IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 September 2022, accepted 3 October 2022, date of publication 6 October 2022, date of current version 14 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3212787

RESEARCH ARTICLE

QKeyShield: A Practical Receiver-Device-Independent Entanglement-Swapping-Based Quantum Key Distribution

MOHAMMED Y. AL-DARWBI[1], **ALI A. GHORBANI**[1], **(Senior Member, IEEE), AND ARASH HABIBI LASHKARI**[2], **(Senior Member, IEEE)**

[1]Faculty of Computer Science, Canadian Institute for Cybersecurity, University of New Brunswick, Fredericton, BN E3B 5A3, Canada
[2]School of Information Technology, York University, Toronto, ON M3J 1P3, Canada

Corresponding author: Mohammed Y. Al-Darwbi (m.aldarowbi@gmail.com)

This work was supported in part by the Canadian Institute for Cybersecurity (CIC), and in part by NSERC Tier 1 Canada Research Chair.

ABSTRACT Quantum key distribution, in principle, provides information-theoretic security based on the laws of quantum mechanics. Entanglement swapping offers a unique ability to create entanglement between qubits that have not previously interacted. Entanglement-swapping setup helps in building a side-channel-free Quantum key distribution. A receiver-device-independent quantum key distribution protocol based on this idea, QKeyShield, is proposed. It adopts the use of a biased operator choice, thus, increasing the rate of generated bits. Several measures have been integrated to protect the sent qubits. Furthermore, security analyses for a list of attacks allowed by quantum mechanics are provided showing that QKeyShield can securely and effectively allow Alice and Bob to agree on a secret key. QKeyShield has certain advantages over earlier protocols including the ability to achieve high usage efficiency and the potential of enabling conference quantum key distribution.

INDEX TERMS Quantum cryptography, quantum key distribution, entanglement, entanglement swapping, DI-QKD, MDI-QKD, 1SDI-QKD, RDI-QKD.

I. INTRODUCTION

While encryption is effective at securing data, the security of the mystery or private cryptographic key is crucial. Any strong encryption technique would be jeopardized by poor key management [1]. In this sense, the encryption technique's effectiveness is dependent on the key's security, which is difficult to ensure using traditional key distribution. A quantum computer can quickly break any key distribution based on integer factoring and discrete logarithms, including ECC, RSA, and other variations of these ciphers [2]. To generate the shared key, Quantum Key Distribution (QKD) can be used instead of asymmetric key agreement techniques. QKD is based on the quantum principles of physics rather than the presumed computational difficulty of mathematical problems. QKD is the most successful application of quantum computing, which allows two legitimate parties, Alice and Bob, to agree on a secret key across a great distance in a format incomprehensible to an eavesdropper. The first QKD protocol was proposed in 1984, describing a protocol that would come to be known as BB84 [3]. BB84 necessitates measurements on two orthogonal basis. For example, bit values can then be assigned as Zero (0) for a vertically polarized photon and One (1) for a horizontally polarized photon. Alice and Bob can detect the presence of an eavesdropper by publicly comparing obtained bits for which they chose the same basis. Artur Ekert proposed an entanglement-based variant of quantum key distribution in 1991, known as the E91 protocol [4]. In the entanglement-based scheme, Alice (Bob) obtains the information by measuring half of a maximally entangled state. In the E91 original protocol, Alice(Bob) would measure polarization along with three different angles. Again, Alice and Bob publicly announce the angular orientations they used for each instance. When Alice and Bob use the same angular orientations, the measurement results will be the raw key. The results obtained using different angular orientations would

The associate editor coordinating the review of this manuscript and approving it for publication was Siddhartha Bhattacharyya.

be publicly announced and used to detect the presence of eavesdroppers. The first direct consequence of using entangled qubits is the provision of fully random bits to both parties where the qubits are correlated with each other (ideally with maximally entangled two-qubit states). Entanglement-based schemes also have the advantage of not requiring a random number generator. As a result, entanglement-based quantum key distribution offers a lot of promise for practical use. Entanglement also alleviates security problems associated with single photon-based key distribution methods. Thus, quantum entanglement's use for quantum key distribution is a hot topic in modern quantum cryptography research.

Entanglement swapping (ES), one of the properties of quantum entanglement, can entangle two quantum systems that do not interact with one another. Entanglement-swapping helps in building a side-channel-free QKD [5], [6] Several experimental studies have been conducted to investigate the ES phenomenon with discrete variables [7], [8] and continuous variables [9], or even with a hybrid approach [10]. For example, the achieved fidelity by the authors of [7] is 84.9 ± 3.6% which infers the violation of the CHSH Bell inequality by more than two standard deviations. Similarly, the swapped state of [10] violates the CHSH Bell inequality by more than 4 standard deviations, and they concluded that the obtained entangled states could be directly used for QKD. ES is used in several QKD protocols such as [11], [12], [13], and [14], where the fact that both Alice and Bob must select randomly between two potential measurements ensures the security of these protocols. Conversely, several entanglement-swapping-based protocols that do not require alternative measurements have been proposed in the literature, first appearing in Cabello's work [15]. Researchers have tried to minimizes the required number of detectors, which are by far the most expensive components in QKD according to NIST [16]. Alternative measurements require three beamsplitters and four detectors per user. QKD protocols that do need alternative measurements can perform the measurement on a single basis which requires only two detectors and one polarization beamsplitter. Schemes that do not require alternative measurements use Hadamard gate - one of the least cost-efficient gates [17]- to provide the required randomization that helps in detecting eavesdroppers. Although QKD protocols can offer secure key distribution, the system's detectors are neither entirely trusted nor guarded. Currently, the majority of quantum hacking methods make use of the receiver's detectors [18]. Device-independent-QKD (DI-QKD) is the most optimistic scenario for closing security holes as no assumptions need to be made regarding the system's devices [19]. Another family of protocols is MDI-QKD, where only the measurement devices are not characterized [20]. The situation where the source and one of the parties are not trusted have been considered in [21] and [22]. Other recent studies consider the situation where only the receiver's device is not trusted, called receiver-device-independent-QKD (RDI-QKD) [23], [24]. Moving to the RDI-QKD scenario can be advantageous for situations where Bob's devices are placed in an unmonitored environment.

In this work, we propose an entanglement-swapping-based RDI-QKD scheme. The main contribution of QKeyShield is fivefold: 1) it minimizes the attack surface and maximizes efficiency by reducing the number of transmitted qubits to one and the number of classical messages to zero per each expected secret bit; 2) it employs a biased probability on performing either Hadamard or identity operators on the shared-state's qubits which assures the protocol's security and efficiency; 3) it is information carrier qubits are kept secret, which filters out several attacks such as the intercept-resend attack, measure-resend attack, and detector blinding attack; 4) it balances several efficiency metrics while achieving a high key rate; and 5) it has the potential to be used as an unconditionally secure conference (multiparty) QKD scheme.

II. PRELIMINARIES

Before presenting the related works and the QKeyShield protocol, let us introduce the quantum states and quantum operations, and illustrate the property of the quantum entanglement swapping, which will be used later. A state of two maximally entangled qubits, the simplest form of entanglement, is called Bell state, and a state of three or more maximally entangled states is called Greenberger–Horne–Zeilinger (GHZ) state. The following are known as the Bell basis in the computational basis $\{|0\rangle, |1\rangle\}$ and Hadamard basis $\{|+\rangle, |-\rangle\}$ [12]:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle \pm |{-}{-}\rangle) \\ |\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle \pm |{-}{+}\rangle) \end{aligned} \tag{1}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Similar to Bell state, let us define the eight GHZ basis for three qubits,

$$\begin{aligned} |P^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \\ |Q^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \\ |R^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \\ |S^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle). \end{aligned} \tag{2}$$

A. QUANTUM OPERATION

Given a known quantum state, it is possible to transform it into any other state, and the mathematical representation is known as a quantum operation. The following are some popular quantum operations:

$$\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{3}$$

where $\mathbb{I}$, X, Y, and Z are called the Pauli operators, and H is called the Hadamard operator. $\mathbb{I}$ is the identity operator that keeps the state intact. The operators X, Y, and Z, respectively, rotate (flip) around the x, y, and z axes of the Bloch sphere by π radians, so $X|1\rangle = |0\rangle$, $Z|+\rangle = |-\rangle$, and $H|1\rangle = |-\rangle$. Unlike many classical and quantum operators, Pauli operators are self-inverse (Hermitian), meaning $H^{\otimes 2} = I$. Similarly, these operations could be applied to states with more than one qubit like any of the entangled state $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$. These states can be an entangled state on the computational basis or Hadamard basis as shown in Equation (1). To illustrate, let us assume that $|\phi_Z^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the Bell state on the computational basis and $|\phi_X^+\rangle = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$ is the Bell state on the Hadamard basis. Thus, Hadamard operator could be applied to transform the entangled state between the X and Z basis, $H|\phi_Z^+\rangle = |\phi_X^+\rangle$, $H|\phi_Z^-\rangle = |\phi_X^-\rangle$, $H^{\otimes 2}|\phi_X^+\rangle = |\phi_X^+ e\rangle$.

All the measurements in this work are done on the computational basis (Z). As per Equation (1), $|\phi^{\pm}\rangle = |\phi_Z^{\pm}\rangle = |\phi_X^{\pm}\rangle$ and $|\psi^{\pm}\rangle = |\psi_Z^{\pm}\rangle = |\psi_X^{\pm}\rangle$, the subscripts (Z, X) are dropped to represent a Bell state independently of the base $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$.

Such a quantum operation could be applied to one qubit of the entangled state but not to the other, creating its dual state [25]. If we apply a Hadamard operation on the first qubit, we get the dual states $\{|W^{\pm}\rangle, |X^{\pm}\rangle\}$. Likewise, when we perform a Hadamard operation on the second qubit, we get the dual states $\{|K^{\pm}\rangle, |D^{\pm}\rangle\}$. To illustrate, let us assume the Hadamard operation, $H^{(1)}$, is applied to the first qubit (indicated by the superscripts (1)) of the entangled state $|\phi^+\rangle$,

$$\begin{aligned} H^{(1)}|\phi^+\rangle &= \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = |W^+\rangle. \end{aligned} \tag{4}$$

The following are the possible states of performing a Hadamard operation on one of the state's qubits,

$$\begin{aligned} H^{(1)}\left|\phi^{\pm}\right\rangle &= |W^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\phi^{\mp}\rangle \pm |\psi^{\pm}\rangle), \\ H^{(1)}\left|\psi^{\pm}\right\rangle &= |X^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\psi^{\mp}\rangle \pm |\phi^{\pm}\rangle), \\ H^{(2)}\left|\phi^{\pm}\right\rangle &= |K^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\phi^{\mp}\rangle + |\psi^{\pm}\rangle), \\ H^{(2)}\left|\psi^{\pm}\right\rangle &= |D^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\phi^{\pm}\rangle - |\psi^{\mp}\rangle). \end{aligned} \tag{5}$$

Equation (5) shows the obtained dual states when performing the Hadamard operation on one of the state's qubits. Performing another Hadamard operation on any of the qubits transforms the dual state back into the original Bell states,

$$\begin{aligned} H^{(1)}|W^{\pm}\rangle &= |\phi^{\pm}\rangle, \quad & H^{(2)}|W^{\pm}\rangle &= |\phi^{\pm}\rangle, \\ H^{(1)}|X^{\pm}\rangle &= |\psi^{\pm}\rangle, \quad & H^{(2)}|X^{\pm}\rangle &= |\psi^{\pm}\rangle, \\ H^{(1)}|K^{\pm}\rangle &= |\phi^{\pm}\rangle, \quad & H^{(2)}|K^{\pm}\rangle &= |\phi^{\pm}\rangle, \\ H^{(1)}|D^{\pm}\rangle &= |\psi^{\pm}\rangle, \quad & H^{(2)}|D^{\pm}\rangle &= |\psi^{\pm}\rangle. \end{aligned} \tag{6}$$

Given an entangled state between Alice and Bob $|\phi^+\rangle_{AB}$, Alice and Bob can perform a local Hadamard operation on her/his qubit which affects the entangled qubits' correlation. If the Hadamard operation is performed on both of the qubits by Alice and Bob, the state $H^{(1)}H^{(2)}|\phi^+\rangle_{AB} = |\phi^+\rangle_{AB}$ will stay intact.

