Optimal Choice of Basis Transformations for Entanglement Swapping Based QKD Protocols

Stefan Schauer and Martin Suda

Safety and Security Department
AIT Austrian Institute of Technology GmbH
Vienna, Austria
Email: stefan.schauer@ait.ac.at, martin.suda.fl@ait.ac.at

***Abstract*—In this article, we discuss the optimality of basis transformations as a security measure for quantum key distribution protocols based on entanglement swapping. To estimate the security, we focus on the information an adversary obtains on the raw key bits from a generic version of a collective attack strategy. In the scenario described in this article, the application of general basis transformations serving as a counter measure by one or both legitimate parties is analyzed. In this context, we show that the angles, which describe these basis transformations, can be optimized compared to the application of a Hadamard operation, which is the standard basis transformation recurrently found in literature. As a main result, we show that the adversary's information can be reduced to an amount of $I_{AE} \simeq 0.20752$ when using a single basis transformation and to an amount of $I_{AE} \simeq 0.0548$ when combining two different basis transformations. This is less than half the information compared to other protocols using a Hadamard operation and thus represents an advantage regarding the security of entanglement swapping based protocols.**

Keywords–quantum key distribution; optimal basis transformations; security analysis; entanglement swapping

I. Introduction

One of the major applications of quantum mechanics is quantum key distribution (QKD). In the last three decades, QKD protocols have been studied at length in theory and in practical implementations [1]–[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 protocols has been discussed in depth and security proofs have been given for example in [9]–[11]. In addition to these prepare and measure protocols, several protocols based on the phenomenon of entanglement swapping have been introduced [12]–[17]. Entanglement swapping has been introduced by Bennett et al. [18], Zukowski et al. [19] as well as Yurke and Stolen [20], respectively. It provides the unique possibility to generate entanglement from particles that never interacted in the past. In the aforementioned 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.

A basic technique to secure a QKD protocol is to use a basis transformation, usually a Hadamard operation, to make it easier to detect an adversary. This is implemented, for example, in the prepare and measure schemes described in [1] and [3] but also in QKD schemes based on entanglement swapping (e.g., [13] [16] [21]). In this article, we analyze the application of a general basis transformation T_x, defined by the angles θ and ϕ (cf. (2)), to secure entanglement swapping based QKD protocols (cf. Figure 1). In the course of that, we are going to identify which values for θ and ϕ are optimal such that an adversary has only a minimum amount of information on the secret raw key.

Although basis transformations have been used as means of improving the security of QKD protocols based on entanglement swapping, this security measure has just 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] [16]). Therefore, we will analyze the *simulation attack*, a general version of a collective attack, which is based on the following idea [22]: 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 (cf. also Figure 2). 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. Such a multi-qubit state would be

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

where the $|\varphi_i\rangle$ are the additional systems introduced by Eve. To perfectly distinguish between Alice's and Bob's results, these state $|\varphi_i\rangle$ have to be pairwise orthogonal. 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. A detailed discussion of this attack strategy can be found in [22].

In the next section, we look in detail at the general definition of basis transformations and their effect onto Bell states and entanglement swapping. Using these definitions, we discuss in the following sections the effects on the security of entanglement swapping based QKD protocols. Therefore, we look at the application of a general basis transformation by one communication party in Section III and at the application of two different basis transformations by each of the communication parties in Section IV. In the end, we sum up the implications of the results on the security of entanglement based QKD protocols.

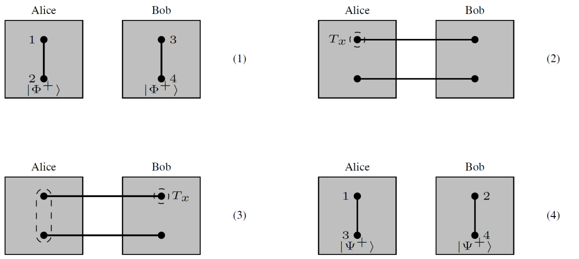

Figure 1. Sketch of a standard setup for an entanglement swapping based QKD protocol. Qubits 2 and 3 are exchanged (cf. picture (2)) and a basis transformation T_x is applied on qubit 1 and inverted by using T_x qubit 2.

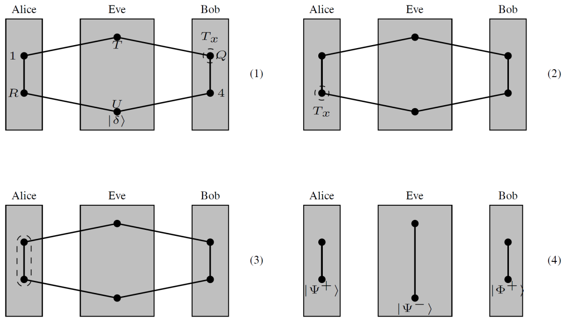

Figure 2. Illustration of the simulation attack on a standard setup for an entanglement swapping based QKD protocol. Due to the basis transformation T_x Eve will destroy the correlation between Alice and Bob.

