Application of the Simulation Attack on Entanglement Swapping Based QKD and QSS Protocols

Stefan Schauer and Martin Suda
Safety and Security Department
AIT Austrian Institute of Technology GmbH
Vienna, Austria
stefan.schauer@ait.ac.at, martin.suda.fl@ait.ac.at

***Abstract*—We discuss the security of quantum key distribution protocols based on entanglement swapping against collective attacks. Therefore, we apply a generic version of a collective attack strategy on the most general entanglement swapping scenario used for key distribution. Further, we focus on basis transformations, which are the most common operations performed by the legitimate parties to secure the communication. In this context, we show that the angles, which describe these basis transformations can be optimized compared to an application of the Hadamard operation. As a main result, we show that the adversary's information is reduced to a new minimum of about 0.45, which is about 10% lower than in other protocols. To become a better overview how and on which protocols this generic version of a collective attack is applicable, the security of different quantum key distribution and quantum secret sharing protocols is discussed. Here we show that applying two basis transformations using different angles the security of a particular protocol can be increased by about 25%.**

***Keywords*—quantum key distribution; entanglement swapping; security analysis; optimal basis transformations.**

I. INTRODUCTION

The security of quantum key distribution (QKD) protocols based on entanglement swapping has been discussed on the surface so far. In a recent article [1], a novel attack strategy and its implications on the security of entanglement swapping based protocols was discussed. This attack strategy will be referred to as *simulation attack* since the major idea is to simulate the correlation between Alice's and Bob's measurement results [2]. In this article, we want to take a closer look at the application of the simulation attack on different QKD and quantum secret sharing (QSS) protocols together with the necessary improvements on the security of these protocols.

QKD is an important application of quantum mechanics and QKD protocols have been studied at length in theory and in practical implementations [3], [4], [5], [6], [7], [8], [9], [10]. Most of these protocols focus on prepare and measure schemes, where single qubits are in transit between the communication parties Alice and Bob. The security of these protocols has been discussed in depth and security proofs have been given for example in [11], [12], [13]. In addition to these prepare and measure protocols, several protocols based on the phenomenon of entanglement swapping have been introduced [14], [15], [16], [17], [18]. In these protocols, entanglement swapping is used to obtain correlated measurement results between the legitimate communication parties. In other words, each party performs a Bell state measurement and due to entanglement swapping their results are correlated and further on used to establish a secret key.

Entanglement swapping has been introduced by Bennett et al. [19], Zukowski et al. [20] as well as Yurke and Stolen [21], respectively. It provides the unique possibility to generate entanglement from particles that never interacted in the past. In detail, Alice and Bob exchange two Bell states of the form $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ such that afterwards Alice is in possession of qubits 1 and 3 and Bob of qubits 2 and 4 (cf. (2) in Figure 1). The overall state can now be written as

$$|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34} = \frac{1}{2}\Big(|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\Big)_{1324} \quad (1)$$

Then, Alice performs a complete Bell state measurement on the two qubits 1 and 3 in her possession, and at the same time the qubits 2 and 4 at Bob's side collapse into a Bell state although they originated at completely different sources. Moreover, the state of Bob's qubits depends on Alice's measurement result (cf. (4) in Figure 1). As presented in eq. (1), Bob always obtains the same result as Alice when performing a Bell state measurement on his qubits.

So far, it has only been shown that QKD protocols based on entanglement swapping are secure against intercept-resend attacks and basic collective attacks (cf. for example [14], [15], [17]). Therefore, we analyze a general version of a collective attack where the adversary tries to simulate the correlations between Alice and Bob [2]. A basic technique to secure these protocols is to use a basis transformation, usually a Hadamard operation, similar to the prepare and measure schemes mentioned above, to make it easier to detect an adversary. In [1], the application of general basis transformations about the angles θ_A and θ_B has been discussed and it has been shown that the information of an adversary can be reduced to a minimum of $\simeq 0.45$. Based on these results we analyze the security of three different protocols with respect to the

simulation attack. In the course of that, we are going to identify, which values for θ_A and θ_B are optimal for these protocols such that an adversary has only a minimum amount of information on the secret key.

In the next section, we are going to shortly review the simulation attack, a generic collective attack strategy where an adversary applies a six-qubit state to eavesdrop Bob's measurement result. A detailed discussion of this attack strategy can be found in [2]. In Section III, we discuss the security of entanglement swapping based QKD protocols against the simulation attack in general. Here, we are focusing on the application of one and two basis transformations and review the optimal angles for these transformations. In the following sections, we discuss the application of the simulation attack on three different protocols: on the prepare & measure QKD protocol by Bennett, Brassard, and Mermin [5] in Section IV, on the entanglement swapping based QKD protocol by Song [17] in Section V and on the QSS protocol by Cabello [16] in Section VI. We will shortly review each of these protocols and provide a detailed security analysis with respect to an application of the simulation attack. At the end, we summarize the results and give a short outlook on the next steps into this topic.

II. The Simulation Attack Strategy

In entanglement swapping based QKD protocols like [14], [15], [16], [17], [18] Alice and Bob rest their security check on the correlations between their respective measurement results coming from the entanglement swapping (cf. eq. (1)). If these correlations are violated to a certain amount, Alice and Bob have to assume that an eavesdropper is present. In 2000, Zhang, Li, and Guo presented an attack strategy, where Eve entangles herself with both parties and manages to obtain full information about the shared key [23]. This collective attack was improved in a previous article [2] to the *simulation attack* and extended to a specific protocol [18] following this basic idea: the adversary Eve tries to find a multi-qubit state, which preserves the correlation between the two legitimate parties. Further, she introduces additional qubits to distinguish between Alice's and Bob's respective measurement results. If she is able to find such a state, Eve stays undetected during her intervention and is able to obtain a certain amount of information about the key. The simulation attack can be generalized to arbitrary entanglement swapping based QKD protocols in a straight forward way, as described in the following paragraphs.

It has been pointed out in detail in [2] that Eve uses four qubits to simulate the correlations between Alice and Bob and she further introduces additional systems, i.e., $|\varphi_i\rangle$, to distinguish between Alice's different measurement results. This leads to the state

$$|\delta\rangle = \frac{1}{2}\Big(|\Phi^+\rangle|\Phi^+\rangle|\varphi_1\rangle + |\Phi^-\rangle|\Phi^-\rangle|\varphi_2\rangle + |\Psi^+\rangle|\Psi^+\rangle|\varphi_3\rangle + |\Psi^-\rangle|\Psi^-\rangle|\varphi_4\rangle\Big)_{PRQSTU} \tag{2}$$

which is a more general version than described in [2]. This state preserves the correlation of Alice's and Bob's measurement results coming from the entanglement swapping (cf. eq. (1)). From eq. (2) it is easy to see that Alice obtains one of the four Bell states when performing a Bell state measurement on qubits P and R. This measurement leaves Bob's qubits Q and S in a Bell state fully correlated to Alice's result. Accordingly, Eve's qubits T and U are in one of the auxiliary states $|\varphi_i\rangle$ she prepared.

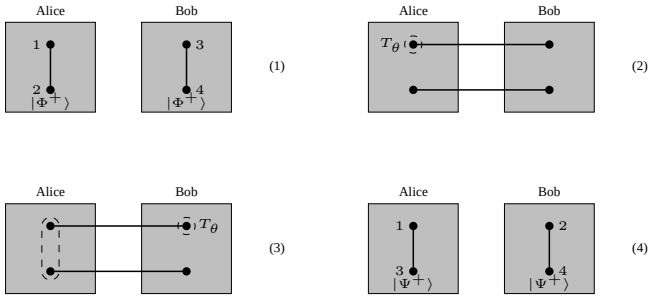

Fig. 1. Illustration of a standard setup for an entanglement swapping based QKD protocol using a basis transformation T_x.

Eve has to choose the auxiliary systems $|\varphi_i\rangle$ such that

$$\langle\varphi_i|\varphi_j\rangle = 0 \qquad i,j \in \{1,...,4\} \;\; i \neq j \tag{3}$$

which allows her to perfectly distinguish between Alice's and Bob's respective measurement results. Thus, she is able to eavesdrop Alice's and Bob's measurement results and obtains full information about the classical raw key generated out of them.

In detail, Eve distributes qubits P, Q, R and S between Alice and Bob such that Alice is in possession of qubits P and R and Bob is in possession of qubits Q and S. When Alice performs a Bell state measurement on qubits P and R the state of qubits Q and S collapses into the same Bell state, which Alice obtained from her measurement (cf. eq. (2)). In particular, if Alice obtains $|\Phi^+\rangle_{PR}$ the state of the remaining qubits is

$$|\Phi^+\rangle_{QS}|\varphi_1\rangle_{TU} \tag{4}$$

and similarly for Alice's other results $|\Phi^-\rangle$ and $|\Psi^\pm\rangle$. This is the exact correlation Alice and Bob would expect from entanglement swapping if no adversary is present (cf. eq. (1) from above). Hence, Eve stays undetected when Alice and Bob compare some of their results in public to check for eavesdroppers. The auxiliary system $|\varphi_i\rangle$ remains at Eve's side and its state is completely determined by Alice's measurement result. Therefore, Eve has full information on Alice's and Bob's measurement results and is able to perfectly eavesdrop the classical raw key.