B. QUANTUM CORRELATION PROPERTY

Entanglement Swapping (ES) is a technique that allows two quantum systems that do not interact directly to become entangled. The beauty of entanglement swapping can be summarized in the idea of having entangled qubits that have never interacted in the past. Let us start by briefly reviewing how this ES-based protocol works. Let us assume that the initial state of the two states are on similar basis (computational basis Z), $|\phi^+\rangle_{12} = |\phi^+\rangle_{34} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; thus, the quantum state of the whole system containing the qubits 1, 2, 3 and 4 can be written as:

$$\begin{aligned} |\Psi\rangle_{1234} &= |\phi^+\rangle_{12} \otimes |\phi^+\rangle_{34} \\ &= \frac{1}{2}(|00\rangle_{12} + |11\rangle_{12}) \otimes (|00\rangle_{34} + |11\rangle_{34}) \\ &= \frac{1}{2}(|0000\rangle_{1234} + |0011\rangle_{1234} + |1100\rangle_{1234} \\ &\quad + |1111\rangle_{1234}). \end{aligned} \tag{7}$$

If we measure the qubits 1, 3 and 2, 4 in the Bell basis, respectively, their measurement outcomes are as follows,

$$\begin{aligned} &|\Psi\rangle_{1324} \\ &= \frac{1}{2}\Big(|0000\rangle_{1324} + |0101\rangle_{1324} + |1010\rangle_{1324} \\ &\qquad + |1111\rangle_{1324}\Big), \\ &= \frac{1}{2}\Big(|00\rangle_{13}|00\rangle_{24} + |01\rangle_{13}|01\rangle_{24} + |10\rangle_{13}|10\rangle_{24} \\ &\qquad + |11\rangle_{13}|11\rangle_{24}\Big), \\ &= \frac{1}{2\sqrt{2}}\Big[(|\phi^+\rangle + |\phi^-\rangle)_{13}|00\rangle_{24} + (|\psi^+\rangle \\ &\qquad + |\psi^-\rangle)_{13}|01\rangle_{24} + (|\psi^+\rangle + |\psi^-\rangle)_{13}|10\rangle_{24} \\ &\qquad + (|\phi^+\rangle + |\phi^-\rangle)_{13}|11\rangle_{24}\Big], \\ &= \frac{1}{2\sqrt{2}}\Big[|\phi^+\rangle_{13}|00\rangle_{24} + |\phi^-\rangle_{13}|00\rangle_{24} \\ &\qquad + |\psi^+\rangle_{13}|01\rangle_{24} + |\psi^-\rangle_{13}|01\rangle_{24} + |\psi^+\rangle_{13}|10\rangle_{24} \\ &\qquad + |\psi^-\rangle_{13}|10\rangle_{24} + |\phi^+\rangle_{13}|11\rangle_{24} + |\phi^-\rangle_{13}|11\rangle_{24}\Big]. \end{aligned} \tag{8}$$

Algebraic manipulation can simplify the expression for Equation (8), which becomes

$$|\Psi\rangle_{1324} = \frac{1}{2}\Big(|\phi^+\rangle_{13}\,|\phi^+\rangle_{24} + |\phi^-\rangle_{13}\,|\phi^-\rangle_{24} + |\psi^+\rangle_{13}\,|\psi^+\rangle_{24} + |\psi^-\rangle_{13}\,|\psi^-\rangle_{24}\Big) \quad (9)$$

Equation (9) demonstrates that the measurement outcomes are completely random as we have four different possibilities which are: $|\phi^+\rangle_{13}\,|\phi^+\rangle_{24}$, $|\phi^-\rangle_{13}\,|\phi^-\rangle_{24}$, $|\psi^+\rangle_{13}\,|\psi^+\rangle_{24}$, or $|\psi^-\rangle_{13}\,|\psi^-\rangle_{24}$. Each of these four possibilities has the same probability of occurrence, 25%. Even though the occurrence of these possibilities is random, the qubits states are correlated. To illustrate, if qubits 1 and 3 measurement result is $|\psi^+\rangle_{13}$, then qubits 2 and 4 must be in the state $|\psi^+\rangle_{24}$ as well. Similarly, if qubits 1 and 3 measurement result is $|\phi^-\rangle_{13}$, then qubits 2 and 4 must be in the state $|\phi^-\rangle_{24}$ as well.

C. BIASED UNITARY OPERATOR CHOICE

The BB84 protocol, published by Bennett and Brassard in 1984, is the most well-known QKD protocol [3]. Alice encodes the secret information in BB84 at random into the rectilinear and diagonal basis and transmits the states to Bob. Bob randomly measures the received states in two basis. They then compare the basis via the classical channel. The key is derived from the states that Alice and Bob use the same measurement basis when measuring them, which means that 50% of the raw data is discarded on average. A simple adjustment to the BB84 technique that may theoretically allow one to achieve 100% efficiency asymptotically has been proposed by the authors of [26]. Their technique is based on two modifications to the BB84 protocol: biased base selection and better error analysis. The initial nonuniformity adjustment enabled Alice and Bob to attain significantly higher efficiency with their raw data. In fact, they demonstrated that this efficiency can be arbitrarily close to 100% in the long key limit. The use of biased selection probability has been extensively studied and tested experimentally [27]. Entanglement-based protocols and decoy-state-based protocols employ biased approaches as well as in [27], [28], and [29], respectively.

In this work, Alice produces a maximally entangled Bell state $|\phi^+\rangle_{AB}$. Alice keeps the qubit (A) of the maximally entangled state $|\phi^+\rangle_{AB}$ for herself and sends the qubit (B) to Bob. Alice (Bob) performs a random unitary operator, Hadamard (H) or identity (I), on her (his) qubits A (B). Alice (Bob) chooses between the two operators, Hadamard and identity, with probabilities p and $(1-p)$, respectively. Alice and Bob choose a number $0 < p \leq \frac{1}{2}$ whose value is publicly revealed. Alice and Bob announce their choices through the public channel. Alice and Bob categorise their choices into four scenarios based on the actual operator employed. When they employ different operators, they discard the two situations. The remaining two cases will be used for key generation and Eve detection.

III. RELATED WORK

The early entanglement-based QKDs protocols depend on the use of alternative measurements, where Alice and Bob use several measurement bases and alternate between them randomly, to make the protocols secure against any eavesdropper attack such as Ekert protocol [4]. This approach has been used in several entanglement-swapping-based QKD, see the correlation equation (8), as well as in [11], [12], [13], and [14]. There are two main drawbacks of the use of alternative measurements. First of all, only a small portion of the transmitted quantum states is used to generate the key while the others are for eavesdropper interference detection, which reduces the key-bit rate. Secondly, a quantum memory is required to store the quantum states sequences until Alice(Bob) tells the other party on the grouped qubits indices and on what basis the measurement should be performed, which makes such solutions impractical for limited resource devices [11], [12], [13]. The advantage of such solutions is that these protocols can differentiate between bit-error-rate (related to device malfunctions of state incoherence) and quantum-bit-error (related to Eve interference).

Conversely, several entanglement-swapping-based protocols that do not require alternative measurements have been proposed in the literature, the first of which appeared in Cabello's work [15]. The idea was revolutionary, which led several authors to propose successful attacks on the Cabello protocol, such as [30]. As a reaction, Cabello published another version of his protocol where Hadamard operation is suggested to make the protocol more secure [31]. Alice performs the Hadamard operation on the first qubit of a randomly prepared shared-state and sends the other qubit to Bob and informs Bob afterward whether he needs to perform the Hadamard operation on the second half or not. The Hadamard operation cannot be performed on each state as Eve can achieve an undetected collective attack by conducting entanglement-swapping between the travelling qubits and their ancilla state, $|\Psi\rangle = H\,|\phi^+\rangle_{Alice}\,|P^+\rangle_{Eve}$.Alice, Bob, and Eve will end up sharing a maximally entangled state $(|P^+\rangle)$. Similar to [32], Cabello suggested that Alice perform a Hadamard operation on her half of a Bell state and sends the other half to Bob and tells him whether she applied the Hadamard operator or not. Alice performs the Hadamard operator on random states; otherwise, the protocol is not secure. The authors of [33] demonstrated that the Chong protocol, [34], is open to a collective attack as simplified and they proposed a modified version where the same benefits of the Hadamard operator have been used. Similar to Cabello's suggestions, the Hadamard operation is performed on random states, otherwise the protocol is not secure [34].

Another type of entanglement-swapping QKD protocol relies on one of the parties, Alice, to generate N Bell states and divide the states qubits into two sequences, such as in [35]. Then, Alice keeps one sequence for herself and sends the other to Bob. Bob chooses a group of qubits at random and performs Bell operator measurements on them in pairs, then informs Alice of the measurement results of the chosen qubits. Alice compares her results to Bob's by doing Bell operator measurements on the corresponding qubit. If Alice's measuring findings match Bob's, she deems Bob to be legal, and the communication proceeds. Unfortunately, Eve can intercept each qubit and conduct an entanglement-swapping-based attack between the sent qubit and a prepared ancilla state. This approach is not secure for two reasons. First of all, Eve conducts no measurement during the security check stage as it is not secret; therefore, no correlation error is introduced. Secondly, once Alice(Bob) chooses two random qubits to conduct Bell measurements on them and informs Bob(Alice) publicly about the chosen qubits indices, Eve can choose the same qubits to perform the measurements on and follow the same procedure. As has been noted, some of the entanglement swapping-based protocols are either insecure due to the lack of randomization [30] that confuses the eavesdropper or due to the use of simple operators such as the bit-flip operator, which has been proven to be insecure [33]. Other protocols are inefficient as they increase the number of exchanged qubits, which increases the attack surface [36]. Some of the protocols have no potential to be used as a conference key distribution due to the use of intermediate trusted node(s) [36]. Increasing the attack surface by sending several qubits or introducing intermediate node(s) gives Eve the ability to perform a successful collective attack or decrease the protocol efficiency.

Despite the fact that QKD protocols can provide secure communication channels, the detectors utilised in the system are neither safeguarded nor entirely trusted. There are possible dangers in real-world implementations due to weaknesses in QKD devices that eavesdroppers might exploit. Most quantum hacking methods now rely on manipulating the detectors of the receiver [18]. In recent years, researchers have made significant contributions to theoretical and experimental research. Device-independent quantum key distribution (DI-QKD) is the most promising scenario for solving security holes [19]. It is not essential to make any assumptions about the underlying workings of the QKD device's security. In DI-QKD, quantum devices are considered as black boxes that produce classical outputs. These devices are thought to run a quantum algorithm, but no assumptions are made about the quantum algorithm that generates the outputs. Several notable advancements in recent years have narrowed the gap between theoretical requirements and practical performance, making DI-QKD a potential research pathway. However, due to hardware technological challenges, DI-QKD remains unattainable for the current state-of-the-art. The DI-QKD, in contrast, needs an extremely high detection efficiency in order to address the difficulty of discovering loopholes in the Bell tests [37]. In search for a better approach than DI-QKD, measurement-device-independent QKD (MDI-QKD) protocols assume that the adversary can control or build the measurement devices (detectors) [20]. The reliance on Charlie's communications is one of MDI-QKD's key drawbacks. Charlie may purposefully postpone transmitting the results in order to render the protocol unusable for real-time applications. On the other hand, it is possible to ensure security while making fewer assumptions. Some protocols rely on relaxed assumptions where only the receiver devices are uncharacterized. Recently, Ioannou et al. published a prepare-and-measure RDI-QKD protocol [23], [24]. Its efficiency is not optimal as it discards more than 50% of the results. Another 1SDI-QKD protocol has been published recently by Taha et al. [38]. They did not consider the parameter estimation step where Eve's presence is detected. Only 25% of the rounds are used for key generation, and classical messages are required for each round. Another related protocol was published in 2021 by Yuan et al. [39]. Their efficiency is not optimal as only 25% of the rounds are used for key generation, and classical messages are required for each round.

IV. QKEYSHIELD PROTOCOL

Consider a scenario where an organization wants to establish secret keys with its customers. The organization may invest a significant amount of money in creating a reliable measuring device, but the customers on the other end of the channel might have low-cost (and unsafe) detectors. Users' measuring devices might be built by the adversary. In light of this, we propose an RDI-QKD in which Alice's measuring device and the entanglement sources are trusted but Bob's measuring device is not. We also assume that we have two types of channels: quantum and classical. Alice sends the swapping qubit to Bob through the quantum channel. Alice and Bob use the classical channel for information reconciliation and privacy amplification. The following enumerated steps describe QKeyShield in detail (see also Figure 1):

1) **Hadamard operation probability:** Alice and Bob choose a number $0 < p \leq \frac{1}{2}$ whose value is publicly revealed. p represents the probability of performing Hadamard operation and $(1-p)$ the probability of performing the identity operator. Assume q_{total} is the total number of transmitted qubits. Bob receives a series of q_{total} qubits from Alice. The value of p is set in such a way that $q_{total}(p^2 - \Delta) = n_1 = \Omega(log q_{total})$, where Δ is a small positive number (i.e., the error due to statistical fluctuations) chosen by Alice and Bob. n_1 and n_2 are the number of test samples chosen from the subsets where they both perform Hadamard operator or identity operator, respectively.
2) **Initial states preparation:** Alice prepares two entangled states, $|\phi^+\rangle_{12}$ and $|\phi^+\rangle_{AB}$, and Bob prepares an entangled state, $|\phi^+\rangle_{34}$, see Figure 1.(a). The initial quantum state of the whole system containing the qubits 1, 2, A,B, 3, and 4 can be written as:

$$\begin{aligned} |\Psi\rangle_{12AB34} &= |\phi^+\rangle_{12} \otimes |\phi^+\rangle_{AB} \otimes |\phi^+\rangle_{34} \\ &= \frac{1}{2\sqrt{2}}(|00\rangle_{12} + |11\rangle_{12}) \\ &\quad \otimes (|00\rangle_{AB} + |11\rangle_{AB}) \\ &\quad \otimes (|00\rangle_{34} + |11\rangle_{34}), \end{aligned} \tag{10}$$

$$|\Psi\rangle_{12AB34} = \frac{1}{2\sqrt{2}}(|000000\rangle + |000011\rangle + |001100\rangle$$

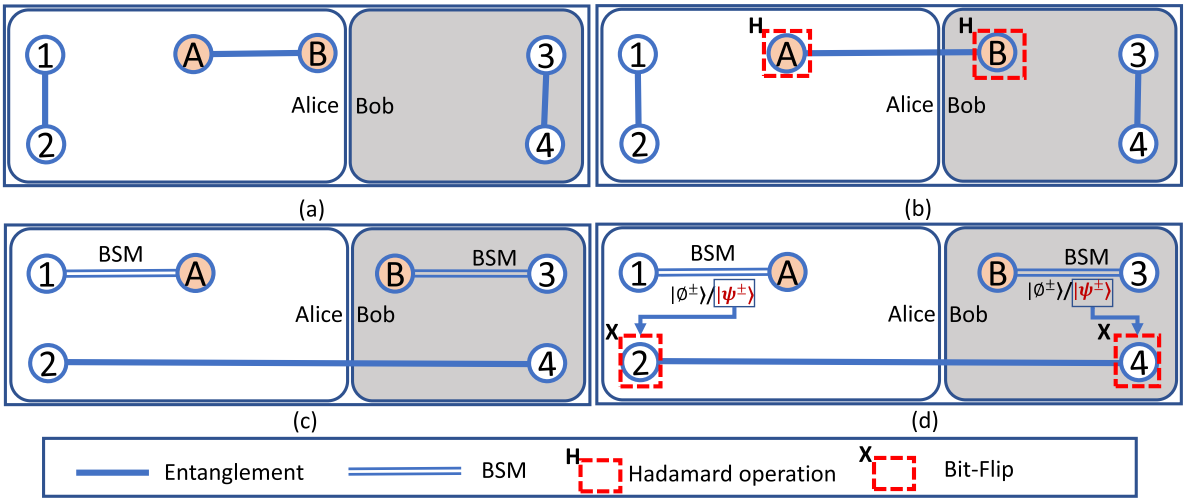


FIGURE 1. QKeyShield protocol steps. Bob's measurement device is uncharacterized and protected from any information leakage to the outside. The system contains six qubits: $(1, 2, A, B)$ are prepared by Alice and $(3, 4)$ are prepared by Bob. The straight line that connects the qubits represents their entanglement. The double straight line links the qubits on which BSM is performed. Alice (Bob) randomly performs Hadamard on qubit $A(B)$ and performs a bit-flip operation when required on qubit 2(4).

