Security of Entanglement Swapping QKD Protocols against Collective Attacks

Stefan Schauer, Martin Suda
Department Safety and Security
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.**

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

I. Introduction

Quantum key distribution (QKD) is an important application of quantum mechanics and QKD protocols have been studied at length in theory and in practical implementations [1], [2], [3], [4], [5], [6], [7], [8]. 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 prototcols has been discussed in depth an security proofs have been given for example in [9], [10], [11]. In addition to these prepare and measure protocols, several protocols based on the phenomenon of entanglement swapping have been introduced [12], [13], [14], [15], [16]. In these protocols, entanglement swapping is used to obtain correlated measurement results between the legitimate communication parties, Alice and Bob. 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. [17], Zukowski et al. [18] as well as Yurke and Stolen [19], respectively. It provides the unique possibility to generate entanglement from particles that never interacted in the past. In detail, Alice and Bob share 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. Figure 1). Then Alice performs a complete Bell state measurement on the two qubits in her possession, which results in

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

After the measurement, 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. As presented in eq. (1) Bob always obtains the same result as Alice when performing a Bell state measurement on his qubits.

The security of QKD protocols based on entanglement swapping has been discussed on the surface so far. It has only been shown that these protocols are secure against intercept-resend attacks and basic collective attacks (cf. for example [12], [13], [15]). Therefore, we analyze a general version of a collective attack where the adversary tries to simulate the correlations between Alice and Bob [20]. 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. Hence, we analyze the security with respect to a general basis transformation about an angle θ_A applied by Alice and a transformation about an angle θ_B applied by Bob. In the course of that, we are going to identify, which values for θ_A and θ_B are optimal 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 [20]. In Section III, we discuss the security of entanglement swapping based QKD protocols agains the simulation attack. Here, we are focussing on the application of one and two basis transformations and define the optimal angles for these transformations. At the end, we summarize the results and give a short outlook on our next steps into this topic.

II. The Simulation Attack Strategy

In entanglement swapping based QKD protocols like [12], [13], [14], [15], [16] Alice and Bob rest their security check

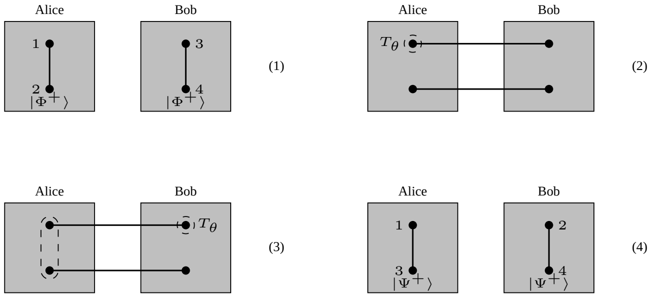

Figure 1. Illustration of a standard setup for an entanglement swapping based QKD protocol using a basis transformation T_x.

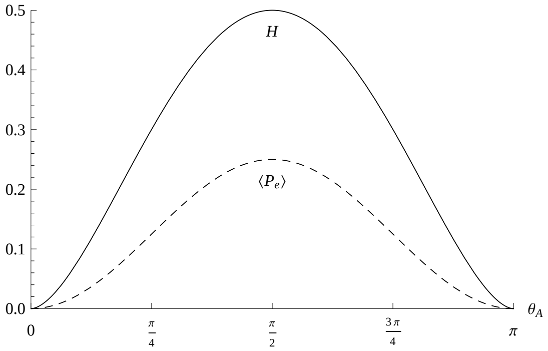

Figure 2. Alice's and Bob's Shannon entropy H and the according average error probability $\langle P_e\rangle$ if either Alice or Bob applies a basis transformation.

onto the correlations between their respective measurement results coming from the entanglement swapping (cf. eq. (1)). If these correlations are violated, Alice and Bob have to assume that an eavesdropper is present. Hence, a general version of a collective attack has the following 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. In a previous article [20], we already described such a collective attack called *simulation attack* for a specific protocol [16]. The generalization is straight forward as described in the following paragraphs. It has been pointed out in detail in [20] that Eve uses 4 qubits to simulate the correlations between Alice and Bob and she introduces additional systems, i.e., $|\varphi_i\rangle$, to distinguish between Alice's different measurement results. This leads to the state

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

which is a more general version than described in [20]. This state preserves the correlation of Alice's and Bob's measurement results coming from the entanglement swapping (cf. eq. (1)). To be able to eavesdrop Alice's and Bob's measurement results Eve has to choose the auxiliary systems $|\varphi_i\rangle$ such that

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

This allows her to perfectly distinguish between Alice's and Bob's respective measurement results and thus gives her 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 (compare eq. (1) and eq. (2)). 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 place. Nevertheless, Eve's second possibility is to intercept the qubits 2 and 3 flying from Alice to Bob and vice versa and to perform entanglement swapping to distribute the state $|\delta\rangle$. This is a straight forward method as already described in [20].