There are different ways for Eve to distribute the state $|\delta\rangle_{P-U}$ between Alice and Bob. One possibility is that Eve is in possession of Alice's and Bob's source and generates $|\delta\rangle_{P-U}$ instead of Bell states. This is a rather strong assumption because the sources are usually located at Alice's or Bob's laboratory, which should be a secure environment. Eve's second possibility is to intercept the qubits 2 and 3 flying from Alice to Bob and vice versa and to use entanglement swapping to distribute the state $|\delta\rangle$. This is a straight forward method as already described in [2].

We want to stress that the state $|\delta\rangle$ is generic for all protocols where 2 qubits are exchanged between Alice and Bob during one round of key generation as, for example, the QKD protocols presented by Song [17], Li et al. [18] or Cabello [14]. As already pointed out in [2], the state $|\delta\rangle$ can also be used for different initial Bell states. Regarding protocols with a higher number of qubits the state $|\delta\rangle$ has to be extended accordingly (cf. Section VI).

III. Security Against Collective Attacks

In the following paragraphs, we discuss Eve's intervention on an entanglement swapping QKD protocol performing a simulation attack, i.e., using the state $|\delta\rangle_{P-U}$. To detect Eve's presence either Alice or Bob or both parties apply a basis transformation as depicted in Figure 1.

A. General Basis Transformations

Similar to the prepare and measure schemes mentioned in the introduction, most of the protocols based on entanglement swapping apply basis transformations to make it easier to detect the presence of an eavesdropper. The basis transformation most commonly used in this case is the Hadamard operation, i.e., a transformation from the Z- into the X-basis. In general, a basis transformation from the Z-Basis into the X-basis can be described as a combination of rotation operations, i.e.,

$$T_x(\theta,\phi) = e^{i\phi} R_z(\phi) R_x(\theta) R_z(\phi) \tag{5}$$

where R_x and R_z are the rotation operations about the X- and Z-axis, respectively. For reasons of simplicity we take $\phi = \pi/2$ in our further discussions and therefore denote the transformation is described solely by the angle θ, i.e., $T_x(\theta)$. From eq. (5) we can directly see that the Hadamard operation equals $T_x(\pi/2)$. To keep the security analysis as generic as possible we discuss a setup where a general basis transformation about an angle θ_A is applied by Alice and a transformation about an angle θ_B is applied by Bob, respectively (cf. Figure 1).

For our further discussions, we will assume that Alice and Bob prepared the initial states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ as described above to make calculations easier. As already pointed out above and in more detail in [2] if Alice and Bob choose $\theta_A = \theta_B = 0$, i.e., they perform no transformation, the protocol is completely insecure. Hence, we will focus on the scenarios where either $T_x(\theta_A)$ or $T_x(\theta_B)$ or both transformations are applied. For all scenarios we assume that Alice applies $T_x(\theta_A)$ on qubit 1 and Bob applies $T_x(\theta_B)$ on qubit 4.

B. Application of a Single Transformation

For the first scenario where only Alice applies the basis transformation the overall state of the system after Eve's distribution of the state $|\delta\rangle_{P-U}$ can simply be described as

$$|\delta'\rangle = T_x^{(1)}(\theta_A)|\delta\rangle_{1QR4TU} \tag{6}$$

where the superscript "(1)" indicates that $T_x(\theta_A)$ is applied on qubit 1. When Eve sends qubits R and Q to Alice and Bob, respectively, the state after Alice's Bell state measurement on qubits 1 and R is

$$\cos\frac{\theta_A}{2}\,|\Phi^-\rangle_{Q4}|\varphi_2\rangle_{TU} + \sin\frac{\theta_A}{2}\,|\Psi^+\rangle_{Q4}|\varphi_3\rangle_{TU} \tag{7}$$

assuming Alice obtained $|\Phi^+\rangle_{1R}$ (for Alice's other three possible results the state changes accordingly). This indicates that in this case Bob's transformation back into the Z-basis does not re-establish the correlations between Alice and Bob properly. Performing the calculations we see that Bob's operation $T_x(\theta_A)$ brings qubits Q, 4, T and U into the form

$$\begin{aligned}&\cos^2\frac{\theta_A}{2}\,|\Phi^+\rangle_{Q4}|\varphi_2\rangle_{TU} + \sin^2\frac{\theta_A}{2}\,|\Phi^+\rangle_{Q4}|\varphi_3\rangle_{TU}\\ &-\frac{\sin\theta_A}{2}\,|\Psi^-\rangle_{Q4}|\varphi_2\rangle_{TU} + \frac{\sin\theta_A}{2}\,|\Psi^-\rangle_{Q4}|\varphi_3\rangle_{TU}\end{aligned} \tag{8}$$

When Bob performs a Bell state measurement we can directly see from this expression that Bob obtains either the correlated result $|\Phi^+\rangle_{Q4}$ with probability

$$\left(\cos^2\frac{\theta_A}{2}\right)^2 + \left(\sin^2\frac{\theta_A}{2}\right)^2 = \frac{3+\cos(2\theta_A)}{4} \tag{9}$$

or an error, i.e., the state $|\Psi^-\rangle_{Q4}$, otherwise. In detail, Eve introduces an error with probability $(\sin^2\theta_A)/2$, which yields an expected error probability

$$\langle P_e\rangle = \frac{1}{4}\sin^2\theta_A \tag{10}$$

Nevertheless, as long as the results are correlated, Eve obtains from her Bell state measurement on qubits T and U the state $|\varphi_2\rangle_{TU}$ with probability $(1+\cos(\theta_A))^2/(3+\cos(2\theta_A))$ and knows that Bob obtained $|\Phi^+\rangle_{Q4}$. Consequently, we obtain the expected collision probability

$$\langle P_c\rangle = \frac{1}{8}\Big(7+\cos 2\theta_A\Big). \tag{11}$$

This directly leads to the Shannon entropy

$$H = \frac{1}{2}\,h\Big(\cos^2\frac{\theta_A}{2}\Big) \tag{12}$$

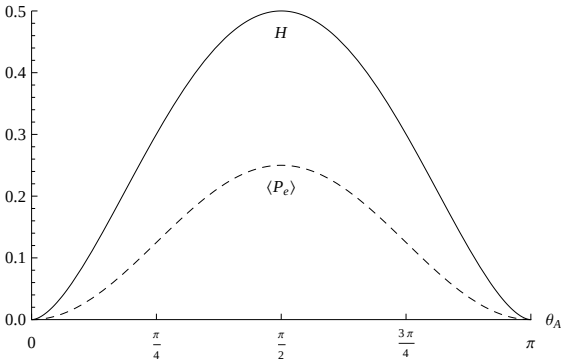

Fig. 2. Alice's and Bob's Shannon entropy H and the according average error probability $\langle P_e\rangle$ if either Alice or Bob applies a basis transformation.

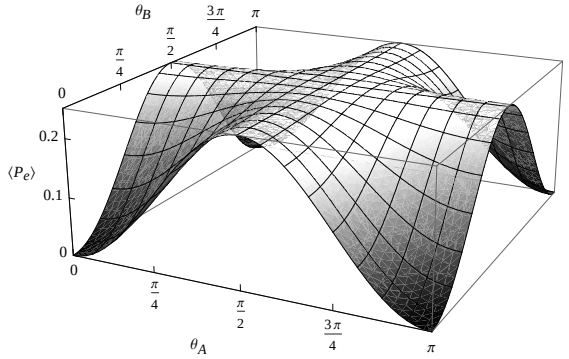

Fig. 3. Eve's expected error probability $\langle P_e \rangle$ if both parties apply a basis transformation with the respective angles θ_A and θ_B.

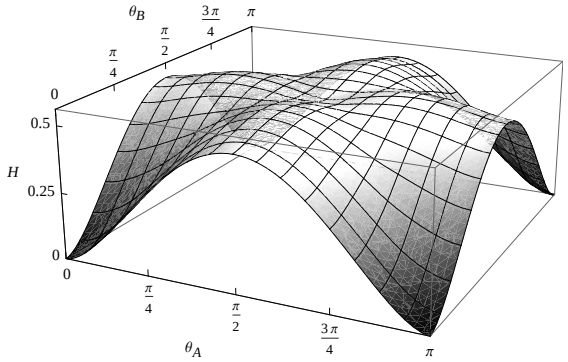

Fig. 4. Alice's and Bob's Shannon entropy H if both parties apply a basis transformation with the respective angles θ_A and θ_B.

where $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy. Looking at $\langle P_e \rangle$ and H in Figure 2 we see that the optimal angle for a single basis transformation is $\pi/2$, i.e., the Hadamard operation, for protocols using only one basis transformation, as it is already known from literature [15], [2], [1]. In this case, the average error probability as well as the Shannon entropy are maximal at $\langle P_e \rangle = 0.25$ and $H = 0.5$ (cf. Figure 2). If only Bob applies the basis transformation, the calculations run analogous and therefore provide the same results. Further, Eve's information on the bits of the secret key is given by the mutual information

$$I_{AE} = 1 - H = 1 - \frac{1}{2} = \frac{1}{2} \tag{13}$$

which means that Eve has 0.5 bits of information on every bit of the secret key. Using error correction and privacy amplification Eve's information can be brought below 1 bit of the whole secret key as long as the error rate is below $\sim 11\%$ [13]. This is more or less the standard threshold value for the prepare and measure QKD protocols.