$$+\,|001111\rangle + |110000\rangle + |110011\rangle$$
$$+\,|111100\rangle + |111111\rangle). \qquad (11)$$

3) **Swapping state preparation:** Alice produces a maximally entangled Bell state $|\phi^+\rangle_{AB}$.
4) **Swapping qubit sending:** Alice keeps the qubit (A) of the maximally entangled state $|\phi^+\rangle_{AB}$ for herself and sends the qubit (B) to Bob, see Figure 1.(b).
5) **Hadamard operation performing:** Alice (Bob) chooses between the two operators, Hadamard and identity, to perform on her (his) qubit A (B) with probabilities p and $(1-p)$, respectively. If Hadamard operation is performed on both of the qubits simultaneously by Alice and Bob, the state $H^{(1)}H^{(2)}\,|\phi^+\rangle_{AB} = |\phi^+\rangle_{AB}$ will stay intact. If the Hadamard operation is performed successively, let us say Alice first as she is the sender, then Bob, we get: $H^{(1)}\,|\phi^+\rangle_{AB} = |W^+\rangle_{AB}$, see Figure 1.(b). Then, Bob receives qubit B and performs the Hadamard operation, which will undo Alice's Hadamard operation, $H^{(2)}\,|W^+\rangle_{AB} = |\phi^+\rangle_{AB}$. Alice randomly chooses to perform a Hadamard operation on her qubit A before sending qubit B to Bob or after sending. If she performs the Hadamard operation after sending, Eve intercepts qubit B of the state $|\phi^+\rangle_{AB}$. If she performs the Hadamard operation before sending, Eve intercepts qubit B of the state $|W^+\rangle_{AB}$. Whether this operation is conducted before or after sending; it won't affect the measurement outcomes; however, it secures the transmission of the qubit B. The security benefit of Alice's random decision is discussed in Section X-A.
6) **Bell state measurement (BSM):** Qubits 1, 2 and A belong to Alice, and qubits B, 3 and 4 belong to Bob. Alice and Bob perform BSM on qubits 1 and A, and B and 3, respectively. Conducting BSM results in projecting the remaining qubits (2 and 4) belonging to Alice (Bob), into one of the Bell states $|\phi^\pm\rangle_{24}$ or $|\psi^\pm\rangle_{24}$,

$$\begin{aligned}
|\Psi\rangle_{1AB324} = \frac{1}{2}\Bigg[&\Big(|\phi^+\rangle_{1A}\,|\phi^+\rangle_{B3}\,|\phi^+\rangle_{24}\\
&+|\phi^+\rangle_{1A}\,|\phi^-\rangle_{B3}\,|\phi^-\rangle_{24}\\
&+|\phi^-\rangle_{1A}\,|\phi^+\rangle_{B3}\,|\phi^-\rangle_{24}\\
&+|\phi^-\rangle_{1A}\,|\phi^-\rangle_{B3}\,|\phi^+\rangle_{24}\Big)\\
&+\Big(|\phi^+\rangle_{1A}\,|\psi^+\rangle_{B3}\,|\psi^+\rangle_{24}\\
&+|\phi^+\rangle_{1A}\,|\psi^-\rangle_{B3}\,|\psi^-\rangle_{24}\\
&+|\phi^-\rangle_{1A}\,|\psi^+\rangle_{B3}\,|\psi^-\rangle_{24}\\
&+|\phi^-\rangle_{1A}\,|\psi^-\rangle_{B3}\,|\psi^+\rangle_{24}\Big)\\
&+\Big(|\psi^+\rangle_{1A}\,|\psi^+\rangle_{B3}\,|\phi^+\rangle_{24}\\
&-|\psi^+\rangle_{1A}\,|\psi^-\rangle_{B3}\,|\phi^-\rangle_{24}\\
&+|\psi^-\rangle_{1A}\,|\psi^+\rangle_{B3}\,|\phi^-\rangle_{24}\\
&-|\psi^-\rangle_{1A}\,|\psi^-\rangle_{B3}\,|\phi^+\rangle_{24}\Big)\\
&+\Big(|\psi^+\rangle_{1A}\,|\phi^+\rangle_{B3}\,|\psi^+\rangle_{24}\\
&-|\psi^+\rangle_{1A}\,|\phi^-\rangle_{B3}\,|\psi^-\rangle_{24}\\
&+|\psi^-\rangle_{1A}\,|\phi^+\rangle_{B3}\,|\psi^-\rangle_{24}\\
&-|\psi^-\rangle_{1A}\,|\phi^-\rangle_{B3}\,|\psi^+\rangle_{24}\Big)\Bigg]. \qquad (12)
\end{aligned}$$

Knowing their own BSM results, Alice and Bob, could determine which Bell state they are sharing $|\phi^\pm\rangle_{24}$, or $|\psi^\pm\rangle_{24}$. They can decide their desired states before starting the protocol, and we do not assume such information is secret. If they choose $|\phi^\pm\rangle_{24}$ as their desired states, they will share the same secret bit "0" or "1" when measuring qubits 2 and 4. Thus, they have to agree on a mechanism that makes sure their shared state is always $|\phi^\pm\rangle_{24}$.

7) **Desired state preparation:** If they choose $|\phi^{\pm}\rangle_{24}$ as their desired state, Alice(Bob) should perform a quantum bit-flip to her(his) unmeasured qubit 2(4) only if her(his) own measurement is $|\psi^{\pm}\rangle_{1A}(|\psi^{\pm}\rangle_{B3})$,

$$|b\rangle_{2(4)} = \begin{cases} X\,|b\rangle_{2(4)}, & if \quad |\psi\rangle_{1A(3B)} = |\psi^{\pm}\rangle \\ I\,|b\rangle_{2(4)}, & otherwise, \end{cases} \tag{13}$$

where $|b\rangle_{2(4)}$ represents Alice's(Bob's) qubit 2(4). By doing so, Alice and Bob collaboratively, decentrally, and without classical communication prepare the desired state between them, see Figure 1.(d) and Table 1. The final shared state is not always $|\phi^{+}\rangle_{AB}$, it might have a phase shift $|\phi^{-}\rangle_{AB}$; however, the probability of measuring the state on the computational base(0 or 1) is unchanged.

8) **Desired state measurement:** Alice and Bob share one of the maximally entangled states $|\phi^{\pm}\rangle_{24} = \frac{1}{\sqrt{2}}(|00\rangle_{24} \pm |11\rangle_{24})$. Alice(Bob) performs a single-qubit measurement on qubit 2 (4) on the computational basis as no alternative measurement is required. They both got either 00 or 11.

9) **Repeat:** Alice and Bob repeat steps 1–8 until they get a sufficiently long string. For convenience, we consider the protocol steps 1–8 as one round.

10) **Sifting:** Alice and Bob will follow the previous protocol steps without sharing with each other the measurement results or the used operators. Once Bob receives the q_{total}-qubits, they start the sifting phase. During the sifting phase, Alice and Bob reveal the operators that are being used for each qubit through the public channel. When they employ different operators, they discard the results. The remaining results are retained for further analysis.

11) **Error estimation (QBER):** Alice and Bob split the approved results into two subsets based on the performed unitary operator (Hadamard or Identity). They then select a predetermined number of samples, say n_1, at random from the subset where they both conduct Hadamard operation, then compare their findings publicly. The estimated quantum bit error rate (QBER) on Hadamard operator $e_1 = \frac{r_1}{n_1}$ is determined by the number of mismatches r_1. Similarly, Alice and Bob choose a fixed number of instances, say n_2, at random from the subset where they both perform identity operations and compare their measurement findings publicly. $e_2 = \frac{r_2}{n_2}$ is the expected error rate based on the amount of mismatches r_2. They require

$$e_1, e_2 < e_{max} - \Delta_e \tag{14}$$

where e_{max} is a specified maximum allowable error rate and Δ_e is a minor positive value. According to Shor–Preskill [32], e_{max} is around 11%. If these two separate limitations are met, they proceed to the next step. Otherwise, they abort.

12) **Information reconciliation and privacy amplification:** If the protocol passed the error estimation step, we are left with $(N - n_1 - n_2)$ measurement results, which we consider as the raw key. Alice and Bob construct the final secret key by performing information reconciliation and privacy amplification, which utilize classical algorithms. Our focus here is on raw key generation and discussion of privacy amplification algorithms (which are based on classical algorithms) is beyond the scope of our focus, which is centered on quantum key generation.

V. ERROR CORRECTION

Following the protocol steps, Alice and Bob will share the maximally entangled state $|\phi^{\pm}\rangle_{24}$. Once they measure their shared state's qubits, Alice and Bob are supposed to share the same classical bits (00 or 11). But, due to decoherence, measurement errors, or other quantum noise, the sifted key will have some erroneous values [40]. Thus, Alice and Bob might share different classical bits (01 or 10). More generally, Alice and Bob choose a number p which represents the probability of performing the Hadamard operation, and $(1-p)$ the probability of performing the identity operator. Normally, p value is chosen to be less than $\frac{1}{2}$ as the biased approach is followed. A faction, p, of the measurements where they both perform Hadamard is used for eavesdropper check and remaining fraction, $1-p$, of measurements, are used to generate the key. QKeyShield always measures along the computational base. The final shared state might have a phase flip $|\phi^{+}\rangle_{AB}$ or $|\phi^{-}\rangle_{AB}$; however, the probability of measuring the state on the computational base(0 or 1) is unchanged. The phase-flip error rate does not affect the final measurement. The bit-flip error rate is given by:

$$e^{bit-flip} = pe_1 + (1-p)e_2 \tag{15}$$

where e_1 and e_2 are the QBERs when Alice and Bob both employ the Hadamard and identity operations, respectively.

The simplest classical error correction code is the three-bit code whose encoder duplicates the bit three times: 0 → 000 and 1 → 111. This method is ineffective in a quantum channel because the no-cloning theorem prohibits the repetition of a single qubit more than three times. To overcome this, a different method has to be used, such as the use of GHZ state that is consists of 3 maximally entangled qubits ($|P\rangle = \frac{1}{2}(|000\rangle + |111\rangle)$). We do not copy these qubits; we create them and entangle them in such a way that they hold the same value once measured. The GHZ state code is capable of detecting and correcting a single error. For generalization purposes, a state of Nq maximally entangled qubits can be called cat state, $|Cat\rangle$,

$$|Cat\rangle = \frac{1}{\sqrt{2}}\left(\prod_{j=1}^{Nq} |b_j\rangle \pm \prod_{j=1}^{Nq} |\bar{b_j}\rangle\right), \quad j = 1, \ldots, Nq \tag{16}$$

where $b \subset \{0, 1\}$ and the bar above b indicates its logical negation. Nq represents the number of qubits in the state. Alice(Bob) can replaces her(his) private state $|\phi^{+}\rangle_{12}$ $(|\phi^{+}\rangle_{34})$

TABLE 1. Desired state preparation illustration. Once the system shown in Equation (12) is measured, it can be found in one of 16 possibilities. These possibilities are aggregated based on the obtained states by both Alice and Bob:$|\phi^{\pm}\rangle_{1A}\,|\phi^{\pm}\rangle_{B3}$, $|\phi^{\pm}\rangle_{1A}\,|\psi^{\pm}\rangle_{B3}$, $|\psi^{\pm}\rangle_{1A}\,|\psi^{\pm}\rangle_{B3}$, *and* $|\psi^{\pm}\rangle_{1A}\,|\phi^{\pm}\rangle_{B3}$. The default shared stated can be either $|\phi^{\pm}\rangle_{24}$ or $|\psi^{\pm}\rangle_{24}$. Alice(Bob) follows Equation (13) to prepare the desired state.

