Proceedings of the 4th International Conference on Applied Physics and Mathematical Modeling
DOI: 10.54254/2753-8818/2026.39230

Quantum Key Distribution: A Review of Principles, Protocols, and Practical Challenges

Julia Hu

Harrow International School Hong Kong, Hong Kong, China
0220251112@harrowhongkong.hk

Abstract. The field of quantum communications has experienced unprecedented growth over the last few decades, with progress readily impacting the way information is transferred between parties. This paper reviews the theoretical foundations of Quantum Key Distribution, or QKD, currently the most mature and readily implemented type of quantum communication, including how quantum entanglement is used and specific types of QKD protocols. In particular, three types of discrete-variable protocols are examined: BB84, E91, and BBM92. From the first QKD protocol, BB84, others such as E91 and BBM92 were built, experimenting with the use of Bell's theorem to advance the security of each protocol. The paper further compares how discrete-variable and continuous-variable protocols are affected by noise, discussing how channel loss and decoherence may limit the efficiency of each protocol. Lastly, some speculation on future prospects is made regarding emerging differential-phase-shift protocols and how they can mitigate the problems seen in current protocols.

Keywords: Quantum Key Distribution, E91 protocol, BBM92, BB84

1. Introduction

Classical communication methods utilising encryption are flawed in their security, mostly due to the lack of a mechanism to detect eavesdropping, where an eavesdropper can in theory intercept information which will not be noticed by the parties communicating, and also copy any information without disrupting it. Both of these problems are resolved by the laws of quantum physics used in quantum communications. The no-cloning theorem prevents the eavesdropper from making perfect copies of unknown quantum states, as any attempt to measure the state inevitably disturbs it. Similarly, any interception or tampering with the transmitted quantum state will unavoidably introduce detectable anomalies. As the need for information security increases, quantum communication is becoming integral to countering emerging cyber threats. Quantum key distribution (QKD), which uses quantum principles to develop a secure secret key, is a major part of bringing the theory of quantum communications into practice.

However, few studies have systematically compared the security mechanisms of major QKD protocols or traced how they evolved from one another. This review therefore compares three QKD protocols, BB84, E91, and BBM92, focusing on how each uses quantum properties to detect eavesdropping and what practical problems, such as channel loss and decoherence, they face. It also

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-8818/2026.39230

briefly discusses continuous-variable and twin-field QKD as future directions, focusing on how they improve detection efficiency and extend transmission distance.

2. Principles and theory

2.1. Quantum superposition and qubits

The Superposition principle of quantum mechanics states that a quantum system is not in a particular state but in a linear combination of different states with a probability distribution describing the chances of finding the system in a particular state [1].

A Qubit, the quantum analogue of a classical bit, is a two-level quantum system whose general state can be written as [2]

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where α and β are complex numbers satisfying

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

When measuring the state of a qubit, this superposition collapses into a classical state of either 0 or 1, with their respective probabilities being $|\alpha|^2$ and $|\beta|^2$. This unavoidable collapse upon measurement is what makes eavesdropping detectable in QKD protocols.

2.2. Quantum entanglement

2.2.1. EPR paradox and Bell's theorem

In their 1935 paper, Einstein, Podolsky and Rosen (EPR) questioned the completeness of quantum mechanics [3]. Their thought experiment involved two particles that had interacted and then become spatially separated. The particles must spin in opposite directions, even though before measurement they are in a superposition of all possible spins. If the particles have opposite spins after measurement, there must have been some communication between them. But if the particles are far enough apart, the information would have to travel faster than light, violating locality. The EPR paper therefore concludes that there must be a local hidden variable that predetermines the spins, rather than the measurements affecting each other.

Bell proved in 1964 that this paradox is incorrect: quantum mechanical predictions contradict EPR's local hidden variable theory [4]. This review uses Mermin's simplified version [5, 6]. For three measurement axes, the probability that measurements along two axes give the same result must satisfy:

$$P(S_1, S_2) \leq P(S_1, S_3) + P(S_3, S_2). \tag{3}$$

where $P(Si, Sj)$ is the probability that the measurements along axes i and j give the same result. This is Bell's inequality.