C. Application of Combined Transformations

When both Alice and Bob apply their respective basis transformation, the overall state changes to

$$|\delta'\rangle = T_x^{(1)}(\theta_A) T_x^{(4)}(\theta_B) |\delta\rangle_{1QR4TU} \tag{14}$$

and after Alice's Bell state measurement on qubits 1 and R and Bob's application of $T_x(\theta_B)$ on qubit Q the state of the remaining qubits is

$$\begin{aligned} &\cos^2 \frac{\theta_A - \theta_B}{2} \, |\Phi^+\rangle_{Q4} |\varphi_1\rangle_{TU} \\ &+ \sin^2 \frac{\theta_A - \theta_B}{2} \, |\Phi^+\rangle_{Q4} |\varphi_4\rangle_{TU} \\ &- \frac{\sin\big(\theta_A - \theta_B\big)}{2} \, |\Psi^-\rangle_{Q4} \Big(|\varphi_1\rangle_{TU} - |\varphi_4\rangle_{TU} \Big) \end{aligned} \tag{15}$$

Consequently, Bob obtains a correlated result with probability $(3 + \cos(2\theta_A - 2\theta_B))/4$ and, following the argumentation from scenario described in Section III-B above, this yields an average error probability (cf. Figure 3 for a plot of this function)

$$\begin{aligned} \langle P_e \rangle = &\frac{1}{8} \sin^2 \theta_A + \frac{1}{8} \sin^2 \theta_B \\ &+ \frac{1}{16} \sin^2\big(\theta_A + \theta_B\big) + \frac{1}{16} \sin^2\big(\theta_A - \theta_B\big) \end{aligned} \tag{16}$$

When the results are correlated Eve obtains either $|\varphi_1\rangle_{TU}$ or $|\varphi_4\rangle_{TU}$, as it is easy to see from eq. (15). Hence, Eve's information on the Alice's and Bob's result is lower compared to the first scenario, i.e., Alice's and Bob's Shannon entropy is higher:

$$\begin{aligned} H = &\frac{1}{4} \, h\Big(\cos^2 \frac{\theta_A}{2}\Big) + \frac{1}{4} \, h\Big(\cos^2 \frac{\theta_B}{2}\Big) \\ &+ \frac{1}{8} \, h\Big(\cos^2 \frac{\theta_A + \theta_B}{2}\Big) + \frac{1}{8} \, h\Big(\cos^2 \frac{\theta_A - \theta_B}{2}\Big) \end{aligned} \tag{17}$$

This is due to the fact that it is more difficult for Eve to react on two separate basis transformations with different angles θ_A and θ_B. Taking the optimal choice for only one basis transformation, i.e., the Hadamard operation, we see that if both parties apply the Hadamard operation at the same time the operations cancel out each other. Hence, the angles θ_A and θ_B have to be different. As we can further see from Figure 4, the Shannon entropy for a combined application of basis transformations is much higher than 0.5 for some regions. In detail, the maximum of the function plotted in Figure 4 is

$$H \sim 0.55 \quad \text{and thus} \quad I_{AE} \sim 0.45 \tag{18}$$

for $\theta_A = \pi/4$ and $\theta_B = \pi/2$ or vice versa. Hence, if just one of the parties applies a Hadamard operation and the other one a transformation about an angle of $\pi/4$, Eve's mutual information is about 10% lower compared to the application of a single basis transformation (cf. eq. (13)). At the same time we see from Figure 3 that for these two values of θ_A and θ_B the error probability is still maximal with $\langle P_e \rangle = 0.25$. This means Alice and Bob are able to further increase the security by the combined application of two basis transformations, one about $\theta = \pi/2$ and the other about $\theta = \pi/4$.

IV. Application on the BBM Protocol

In 1992, Bennett, Brassard, and Mermin presented a variant of the Ekert protocol [4], where they show that a test of the CHSH-inequalities [22] is not necessary for the security of the protocol [5]. Instead of the CHSH-inequalities, Alice and Bob use two complementary measurement bases as in the BB84 protocol [3] and randomly apply them on the received qubits. Due to the entangled state Alice and Bob obtain perfectly correlated results from their measurement if no adversary is present.

A. Protocol Description

In detail, Alice and Bob use a source emitting maximally entangled qubit pairs, e.g., in the Bell-state $|\Psi^-\rangle_{12}$. This source is located between Alice and Bob and one qubit of the state is flying to Alice and the other one to Bob. When looking at physical implementations of the BBM protocol the source is usually located at the laboratory of one of the communication parties. Hence, we will assume that the source is located at Alice's lab and she sends the second qubit of each pair to Bob (cf. Figure 5). After receiving the qubit, both communication parties randomly and independently choose either the Z- or the X-basis to measure their qubit. Due to the entanglement of the qubits in the state $|\Psi^-\rangle_{12}$ Alice's measurement completely determines the state of Bob's qubit, i.e., if Alice measures a $|1\rangle$, Bob's qubit is in the state $|0\rangle$, and vice versa. If he measures in a different basis than Alice, Bob destroys the information carried by the qubit and thus will not obtain a correlated result. To identify where they used different bases both parties publicly compare all of their measurement bases and discard the results where they had chosen differently. The remaining results should be perfectly correlated and the communication parties compare a randomly selected fraction in public. If there is too much discrepancy between their results they have to assume that an adversary is present and they start over the protocol. It has also been shown by Bennett et al. in this paper that the security of this version of the protocol is equal to the security of the BB84 scheme [5].

The random measurement in either the Z- and X-basis can also be interpreted as a random application of the Hadamard operation by Alice. As pointed out above, the Hadamard operation is a complete basis transformation from the Z- into the X-basis, i.e., by an angle $\theta_A = \pi/2$. Therefore, it can be said that both Alice and Bob randomly apply the Hadamard operation on the qubits they receive and measure it in the Z-basis afterwards. In the end, both parties compare in public where they used the Hadamard operation and similar to the original protocol they discard the results where only one of them applied the Hadamard operation.

B. Security Analysis

Looking at this interpretation we want to discuss whether the Hadamard operation is optimal in this scenario. Therefore, we will discuss the information an eavesdropper Eve is able to obtain when performing a simulation attack. Further, we assume that Alice and Bob are not limited to the Hadamard operation but they use a general basis transformation $T_x(\theta_A)$.

Fig. 5. Illustration of the BBM protocol [5]. Here, Alice performs a measurement in the Z-basis.

To fit to the setting of the BBM protocol the adversary Eve has to prepare a slightly different $|\delta\rangle$ for the simulation attack, i.e.,

$$|\delta\rangle_{RST} = \frac{1}{\sqrt{2}}\Big(|0\rangle|1\rangle|\varphi_1\rangle + |1\rangle|0\rangle|\varphi_2\rangle\Big)_{RST} \tag{19}$$

This state perfectly simulates the correlation between Alice's and Bob's result in case they do not apply any operation. As described above, the auxiliary states $|\varphi_1\rangle$ and $|\varphi_2\rangle$ have to be orthogonal (cf. eq. (3)) such that they can be distinguished by Eve. For reasons of simplicity, we will assume that Eve intercepts the qubits coming from Alice and uses entanglement swapping on qubits 2 and R to establish the state $|\delta\rangle_{1ST}$ between Alice and Bob, where Bob is now in possession of qubit S.

Following the protocol Alice and Bob randomly perform the basis transformation $T_x(\theta_A)$ on their respective qubits 1 and S. Since they discard all results where just one of them applies $T_x(\theta_A)$ we are only interested in two scenarios: either none or both of them perform $T_x(\theta_A)$. In scenario one, it is easy to see from the structure of the state $|\delta\rangle_{1ST}$ that Eve's qubits are in the state $|\varphi_1\rangle_T$ whenever Alice obtains $|0\rangle$ and in the state $|\varphi_2\rangle_T$ whenever Alice obtains $|1\rangle$. In this case Eve is able to perfectly eavesdrop the respective raw key bits.