Possible system states	Obtained state $\lvert\psi\rangle_{24}$	Alice's operator	Bob's operator	**Desired state** $\lvert\psi\rangle_{24}$
$\big(\lvert\phi^+\rangle_{1A}\lvert\phi^+\rangle_{B3}\lvert\phi^+\rangle_{24}+\lvert\phi^+\rangle_{1A}\lvert\phi^-\rangle_{B3}\lvert\phi^-\rangle_{24}$ $+\lvert\phi^-\rangle_{1A}\lvert\phi^+\rangle_{B3}\lvert\phi^-\rangle_{24}+\lvert\phi^-\rangle_{1A}\lvert\phi^-\rangle_{B3}\lvert\phi^+\rangle_{24}\big)$	$\lvert\phi^{\pm}\rangle_{24}$	-	-	$\lvert\phi^{\pm}\rangle_{24}$
$\big(\lvert\phi^+\rangle_{1A}\lvert\psi^+\rangle_{B3}\lvert\psi^+\rangle_{24}+\lvert\phi^+\rangle_{1A}\lvert\psi^-\rangle_{B3}\lvert\psi^-\rangle_{24}$ $+\lvert\phi^-\rangle_{1A}\lvert\psi^+\rangle_{B3}\lvert\psi^-\rangle_{24}+\lvert\phi^-\rangle_{1A}\lvert\psi^-\rangle_{B3}\lvert\psi^+\rangle_{24}\big)$	$\lvert\psi^{\pm}\rangle_{24}$	-	$X\lvert b\rangle_4$	$\lvert\phi^{\pm}\rangle_{24}$
$\big(\lvert\psi^+\rangle_{1A}\lvert\psi^+\rangle_{B3}\lvert\phi^+\rangle_{24}-\lvert\psi^+\rangle_{1A}\lvert\psi^-\rangle_{B3}\lvert\phi^-\rangle_{24}$ $+\lvert\psi^-\rangle_{1A}\lvert\psi^+\rangle_{B3}\lvert\phi^-\rangle_{24}-\lvert\psi^-\rangle_{1A}\lvert\psi^-\rangle_{B3}\lvert\phi^+\rangle_{24}\big)$	$\lvert\phi^{\pm}\rangle_{24}$	$X\lvert b\rangle_2$	$X\lvert b\rangle_4$	$\lvert\phi^{\pm}\rangle_{24}$
$\big(\lvert\psi^+\rangle_{1A}\lvert\phi^+\rangle_{B3}\lvert\psi^+\rangle_{24}-\lvert\psi^+\rangle_{1A}\lvert\phi^-\rangle_{B3}\lvert\psi^-\rangle_{24}$ $+\lvert\psi^-\rangle_{1A}\lvert\phi^+\rangle_{B3}\lvert\psi^-\rangle_{24}-\lvert\psi^-\rangle_{1A}\lvert\phi^-\rangle_{B3}\lvert\psi^+\rangle_{24}\big)$	$\lvert\psi^{\pm}\rangle_{24}$	$X\lvert b\rangle_2$	-	$\lvert\phi^{\pm}\rangle_{24}$

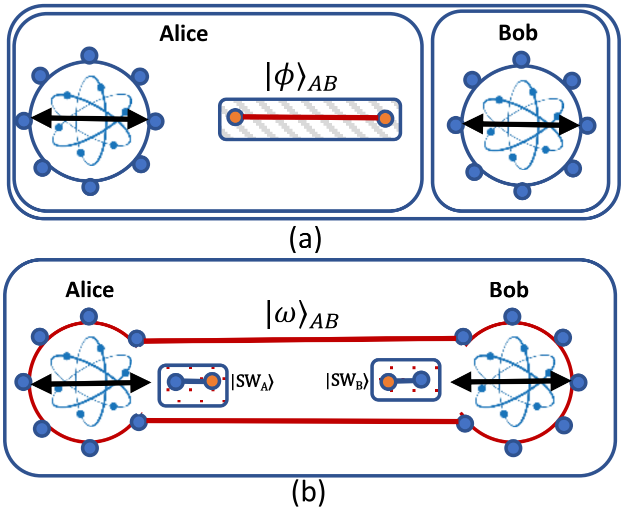


FIGURE 2. QKeyShield protocol. (a) the initial state where Alice and Bob prepare *Cat* state that consists of N_q qubits. Alice prepares another entangled state ($|\phi\rangle_{AB}$). Alice sends the qubit *B* to Bob. (b) Alice and Bob performs BSM on $|SW_A\rangle$ and $|SW_B\rangle$ which results in creating a larger *Cat* state (qubits linked in red).

by a Cat state $|Cat\rangle$. Alice(Bob) can decide how many repetitive qubits (Nq) she(he) wants to use for the error correction.

Alice (Bob) performs a BSM between qubit A (B) and one of her(his) Cat state qubits, $|b_j\rangle$, which will results in a new entangled pair, let us call it $|SW\rangle_A$ ($|SW\rangle_B$), see Figure 2. Conducting BSM results in projecting all the remaining qubits of Alice and Bob, which are $(2 \times (Nq-1))$ into an entangled state, let it be $|\omega\rangle$,

$$|\omega\rangle = \frac{1}{\sqrt{2}}\Big(\prod_{j=1}^{2Nq-2}|b_j\rangle \pm \prod_{j=1}^{2Nq-2}|\bar{b_j}\rangle\Big). \tag{17}$$

Alice(Bob) measures the state $|SW_A\rangle$ ($|SW_B\rangle$) to know if a bit-flip operation on the remaining qubits ($|Cat\rangle^{Nq-1}$) is required,

$$|Cat\rangle = \begin{cases} X\,|Cat\rangle^{Nq-1}, & if \quad |SW\rangle_{A(B)} = |\psi\pm\rangle \\ I\,|Cat\rangle^{Nq-1}, & otherwise. \end{cases} \tag{18}$$

Assuming that $Nq - 1 = 3$, Alice (Bob) measure three qubts and map the obtained code words into a single bit, $\{000, 001, 010, 100\} \rightarrow 0$ and $\{011, 101, 110, 111\} \rightarrow 1$. By doing so, they can decrease the probability of mismatch between them.

VI. TIME-REVERSED QKEYSHIELD

The time-reversal scenario where the single-qubit measurement is conducted before the swapping operation (BSM) has first appeared in [41] and its security has been proven in [6]. Interestingly, QKeyShiled can also be implemented in a time-reversal fashion, see Figure 3. This is because BSM operations commute with Alice's and Bob's single-qubit measurements. As a result, the measurements might be reversed in sequence. That is, Alice and Bob do not need to wait for the BSM results to measure half of their Bell states, but they can measure them beforehand. This converts the original QKeyShiled protocol into an analogous prepare-and-measure technique, in which the unmeasured qubits 1 (3) of Alice(Bob) can be considered as BB84 states. Similar to step (6) of the QKeyShield protocol, Alice (Bob) performs BSM between qubit A (B) and her(his) qubit 1 (3). It's worth noting that BSM provides no information about the individual bit values that are obtained when measuring qubits 2(4); however, it helps in preparing the desired shared classical bit, detecting Eve's intervention, and testing Bob's device credibility. Similar to step (7), Alice (Bob) performs a **classical** bit-flip to her(his) obtained bit only if her(his) BSM result is $|\psi^{\pm}\rangle_{1A}(|\psi^{\pm}\rangle_{B3})$. Most significantly, Alice and Bob follow the same error estimation strategy used in the original QKeyShield.

Using the time-reversed mode, the information is obtained beforehand, which provides another layer of security. It helps in securing the protocol against detector blinding attacks. This version and the original version are almost similar; therefore, throughout the rest of this paper, we only mention QKeyShield.

VII. SECURITY DEFINITIONS

QKD's security is assessed in comparison to a flawless key distribution method in which Alice and Bob share a real

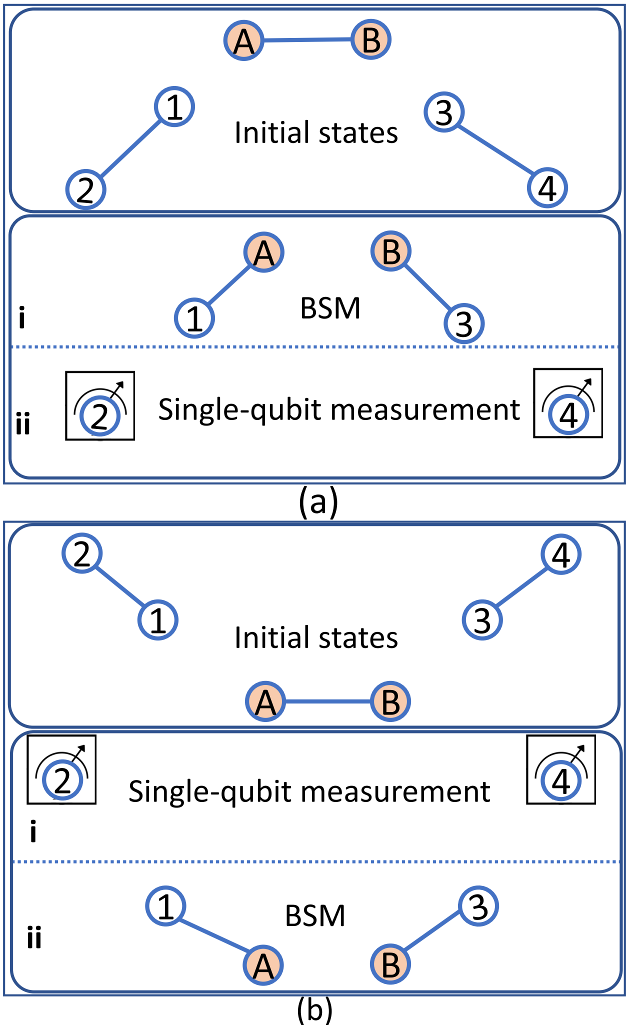


FIGURE 3. **(a) QKeyShield (b) Time-reversed QKeyShield.**

random secret key. QKeyShield would consider a key (K) to be a perfect key if it is a random bit string whose value is fully independent of Eve's knowledge. The deviation ε from a perfect key can be used to determine the security of K which is formulated in terms of security definitions that were proposed in [42]. Let S_A and S_B represent Alice's and Bob's bit strings.

Definition 1 (Correctness): The protocol is said to be $\varepsilon_{correct}$ if

$$Pr[S_A \neq S_B] \leq \varepsilon_{correct}, \tag{19}$$

that is, the probability (Pr) that Alice's and Bob's keys are not identical is not greater than $\varepsilon_{correct}$.

Definition 2 (Secrecy): With respect to an adversary holding a quantum system E, a protocol is said to be ε_{secret} if the joint state satisfies:

$$\frac{1}{2}\,\|\rho_{AB} - \tau_K \otimes \rho_E\|_1 \leq \varepsilon_{secret} \tag{20}$$

where $\|.\|_1$ is the trace norm, τ_K is the mixed state of K. That is, ρ_{AB} is ε_{secret} close the perfect key. ε_{secret} can be interpreted as the maximum tolerated failure probability, where failure indicates that Eve might have gained some knowledge.

Definition 3 (Security): A protocol is considered to be ε_{secure} if its both $\varepsilon_{correct}$ and ε_{secret}, with

$$\varepsilon_{correct} + \varepsilon_{secret} \leq \varepsilon_{secure}. \tag{21}$$

QKeyShield assures that if $\varepsilon_{correct} + \varepsilon_{secret} \leq \varepsilon_{secure}$, a key would be generated, otherwise it aborts.

VIII. KEY RATE

Let the percentage of the used qubits in key generation (η) be

$$\eta = \frac{q_k}{q_{total}}, \tag{22}$$

where q_k is the number of used qubits in the key generation and q_{total} is the total qubits transmitted(it is used interchangeably with N, where N represents the total number of the protocol rounds). QKeyShield minimizes the number of discarded results as it adopts the use of a biased selection approach along with adequate error analysis; therefore, the probability of a qubit to used in the key generation is high. The number of discarded measurement results (bits) can be given by

$$\eta_{dis} = 2 \times p \times (1 - p) \times N. \tag{23}$$

where p represents the probability of performing the Hadamard operation and it is bounded by $0 < p \leq 0.5$; and $(1 - p)$ represents the probability of performing the identity operator. After we discard the mismatched measurements, we divide the remaining results between error estimation and the sifted key. As discussed earlier, two test sets, n_1 and n_2, of length $(1-p)\times N$ are taken from both measurements. Thus, the total number of bits used for error estimations read

$$\eta_{ES} = 2 \times (1 - p) \times N. \tag{24}$$

The remaining measurements results are the sifted key and can be given by

$$\eta_{sif} = (p^2 - (1 - p)^2) \times N, \tag{25}$$

After the error estimation step, Alice and Bob are left with M measurement results, $M = N - n_1 - n_2$. Alice and Bob perform local error correction, discussed in Section V, to form their raw key, denoted K_A^M and K_B^M, respectively. Then Bob performs a one-way error correction over the public channel to compare his key to Alice's key. This error correction procedure reveals b_{leak} bits of information. The maximum tolerable probability of $K_A^M \neq K_B^M$ after error correction is denoted as ε_{EC}. To find out if the final raw keys are corrected, Alice computes a hash h_A of length $\lceil \log(\frac{1}{\varepsilon_{EC}}) \rceil$ from her raw key K_A^M. She sends the hash function and h_A to Bob over a public channel. Then Bob computes h_B. If $h_A \neq h_B$, the protocol aborts. The total leaked information during the error correction is given by $b_{leak} + \lceil \log(\frac{1}{\varepsilon_{EC}}) \rceil \leq b_{leak} + \log(\frac{2}{\varepsilon_{EC}\,\varepsilon_{secure}^2})$. If the error correction step is successful, Alice and Bob then perform privacy amplification to distill a shorter secret key. They apply the same two-universal hash to the error corrected keys

K_A^M and K_B^M of length n to obtain shorter keys S_A and S_B of length L. The maximum tolerable probability of $K_A^M = K_B^M$ after privacy amplification is denoted as ε_{PA}. The secret key length L satisfies

$$L \leq H_{min}^{\varepsilon}(K_A^M|E) - b_{leak} - \log_2(\frac{2}{\varepsilon_{EC}\varepsilon_{secure}^2}), \qquad (26)$$

where $H_{min}^{\varepsilon}(K_A^M|E)$ is the conditional smooth min-entropy of Alice's key and Eve's knowledge. Computing $H_{min}^{\varepsilon}(K_A^M|E)$ is a challenge as Eve information is not accessible to Alice and Bob; therefore, the correlation between K_A^M and K_B^M can be used to bound the correlation between Alice and Eve [21], which gives

$$H_{min}^{\varepsilon}(K_A^M|E) \geq D_q n - H_{max}^{\varepsilon}(K_A^M|K_B^M), \qquad (27)$$

where $H_{max}^{\varepsilon}(K_A^M|K_B^M)$ corresponds to the amount of information that Bob needs to reconstruct Alices' key K_A^M with ε error probability ($H_{max}^{\varepsilon}(K_A^M|K_B^M) = nH(e_{max})$); D_q corresponds to the preparation device quality and we assume that the source is ideal, that is, $D_q = 1$; e_{max} is a specified maximum allowable error rate; and $H(x)$ is the binary Shannon entropy, $H(x) = -xlog_2(x) - (1-x)log_2(1-x)$. The secret key length reads:

$$L \leq n(1 - H(e_{max})) - b_{leak} - \log_2(\frac{2}{\varepsilon_{EC}\varepsilon_{secure}^2}), \qquad (28)$$