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 [15], Li et al. [16] or Cabello [12]. As already pointed out in [20], the state $|\delta\rangle$ can also be used for different initial Bell states. For protocols with a higher number of qubits the state $|\delta\rangle$ has to be extended accordingly.

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 transformations 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.,

$$T(\theta, \phi) = e^{i\phi} R_z(\phi) R_x(\theta) R_z(\phi) \tag{4}$$

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_θ. From eq. (4) we can directly see that the Hadamard operation equals T_θ for $\theta = \pi/2$. 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 (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 described in [20] 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_{θ_A} or T_{θ_B} or both transformations are applied. For all scenarios we assume that Alice applies T_{θ_A} on qubit 1 and Bob applies T_{θ_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

$$|\delta'\rangle = T^{(1)}_{\theta_A} |\delta\rangle_{1QR4TU} \tag{5}$$

where the superscript "(1)" indicates that T_{θ_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

$$\cos\frac{\theta_A}{2}\, |\Phi^-\rangle_{Q4}|\varphi_2\rangle_{TU} + \sin\frac{\theta_A}{2}\, |\Psi^+\rangle_{Q4}|\varphi_3\rangle_{TU} \tag{6}$$

assuming Alice obtained $|\Phi^+\rangle_{1R}$ (for Alice's other three possible results the state changes accordingly). This leads to the assumption 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_{θ_A} brings qubits Q, 4, T and U into the form

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

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

$$\left(\cos^2\frac{\theta_A}{2}\right)^2 + \left(\sin^2\frac{\theta_A}{2}\right)^2 = \frac{3+\cos(2\theta_A)}{4} \tag{8}$$

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

$$\langle P_e\rangle = \frac{\sin^2\theta_A}{4} \tag{9}$$

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

$$\langle P_c\rangle = \frac{1}{8}\Big(7 + \cos(2\theta_A)\Big). \tag{10}$$

This directly leads to the Shannon entropy

$$H = \frac{1}{2}\, h\Big(\cos^2\frac{\theta_A}{2}\Big) \tag{11}$$

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. If only Bob applies the basis transformation the claculations run analogous to this scenario and therefore provide the same results.

C. Application of Combined Transformations

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

$$|\delta'\rangle = T^{(1)}_{\theta_A} T^{(4)}_{\theta_B} |\delta\rangle_{1QR4TU} \tag{12}$$

and after Alice's Bell state measurement on qubits 1 and R and Bob's application of T_{θ_B} on qubit Q the state of the remaining qubits is

$$\begin{aligned} &\cos^2\frac{\theta_A-\theta_B}{2}\, |\Phi^+\rangle_{Q4}|\varphi_1\rangle_{TU} \\ &+\sin^2\frac{\theta_A-\theta_B}{2}\, |\Phi^+\rangle_{Q4}|\varphi_4\rangle_{TU} \\ &-\frac{\sin(\theta_A-\theta_B)}{2}\, |\Psi^-\rangle_{Q4}\Big(|\varphi_1\rangle_{TU} - |\varphi_4\rangle_{TU}\Big) \end{aligned} \tag{13}$$

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)

$$\langle P_e\rangle = \frac{1}{16}\Big(3 - \cos 2\theta_A - 2\cos^2\theta_A \cos 2\theta_B\Big) \tag{14}$$

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. (13). Hence, Eve's

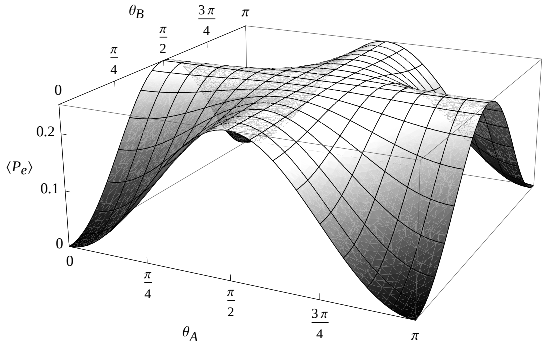

Figure 3. Eve's expected error probability $\langle P_e \rangle$ if both parties apply a basis transformation with the respective angles θ_A and θ_B.