In the second scenario, the application of the basis transformation $T_x(\theta_A)$ on qubits 1 and S changes the overall state to

$$|\delta'\rangle = T_x(\theta_A)^{(1)}|\delta\rangle_{1ST}, \tag{20}$$

where the superscript "(1)" denotes an application on qubit 1. This results in the state

$$\begin{aligned}\frac{1}{\sqrt{2}}\Bigg(&\sin\frac{\theta_A}{2}\Big(|00\rangle|\varphi_2\rangle + |11\rangle|\varphi_1\rangle\Big)\\ &+\cos\frac{\theta_A}{2}\Big(|01\rangle|\varphi_1\rangle - |10\rangle|\varphi_2\rangle\Big)\Bigg)\end{aligned} \tag{21}$$

before Alice performs her measurement on qubit 1. Assuming Alice obtains $|0\rangle_1$ from her measurement and Bob applies $T_x(\theta_A)$ on qubit S this changes the state described in the previous equation into

$$\begin{aligned}&\frac{\sin\theta_A}{2}\,|0\rangle_S|\varphi_1\rangle_T + \frac{\sin\theta_A}{2}\,|0\rangle_S|\varphi_2\rangle_T\\ &-\cos^2\frac{\theta_A}{2}\,|1\rangle_S|\varphi_1\rangle_T + \sin^2\frac{\theta_A}{2}\,|1\rangle_S|\varphi_2\rangle_T\end{aligned} \tag{22}$$

From this expression we can directly see that Bob obtains from his Bell state measurement either the correlated result

$|1\rangle_S$ with probability

$$\left(\cos^2\frac{\theta_A}{2}\right)^2 + \left(\sin^2\frac{\theta_A}{2}\right)^2 = \frac{3+\cos(2\theta_A)}{4} \qquad (23)$$

or an error, i.e., the state $|0\rangle_S$, otherwise. Hence, Eve introduces an error with probability $(\sin^2\theta_A)/2$, which yields an expected error probability

$$\langle P_e\rangle = \frac{\sin^2\theta_A}{4} \qquad (24)$$

These are the same results as described in Section III-B above (cf. eq. (10)). Accordingly, performing the same computations as above, we obtain the mutual information I_{AE}, i.e., the information Eve is able to obtain about the raw key, as

$$I_{AE} = 1 - H = 1 - \frac{1}{2}\,h\Big(\cos^2\frac{\theta_A}{2}\Big) \qquad (25)$$

which is equal to the general result in eq. (13) from Section III-B. Hence, we can conclude that for the BBM protocol the optimal choice is a basis transformation about an angle $\theta_A = \frac{\pi}{2}$, i.e., the Hadamard operation.

V. Application on Song's QKD Protocol

In 2004, Song published a QKD scheme based on entanglement swapping, which is supposed to spare alternative measurements [17]. In this scheme Song uses a rather unusual basis transformation (compared to the Hadamard operation most commonly used in other protocols) with $\theta = 2\pi/3$. Hence, based on the discussions in the previous sections it is indicated that the security of the protocol can be further increased by using a different angle θ.

A. Protocol Description

In each round of the protocol, Alice and Bob prepare two qubits in their laboratories, which are either in the Bell basis or in a transformed basis. The transformation is done by the operation $T = T_x(2\pi/3)$, which is denoted in matrix form as

$$T = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \qquad (26)$$

Alice and Bob prepare random Bell states and then randomly choose between applying $\mathbb{1}$ or T onto qubit 2 and 4, respectively, in their possession. The application of T changes $|\Phi^\pm\rangle$ to $|\eta^\pm\rangle$ and $|\Psi^\pm\rangle$ to $|\nu^\pm\rangle$, where the state in the alternative basis are denoted as

$$\begin{aligned} |\eta^\pm\rangle &= \frac{1}{2}|\Phi^\mp\rangle + \frac{\sqrt{3}}{2}|\Psi^\pm\rangle \\ |\nu^\pm\rangle &= \frac{\sqrt{3}}{2}|\Phi^\pm\rangle - \frac{1}{2}|\Psi^\mp\rangle. \end{aligned} \qquad (27)$$

For our further discussion suppose that Alice prepares $|\Psi^+\rangle_{12}$ and Bob prepares $|\Phi^-\rangle_{34}$. Additionally, Bob applies T onto qubit 4 such that $|\Phi^-\rangle_{34}$ is changed into $|\eta^-\rangle_{34}$ (cf. (1) and (2) in Figure 6). The two parties exchange qubits 2 and 4 and publicly confirm the arrival of the respective qubit.

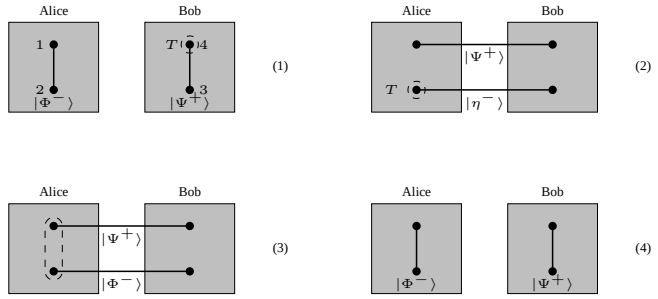

Fig. 6. Illustration of the protocol presented by Song [17]. Here, only Bob applies the basis transformation onto his qubit.

Before measuring, Alice and Bob announce publicly whether they applied the basis transformation T or not. If one party performed the basis transformation, the other party reverses the transformation by applying T onto the received qubit. In our case Alice applies T on qubit 4 (cf. (2) in Figure 6). Then, both parties perform Bell state measurements on the qubits in their possession. Based on their own outcome of the Bell state measurement both parties can compute each other's result. Following our example, if Alice obtains $|\Phi^-\rangle_{14}$, Bob obtains $|\Psi^+\rangle_{23}$.

B. Security Analysis

Song discussed a basic version of an intercept-resend attack as well as the ZLG attack [23] in his article [17] and showed in principle that the protocol is secure against this kind of attack. Nevertheless, he gave no expected error rate or mutual information for Eve, which would be of great interest since the operation T is an unusual basis transformation by an angle of $2\pi/3$ and is different from the more common choice of the Hadamard operation. Hence, we are going to look at these values in detail in the next paragraphs.

Due to arguments discussed in Section III above, we can immediately show that Song's protocol is completely open to the simulation attack when Alice does not apply the transformation T. In this case, Alice and Bob just perform the entanglement swapping and Eve can intercept qubits 2 and 4 in transit. As it is described in detail above, Eve distributes the state $|\delta\rangle$ from eq. (2) between Alice, Bob and herself using entanglement swapping and sends qubits Q to Bob and S to Alice, respectively (cf. (1) in Figure 7). When Alice and Bob perform their Bell state measurements, the correlation between their results is preserved due to the structure of the state $|\delta\rangle$. After Alice and Bob are finished Eve is able to obtain full information about Alice's and Bob's secret measurement based on the state of qubits T and U in her possession.

If either Alice or Bob performs the transformation T, we have the scenario described in Section III. Eve is not able to compensate the random application of the transformation while still preserving the correlation when T is not applied. Hence, Eve's intervention introduces an error, i.e., the parties do not obtain correlated results all the time. Taking the example from Section III above, Bob applies T onto qubit 4 and therefore Alice also applies T onto qubit S she receives from

Eve (cf. (2) in Figure 7). When Alice obtains $|\Phi^-\rangle_{1S}$ from her measurement Bob obtains the correlated result $|\Psi^+\rangle_{23}$ only with probability $5/8$. In other words, Eve introduces an error with probability $3/8$, which leads to an expected error probability for this scenario of

$$\langle P_e \rangle = \frac{1}{4} \sin^2 \frac{2\pi}{3} = \frac{3}{16} \tag{28}$$

which is significantly lower than $1/4$. Hence, Eve has a better opportunity to eavesdrop the key in this protocol than, for example, in the revised version of the Cabello protocol [15] or the protocol by Li et al [18]. Due to the fact that the transformation T maps onto an unbiased superposition of states (cf. eq. (27) above) Eve is able to extract more information than usual from her attack strategy. The Shannon entropy for the simulation attack on Song's protocol is

$$H = \frac{1}{2}\, h\Big(\cos^2 \frac{\pi}{3}\Big) = \frac{1}{8}\Big(2 + 3 \log \frac{4}{3}\Big) \tag{29}$$

which further leads to Eve's mutual information

$$I_{AE} = 1 - H\big(S|M\big) \simeq 0.594 \tag{30}$$

Assuming that both parties perform the basis transformation T the protocol becomes insecure again. Due to Eve's entanglement swapping the operation T is brought from qubits 2 and 4 onto qubits 1 and 3, which leads to the state

$$T^{(1)} T^{(3)} |\delta\rangle_{1Q3STU} \tag{31}$$

When Alice and Bob apply the basis transformation T on qubits Q and S they receive from Eve, the state changes again into

$$T^{(1)} T^{(Q)} T^{(3)} T^{(S)} |\delta\rangle_{1Q3STU} \tag{32}$$

When Alice performs her Bell state measurement onto qubits 1 and S, it has the effect that the operations $T^{(1)}$ and $T^{(S)}$ are swapped onto qubits Q and 3 thus reverting the effect of T at Bob's side and re-establishing the state $|\delta\rangle$. Hence, Bob's measurement on qubits Q and 3 results into a state completely correlated to Alice's result. Further, Eve's qubits T and U are also correlated to Bob's result such that she has full information about the key when Alice and Bob announce their initial states.