According to the security definitions, If QKeyShield always aborts, it is still secure. Consequently, *completeness* is another crucial aspect that should be taken into account. It represents the protocol probability of not aborting, $1-\varepsilon_{abort}$ for small ε_{abort}. Due to the biased approach, QKeyShield allows for a significantly higher sifting efficiency. The sifted key is extracted from the measurements of the dominant operator, let say the identity operator, and the measurements of the non-dominant operator are used for error estimation. Finlay, the secret key rate for finite N reads

$$\delta_{fin} = \omega(1 - \varepsilon_{abort})\frac{L}{q_{total}(\eta_{sif}, \eta_{ES})}, \qquad (29)$$

where $q_{total}(\eta_{sif}, \eta_{ES}) = \eta_{sif} + \eta_{ES} + 2\sqrt{\eta_{sif}\eta_{ES}}$ represents the total number of required qubits that should be sent until η_{sif} sifted key bits and η_{ES} error estimation bits are collected; and ω is the experiments repetition rate, i.e. the inverse of the time required for a single experiment. When q_{total} is sufficiently large, the sifted key tend to infinity $\eta_{sif} \to \infty$, thus $L/q_{total}(\eta_{sif}, \eta_{ES}) \to 1$. For arbitrary security bound, $\varepsilon > 0$, the formula of the asymptotic secret key rate can be given by

$$\delta = 1 - H(e_1) - H(e_2), \qquad (30)$$

where $H(.)$ is the binary Shannon entropy; and e_1 and e_2 are the QBERs when Alice and Bob both employ the Hadamard and identity operation, respectively. This equation represents the upper bound on the secret key rate, which is only possible with ideal implantation.

IX. FINITE-KEY SECURITY PROOF

We remark that the security definitions listed in Section VII are *composable*. That is to say, the security of the resulting combination can be deduced from the security of the individual components proofs.

Lemma 1 (Security of QKeyShield): QKeyShield protocol is ε_{total} secure, with $\varepsilon_{total} \geq \varepsilon_{EC} + \varepsilon_{secure} + \varepsilon_{PA}$

Proof: To begin, we show that QKeyShield is ε_{EC}. Alice and Bob obtained the hashes $h_A \neq h_B$ of length $\lceil \log_2(\frac{1}{\varepsilon_{EC}}) \rceil$ by performing a two-universal hash function on their raw keys. The probability of two hashes of length $\lceil \log_2(\frac{1}{\varepsilon_{EC}}) \rceil$ of two different inputs to coincide is small, $2^{-\lceil \log_2(\frac{1}{\varepsilon_{EC}}) \rceil}$.

$$\begin{aligned} Pr[h_A = h_B, K_A^M \neq K_B^M] &\leq Pr[h_A = h_B | K_A^M \neq K_B^M] \\ &\leq 2^{-\lceil \log_2(\frac{1}{\varepsilon_{EC}}) \rceil} \leq \varepsilon_{EC}. \end{aligned} \qquad (31)$$

It is observed that when the protocol aborts, S_A and S_B always coincide, thus $Pr[S_A \neq S_B, h_A \neq h_B] = 0$. By employing this in Equation 31, we demonstrate the protocol is ε_{EC}:

$$\begin{aligned} Pr[S_A \neq S_B] &\leq Pr[S_A \neq S_B, h_A = h_B] \\ &\leq Pr[K_A^M \neq K_B^M, h_A = h_B] \leq \varepsilon_{EC}. \end{aligned} \qquad (32)$$

To demonstrate the protocol's secrecy, the Quantum Leftover hashing lemma [43], [44] is used to give us the upper bound that follows,

$$\frac{1}{2}\|\rho_{AB} - \tau_K \otimes \rho_E\|_1 \leq \varepsilon_{secret} + \frac{1}{2}\sqrt{2^{L - H_{min}^{\varepsilon}(K_A^M|E_C E)}} \qquad (33)$$

where L is the length of S_A after the privacy amplification and E represents the total information that Eve learned about K_A^M. This comprises her quantum system E_Q, information gained during Alice and Bob classical communication E_C, and the knowledge about the used hash function E_F, $E = E_q E_C E_F$. By employing the min entropy chain-rule [43]:

$$H_{min}^{\varepsilon}(K_A^M|E_C E) \geq H_{min}^{\varepsilon}(K_A^M|E) - log_2|E_C| \qquad (34)$$

where $log_2|E_C|$ represents Eve's gained knowledge during the error correction and is given by $log_2|E_C| = b_{leak} - \log_2(\frac{2}{\varepsilon_{EC}\varepsilon_{secure}^2})$. By substituting this in Equation 34,

$$\begin{aligned} H_{min}^{\varepsilon}(K_A^M|E_C E) \geq H_{min}^{\varepsilon}(K_A^M|E) - b_{leak} \\ - \log_2(\frac{2}{\varepsilon_{EC}\varepsilon_{secure}^2}) \end{aligned} \qquad (35)$$

By inserting Equation 35 into 33 we obtain:

$$\begin{aligned} \frac{1}{2}\|\rho_{AB} - \tau_K \otimes \rho_E\|_1 &\leq \varepsilon_{secret} \\ &+ \frac{1}{2}\sqrt{2^{L-(H_{min}^{\varepsilon}(K_A^M|E) - b_{leak} - \log_2(\frac{2}{\varepsilon_{EC}\varepsilon_{secure}^2}))}} \end{aligned} \qquad (36)$$

$$\begin{aligned} \frac{1}{2}\|\rho_{AB} - \tau_K \otimes \rho_E\|_1 \\ \leq \varepsilon_{secret} + \frac{1}{2}\sqrt{2^{log_2(2\varepsilon_{PA})^2}} \\ = \varepsilon_{secret} + \varepsilon_{PA}. \end{aligned} \qquad (37)$$

In the above, we have proven the QKeyShield secrecy and by combining this with ε_{EC} proof, we have demonstrated that QKeyShiled is $\varepsilon_t otal$ secure with $\varepsilon_{total} \geq \varepsilon_{EC} + \varepsilon_{secure} + \varepsilon_{PA}$. □

X. EAVESDROPPING STRATEGIES

In this section we explored all the attacks that are allowed by quantum mechanics.

A. ENTANGLE-MEASURE ATTACK

Eve intercepts the transmitted qubit to Bob and entangles it with her ancilla state (prepared, say, in the state $|E\rangle$) by performing unitary operators. Eve then transmits the travelling qubit to Bob. Finally, Eve measures the auxiliary qubit in her hands to learn more about the shared key. As Alice randomly chooses to perform Hadamard operation on her qubit A before sending qubit B to Bob or after sending, the intercepted state by Eve is either $|\phi^+\rangle_{AB}$ or $|W^+\rangle_{AB}$. Eve's goal is to intercept the qubits sent from Alice to Bob and attach her ancilla state, let's say $|E\rangle$, to the intercepted qubits. Eve has no information about the intercepted state, so she uses the same unitary operator and the same ancilla state. Eve's unitary operation U_e performed on the composite system of the shared-state can be written as:

$$U_{\mathrm{e}}\,|\phi^+\rangle\,|E\rangle = |\phi^+\rangle\,|E_{\phi^+}\rangle\,, \tag{38}$$

$$U_{\mathrm{e}}\,|W^+\rangle\,|E\rangle = |W^+\rangle\,|E_{W^+}\rangle\,, \tag{39}$$

where the states $|E_{\phi^+}\rangle$ and $|E_{W^+}\rangle$ are simply the states that Eve holds after he unitary transformation depending on the initial state that Alice has send. We know that the initial states $|\phi^+\rangle$ and $|W^+\rangle$ are not orthogonal to each other; therefore, we can now compare the scalar product of the states on the right hand side with the states on the left hand side of Equations 38 and 39.

$$\langle\phi^+|W^+\rangle\,\langle E|E\rangle = \langle\phi^+|W^+\rangle\,\langle E_{\phi^+}|E_{W^+}\rangle \tag{40}$$

The scalar product of Eve's initial states $\langle E|E\rangle$ is equal to one. If Eve does not disturb Alice's state, i.e $\langle\phi^+|W^+\rangle$ has not changed on the right hand side, the scalar product of $\langle E_{\phi^+}|E_{W^+}\rangle$ has to be one as well, which directly implies that the two states have to be the same. That means, no matter which state Alice prepares, Eve always gets the same state. On the other hand, if Eve disturbs Alice's state, she can gain some information about Alice's state.

$$\langle\phi^+|W^+\rangle\,\langle E|E\rangle = \langle\acute{\phi}^+|\acute{W}^+\rangle\,\langle E_{\phi^+}|E_{W^+}\rangle \tag{41}$$

The more distinguishable Eve's states $|E_{\phi^+}\rangle$ and $|E_{W^+}\rangle$, the more disturbed the states $|\acute{\phi}^+\rangle$ and $|\acute{W}^+\rangle$. The scalar product $\langle\acute{\phi}^+|\acute{W}^+\rangle$ has to increase so $\langle E_{\phi^+}|E_{W^+}\rangle$ decreases. This implies that the more disturbance Eve introduces to the system, the more information she gains. In the above, we have proven the QKeyShield's ability to resist the entangle-measure attack.

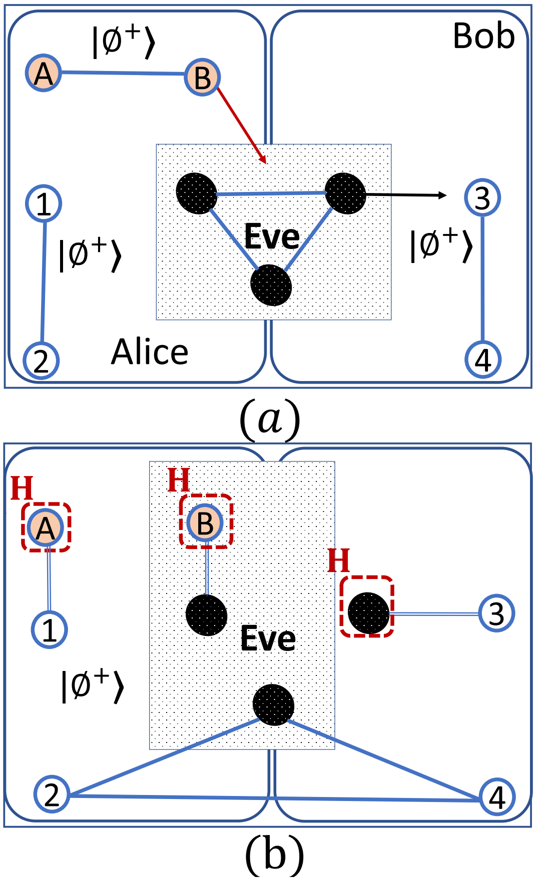


FIGURE 4. Illustration of how Eve may attempt to perform a collective attack strategy.

B. COLLECTIVE ATTACK

The essential concept behind a collective attack is as follows: the adversary Eve attempts to find a multi-qubit state that retains the correlation between the two legitimate parties (Alice and Bob). She also provides new qubits to distinguish between Alice's and Bob's measurement findings. If Eve manages to find such a state, she can remain unnoticed throughout her intervention and obtain the shared key. As shown in Figure 4, Eve might prepare a multi-qubit complex state and try to perform a collective attack.

Before explaining Eve's attack, let us summarize the QKeyShield basic principles that Alice and Bob will obey:

- First, Alice(Bob) performs Hadamard/identity operation on the share-state $|\phi^{\mp}\rangle_{AB}$ qubits based on biased probability.
- Then, Alice(Bob) measures the state $|\psi\rangle_{1A}(|\psi\rangle_{3B})$ and performs a quantum bit-flip on its unmeasured qubit 2(4) if the measurement results are $|\psi^{\pm}\rangle$.
- Alice and Bob's goal is to end up sharing maximally entangled state $|\phi^{\pm}\rangle_{24}$.

Eve's attack purpose is to make the system end up in a state $|P^{\pm}\rangle_{2E4} = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$, where 2 is Alice's qubit, 4 is Bob's qubit, and E is Eve's qubit. A MATLAB-based simulator of QKeyShield has been developed to investigate Eve's possible collective attack scenarios.

TABLE 2. Many scenarios that might occur when an eavesdropper applies the incorrect operators providing that eavesdropper's initial state is $|P^{\pm}\rangle_{DEF}$. Alice chooses between the two operators, H and I, to perform on her qubit A with probabilities p and $(1 - p)$, respectively. Then she sends qubit B to Bob. After that, Eve intercepts qubit (B) and performs either H or I operator on it with probabilities p_1 and p_2, respectively. Then, she sends its qubit, F, to Bob after performing either H or I operator on it with probabilities p_1 and p_2, respectively. Finally, Bob chooses between the two operators, H and I, to perform on the received qubit F with probabilities p and $(1 - p)$, respectively.