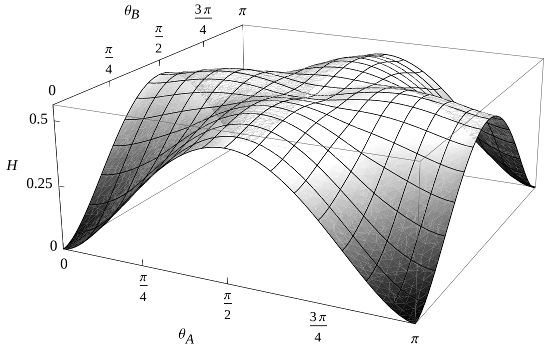

Figure 4. Alice's and Bob's Shannon entropy H if both parties apply a basis transformation with the respective angles θ_A and θ_B.

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:

$$\begin{aligned} H =& \frac{1}{4}\, h\Big(\cos^2 \frac{\theta_A}{2}\Big) + \frac{1}{4}\, h\Big(\cos^2 \frac{\theta_B}{2}\Big) \\ &+ \frac{1}{8}\, h\Big(\cos^2 \frac{\theta_A + \theta_B}{2}\Big) + \frac{1}{8}\, h\Big(\cos^2 \frac{\theta_A - \theta_B}{2}\Big) \end{aligned} \quad (15)$$

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 and is easy to see from the plot of the Shannon entropy H in Figure 4.

IV. Results

For the scenarios where either Alice or Bob applies a basis transformation at random, the optimal value for θ_A and θ_B, respectively, is $\pi/2$. Therefore, the Hadamard operation is the optimal choice in this scenario for protocols using only one basis transformation, as it is already known from literature [13], [20]. 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). Further, Eve's information on the bits of the secret key is given by the mutual information

$$I_{AE} = 1 - H = 1 - \frac{1}{2} = \frac{1}{2} \quad (16)$$

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 $\sim 11\%$ [11]. This is more or less the standard threshold value for the prepare and measure QKD protocols.

A combined application of the Hadamard operation by both parties would indicate at a first glance that the security is further increased. But when we look at Figure 4 we see that a random application of the Hadamard operation by both Alice and Bob gives the same result as the application on just one side. This is due to the fact that in case both parties apply the Hadamard operation at the same time the operations cancel out each other. But as we can further see from Figure 4, the Shannon entropy for a combined application of basis transformations is much higher for some regions. In detail, the maximum of the function plotted in Figure 4 is

$$H \sim 0.55 \quad \text{and thus} \quad I_{AE} \sim 0.45 \quad (17)$$

for $\theta_A = \pi/4$ and $\theta_B = \pi/2$ or vice versa. Hence, if just one of the parties applies a Hadadmard operation and the other one a transformation about an angle of $\pi/4$ Eve's mutual information is about 10% lower. 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 reduce Eve's information about the raw key by the combined application of two basis transformations, one about $\theta = \pi/2$ and the other about $\theta = \pi/4$.

V. Conclusion and Further Research

In this article, we discussed the optimality of basis transformations to secure entanglement swapping based QKD prototcols. Starting from a generic entanglement swapping scenario we used a collective attack strategy to analyse 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_θ reduces to the Hadamard operation, i.e., the angle $\theta = \pi/2$ allows a maximal mutual information of $I_{AE} = 0.5$. Whereas, 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 $\theta_B = \pi/2$. This decreases the mutual information of an adversary further to $I_{AE} \sim 0.45$.

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 direclty into this framework. Besides the transformation from the Z- into the Y- basis we are going to insepct the effects of the simpler rotation operations on the results. Since basis transformations can be described in terms of rotation operations it could be easier to apply rotation operations in this framework. Due to the similar nature of basis transformations and rotation operations we assume that the results will be the same as presented here.

To keep the setting as general as possible the 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] 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, pp. 175–179, 1984.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

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

[11] 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.

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

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

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

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

[16] 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.

[17] 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.

[18] 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.

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

[20] S. Schauer and M. Suda, “A Novel Attack Strategy on Entanglement Swapping QKD Protocols,” *Int. J. of Quant. Inf.*, vol. 6, no. 4, pp. 841–858, 2008.