The expected error probability from eq. (28) as well as the mutual information from eq. (30) indicate that the choice of $T = T_x(2\pi/3)$ is not optimal. Looking at Section III-B and eq. (10) and eq. (13) therein, we see that a basis rotation about an angle $\pi/2$, i.e., the Hadamard, instead of the operation T increases the expected error probability by $\simeq 33\%$ to $\langle P_e \rangle = 0.25$ and at the same time decreases the mutual information by $\simeq 16\%$ to $I_{AE} = 0.5$. Alternatively, a combined application of two basis transformations $T_x(\pi/2)$ and $T_x(\pi/4)$ by Alice and Bob further decreases the mutual information I_{AE}. As described in Section III-C two different basis rotations, randomly applied by Alice and Bob, leave the expected error probability $\langle P_e \rangle = 0.25$ but reduces Eve's information about the raw key by almost 25% to $I_{AE} = \simeq 0.45$ compared to the single application of T.

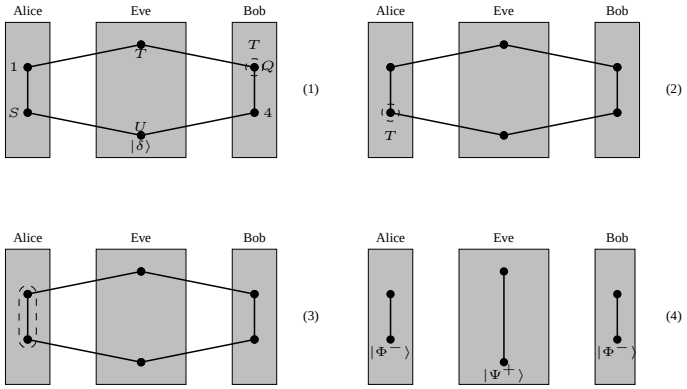

Fig. 7. Illustration of the simulation attack strategy on the protocol presented in [17]. Here, only Bob applies the basis transformation T onto qubit Q in his possession.

VI. Application on Cabello's QSS Protocol

In the year 2000, Cabello described a QSS protocol based on entanglement swapping [16]. The idea is to share a classical key between two parties, Bob and Charlie, such that they can communicate with Alice only if they collaborate and bring their shares together. The entanglement between the three parties is realized using a maximally entangled 3-qubit state, i.e., a GHZ state [24]. In our further discussions we will denote the GHZ states as

$$\begin{aligned}
|P_{00}^{\pm}\rangle &= \frac{1}{\sqrt{2}}\Big(|000\rangle \pm |111\rangle\Big) \\
|P_{01}^{\pm}\rangle &= \frac{1}{\sqrt{2}}\Big(|001\rangle \pm |110\rangle\Big) \\
|P_{10}^{\pm}\rangle &= \frac{1}{\sqrt{2}}\Big(|010\rangle \pm |110\rangle\Big) \\
|P_{11}^{\pm}\rangle &= \frac{1}{\sqrt{2}}\Big(|011\rangle \pm |100\rangle\Big)
\end{aligned} \tag{33}$$

The security of this protocol against the ZLG attack [23] has already been discussed by Lee, Lee, Kim, and Oh in [25]. They presented an adaption of the ZLG attack strategy, where the adversary Eve entangles herself with both Bob and Charlie using two Bell states. By intercepting the qubits coming from Alice and forwarding qubits from her Bell states, Eve is able to obtain Bob's and Charlie's secret measurement results. According to these results Eve is able to alter Alice's intercepted qubits such that her intervention is not detected.

In addition to their security analysis, Lee, Lee, Kim, and Oh presented a revised version of the protocol in [25], which includes the random application of Hadamard operation at Bob's and Charlie's laboratory. In the following paragraphs we are going to describe, how the simulation attack works on this protocol and whether the Hadamard operation is optimal in this context. We are going to show that using the simulation attack strategy the protocol is open to an attack to stress the fact that it is also applicable on QSS protocols.

TABLE I. ALICE'S GHZ STATE AFTER BOB'S AND CHARLIE'S MEASUREMENT.

	$\|\Phi^+\rangle_{4A}$	$\|\Phi^-\rangle_{4A}$	$\|\Psi^+\rangle_{4A}$	$\|\Psi^-\rangle_{4A}$
$\|\Phi^+\rangle_{5B}$	$\|P^+_{00}\rangle_{1CD}$	$\|P^-_{00}\rangle_{1CD}$	$\|P^+_{10}\rangle_{1CD}$	$\|P^-_{10}\rangle_{1CD}$
$\|\Phi^-\rangle_{5B}$	$\|P^-_{00}\rangle_{1CD}$	$\|P^+_{00}\rangle_{1CD}$	$\|P^-_{10}\rangle_{1CD}$	$\|P^+_{10}\rangle_{1CD}$
$\|\Psi^+\rangle_{5B}$	$\|P^+_{01}\rangle_{1CD}$	$\|P^-_{01}\rangle_{1CD}$	$\|P^+_{11}\rangle_{1CD}$	$\|P^-_{11}\rangle_{1CD}$
$\|\Psi^-\rangle_{5B}$	$\|P^-_{01}\rangle_{1CD}$	$\|P^+_{01}\rangle_{1CD}$	$\|P^-_{11}\rangle_{1CD}$	$\|P^+_{11}\rangle_{1CD}$

A. Protocol Description

As already pointed out in the previous paragraph the original protocol by Cabello [16] is not secure and thus we will discuss the revised version given in [25] here. The revised version in general uses the Quantum Fourier Transformation (QFT) defined as

$$|j\rangle \overset{QFT}{\longmapsto} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\Pi ijk/N} |k\rangle \tag{34}$$

to secure the qubits in transit (cf. for example [26] for details on the QFT). Since we are using qubits, the dimension $N = 2$ and the QFT reduces to the Hadamard operation for this special case. Therefore, we will use the Hadamard operation in the following considerations.

In this protocol, three parties are involved, which are able to distribute a key among them or share a secret between two of them. The aim is to use the 3-qubit entanglement of the GHZ state to achieve these tasks. Therefore, Alice, Bob, and Charlie are in possession of an entangled pair, i.e., $|\Phi^+\rangle_{12}$, $|\Phi^+\rangle_{4C}$, and $|\Phi^+\rangle_{5D}$, respectively. Further, Alice generates the GHZ state $|P^+_{00}\rangle_{3AB}$ at her side. She keeps qubit 3 of the GHZ state and sends qubits A and B to Bob and Charlie, respectively. At the same time, Bob and Charlie send their respective qubits C and D to Alice (cf. (1) in Figure 8). Additionally, Bob and Charlie randomly apply the Hadamard operation on qubits 4 and 5 still in their possession. After Alice received the qubits from Bob and Charlie she performs a Bell state measurement on qubits 2 and 3 and Bob and Charlie act similarly on their qubits 4 and A as well as 5 and B, respectively (cf. (2) in Figure 8). If both Bob and Charlie do not apply the Hadamard operation, the protocol is the same as in the original version by Cabello [16]. If either of them applies the Hadamard operation onto his qubit the GHZ state after Bob's measurement is altered as

$$\begin{aligned}\frac{1}{2}\Big(&|\Phi^+\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P^-_{00}\rangle + |P^+_{10}\rangle\big)_{1CB}\\ &+|\Phi^-\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P^+_{00}\rangle + |P^-_{10}\rangle\big)_{1CB}\\ &+|\Psi^+\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P^-_{00}\rangle - |P^+_{10}\rangle\big)_{1CB}\\ &-|\Psi^-\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P^+_{00}\rangle - |P^-_{10}\rangle\big)_{1CB}\Big)\end{aligned} \tag{35}$$

and similarly for Charlie's measurement (in this case the GHZ state changes to either $|P^{\pm}_{00}\rangle$ or $|P^{\pm}_{01}\rangle$). In case both parties

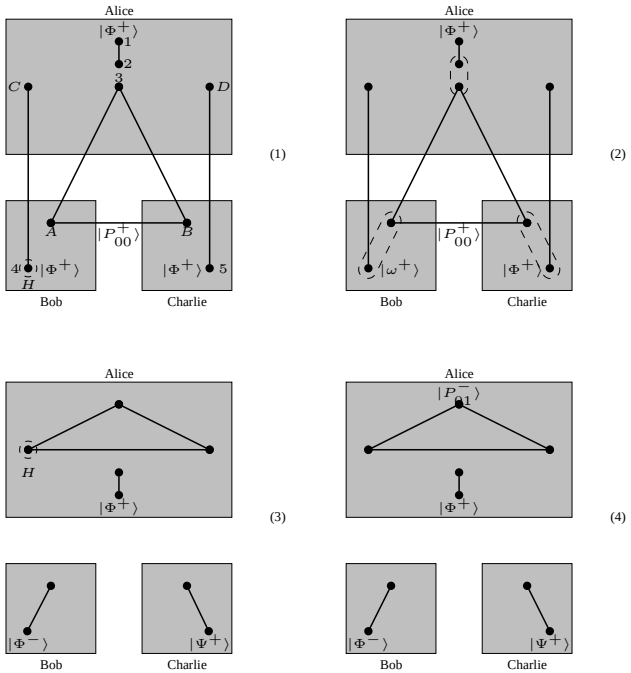

Fig. 8. Illustration of the QSS scheme described in [25].

apply the Hadamard operation the GHZ state changes into

$$\begin{aligned}\frac{1}{2}\Big(&|\Phi^+\rangle_{5B}\frac{1}{2}\big(|P^+_{00}\rangle + |P^-_{01}\rangle + |P^-_{10}\rangle + |P^+_{11}\rangle\big)_{1CD}\\ &+|\Phi^-\rangle_{5B}\frac{1}{2}\big(|P^-_{00}\rangle + |P^+_{01}\rangle + |P^+_{10}\rangle + |P^-_{11}\rangle\big)_{1CD}\\ &+|\Psi^+\rangle_{5B}\frac{1}{2}\big(|P^-_{00}\rangle - |P^+_{01}\rangle + |P^+_{10}\rangle - |P^-_{11}\rangle\big)_{1CD}\\ &-|\Psi^-\rangle_{5B}\frac{1}{2}\big(|P^+_{00}\rangle + |P^-_{01}\rangle - |P^-_{10}\rangle + |P^+_{11}\rangle\big)_{1CD}\Big)\end{aligned} \tag{36}$$

if Bob obtained $|\Phi^+\rangle_{4A}$ and equivalently for $|\Phi^-\rangle_{4A}$ and $|\Psi^{\pm}\rangle_{4A}$. Then, Bob and Charlie publicly announce their decision and Alice performs the Hadamard operation on the qubits she received from Bob and Charlie according to their decision (cf. (3) and (4) in Figure 8). Alice's Hadamard operation brings the GHZ state back to the state corresponding to the correlation described in Table I.