Quantum mechanics, however, predicts a different result. For an entangled singlet state, the probability of opposite outcomes when the measurement axes are separated by an angle θ is $\sin^2(\theta/2)$. With suitable choices of axes, one obtains $3/4 \nleq 1/4 + 1/4$, a clear violation of Bell's

DOI: 10.54254/2753-8818/2026.39230

inequality [7, 8]. In 1980, 1981 and 1982 Alain Aspect and colleagues conducted real life experiments that further proved Bell's findings [9, 10].

This non-local correlation is the defining feature of quantum entanglement [11]: a set of particles whose states cannot be described independently. This property has enabled significant advances in quantum communication, which the following subsection discusses.

2.2.2. Uses in quantum communication

Violation of Bell's inequalities reveals two fundamental characteristics upon which quantum communication systems are built [12].

The first is the no-cloning theorem. Originally rooted in Park's no-go theorem, the modern formulation states that an unknown quantum state cannot be perfectly copied. This is because any attempt to measure the state inevitably disturbs it, collapsing the superposition and yielding only classical information. In quantum communication, the two legitimate parties can compare a subset of their measurement results over a public channel to estimate the error rate. If an eavesdropper tries to duplicate the transmitted quantum states, the disturbance causes the actual error rate to deviate from the expected value, exposing the eavesdropper without providing any useful information.

The second characteristic, which follows from the first, is inherent eavesdropping detection: because any interaction with the quantum channel alters the states, the legitimate users can test the security of the system at any time, and if tampering is detected, they discard the compromised key to ensure the final secret key remains secure.

3. Applications in communication

3.1. Quantum key distribution

The most widely implemented method of quantum communication at present is quantum key distribution (QKD). Its main purpose is to establish a shared secret key between two parties, Alice and Bob, while preventing a potential eavesdropper, Eve, from learning the key. Alice and Bob can then use this key for encryption and authentication in later exchanges, so that Eve cannot read their encrypted messages or impersonate one of them.

The security of QKD comes from the properties of qubits discussed earlier. Because information is encoded in quantum states, an eavesdropper cannot measure or copy these states without disturbing them. If Eve attempts to measure a qubit, the disturbance can be detected by Alice and Bob when they compare part of their measurement results over the classical channel. They can then estimate the error rate and decide whether the key is secure. This differs from classical key distribution, where key leakage may be difficult to detect.

In a typical QKD scheme, Alice and Bob communicate over two channels: a quantum channel and a classical channel. Eve is assumed to be able to listen in on the classical channel and interact with the quantum channel, but the laws of quantum mechanics prevent her from doing so without leaving a detectable trace. In the prepare-and-measure approach, Alice first chooses a sequence of symbols $s_1, s_2, \ldots, s_n$ and prepares the corresponding quantum state.

$S_n = \{s_1, s_2, \ldots, s_n\}$ which is the tensor product of the states of all the individual symbols. She then sends $|\psi(S_n)\rangle$ to Bob over the quantum channel, and Bob measures the state upon receipt; this is known as the prepare-and-measure scheme.

DOI: 10.54254/2753-8818/2026.39230

3.2. Security of QKD

The security of QKD relies on the fact that any attempt by Eve to gain information about the transmitted quantum states will disturb them. Because these states are fragile, measurement or copying leaves detectable traces that Alice and Bob can identify when they compare part of their measurement results. If such traces are found, they discard the key and run the protocol again until they are confident that Eve has not obtained useful information. The no-cloning theorem also prevents Eve from making perfect copies of unknown quantum states, since any attempt to copy or measure the state inevitably disturbs it and can be detected [13].

