it vulnerable to implementation weaknesses and quantum attacks especially in noisy environments. This integration introduces unforeseen instability in these domains. More critically, it has revealed limitations in the protocol's function to secure itself against advanced attacks.

One of the most critical yet underexplored barriers in this integration is the BB84's reliance on a prepare and measure feature without the component of entanglement. In the BB84 protocol, Alice has to independently prepare these quantum states, and Bob has to independently choose measurement bases. In the BB84, half of those transmitted qubits have to be discarded during the basis sifting process and error correction [22][23]. While secure in principle, this specific framework amplified sensitivity to imperfections in hardware and classical feedback instabilities. Even small fluctuations in the phase or polarization can harm the entire system [10], and there are no mechanisms to distinguish between natural disturbances and eavesdropping.

By contrast however, entanglement based protocols such as Ekert's E91[8] and measurement device quantum key distribution [12] are able to reveal similarities that are stronger than anything achievable classically. Specifically, these entangled photon pairs guarantee outcome correlations, regardless of their distance between each other, and remove the need for independent state generation and even reduce the need to have harmful feedback systems. In these protocols, their security is also not derived from their disturbance detection ability but also can be verified immediately through the violations of the Bell inequalities, thereby ensuring that the device is verified even in the presence of disturbances [14][15]. Bell's inequalities are conditions that must be satisfied by any theory based on local realism. The idea that particle properties are defined by hidden variables and are resistant to external factors. Quantum systems can violate these inequalities, essentially demonstrating entanglement. In protocols like the E91, these violations show that the entangled quantum states haven't been tampered with. This makes such systems independent, meaning their security comes not from hardware but rather from the quantum states themselves.

This architectural distinction has both pros and cons. The BB84 requires constant basis alignment management – calibration and post-processing. Each step produces new and new opportunities for instability. Studies have shown that entanglement based approaches can also tolerate higher levels of channel noise and loss while still extracting secure keys. The implications is that the entanglement procedure mitigates many of the engineering and security issues that the BB84 struggles with when integrated into classical communication networks [20][19][25].

Thus, the most overlooked area is not simply that BB84 is harder to implement than entanglement based function, but it is that the lack of the entanglement is the chief reason that the BB84 protocol is fundamentally less secure. This lack thereof creates fragile loops and susceptibility to classical issues. It opens and creates possibilities for certain attacks.  This absence specifically causes BB84 to be subject to architecture, where its intrusion detection and error correction rely entirely on classical calibration. This makes BB84 highly vulnerable to quantum non-demolition attacks such as the Photon Number Splitting attack, which exploit multi-photon emissions in weak laser pulses without causing detectable errors. As a result, the protocol's theoretical strengths become its main weakness [25].

Put simply, the gap between BB84's theory and unstable practice is not just a matter of implementation difficulty but rather is rooted in the fundamental architectural limitations of the protocol. Because BB84 does not use entanglement, it relies on classical systems to generate, transmit, and measure states. These specific weaknesses grow more noticeable when transitioning from controlled lab conditions to real networks, where noise and imperfections are impossible to avoid.

In contrast, entanglement-based protocols offer stronger security guarantees, not just architectural resilience. Entangled photons are generated simultaneously and have correlated outcomes regardless of distance, making their security dependent on their correlations. Because these correlations are inherently quantum and cannot be explained by classical physics, they offer a built-in mechanism for validating securities.

These attacks exploit emissions in weak laser pulses without causing  disturbance. In a standard BB84 form, attacks can pass undetected. But in the entanglement version, quantum correlations even in the presence of channel loss.

As quantum systems are gradually integrated into classical networks, maintaining security across channels and disturbances become more challenging. In this way, the BB84's reliance on classical feedback may introduce weaknesses. Entanglement-based protocols offer a more promising approach to supporting secure implementation within more complex infrastructures.

## References

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179). IEEE.
2. Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information (10th anniversary ed.). Cambridge University Press.
3. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172
4. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (pp. 212–219). ACM. https://doi.org/10.1145/237814.237866
5. Singh, S. (2000). The code book: The science of secrecy from ancient Egypt to quantum cryptography. Anchor Books.
6. Kahn, D. (1996). The codebreakers: The comprehensive history of secret communication from ancient times to the Internet. Scribner.
7. Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). Wiley.
8. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661
9. Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802–803. https://doi.org/10.1038/299802a0
10. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301
11. Lo, H.-K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410), 2050–2056. https://doi.org/10.1126/science.283.5410.2050
12. Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503. https://doi.org/10.1103/PhysRevLett.108.130503
13. Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. Physical Review A, 61(5), 052304. https://doi.org/10.1103/PhysRevA.61.052304
14. Branciard, C., Gisin, N., Kraus, B., & Scarani, V. (2005). Security of two quantum cryptography protocols using the same four qubit states. Physical Review A, 72(3), 032301. https://doi.org/10.1103/PhysRevA.72.032301

15. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., … & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502
16. Shor, P., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 85(2), 441–444. https://doi.org/10.1103/PhysRevLett.85.441
17. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145
18. Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. Physical Review Letters, 68(5), 557–559. https://doi.org/10.1103/PhysRevLett.68.557
19. Renner, R. (2008). Security of quantum key distribution. International Journal of Quantum Information, 6(1), 1–127. https://doi.org/10.1142/S0219749908003256
20. Tittel, W., & Weihs, G. (2001). Photonic entanglement for fundamental tests and quantum communication. Quantum Information & Computation, 1(2), 3–56.
21. Bennett, C. H., Brassard, G., Crépeau, C., & Maurer, U. M. (1995). Generalized privacy amplification. IEEE Transactions on Information Theory, 41(6), 1915–1923. https://doi.org/10.1109/18.476316
22. Brassard, G., & Salvail, L. (1994). Secret key reconciliation by public discussion. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 410–423). Springer. https://doi.org/10.1007/3-540-48285-7_35
23. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., & Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. Physical Review A, 54(5), 3824–3851. https://doi.org/10.1103/PhysRevA.54.3824
24. Takesue, H., Nam, S. W., Zhang, Q., Hadfield, R. H., Honjo, T., Tamaki, K., & Yamamoto, Y. (2007). Quantum key distribution over 40-dB channel loss using superconducting single-photon detectors. Nature Photonics, 1(6), 343–348. https://doi.org/10.1038/nphoton.2007.22
25. Sabottke, C. F., Richardson, C. D., & Anisimov, P. M. (2011). Thwarting the photon number splitting attack with entanglement enhanced BB84 quantum key distribution. arXiv. https://arxiv.org/abs/1111.4510