B. Security Analysis

Also in this case the strategy of the simulation attack is to find a state, which simulates the correlations given in Table I and provides Eve with additional information about Bob's and Charlie's measurement results. The version of the state $|\delta\rangle$ given in eq. (2) would be a possible choice, but not a very good one. A better version for $|\delta\rangle$ is

$$\begin{aligned}|\delta\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle|\varphi_1\rangle|\delta_1\rangle\big) + |\Phi^-\rangle|\varphi_2\rangle|\delta_2\rangle\big)\\ &+|\Psi^+\rangle|\varphi_3\rangle|\delta_3\rangle\big) + |\Psi^-\rangle|\varphi_4\rangle|\delta_4\rangle\big)\Big)_{E_1-E_{11}}\end{aligned} \tag{37}$$

where $|\delta_1\rangle$ - $|\delta_4\rangle$ are defined as

$$\begin{aligned}
|\delta_1\rangle &= \frac{1}{2}\big(|\Phi^+\rangle|\varphi_5\rangle|P_{00}^+\rangle + |\Phi^-\rangle|\varphi_6\rangle|P_{00}^-\rangle \\
&\quad |\Psi^+\rangle|\varphi_7\rangle|P_{01}^+\rangle + |\Psi^-\rangle|\varphi_8\rangle|P_{01}^-\rangle\big) \\
|\delta_2\rangle &= \frac{1}{2}\big(|\Phi^+\rangle|\varphi_5\rangle|P_{00}^-\rangle + |\Phi^-\rangle|\varphi_6\rangle|P_{00}^+\rangle \\
&\quad +|\Psi^+\rangle|\varphi_7\rangle|P_{01}^-\rangle + |\Psi^-\rangle|\varphi_8\rangle|P_{01}^+\rangle\big) \\
|\delta_3\rangle &= \frac{1}{2}\big(|\Phi^+\rangle|\varphi_5\rangle|P_{10}^+\rangle + |\Phi^-\rangle|\varphi_6\rangle|P_{10}^-\rangle \\
&\quad +|\Psi^+\rangle|\varphi_7\rangle|P_{11}^+\rangle + |\Psi^-\rangle|\varphi_8\rangle|P_{11}^-\rangle\big) \\
|\delta_4\rangle &= \frac{1}{2}\big(|\Phi^+\rangle|\varphi_5\rangle|P_{10}^-\rangle + |\Phi^-\rangle|\varphi_6\rangle|P_{10}^+\rangle \\
&\quad +|\Psi^+\rangle|\varphi_7\rangle|P_{11}^-\rangle + |\Psi^-\rangle|\varphi_8\rangle|P_{11}^+\rangle\big)
\end{aligned} \tag{38}$$

Similarly to the auxiliary systems defined in Section II the states $|\varphi_1\rangle$ to $|\varphi_8\rangle$ have to fulfill

$$\begin{aligned}
\langle\varphi_i|\varphi_j\rangle &= 0 \qquad i,j \in \{1,...,4\} \;\; i \neq j \qquad \text{and} \\
\langle\varphi_i|\varphi_j\rangle &= 0 \qquad i,j \in \{5,...,8\} \;\; i \neq j
\end{aligned} \tag{39}$$

For reasons of simplicity we will assume that the states $|\varphi_i\rangle$ are 2-qubit states, since they are the smallest states fulfilling the equation above. Based on that, it can be immediately verified that this state simulates all possible correlations from Table I and that the qubit pairs E_3, E_4 and E_7, E_8 can be used to obtain full information about Bob's and Charlie's measurement results.

Focusing on an external adversary Eve, we assume again that she is able to distribute the state $|\delta\rangle$ between Alice, Bob, and Charlie using entanglement swapping. This means, Eve prepares the state $|\delta\rangle$ from eq. (37) and intercepts qubits A and B coming from Alice and performs a GHZ state measurement on them together with qubit E_9 (cf. (1) in Figure 9). Further, she intercepts qubits C and D coming from Bob and Charlie, respectively, and performs a Bell state measurement on the pairs E_1, C as well as E_5, D. Eve sends qubits E_2 to Bob, E_6 to Charlie and qubits E_{10} and E_{11} to Alice such that the state $|\delta\rangle$ is now distributed between all 4 parties. The definition of $|\delta\rangle$ indicates that Bob's and Charlie's measurements on the qubits in their possession yield random results but the respective qubits still in Eve's possession are in the same state, afterwards (cf. (3) in Figure 9). Additionally, the three qubits 3, E_{10} and E_{11} at Alice's laboratory are always in a correlated state to Bob's and Charlie's results. Assuming again that Bob obtained $|\Psi^+\rangle_{4E_2}$ and Charlie obtained $|\Phi^-\rangle_{5E_6}$, qubits 3, E_{10} and E_{11} are in the state $|P_{10}^-\rangle$, which corresponds to the state Alice expects to find if she obtains $|\Phi^+\rangle_{23}$ (cf. (4) in Figure 9 and also Table I). Also Alice's secret measurement on qubits 2 and 3 does not leave these three qubits in a state violating the expected correlation since her measurement changes the GHZ state accordingly.

In the revised version of Cabello's protocol, Bob and Charlie randomly apply a Hadamard operation on one qubit in their possession, which is not taken into account in the considerations above. If Bob applies the Hadamard operation on his qubit 4, the overall state $|\delta\rangle$ introduced by Eve described in eq. (37) above changes into

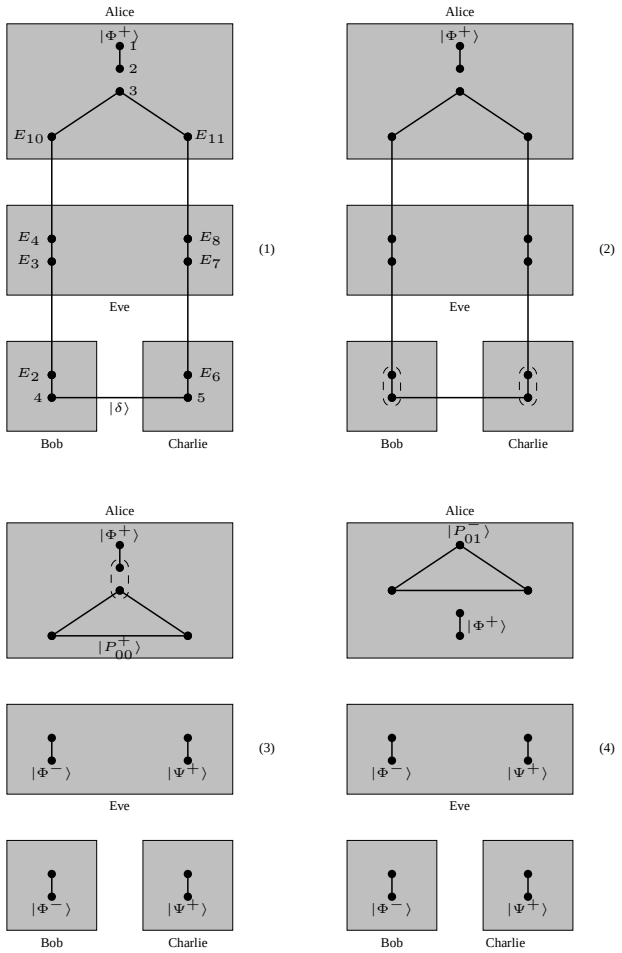

Fig. 9. Illustration of the simulation attack on the QSS scheme described in [25]. Here, no basis transformation is applied.

$$\begin{aligned}
\frac{1}{2\sqrt{2}}\Big(&|\Phi^+\rangle\Big(|\varphi_2\rangle|\delta_2\rangle + |\varphi_3\rangle|\delta_3\rangle\Big) \\
&+|\Phi^-\rangle\Big(|\varphi_1\rangle|\delta_1\rangle - |\varphi_4\rangle|\delta_4\rangle\Big) \\
&+|\Psi^+\rangle\Big(|\varphi_1\rangle|\delta_1\rangle + |\varphi_4\rangle|\delta_4\rangle\Big) \\
&-|\Psi^-\rangle\Big(|\varphi_2\rangle|\delta_2\rangle - |\varphi_3\rangle|\delta_3\rangle\Big)\Big)_{E_1-E_{11}}
\end{aligned} \tag{40}$$

and similarly for Charlie's Hadamard operation on qubit 5. This affects Eve's as well as Alice's measurement results such that Eve is not able to stay undetected any more.