QKD can provide unconditional security, or information-theoretic security, in the sense that no restriction is placed on Eve's computational power. She may listen to all classical communication and interact with the quantum channel, but the laws of physics limit the information she can obtain. However, this security depends on Alice and Bob being able to authenticate the classical channel. Without authentication, Eve could launch a man-in-the-middle attack and compromise the system. In practice, Alice and Bob often use a short pre-shared secret key for authentication, while QKD generates a longer secret key.

In many prepare-and-measure QKD protocols, unconditional security requires the states to be non-orthogonal ($\langle\psi\phi\rangle \neq 0$). In other words, the states must have some overlap and cannot be perfectly distinguished in a single measurement. This prevents Eve from copying Alice's photons without being detected, which would otherwise compromise the whole system.

3.3. Types of QKD protocols

There are currently three main types of QKD protocols: discrete-variable (DV), continuous-variable (CV), and distributed-phase-reference (DPR). DV protocols were the first to be devised and remain the most widely used. They usually use photons as information carriers and photon counting as the detection method. However, photon counting is relatively inefficient because of dark counts, which are detector clicks caused by noise rather than incoming photons, and long dead time, which is the time required to reset the detector after each count.

These limitations led to CV protocols, which use homodyne detection instead. Homodyne detection measures the quadrature components of the light field: a weak signal interferes with a strong local oscillator, and the photocurrent reveals the amplitude or phase quadrature. This method can achieve higher repetition rates than photon counting because it is not limited by dead time, but it produces noisier measurements. The noise comes mainly from intrinsic vacuum noise, excess noise from detector electronics, and transmission noise. The key trade-off is that DV protocols typically produce a key with a lower error rate at a slower rate, while CV protocols can generate keys faster but with more noise, requiring error correction and privacy amplification.

DPR protocols were developed with practicality as the primary goal. They use photon counting, as in DV protocols, but also monitor the quantum channel by exploiting the coherence of light pulses. This additional feature places them in a separate category.

3.4. BB84 protocol

This protocol, and the ones that follow, are all discrete-variable protocols. BB84 is the first QKD protocol and often the simplest method [14].

Alice prepares a sequence of single photons, or weak coherent pulses with a very low mean photon number, each encoded in its polarisation state. Both parties can measure the polarisation of

DOI: 10.54254/2753-8818/2026.39230

the photons in two bases: the horizontal/vertical basis, or the +45/-45 basis. These polarisations code for bits as follows:

$$|\mathrm{H}\rangle \quad \text{for } 0_{+}$$

$$|\mathrm{V}\rangle \quad \text{for } 1_{+}$$

$$|+45\rangle \text{ for } 0_{\times}$$

$$|-45\rangle \text{ for } 1_{\times}$$

It can be seen that these states are non-orthogonal, as $|\pm 45\rangle = \frac{1}{\sqrt{2}}\left(|\mathrm{H}\right\rangle \pm |\mathrm{V}\left\rangle\right)$.

Alice and Bob then repeat a process. Alice prepares a photon in one of the four polarisation states, chosen at random, and sends it to Bob through the quantum channel. Bob receives it and measures it in either the H/V or the diagonal basis, also chosen at random. After transmission, Alice and Bob use the classical channel to reveal only which basis each used for each photon, and they discard the bits for which their bases differed. Statistically, this leaves them with roughly half the original bits, forming the raw key. They then select a random sample of the raw key and compare it publicly. This sample is used to estimate the error rate and is then discarded. If Eve did not measure the photons, the error rate should remain close to the expected background level. If errors are found, Alice and Bob perform error correction and privacy amplification in post-processing. At the end of this process, they are left with either a secret key of length determined by the error rate, or no key if the raw key has been fully compromised.