Alice	Eve	Bob	Shared state $\|\psi\rangle_{2E4}$	Inferred key	Alice & Bob use the same operators?	Results Correctness	Eve detected?
I	I I	I	$\|P^{\pm}\rangle$	000 or 111	Yes	*Correct*	No
I	I I	H	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle$	Random	No	Incorrect	Discarded
I	I H	I	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle$	Random	Yes	**Incorrect**	**Yes**
I	I H	H	$\|P^{\pm}\rangle$	000 or 111	No	Correct	Discarded
I	H I	I	$\|P^{\pm}\rangle, \|S^{\pm}\rangle$	Random	Yes	**Incorrect**	**Yes**
I	H I	H	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle, \|R^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	No	Incorrect	Discarded
I	H H	I	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle, \|R^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	Yes	**Incorrect**	**Yes**
I	H H	H	$\|P^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	No	Incorrect	Discarded
H	I I	I	$\|P^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	No	Incorrect	Discarded
H	I I	H	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle, \|R^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	Yes	**Incorrect**	Yes
H	I H	I	$\|P^{\pm}\rangle, \|Q^{\pm}\rangle, \|R^{\pm}\rangle$, or $\|S^{\pm}\rangle$	Random	NO	Incorrect	Discarded
H	I H	H	$\|P^{\pm}\rangle$ or $\|S^{\pm}\rangle$	Random	Yes	**Incorrect**	Yes
H	H I	I	$\|P^{\pm}\rangle$	000 or 111	No	Correct	Discarded
H	H I	H	$\|P^{\pm}\rangle$ or $\|Q^{\pm}\rangle$	Random	Yes	**Incorrect**	Yes
H	H H	I	$\|P^{\pm}\rangle$ or $\|Q^{\pm}\rangle$	Random	No	Incorrect	Discarded
H	H H	H	$\|P^{\pm}\rangle$	000 or 111	Yes	*Correct*	No

In the first scenario, see Figure 4, Eve prepares a GHZ state which is $|P^{\pm}\rangle$. Eve intercepts the B qubit that has been sent to Bob, and she follows the same protocol by performing a Hadamard/identity operation on the intercepted qubit and then conducting a Bell operator measurement between the intercepted qubit and one of its qubits. Then, by following the protocol steps, she conducts a quantum bit-flip on her unmeasured qubits. After that, she performs a Hadamard/identity operation on one of its unmeasured qubits and sends it to Bob. Alice(Bob) follows the same steps as usual, which will project the unmeasured state into one of the states summarized in Table 2. Whenever Eve tries to gain information, the shared state of legitimate parties (Alice and Bob) is disrupted.

This attack can be performed on the time-reversed QKeyShield as well with small differences. The presence of Eve will affect Alice's and Bob's BSM results, which will affect the final shared bits due to the performed bit-flip operations.

In search for the best multi-qubit state which preserves the correlation between Alice and Bob, Eve can choose her initial state to be any GHZ states, such as $|P^{\pm}\rangle$, $|Q^{\pm}\rangle$, $|R^{\pm}\rangle$, and $|S^{\pm}\rangle$. By exploring Eve's options, we found out that no matter what initial state Eve uses, the results of the legitimate parties (Alice and Bob) are always disrupted.

As can be seen in Table 2, 50% of the results are discarded as Alice and Bob use different operators. On the other hand, 50% of the possibilities Alice and Bob use the same unitary operator; however, the presence of Eve affects 75% of them. Even though the affected results will be used for detecting Eve, only a small portion of the results are used for the key generation. Figure 5 shows the theoretical amount of useful and discarded results while varying the biased selection probability. The use of fair operator selection probability, p=0.5, indicates that 50% of the results are discarded. On the other hand, when we have a completely biased scheme, $p = 0$, no results will be discarded; however, Eve cannot be detected. The use of bias operator selection probability minimizes the amount of results that will be discarded. To detect Eve while using biased probability, we need n_1 and n_2 test samples chosen from the subsets where they both perform the Hadamard operator or identity operator, respectively. The number of test samples n_1 and n_2 should be at least of order $\Omega(log_2 q_{total})$.

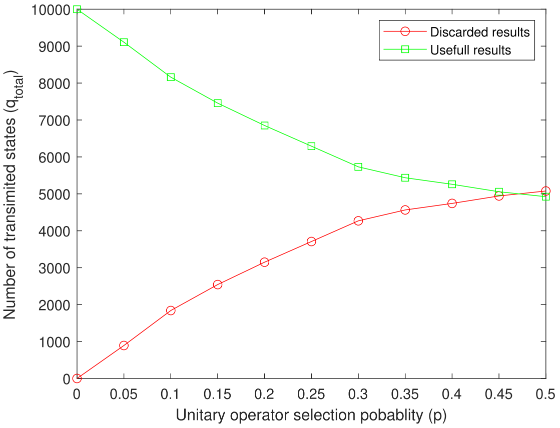


FIGURE 5. Number of discarded results compared to the useful ones while $q_{total} = 10000$ and the selection probability varies $0 \leq p \leq \frac{1}{2}$. Fair random-based protocols such as RDI-QKD [24] discard at least 50% of the results.

C. COHERENT ATTACK

In this attack, Eve creates a global auxiliary system that interacts with all qubits transmitted through the channel via a global unitary operator [45]. Eve saves the outputs of the auxiliary systems in a quantum memory, waits for Alice and Bob to complete their procedure over the public channel, and then performs an optimum joint measurement on the quantum memory.

In QKeyShield, all of the transmitted qubits are independent of one another, and all of the measurements are performed on each round in a completely independent manner as no classical messages are required. In addition to that, QKeyShield is an entanglement-swapping-based protocol, which means Eve isn't interacting with information carriers qubits, implying that a coherent attack is not more powerful than an individual or collective attack.

D. DETECTOR BLINDING ATTACK

Entanglement-swapping has been utilized in the past for building a side-channel-free QKD [5], [6]. The entanglement-swapping dual teleportation channel serves as an ideal Hilbert space filter. QKeyShield is an entanglement-swapping-based scheme that allows Alice's and Bob's qubits that do not interact directly to become entangled. Unlike BB84 [3] and BBM92 [46], the qubit sent by Alice to Bob is not an information carrier; however, it is used to help Alice and Bob to establish secret entangled qubits, that are the information carrier. Bob's device performs three main operations before measuring the secret qubit. It starts by randomly performing a Hadamad operation on the received qubit. Then it conducts BSM. After that, a bit-flip operation is performed on the secret qubit if required. Finally, the secret qubit is measured. A blinding attack will affect the BSM, which will increase the error rate when measuring the secret qubit. Moreover, the time-reversed QKeyShield is more robust against detector blinding attacks as the information is extracted in advance and Eve's input cannot manipulate them.

XI. PROTOCOL EFFICIENCY

QKeyShield is an efficient QKD protocol as it manages to balance several efficiency metrics: communication (information-theoretical) efficiency, resource efficiency, key-rate efficiency, and sifting-time efficiency. We compute the communication efficiency, resource efficiency, and sifting efficiency for each round (protocol steps 1–8).

A. COMMUNICATION EFFICIENCY (σ)

To compute the protocol communication efficiency, the definition proposed by Cabello in [47] is used,

$$\sigma = \frac{b_s}{q_t + \acute{b_t}}, \tag{42}$$

where b_s represents the expected number of secret bits obtained by Alice(Bob), q_t is the number of qubits exchanged, and $\acute{b_t}$ represents the number of classical bits sent (to be realistic, we can consider it the number of classical messages sent).

The sent classical messages for the purpose of sifting are not included in this communication efficiency (only the messages that are used in each round for inferring the key). Communication efficiency σ comparison was introduced in [47] where several protocols were compared, such as Cabello, Ekert, Bennett (BB84), etc. The proposed QKeyShield has outperformed Cabello's protocol because every transmission of a single qubit can generate one classical bit of the shared key with local measurements and without the use of classical communication. Thus, the QKeyShield protocol is 100% efficient in terms of σ. The high discard rate of [24] allows for a maximum of 0.5 percent of acquiring a classical bit, similar to the case of the B92 protocol reported in [47].

TABLE 3. Communication efficiency σ of different entanglement-swapping-based QKD protocols along with the most recent related protocols.

Protocol	b_s	q_t	$\acute{b_t}$	Communication efficiency (σ)
QKeyShield	1	1	0	1
[31]	2	2	1	0.67
[36]	4	5	3	0.5
[12]	2	2	1	0.67
[48]	1	2	1	0.33
[14]	2	2	4	0.33
[25]	2/1	2	2	0.312
[49]	1	2	1	0.33
[4]	1	2	0	0.5
[50]	1	2	1	0.33
[51]	1	1	1	0.5
[52]	1	1	1	0.5
[39]	1	3	1	0.25
[24]	0.5	1	0	0.5

B. RESOURCES EFFICIENCY (U)

Some protocols use the communication efficiency definition (σ) to show that their efficiency is 100%; however, they ignore that their protocols require either huge quantum memory for storing all the qubits sequences used in the protocol or several relay nodes. To evaluate the efficiency of the used resources per each protocol in obtaining a single classical bit, we have included several criteria, which are: $C1$ represents the number of required Bell states; $C2$ indicates whether the protocol causes a time delay in each round or not, i.e., Alice or Bob wait for each other's results to infer the key; $C3$ is the number of the performed BSMs; $C4$ represents the number of quantum memory cells required; $C5$ is the number of used relay nodes; and $C6$ is the number of detectors in the measurements. The proposed resource efficiency evaluation is sophisticated and general, as well as beneficial—it encompasses different criteria. The resource efficiency does not take into consideration everything performed in a QKD protocol (only the required qubits, BSMs, time delay, quantum memory cells, and relay nodes). The performed operations by each protocol, such as Hadamard and bi-flip, are not considered as well.

To identify the resource efficiency of each protocol, a multicriteria decision problem needs to be solved; therefore, the well-known Analytic Hierarchy Process (AHP) method is used [53]. Pairwise comparison is used in AHP to establish preferences between criteria, where a numerical scale that ranges from 1 to 8 is used [54]. The value 8 indicates that one criterion is highly more significant than the other, and the

TABLE 4. **Example of pairwise comparison: two scenarios were considered: 1) all the criteria are "equal significant" to each other, and 2) some criteria are "more significant" than others ($C4 > C2 > C5 > C1, C3, C6$).**

Criteria	$C1$	$C2$	$C3$	$C4$	$C5$	$C6$	(W)	$(\bar{W})$
Scenario(1)							W^{eq}	$\bar{W}^{eq}$
$C1$	1	1	1	1	1	1	6	0.16
$C2$	1	1	1	1	1	1	6	0.16
$C3$	1	1	1	1	1	1	6	0.16
$C4$	1	1	1	1	1	1	6	0.16
$C5$	1	1	1	1	1	1	6	0.16
$C6$	1	1	1	1	1	1	6	0.16
Total							36	
Scenario(2)							W^{var}	$\bar{W}^{var}$
$C1$	1	0.25	1	0.125	0.5	1	2.88	0.06
$C2$	4	1	4	0.5	2	4	11.5	0.23
$C3$	1	0.25	1	0.125	0.5	1	2.88	0.06
$C4$	8	2	8	1	2	8	21	0.47
$C5$	2	0.5	2	0.5	1	1	6	0.1
$C6$	1	0.25	1	0.125	1	1	6	0.066
Total							65.38	

TABLE 5. **Resources efficiency of different entanglement-swapping-based QKD protocols per each obtained classical bit.**

Protocol	$C1$	$C2$	$C3$	$C4$	$C5$	$C6$	U **where** $\bar{W} = \bar{W}^{eq}$	U **where** $\bar{W} = \bar{W}^{var}$
QKeyShield	6	0	3	0	0	2	0.93	**0.97**
[31]	3	1	1.5	1	0	2	0.94	0.93
[36]	3	1	2	0	0.75	4	0.92	0.95
[12]	4	1	2	4	0	4	0.89	0.85
[14]	2	1	1	1	0	4	0.92	0.90
[25]	4	1	2	0	0	4	0.92	0.95
[49]	4	1	1	2	1	4	0.90	0.89
[48]	4	1	1	0	1	4	0.92	0.95
[52]	1	1	1	2	0	4	0.93	0.91
[51]	1	1	2	2	0	4	0.92	0.90
[38]	2	2	1	2	1	4	0.91	0.89
[39]	3	3	1	0	1	4	0.91	0.92
[24]	0.5	3	0	0	0	4	**0.95**	0.95

value 1 shows that both criteria are equally significant. As a result, if the significance of one criterion is stated in relation to another, the significance of the second criterion in relation to the first is the reciprocal,

$$C_{ij} = \frac{1}{C_{ji}}, \tag{43}$$

where C_{ij} represents the pairwise comparison between the criterion C_i and C_j. The value 1/8 suggests that one criterion is extremely less significant than the other. The weight of each criterion is given by

$$W_i = \sum_{i=1}^{5} C_i, \tag{44}$$

while the normalized weight is given by

$$\bar{W_i} = \frac{W_i}{\sum_{i=1}^{5} W_i}. \tag{45}$$

The table (4) shows the pairwise comparison of two scenarios. In the first scenario, we considered that all the criteria are equally significant. In terms of time delay or technological challenges, some of these criteria are more expensive than others. For example, when a protocol causes a time delay, it becomes slow in establishing a shared key. Additionally, due to the limitations of current quantum memory technology, the use of quantum memory makes the protocol less efficient than others. Finally, the use of intermediate nodes (relay nodes) indicates that the protocol is slower and more expensive. From these points of view, we cannot consider that all the criteria are equally significant. The proposed resource efficiency evaluation is general and it allows us to design different scenarios that match different case study requirements. In the second scenario in the table (4), we think that time delay, quantum memory, and relay nodes are more significant than other criteria. Thus, we consider that: $C4$ is more significant than $C2$; $C2$ is more significant than $C5$; $C5$ is more significant than $C1$ and $C3$; and $C1$, $C3$, and $C6$ are equally significant to each other. The normalized weights obtained from the pairwise comparison are used to evaluate different entanglement-swapping-based QKD protocols, see Table 5. The protocol resource efficiency, U_k, is given by

$$U_k = 1 - \left(\frac{\sum_{i=1}^{5} C_{ki} * \bar{W_i}}{\sum_{k=1}^{a} \sum_{i=1}^{5} C_{ki} * \bar{W_i}}\right) \tag{46}$$

where C_{ki} represents the value of the criterion Ci of the protocol k, and a represents the total number of compared protocols. C_{ki} values are given by: $C_{k1} = \frac{\#qubits}{b_s}$; $C_{k2} = \{0, 1\}$ where 0 means that Alice and Bob do not wait for each other to proceed in measuring their qubits, and 1 means that Alice (Bob) waits for Bob's (Alice's) results to proceed in measuring her(his) qubit; $C_{k3} = \frac{\#BSMs}{b_s}$; $C_{k4} = \frac{\#quantum\_memory\_cells}{b_s}$; $C_{k5} = \frac{\#relay\_nodes}{b_s}$; and C_{k5} equal the number of used detectors.