To have a more general view on the revised protocol, we assume that Bob and Charlie are not restricted to the Hadamard operation but apply a basis transformation $T_x(\theta_B)$ and $T_x(\theta_C)$. First, assuming that only Bob applied $T_x(\theta_B)$ operation the overall state changes into

$$\sin\frac{\theta_B}{2}|\varphi_1\rangle \otimes |\delta_1\rangle + \cos\frac{\theta_B}{2}|\varphi_4\rangle \otimes |\delta_4\rangle \tag{41}$$

if Bob's result is $|\Psi^+\rangle_{4E_2}$. Hence, at this time Eve obtains from a measurement on qubits E_3 and E_4 either $|\varphi_1\rangle_{E_3E_4}$ or $|\varphi_4\rangle_{E_3E_4}$ but both do not correspond to Bob's result. Thus, the best strategy for Eve is to delay her measurement until she knows whether Bob applied the basis transformation $T_x(\theta_B)$ or not, as described below. Similarly, if just Charlie applies $T_x(\theta_C)$ the overall state after Bob's result $|\Psi^+\rangle_{4E_2}$ is

$$|\varphi_3\rangle \otimes T_x(\theta_C)|\delta_3\rangle \tag{42}$$

with

$$\begin{aligned} &T_x(\theta_C)|\delta_3\rangle = \\ &\frac{1}{2}\Big[|\Phi^+\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_6\rangle|P_{10}^-\rangle + \sin\frac{\theta_C}{2}|\varphi_7\rangle|P_{11}^+\rangle\Big) \\ &+|\Phi^-\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_5\rangle|P_{10}^+\rangle + \sin\frac{\theta_C}{2}|\varphi_8\rangle|P_{11}^-\rangle\Big) \\ &+|\Psi^+\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_8\rangle|P_{11}^-\rangle + \sin\frac{\theta_C}{2}|\varphi_5\rangle|P_{10}^+\rangle\Big) \\ &+|\Psi^-\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_7\rangle|P_{11}^+\rangle + \sin\frac{\theta_C}{2}|\varphi_6\rangle|P_{10}^-\rangle\Big)\Big] \end{aligned} \tag{43}$$

In this case, Eve obtains the same result as Bob but further on her measurement on qubits E_7E_8 yields a result uncorrelated to Charlie's measurement outcome due to his basis transformation. In the last case where both Bob and Charlie apply their basis transformations $T_x(\theta_B)$ and $T_x(\theta_C)$, respectively, the overall state changes to

$$\sin\frac{\theta_B}{2}|\varphi_1\rangle \otimes T_x(\theta_C)|\delta_1\rangle + \cos\frac{\theta_B}{2}|\varphi_4\rangle \otimes T_x(\theta_C)|\delta_4\rangle \tag{44}$$

in case Bob obtains $|\Psi^+\rangle_{4E_2}$ from his measurement. From eq. (43) above we can see that after Charlie's measurement the state of the remaining qubits is

$$\begin{aligned} &\sin\frac{\theta_B}{2}|\varphi_1\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_5\rangle|P_{00}^+\rangle + \sin\frac{\theta_C}{2}|\varphi_8\rangle|P_{01}^-\rangle\Big) \\ &+\cos\frac{\theta_B}{2}|\varphi_4\rangle\Big(\cos\frac{\theta_C}{2}|\varphi_5\rangle|P_{10}^-\rangle + \sin\frac{\theta_C}{2}|\varphi_8\rangle|P_{11}^+\rangle\Big) \end{aligned} \tag{45}$$

assuming Charlie obtains $|\Phi^-\rangle_{5E_6}$. It is described in eq. (45) that Eve's results are completely uncorrelated to the two secret results of Bob and Charlie. Thus, the optimal strategy for Eve is to delay her measurements on qubits E_3E_4 and E_7E_8 until Bob and Charlie finished their measurements and publicly announce their choice regarding the application of the Hadamard operation. Eve performs the measurement on her qubit pairs afterwards, obtaining Bob's and Charlie's result only with a certain probability.

In all three cases discussed in the previous paragraphs, Alice applies the operation $T_x(\theta_B)$ on qubits E_{10} and operation $T_x(\theta_C)$ on E_{11}, respectively, to reverse the effect of Bob's and Charlie's operations. This changes the GHZ state into a superposition of GHZ states. Hence, Alice obtains a GHZ state corresponding to Bob's and Charlie's secrets only to a certain amount. Following our example where only Bob used the Hadamard operation as described in eq. (41) we see after a little calculation that for Charlie's result $|\Phi^-\rangle_{5E_6}$ the state of the remaining qubits is

$$\begin{aligned} &\sin\frac{\theta_B}{2}|\varphi_1\rangle_{E_3E_4}|\varphi_6\rangle_{E_7E_8}|P_{00}^-\rangle_{1E_{10}E_{11}} \\ &+\cos\frac{\theta_B}{2}|\varphi_4\rangle_{E_3E_4}|\varphi_6\rangle_{E_7E_8}|P_{10}^+\rangle_{1E_{10}E_{11}} \end{aligned} \tag{46}$$

Therefore, Alice obtains the GHZ state correlated to Bob's and Charlie's result only with a certain probability. Hence, Eve's intervention introduces on average an error rate of

$$\big\langle P_e\big\rangle = \frac{1}{4}\sin^2\theta_B + \frac{1}{4}\sin^2\theta_C - \frac{1}{16}\sin^2\theta_B\sin^2\theta_C \tag{47}$$

Furthermore, Eve's results are correlated to Bob's and Charlie's results only with a certain probability such that she is not able to obtain much information about Alice's secret. In detail, the Shannon entropy for Alice, Bob, and Charlie is

$$H = \frac{7}{16}\Big(h\big(\cos^2\theta_B\big) + h\big(\cos^2\theta_C\big)\Big) \tag{48}$$

When looking at Figure 10 and Figure 11 we see that the average error probability $\big\langle P_e\big\rangle$ as well as the Shannon entropy H have their maximum when $\theta_B = \theta_C = \pi/2$, i.e., the optimal choice for the basis transformation is the Hadamard operation. In this case,

$$\big\langle P_e\big\rangle = \frac{1}{4} + \frac{1}{4} - \frac{1}{16} = \frac{7}{16} \tag{49}$$

and

$$H = \frac{7}{16}\Big(h\Big(\frac{1}{2}\Big) + h\Big(\frac{1}{2}\Big)\Big) = \frac{7}{8} \tag{50}$$

and thus both values are much larger compared to the results from previous sections. Accordingly, Eve's mutual information is rather low at

$$I_{AE} = 1 - H = \frac{1}{8} \tag{51}$$

compared to the results from above.

A scenario dealing with an adversary from the inside, i.e., Charlie as malicious party who wants to obtain Alice's secret without the help of Bob, is a more severe threat for a QSS protocol. Here, Charlie also prepares the state $|\delta\rangle$ from eq. (37) instead of his Bell state and intercepts the qubits coming from Alice and Bob. He performs a GHZ state measurement on A, B and E_9 as well as a Bell state measurement on E_1 and C to entangle himself with Alice and Bob. Then, he forwards qubits E_{10}, E_{11} to Alice and E_2 to Bob and jointly measures his qubits E_5 and E_6. We have to remark that in this case with the adversary coming from the inside, qubits E_7 and E_8 of the state $|\delta\rangle$ can be ignored since Charlie is, of course, fully aware of his own secret measurement result. Whenever Bob does not use the basis transformation $T_x(\theta_B)$ we have already seen that qubits E_3 and E_4 in Charlie's possession are perfectly correlated to Bob's result giving Charlie full information about Bob's result. We already showed that based on the structure of the state $|\delta\rangle$ the three qubits in Alice's possession are always in a GHZ state corresponding to Bob's and Charlie's secret results.

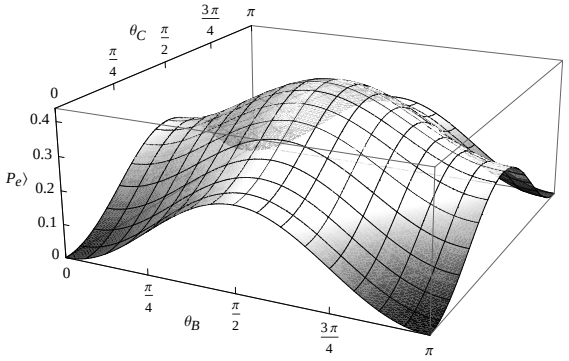

Fig. 10. Eve's expected error probability $\langle P_e \rangle$ if both parties apply a basis transformation with the respective angles θ_B and θ_C.