3.5. E91 protocol

This protocol was developed by Ekert in 1991 and is groundbreaking for being the first to use quantum entanglement and Bell's theorem to detect eavesdropping [15]. A source emits a pair of entangled photons in the singlet state, meaning their measurement outcomes are perfectly anti-correlated when measured along the same axis. One photon is sent to Alice and the other to Bob. Once received, Alice and Bob independently measure the spin of their photons along an axis of their choice: [axis 1] and [axis 2], where both are unit vectors and [condition]. Each measurement can yield results +1 or −1 depending on the spin of the photons. Once measured, the inherent spin of the entangled photons would be exactly opposite, but depending on the orientation on which Alice and Bob measure, they could yield a series of different results. The orientations [ ] and [ ], [ ] and [ ] are in the same orientation. For these measurements, the correlation coefficient between a given set of measurements is defined as

$$\mathrm{E}(\mathrm{a_i}, \mathrm{b_j}) = \mathrm{P_{++}}(\mathrm{a_i}, \mathrm{b_j}) + \mathrm{P_{--}}(\mathrm{a_i}, \mathrm{b_j}) - \mathrm{P_{+-}}(\mathrm{a_i}, \mathrm{b_j}) - \mathrm{P_{-+}}(\mathrm{a_i}, \mathrm{b_j}) \tag{4}$$

DOI: 10.54254/2753-8818/2026.39230

where $P_{\pm\pm}(a_i, b_j)$ is the probability that ± 1 was obtained along both a_i and b_j. Using the rules of quantum mechanics, it is expected that

$$E(a_i, b_j) = -a_i \bullet b_j \tag{5}$$

Similarly, the Bell parameter S, defined as

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \tag{6}$$

can be expected to return a value to $S = -2\sqrt{2}$. Note here that the coefficients used in the calculation of S are those where Alice and Bob have chosen different orientations for their measurements.

After a sufficient number of measurements, Alice and Bob communicate over a public channel to compare the axes they used. They first discard events where either detector failed to register a photon. The measurements where they chose different orientations are used to evaluate S, If $S = -2\sqrt{2}$; the channel is considered secure; if S falls within the classical bound [-2, 2] eavesdropping is indicated. The measurements where they used the same orientations yield perfectly anti-correlated results and form the raw key.

Any attempt by Eve to intercept the photons or insert her own data will disturb the quantum correlations and cause S to deviate from $-2\sqrt{2}$. If S falls within [-2, 2], it implies that an eavesdropper has introduced elements of physical reality into the system. All measurements from this round would then be aborted and Alice and Bob will start a new round of measurements until they are confident that S is within the expected range and that no eavesdropper has interfered with the process.

3.6. BBM92 protocol

This protocol, developed a year after E91, builds on Ekert's protocol to prove that the principles of the E91 protocol can be used even without the aid of Bell's theorem [16]. The authors argue that the main worry for the two legitimate parties, Alice and Bob, is not that the eavesdropper, Eve, might obtain any useful information by listening in to their conversations, but instead that Eve will be able to obtain a source that can somehow produce three entangled photons and use this to stand in place of the original source, therefore being able to replicate their secret key by taking measurements on the photons in the orientations Alice and Bob agree to in their public channel. The authors prove that this is not possible, and using that, they create an enhanced version of their previous protocol BB84, which does not use Bell's theorem.

First, Eve needs to set up two EPR particles, to be sent to Alice and Bob in place of their intended EPR source, such that they interact with her own system so as to allow her to measure their spins as well. The particles will need to have a general state of

$$|\Psi\rangle = |\uparrow\uparrow\rangle |A\rangle + |\downarrow\downarrow\rangle |B\rangle + |\uparrow\downarrow\rangle |C\rangle + |\downarrow\uparrow\rangle |D\rangle \tag{7}$$

where $|\uparrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$, $|\uparrow\downarrow\rangle$, and $|\downarrow\uparrow\rangle$ are all the possible combinations of spin states sent to Alice and Bob, and $|A\rangle, |B\rangle, |C\rangle$, $|D\rangle$ are the states Eve chooses for her system, which will be based on Alice and Bob's choices, provided through their conversation in the public channel. If she is not to be detected, Eve's measurements must be anti-correlated to Alice and Bob's when they measure along the same axis, since the photons are in the singlet state, making the only state available to her

DOI: 10.54254/2753-8818/2026.39230

$$|\Psi\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)\,|C\rangle \tag{8}$$

Therefore, Eve's system must be entirely uncorrelated with the EPR particles sent to Alice and Bob.