The first scenario in table 5 where all the criteria are equally significant shows that [24] protocol is the most efficient because it is a prepare-measure protocol. It uses single qubit along with classical messages to obtain a classical bit. In the second scenario, QKeyShield is the best as it eliminates the need for costly criteria such as delay time, classical messages, relay nodes, detectors, and quantum memory. Other protocols that suffer from a time delay can be considered infeasible for hard real-time applications. QKeyShield's resource efficiency makes it feasible for practical applications.

C. KEY RATE EFFICIENCY (δ_{fin})

Besides minimizing the communication overhead and increasing the resource utilization, QKeyShield has a high key rate efficiency. It minimizes the number of discarded results as it adopts a biased selection approach along with adequate error analysis. Therefore, the probability of a qubit being used in the key generation is high. To assure the security of the transmitted qubits, QKD protocols fall into two main categories: either random-based or memory-assisted, see Figure 6. In the random-based protocols, the legitimate parties choose the measurement basis (or the performed unitary operator) randomly. Some random-based protocols are fair, while others are biased. QKeyShield is biased. Some protocols measure on a different basis (X or Z). Others, choose

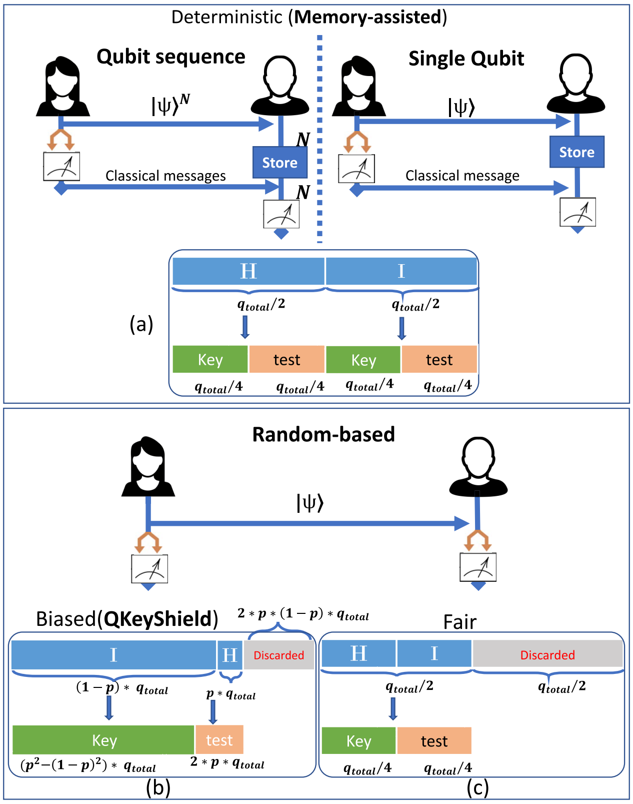


FIGURE 6. Comparison of the expected sifting efficiencies. (a) with the help of quantum memory and classical messages, a deterministic approach is used in several protocols [12], [14], [31], [49] and 50% of the obtained bits end up in the sifted key. (b) QKeyShield uses the biased approach; thus, the estimated proportion of bits with operators conflicts drops from half to $2 * p * (1 - p) \times q_{total}$ and the estimated proportion of bits that end up in the sifted key increases to $(p^2 - (1 - p)^2) \times q_{total}$. (c) a fair approach that is used in most traditional QKD protocols [25], [48], [50] and in most recent protocols such as [24] where only 25% of the obtained bits end up in the sifted key because the probability of performing the Hadamard operator is $p = 0.5$.

randomly between sending decoy state or normal state [29]. QKeyShield chooses different operators randomly (H or I). However, the probabilities is the same as we have two random realizations. In the memory-assisted, one of the parties chooses the random action (whether measurement basis or unitary operator) and informs the other party about the chosen action. In the memory-assisted approach, Bob does not perform the Hadamard operator randomly; rather, he stores the received qubits and waits for Alice to inform him if a Hadamard operation is required, as in Cabello's protocol. With the help of classical messages and quantum memory that cause great time delay in memory-assisted protocols, 50% of the obtained bits end up in the raw key. The classical messages in this comparison are the ones that are sent before the measurements by the other party. Aside from QKeyShield, none of the examined protocols (see Tables 3 and 5) used bias selection in performing the unitary operators. As shown in Figure 6, QKeyShield allows for a significantly higher sifted key length. When q_{total} is sufficiently large, QKeyShield's efficiency can be made asymptotically close to 100%.

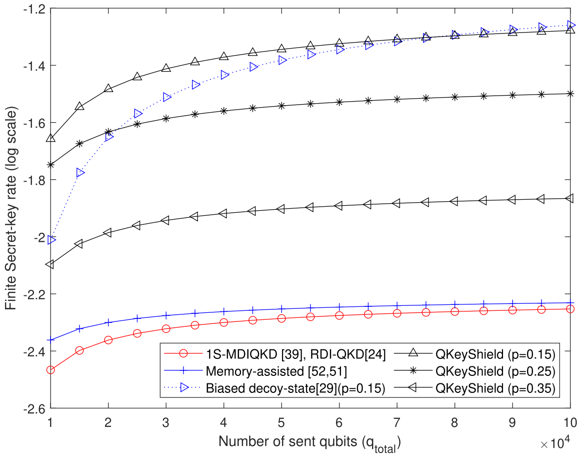


FIGURE 7. Finite Secret-key rate $\log_2(\delta_{fin})$ of the three categories shown in Figure 6. Parameters: $\omega = 1$, $e_{max} = 0.11$, $b_{leak} = 1.05h(e_{max})$, $\varepsilon_{EC} = 10^{(-10)}$, and $\varepsilon_{abort} = 10^{-1}$. The value of p of QKeyShield is set in such a way that $q_{total}(p^2 - \Delta) = n_1 = \Omega(log q_{total})$, where Δ is a small positive number (i.e., the error due to statistical fluctuations) chosen by Alice and Bob.

Figure 7 shows numerical comparison in terms of finite secret key rate between three approaches: memory-assisted protocols [51], [52]; random-based protocols with fair selection ($p = 0.5$) [39]; and the biased approach used by QKeyShield where p is set with regards to q_{total} to provide the highest efficiency for the provided three scenarios. QKeyShield's flexibility in choosing the biased probability, p, improves the protocol key rate efficiency. Not all biased approaches perform well all the time, such as the based decoy QKD [29]. They did not mention the probabilities that Alice uses to choose between signal states, decoy pulses, or vacuum pulses. If we assume that the signal states generation probability is similar to Bob's biased probability when measuring on the Z basis, the protocol will achieve its maximum sifted key rate; however, it provides fewer error estimation pulses. As it can be seen, [29] requires large q_{total} to achieve higher key rate. It is worth mentioning that, only a biased memory-assisted protocol can achieve a higher key rate than QKeyShield.

D. KEY ESTABLISHMENT DELAY (T_{sif})

Many real-time applications are sensitive to delays in packet delivery. Therefore, any key distribution scheme should take this into consideration and hence minimizes the delay. The total delay of the sifted key establishment can be given by

$$T_{sif} = N(q_t \times t_{qm} + \acute{b}_t \times t_{cm}) + 2t_{cm} \tag{47}$$

where t_{qm} is the propagation time of the quantum messages, t_{cm} is the propagation time for the classical messages, and $2t_{cm}$ is delay caused by the two messages that are sent by Alice and Bob to inform each other about their random choices. Figure 8 shows a numerical comparison between the surveyed protocols and QKeyShield. It shows that QKeyShiled is the fastest as it eliminates the need for classical messages and minimized the quantum messages to

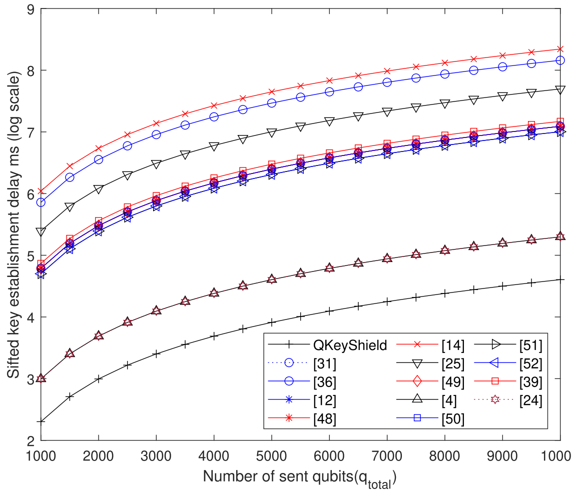


FIGURE 8. Sifted key establishment delay.

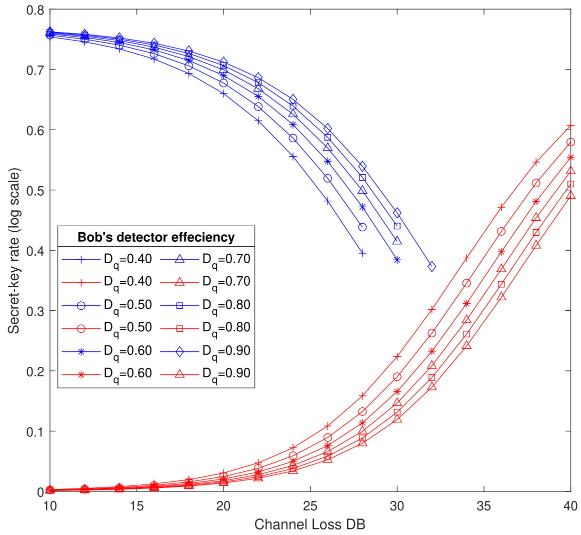


FIGURE 9. Illustration of the channel disturbance (D_r) effects on the key rate. The key rates are depicted in blue and the channel disturbance rates are depicted in red. The parameters are as in figure 7 except Bob's detector efficiency is $D_q \in \{0.6, 0.7, 0.8, 0.9\}$, $q_{total} = 10^5$, and the fibre channel loss is 0.2/km.

the bare minimum. It is assumed that $t_{qm} = 10^{-2}$ms and $t_{cm} = 10^{-1}$ ms.

E. DETECTORS EFFICIENCIES

Most DI-QKD protocols require highly efficient detectors. DI-QKD requires the detector quality/efficiency to be $D_q > 91.1\%$ [22]. On the other hand, 1SDI-QKD allows the use of less efficient detectors, $D_q > 65.9\%$ [22]. That means, we can use the current arbitrary low-quality detectors. This feature makes RDI-QKD protocols practical in situations in which Bob's measurement device is not trusted. Figure 9 shows the key rate along with the channel disturbance as a function of the channel loss. We assume that the channel is a fibre link. The visibility of the signal can be given by:

$$V = \frac{\mu 10^{-\alpha F_L/10} D_q}{\mu 10^{-\alpha F_L/10} + 2P_e} \tag{48}$$

where α represents the fibre attenuation $\alpha = 0.2$, P_e is the probability of an error count per clock cycle $P_e = 8.5 \times 10^{-7}$, [55], μ is the average number of photons leaving Alice's device, and D_q is Bob's detector efficiency. The fidelity can be given by:

$$F = \frac{1+3V}{4}. \tag{49}$$

The channel disturbance is $D_r = 1-F$. In the event that Alice and Bob find out the channel fidelity is insufficient based on the results of their testing, they abort and restart the protocol. They proceed if they are confident that the fidelity is high.

XII. DISCUSSION

In this work, we consider a scenario where an organization wants to establish secret keys with its customers. The organization may invest a significant amount of money to create reliable measuring devices and place them in a secure environment, but the customers on the other end of the channel might have low-cost detectors that are placed in isolated areas. We proposed an RDI-QKD protocol called QKeyShield. The entanglement source and Alice's measuring device are trusted/characterized but Bob's measuring device is not. In this work, we find that QKeyShield is an efficient and secure RDI-QKD protocol. We found out that despite the fact that entanglement-swapping-based protocols use extra Bell states and BSM, they allow for performing local error correction, defending against detector blinding attacks, and having two modes of the protocol, namely, QKeyShield and the time-reversed QKeyShield. These two modes allow us to utilize the features of both entanglement-based and prepare-measure-based protocols. The time-reversal mode of QKeyShield provides another layer of security. That is, Alice does not need to wait for her BSM results and Bob's BSM results to measure half of her Bell states, but she can measure them beforehand. This converts QKeyShield into a prepare-measure protocol; however, the sent qubits are just to detect Eve's presence and to test Bob's measurement device.

We found that QKeyShield is more efficient than the prior protocols in terms of communication efficiency, resource efficiency, sifting efficiency, key establishment delay, and detection efficiency. It eliminates the need for classical messages, quantum memory, and relay nodes. It minimises the number of discarded results, the number of required detectors, the required detector quality/efficiency, the number of exchanged qubits, and key establishment delay. QKeyShield increases the key rate, which makes it a practical QKD protocol.