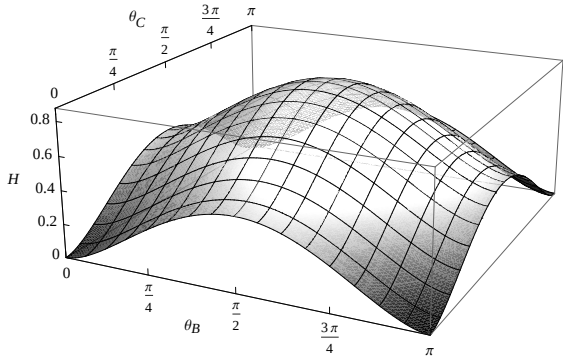

Fig. 11. Eve's Shannon entropy $\langle P_e \rangle$ if both parties apply a basis transformation with the respective angles θ_B and θ_C.

Whenever Bob chooses to use the basis transformation $T_x(\theta_B)$ the exact state of the remaining qubits is of the form described in eq. (41), if he obtained $|\Psi^+\rangle_{4E_2}$. Since Charlie is fully aware of his measurement results the scenario is equal to the attack of an external adversary if only Bob applies the basis transformation. Therefore, based on the calculations above, we see that Eve introduces an average error rate

$$\langle P_e \rangle = \frac{1}{4} \sin^2 \theta_B \tag{52}$$

similar to the probability in eq. (10) above. Hence, $\langle P_e \rangle$ becomes maximal with $\theta_B = \pi/2$ such that

$$\langle P_e \rangle = \frac{1}{4} \tag{53}$$

Accordingly, the Shannon entropy for Alice and Bob is

$$H = \frac{1}{2}\, h\Big(\cos^2 \frac{\theta_B}{2}\Big) \tag{54}$$

also taking its maximum with $\theta_B = \pi/2$ such that

$$H = \frac{1}{2}\, h\Big(\frac{1}{2}\Big) = \frac{1}{2} \tag{55}$$

leaving Eve's mutual information at

$$I_{AE} = 1 - H = 1 - \frac{1}{2} = \frac{1}{2} \tag{56}$$

which is equal to the results from the previous sections.

VII. Conclusion and Further Research

In this article, we discussed the optimality of basis transformations to secure entanglement swapping based QKD protocols. Starting from a generic entanglement swapping scenario, we used a collective attack strategy to analyze the amount of information an adversary is able to obtain. We showed that in case only one party applies a basis transformation, the operation $T_x(\theta_A)$ reduces to the Hadamard operation, i.e., the angle $\theta_A = \pi/2$ allows a maximal mutual information of $I_{AE} = 0.5$. Whereas, the main result of this article is the fact that if both parties apply a transformation, the optimal choice for the angles θ_A and θ_B describing the basis transformations is $\theta_A = \pi/4$ and $\theta_B = \pi/2$. As a consequence, this decreases the mutual information of an adversary further to $I_{AE} \sim 0.45$, which improves the security.

Additionally, we discussed 3 different protocols, the BBM protocol [5], Song's QKD protocol [17] and Cabello's QSS protocol [16] to show how the simulation attack is applied on various kinds of protocols. We showed that for the BBM protocol the optimal angle for the basis transformation is $\pi/2$, i.e., the Hadamard operation, due to the fact that no entanglement swapping is performed and a measurement on only one entangled state is applied. Nevertheless, the simulation attack describes the most general collective attack strategy on this kind of protocol.

Regarding Song's QKD protocol we were able to show that the basis transformation by an angle $2\pi/3$ is by no means optimal. Using the results from the simulation attack, the optimal choice for a basis rotation is to use two different angles $\pi/2$ and $\pi/4$ to reduce Eve's mutual information about the raw key by about 25% from 0.594 to $\simeq 0.45$ and thus increasing the security.

Looking at a QSS protocol instead of a key distribution protocol we examined the application of the simulation attack on Cabello's QSS protocol. In this case, the optimal angle for the basis transformation is again $\pi/2$, i.e., the Hadamard operation. This is true for Bob's and Charlie's basis transformation since both operations act separately on the GHZ state in Alice's possession. Nevertheless, the average error probability and Alice's, Bob's, and Charlie's Shannon entropy are rather high with $\langle P_e \rangle = 7/16$ and $H = 7/8$, respectively, for an adversary from the outside. Dealing with an adversary form the inside, i.e., a malicious Charlie, $\pi/2$ is still optimal. This reduces the average error probability and the Shannon entropy to the more common $\langle P_e \rangle = 1/4$ and $H = 1/2$, respectively, because Charlie has to cope with Bob's basis transformation alone.

The next questions arising directly from these results are how, if at all, the results change if basis transformations from the Z- into the Y-basis are applied. A first inspection shows that such basis transformations can not be plugged in directly into this framework. Hence, besides the transformation from the Z- into the Y- basis, the effects of the simpler rotation

operations on the results have to be inspected during further research. Since basis transformations can be described in terms of rotation operations it could be easier to apply rotation operations in this framework. Nevertheless, due to the similar nature of basis transformations and rotation operations it can be assumed that the results will be comparable to the results presented here.

To keep the setting as general as possible, a further main goal is to allow Alice and Bob to use arbitrary unitary operations instead of just basis transformations to secure the protocol. This should make it even more difficult for Eve to gain information about the raw key.

ACKNOWLEDGMENTS

We would like to thank Christian Kollmitzer, Oliver Maurhart as well as Beatrix Hiesmayr and Marcus Huber for fruitful discussions and interesting comments.

REFERENCES

[1] S. Schauer and M. Suda, "Security of Entanglement Swapping QKD Protocols against Collective Attacks," in *ICQNM 2012 , The Sixth International Conference on Quantum, Nano and Micro Technologies*. IARIA, 2012, pp. 60–64.

[2] ——, "A Novel Attack Strategy on Entanglement Swapping QKD Protocols," *Int. J. of Quant. Inf.*, vol. 6, no. 4, pp. 841–858, 2008.

[3] C. H. Bennett and G. Brassard, "Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*. IEEE Press, 1984, pp. 175–179.

[4] A. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography without Bell's Theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, 1992.

[6] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States," *Phys. Rev. Lett*, vol. 81, no. 14, pp. 3018–3021, 1998.

[7] A. Muller, H. Zbinden, and N. Gisin, "Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fibre," *Europhys. Lett.*, vol. 33, no. 5, pp. 335–339, 1996.

[8] A. Poppe, A. Fedrizzi, R. Usin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical Quantum Key Distribution with Polarization Entangled Photons," *Optics Express*, vol. 12, no. 16, pp. 3865–3871, 2004.

[9] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC Quantum-Key-Distribution Network in Vienna," *Int. J. of Quant. Inf.*, vol. 6, no. 2, pp. 209–218, 2008.

[10] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC Quantum Key Distribution Network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[11] N. Lütkenhaus, "Security Against Eavesdropping Attacks in Quantum Cryptography," *Phys. Rev. A*, vol. 54, no. 1, pp. 97–111, 1996.

[12] ——, "Security Against Individual Attacks for Realistic Quantum Key Distribution," *Phys. Rev. A*, vol. 61, no. 5, p. 052304, 2000.

[13] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[14] A. Cabello, "Quantum Key Distribution without Alternative Measurements," *Phys. Rev. A*, vol. 61, no. 5, p. 052312, 2000.

[15] ——, "Reply to "Comment on "Quantum Key Distribution without Alternative Measurements"","," *Phys. Rev. A*, vol. 63, no. 3, p. 036302, 2001.

[16] ——, "Multiparty Key Distribution and Secret Sharing Based on Entanglement Swapping," *quant-ph/0009025 v1*, 2000.

[17] D. Song, "Secure Key Distribution by Swapping Quantum Entanglement," *Phys. Rev. A*, vol. 69, no. 3, p. 034301, 2004.

[18] C. Li, Z. Wang, C.-F. Wu, H.-S. Song, and L. Zhou, "Certain Quantum Key Distribution achieved by using Bell States," *International Journal of Quantum Information*, vol. 4, no. 6, pp. 899–906, 2006.

[19] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[20] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Event-Ready-Detectors" Bell State Measurement via Entanglement Swapping," *Phys. Rev. Lett.*, vol. 71, no. 26, pp. 4287–4290, 1993.

[21] B. Yurke and D. Stolen, "Einstein-Podolsky-Rosen Effects from Independent Particle Sources," *Phys. Rev. Lett.*, vol. 68, no. 9, pp. 1251–1254, 1992.

[22] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Phys. Rev. Lett.*, vol. 23, no. 15, pp. 880–884, 1969.

[23] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Comment on "Quantum Key Distribution without Alternative Measurements"," *Phys. Rev. A*, vol. 63, no. 3, p. 036301, 2001.

[24] D. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's Theorem," in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, M. Kafatos, Ed. Kluwer, 1989, pp. 69–72.

[25] J. Lee, S. Lee, J. Kim, and S. D. Oh, "Entanglement Swapping Secures Multiparty Quantum Communication," *Phys. Rev. A*, vol. 70, no. 3, p. 032305, 2004.

[26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.