As in E91, Alice and Bob randomly measure along the x or z axis, publicly compare axes, discard mismatches, and keep same-axis anti-correlated events as the raw key. They estimate the error rate from a subset, then perform error correction and privacy amplification if the rate is below threshold. Unlike E91, BBM92 needs no Bell parameter evaluation; it is an entanglement-based version of BB84.

4. Challenges of current models and protocols

4.1. Channel loss

Both discrete-variable (DV) and continuous-variable (CV) protocols experience channel loss, though CV protocols are generally more sensitive to excess noise. A major contributor is the intensity of the quantum signals, which cannot be increased arbitrarily without compromising security. If the detector is unable to detect the particle, no measurement can be performed. Other factors include mechanical issues, absorption of the signal by channel material, and Rayleigh scattering, where the channel material causes the particle to scatter in random directions, leading to loss of information. As a result, during most applications of protocols, the first step the two parties undertake after the measurement of the states of quantum particles is to discard data where either one or both of them did not detect a particle. This results in a significant waste of resources, including energy, material, and financial input.

4.2. Decoherence and noisy environments

Decoherence occurs when a qubit interacts with its environment, altering the particle and causing information loss [17]. Much of this can be caused by a noisy environment, leading to two types of decoherence: amplitude damping, where energy is lost, and phase damping, where information is lost without energy loss. Amplitude damping is usually caused by the channel material absorbing the qubit, whereas phase damping can result from factors such as random scattering and disruption of electrical charges. This wastes resources because more qubits are needed to produce a secure bit. All channel media suffer from some level of noise, though some more than others. The most accessible and frequently used optical fibres are prone to unwanted interactions with particles, and optical attenuation causes signals to weaken as fibre length increases. Free-space optics are often used in space and are therefore susceptible to atmospheric attenuation with a similar effect; satellite-based FSO was developed as a better alternative. While it is less prone to decoherence and noise than the previous two, it still suffers from some attenuation and turbulence.

4.3. Future prospects

Continuous-variable and differential-phase-shift protocols were developed quite recently, with one well-known continuous-variable protocol, S09, being proposed in 2009 [18]. As mentioned above, continuous-variable protocols were developed to make up for the inefficiency of detection in most discrete-variable protocols, and utilise homodyne detection as a more efficient detection method. Differential-phase-shift protocols first appeared in the early 2000s, and were developed for ease of operation by the two communicating parties in real-life applications. With similarly secure proofs,

DOI: 10.54254/2753-8818/2026.39230

DPS protocols were developed by experimental groups rather than theorists, with the practicality of their procedures in mind [17].

As the need for quantum communication channels increases, a solution to the problem of distance becomes crucial. Conventional QKD protocols are limited by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [19], where for a certain channel transmittance η, the secret key rate R is bounded by

$$R \leq -log_2(1-\eta) \tag{9}$$

without quantum repeaters in between, due to various hardware issues such as thermodynamics and degradation. This created a need for another type of protocol that can exceed this bound, which resulted in twin-field QKD (TF-QKD) [20]. This technique changes the key rate scaling, the decrease in key generation rate with increasing distance, by having Alice and Bob send pulses to an intermediate node, which performs the measurements. This changes the channel transmittance to $\sqrt{\eta}$, increasing the allowed channel length up to 1000 km using normal optical fibre [21]. This points towards a potential quantum internet in the future.

5. Conclusion

Through a comparison of the BB84, E91, and BBM92 protocols, this paper traces the eavesdropping detection mechanisms used in QKD, from non-orthogonal states to non-local entanglement. BB84 provides the simplest approach, E91 introduces entanglement and Bell's theorem, and BBM92 shows that entanglement alone can maintain eavesdropping detection without Bell's theorem. These protocols reflect the gradual development and enhancement of security in QKD.