Finally, the security of QKeyShield is assured by the well-established quantum features such as the no-cloning theorem [56], non-locality [57], or the monogamy (i.e., non-shareability) of entanglement [58]. We have proved the protocol's security in general and its security against entangle-measure attacks. It is secure against the existing attacks allowed by quantum mechanics, which has been demonstrated by exploring all the attacks that are allowed by quantum mechanics. It ensures that Eve's intervention is detectable through the use of several measures. The trusted party, Alice, randomly chooses to perform a Hadamard operation on her qubit A before sending qubit B to Bob or after sending. The security QKeyShield protocol depends on the probability of performing the Hadamard (identity) operator. The probability of performing the Hadamard operation (p) is chosen in such a way that, $n_1, n_2 \geq \Omega(log_2 q_{total})$, where n_1 and n_2 are the numbers of test samples chosen from the subsets where they both perform the Hadamard operator or identity operator, respectively. Two error rates, e_1 and e_2, are obtained from the test samples to evaluate the untrustworthiness of Bob's devices and Eve's intervention. Due to the randomization probability, p, Eve does not know which operator has been used by both Alice and Bob; hence, any eavesdropping attack will affect the correlation between Alice's and Bob's measurement results. In the absence of Eve, Alice's and Bob's measurement outcomes when they use the same operator should exhibit deterministic correlations. If different operators are used by Alice and Bob, their measurement results will not be correlated. Therefore, Eve should perform either the Hadamard operator or the identity operator to ensure her results are correlated with Alice's and Bob's results. Luckily, Eve does not know which operator has been used by both Alice and Bob; hence, any eavesdropping attack would violate the security definitions discussed above. Having enough test samples from each subset, QKeyShield is said to be ε_{secure} protocol.

XIII. CONCLUSION

In this work, we devised an efficient QKD protocol based on entanglement swapping, called QkeyShield, by which a secret key can be established securely between two parties over an ideal quantum channel. It has integrated several measures to improve its practicality. It optimizes several factors: communication, resources, key rate, and key establishment delay. The proposed protocol requires only two medium-quality detectors that are currently on the market. It has two modes, normal mode and time-reversed, that give us the benefits of both entanglement-based and prepare-measure-based protocols. The proposed protocol is not prone to detector blinding attacks due to the use of entanglement-swapping and the time-reversed mode.

REFERENCES

[1] S. Mrdovic and B. Perunicic, "Kerckhoffs' principle for intrusion detection," in *Proc. Netw. 13th Int. Telecommun. Netw. Strategy Planning Symp.*, Sep. 2008, pp. 1–8.

[2] M. Y. Al-darwbi, A. A. Ghorbani, and A. H. Lashkari, "KeyShield: A scalable and quantum-safe key management scheme," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 87–101, 2021.

[3] C. Bennet, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comp., Syst. Signal*, Bengaluru, India, Dec. 1984, pp. 1–6.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[5] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130502.

[6] H. Inamori, "Security of practical time-reversed EPR quantum key distribution," *Algorithmica*, vol. 34, no. 4, pp. 340–365, Nov. 2002.

[7] Q.-C. Sun, Y.-L. Mao, Y.-F. Jiang, Q. Zhao, S.-J. Chen, W. Zhang, W.-J. Zhang, X. Jiang, T.-Y. Chen, L.-X. You, L. Li, Y.-D. Huang, X.-F. Chen, Z. Wang, X. Ma, Q. Zhang, and J.-W. Pan, "Entanglement swapping with independent sources over an optical-fiber network," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 3, Mar. 2017, Art. no. 032306.

[8] M. M. Weston, S. Slussarenko, H. M. Chrzanowski, S. Wollmann, L. K. Shalm, V. B. Verma, M. S. Allman, S. W. Nam, and G. J. Pryde, "Heralded quantum steering over a high-loss channel," *Sci. Adv.*, vol. 4, no. 1, Jan. 2018.

[9] N. Takei, H. Yonezawa, T. Aoki, and A. Furusawa, "High-fidelity teleportation beyond the no-cloning limit and entanglement swapping for continuous variables," *Phys. Rev. Lett.*, vol. 94, no. 22, Jun. 2005, Art. no. 220502.

[10] S. Takeda, M. Fuwa, P. van Loock, and A. Furusawa, "Entanglement swapping between discrete and continuous variables," *Phys. Rev. Lett.*, vol. 114, no. 10, Mar. 2015, Art. no. 100501.

[11] G. Gan, "Quantum key distribution scheme with high efficiency," *Commun. Theor. Phys.*, vol. 51, no. 5, p. 820, 2009.

[12] G. Gao, "Quantum key distribution by comparing bell states," *Opt. Commun.*, vol. 281, no. 4, pp. 876–879, Feb. 2008.

[13] H. Yuan, J. Song, L.-F. Han, K. Hou, and S.-H. Shi, "Improving the total efficiency of quantum key distribution by comparing bell states," *Opt. Commun.*, vol. 281, no. 18, pp. 4803–4806, Sep. 2008.

[14] D. Song, "Secure key distribution by swapping quantum entanglement," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 3, Mar. 2004, Art. no. 034301.

[15] A. Cabello, "Quantum key distribution without alternative measurements," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 5, Apr. 2000, Art. no. 052312.

[16] O. T. Slattery, "Cost effective QKD system developed by Nist," NIST, USA, Tech. Rep., 2009. [Online]. Available: https://www.nist.gov/itl/cost-effective-qkd-system-developed-nist

[17] S. Lee, S.-J. Lee, T. Kim, J.-S. Lee, J. Biamonte, and M. Perkowski, "The cost of quantum gate primitives," *J. Multiple-Valued Log. Soft Comput.*, vol. 12, pp. 561–573, Apr. 2006.

[18] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2004, p. 136.

[19] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, "Device-independent quantum key distribution with local bell test," *Phys. Rev. X*, vol. 3, no. 3, 2013, Art. no. 031006.

[20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[21] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, no. 11, Mar. 2011, Art. no. 110506.

[22] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A, Gen. Phys.*, vol. 85, no. 1, Jan. 2012, Art. no. 010301.

[23] M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J.-D. Bancal, N. Maring, H. Zbinden, and N. Brunner, "Receiver-device-independent quantum key distribution," *Quantum*, vol. 6, p. 718, May 2022.

[24] M. Ioannou, P. Sekatski, A. A. Abbott, D. Rosset, J.-D. Bancal, and N. Brunner, "Receiver-device-independent quantum key distribution protocols," *New J. Phys.*, vol. 24, no. 6, Jun. 2022, Art. no. 063006.

[25] F. Guo, T. Liu, Q. Wen, and F. Zhu, "Quantum key distribution based on entanglement swapping between two bell states," *Int. J. Quantum Inf.*, vol. 4, no. 5, pp. 769–779, Oct. 2006.

[26] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *J. Cryptol.*, vol. 18, pp. 133–165, Apr. 2005.

[27] Y. Cao, "Entanglement-based quantum key distribution with biased basis choice via free space," *Opt. Exp.*, vol. 21, no. 22, pp. 27260–27268, 2013.

[28] C. Erven, X. Ma, R. Laflamme, and G. Weihs, "Entangled quantum key distribution with a biased basis choice," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045025.

[29] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-state quantum key distribution with biased basis choice," *Sci. Rep.*, vol. 3, no. 1, pp. 1–4, Dec. 2013.

[30] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Comment on, 'quantum key distribution without alternative measurements' [Phys. Rev. A 61, 052312 (2000)]," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 3, 2001, Art. no. 036301.

[31] A. Cabello, "Addendum to, 'quantum key distribution without alternative measurements,'" *Phys. Rev. A, Gen. Phys.*, vol. 64, no. 2, 2001, Art. no. 024301.

[32] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, p. 441, Jul. 2000.

[33] S. Schauer and M. Suda, "A novel attack strategy on entanglement swapping QKD protocols," *Int. J. Quantum Inf.*, vol. 6, no. 4, pp. 841–858, Aug. 2008.

[34] C. Li, Z. Wang, C. Wu, H.-S. Song, and L. Zhou, "Certain quantum key distribution achieved by using bell states," *Int. J. Quantum Inf.*, vol. 4, no. 6, pp. 899–906, Dec. 2006.

[35] N. Zhou, L. Wang, L. Gong, X. Zuo, and Y. Liu, "Quantum deterministic key distribution protocols based on teleportation and entanglement swapping," *Opt. Commun.*, vol. 284, no. 19, pp. 4836–4842, Sep. 2011.

[36] J. Dong and J. Teng, "Quantum key distribution protocol of mesh network structure based on $n + 1$ EPR pairs," *J. Syst. Eng. Electron.*, vol. 21, no. 2, pp. 334–338, Apr. 2010.

[37] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Mar. 2012, Art. no. 130503.

[38] J. Xin, X.-M. Lu, X. Li, and G. Li, "One-sided device-independent quantum key distribution for two independent parties," *Opt. Exp.*, vol. 28, no. 8, pp. 11439–11450, 2020.

[39] D. Castañeda Valle, L. F. Quezada, and S. Dong, "Bell-GHZ measurement-device-independent quantum key distribution," *Annalen der Physik*, vol. 533, no. 9, Sep. 2021, Art. no. 2100116.

[40] G. Jaeger, *Quantum Information*. New York, NY, USA: Springer, 2007, pp. 81–89.

[41] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 4, p. 2651, Oct. 1996.

[42] R. Renner and R. Konig, "Second theory of cryptography conference TCC," *Lect. Notes Comput. Sci.*, vol. 3378, pp. 407–425, May 2005.

[43] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Commun.*, vol. 3, no. 1, pp. 1–6, Jan. 2012.

[44] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.* vol. 6, no. 1, pp. 1–127, Feb. 2008.

[45] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 2, Feb. 2016, Art. no. 022325.

[46] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, p. 557, 1992.

[47] A. Cabello, "Quantum key distribution in the Holevo limit," *Phys. Rev. Lett.*, vol. 85, no. 26, p. 5635, 2000.

[48] C.-Y. Zhang and Z.-J. Zheng, "Entanglement-based quantum key distribution with untrusted third party," *Quantum Inf. Process.*, vol. 20, no. 4, pp. 1–20, Apr. 2021.

[49] L. Qin, Y. Li, and S. Wang, "A key distribution protocol based on quantum entanglement swapping for unmanned surface vehicle," *J. Phys., Conf. Ser.*, vol. 1976, no. 1, Jul. 2021, Art. no. 012034.

[50] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, Aug. 2012, Art. no. 130503.

[51] M. Ampatzis and T. Andronikos, "QKD based on symmetric entangled Bernstein–Vazirani," *Entropy*, vol. 23, no. 7, p. 870, Jul. 2021.

[52] H. Qin, W. Sun, and W. K. S. Tang, "Quantum secure direct communication based on single particles," *Opt. Quantum Electron.*, vol. 54, no. 8, pp. 1–11, Aug. 2022.

[53] R. W. Saaty, "The analytic hierarchy process—What it is and how it is used," *Math. Model.*, vol. 9, nos. 3–5, pp. 161–176, 1987.

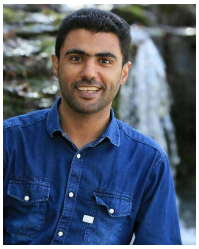
[54] H. A. Taha, *Operations Research: An Introduction*. London, U.K.: Pearson, 2003.

[55] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, May 2004.

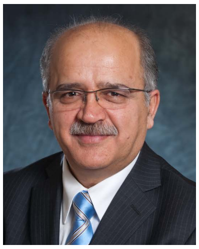
[56] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[57] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Rev. Mod. Phys.*, vol. 86, no. 2, p. 419, Apr. 2014.

[58] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 5, Apr. 2000, Art. no. 052306.



MOHAMMED Y. AL-DARWBI received the B.S. degree in computer science from Dhamar's University, Dhamar, Yemen, and the M.Sc. degree in computer networks from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He is currently pursuing the Ph.D. degree in cybersecurity with the Canadian Institute for Cybersecurity, University of New Brunswick, NB, Canada. His research interests include intrusion detection, key management, quantum key distribution, and cyber threat intelligence.



ALI A. GHORBANI (Senior Member, IEEE) has held a variety of positions in academia for the past 37 years. He is currently a Professor of computer science, a Tier 1 Canada Research Chair in cybersecurity, and the Director at the Canadian Institute for Cybersecurity, which he established in 2016. He served as the Dean at the Faculty of Computer Science, University of New Brunswick, from 2008 to 2017. He is also the Founding Director at the Laboratory for Intelligence and Adaptive Systems Research. He has spent over 27 years of his 37-years academic career carrying out both fundamental and applied research in the areas of cybersecurity, machine learning, and web intelligence. His current research interests include cybersecurity, web intelligence, and critical infrastructure protection. In 2007, he received the University of New Brunswick's Research Scholar Award. Since 2010, he has obtained more than 15M dollar to fund eight large multi-project research initiatives. He is the co-inventor on three awarded patents in the area of network security and web intelligence. He has published over 260 peer-reviewed articles during his career. He has supervised over 170 research associates, postdoctoral fellows, graduate and undergraduate students during his career. His book, *Intrusion Detection and Prevention Systems: Concepts and Techniques*, was published by Springer, in October 2010. He is the co-founder of the Privacy, Security, Trust (PST) Network in Canada and its international annual conference. He developed a number of technologies that have been adopted by high-tech companies. He co-founded two startups, Sentrant Security and EyesOver Technologies, in 2013 and 2015, respectively. He was twice one of the three finalists for the Special Recognition Award at the 2013 and 2016 New Brunswick KIRA Award for the knowledge industry. He was a recipient of the 2017 Startup Canada Senior Entrepreneur Award. He served as the Co-Editor-In-Chief for *Computational Intelligence*: An International Journal, from 2007 to 2017.

ARASH HABIBI LASHKARI (Senior Member, IEEE) is currently a Tier 2 Canada Research Chair in cybersecurity and an Associate Professor at York University. He is the author of ten published books and over 110 peer-reviewed articles on various cybersecurity-related topics. His current research interests include designing and developing malicious behavior detection and mitigation technology to protect network systems against cyberattacks.