This paper mostly compares BB84, E91, and BBM92. It does not attempt a complete survey of QKD, nor does it cover experimental implementations or full security proofs. Continuous-variable, differential-phase-shift, and twin-field QKD are left for future work, particularly for improving detection efficiency and transmission distance.

References

[1] The superposition principle. (2024a, February 8). *Physics LibreTexts*. https://phys.libretexts.org/Workbench/Quantum_Mechanics_and_Quantum_Computation_(Vazorani)/01%3A_Introduction/1.03%3A_The_Superposition_Principle

[2] Qubits. (2024b, February 8). *Physics LibreTexts*. https://phys.libretexts.org/Workbench/Quantum_Mechanics_and_Quantum_Computation_(Vazorani)/01%3A_Introduction/1.07%3A_Qubits

[3] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review, 47*(10), 777–780.

[4] Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika, 1*(3), 195–200.

[5] Mermin, N. D. (1981). Bringing home the atomic world: Quantum mysteries for anybody. *American Journal of Physics, 49*(10), 940–943.

[6] 12: A quantum paradox and the experiments. (2021, September 23). *Physics LibreTexts*. https://phys.libretexts.org/Bookshelves/Quantum_Mechanics/Introduction_to_the_Physics_of_Atoms_Molecules_and_Photons_(Benedict)/01%3A_Chapters/12%3A_A_quantum_paradox_and_the_experiments

[7] Chong, Y. D. (2021, April 16). 3.3: The Einstein-Podolsky-Rosen "paradox." *Physics LibreTexts*. https://phys.libretexts.org/Bookshelves/Quantum_Mechanics/Quantum_Mechanics_III_(Chong)/03%3A_Quantum_Entanglement/3.03%3A_The_Einstein-Podolsky-Rosen_Paradox

[8] Chong, Y. D. (2021b, May 1). 3.4: Bell's theorem. *Physics LibreText*. https://phys.libretexts.org/Bookshelves/Quantum_Mechanics/Quantum_Mechanics_III_(Chong)/03%3A_Quantum

DOI: 10.54254/2753-8818/2026.39230

_Entanglement/3.04%3A_Bell's_Theorem
[9] Aspect, A., Grangier, P., & Roger, G. (1981). Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters, 47*(7), 460.
[10] Aspect, A., Grangier, P., & Roger, G. (1982). Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities. *Physical Review Letters, 49*(2), 91.
[11] Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Rev. Mod. Phys., 81*, 865–942. https://doi.org/10.1103/RevModPhys.81.865
[12] Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., Peev, M., & Scarani, V. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301
[13] Wootters, W., & Zurek, W. (1982). A single quantum cannot be cloned. *Nature, 299*, 802–803. https://doi.org/10.1038/299802a0
[14] 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). Bangalore, India.
[15] 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
[16] Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. *Physical Review Letters, 68*(5), 557.
[17] Khan, M. A., Ghafoor, S., Zaidi, S. M. H., Khan, H., & Ahmad, A. (2024). From quantum communication fundamentals to decoherence mitigation strategies: Addressing global quantum network challenges and projected applications. *Heliyon, 10*, e34331.
[18] Pirandola, S., Laurenza, R., Ottaviani, C., et al. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications, 8*, 15043.
[19] Giles, M. (2019, February 14). Explainer: What is quantum communication? *MIT Technology Review*. https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/
[20] Lucamarini, M., Yuan, Z. L., Dynes, J. F. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature, 557*, 400–403 (2018).
[21] Liu, Y., Zhang, W.-J., Jiang, C., Chen, J.-P., Zhang, C., Pan, W.-X., Ma, Di, Dong, H., Xiong, J.-M., Zhang, C.-J., Li, H., Wang, R.-C., Wu, J., Chen, T.-Y., You, L., Wang, X.-B., Zhang, Q., & Pan, J.-W. (2023). Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett., 130*, 210801.