II. Basis Transformations

In QKD, the most common way to detect the presence of an adversary is to use a random application of a basis transformation by one of the legitimate communication parties. This method can be found in prepare and measure protocols (e.g., in [1] or [3]) as well as entanglement swapping based protocols (e.g., in [13] [16] or the improved version of the protocol in [17]). The idea is to randomly alter the initial state to make it impossible for an adversary to eavesdrop the information transmitted without introducing a certain error rate, i.e., without being detected. The operation most commonly used in these protocols is the Hadamard operation, which is a transformation from the Z- into the X-basis. In general, a transformation T_x from the Z basis into the X-basis can be described as a rotation about the X-axis by some angle θ combined with two rotations about the Z-axis by some angle ϕ, i.e.,

$$T_x\big(\theta,\phi\big) = e^{i\phi} R_z\big(\phi\big) R_x\big(\theta\big) R_z\big(\phi\big). \tag{2}$$

The rotations about the X- or Z-axis are described in the most general way by the operators (cf. for example [23] for further details on rotation operators)

$$\begin{aligned} \mathrm{R}_x\big(\theta\big) &= \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ \mathrm{R}_z\big(\theta\big) &= \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \end{aligned} \tag{3}$$

Based on these operators, we directly obtain the effect of $T_x(\theta,\phi)$ on the computational basis

$$\begin{aligned} T_x\big(\theta,\phi\big)|0\rangle &= \cos\frac{\theta}{2}|0\rangle - i\, e^{i\phi}\sin\frac{\theta}{2}|1\rangle \\ T_x\big(\theta,\phi\big)|1\rangle &= -i\, e^{i\phi}\sin\frac{\theta}{2}|0\rangle + e^{2i\phi}\cos\frac{\theta}{2}|1\rangle. \end{aligned} \tag{4}$$

From these two equations above we immediately see that the Hadamard operation is just the special case where $\theta = \phi = \pi/2$.

In QKD protocols based on entanglement swapping, the basis transformation is usually applied onto one qubit of a Bell state. Taking the general transformation $T_x(\theta,\phi)$ from (2) into account, the Bell state $|\Phi^+\rangle$ changes into

$$\begin{aligned} T_x^{(1)}\big(\theta,\phi\big)|\Phi^+\rangle_{12} =& \cos\frac{\theta}{2}\ \frac{1}{\sqrt{2}}\Big(|00\rangle + e^{2i\phi}|11\rangle\Big) \\ & -i\, e^{i\phi}\sin\frac{\theta}{2}\ \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \end{aligned} \tag{5}$$

and accordingly for the other Bell states. The superscript "(1)" in (5) indicates that the transformation $T_x\big(\theta,\phi\big)$ is applied on qubit 1. As a consequence, the application of $T_x(\theta,\phi)$ before the entanglement swapping is performed changes the results based on the angles θ and ϕ. In detail, we have the state

$$\begin{aligned} T_x^{(1)}\big(\theta,\phi\big)&|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \\ &\frac{1}{2}\Big(|\Phi^+\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Phi^+\rangle_{24} \\ &\quad+|\Phi^-\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Phi^-\rangle_{24} \\ &\quad+|\Psi^+\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Psi^+\rangle_{24} \\ &\quad+|\Psi^-\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Psi^-\rangle_{24}\Big) \end{aligned} \tag{6}$$

upon which Alice performs her Bell state measurement on qubits 1 and 3 (cf. Figure 1). Here, the superscripts "(1)" and "(2)" in (6) indicate that after Alice's Bell state measurement on qubits 1 and 3 the transformation $T_x\big(\theta,\phi\big)$ swaps from qubit 1 onto qubit 2. When Bob performs his Bell state measurement on qubits 2 and 4, he obtains a result correlated to Alice's measurement outcome only with probability (cf. (5) and (6) above)

$$P_{corr} = \cos^2\frac{\theta}{2}\ \cos^2(\phi). \tag{7}$$

Otherwise, he obtains an uncorrelated result, which becomes a problem because Bob is no longer able to compute Alice's state based on his result and vice versa.

Fortunately, Bob can resolve this problem by transforming the state back into its original form. Following (6), where Alice performs $T_x\big(\theta,\phi\big)$ on qubit 1, he achieves that by applying the inverse $T_x^{-1}\big(\theta,\phi\big)$ on qubit 2 of his state. As we will see in the following section, if an adversary interferes with the communication, the effects of Alice's basis transformation can not be represented as in (6) any longer. Thus, even if Bob applies the inverse transformation, Alice's and Bob's results are uncorrelated to a certain amount. This amount is reflected in an error rate detected by Alice and Bob during post processing.

III. Single Application of General Basis Transformations

Previous works ([24] [25]) already deal with the scenarios where Alice or Bob or both parties randomly apply a simplified version of basis transformations. Therein, the simplification addresses the angle ϕ, i.e., the rotation about the Z-axis. In the security discussions in [24], the angle ϕ is fixed at $\pi/2$ for reasons of simplicity. That means, the rotation about the Z-axis is constant at an angle of $\pi/2$ such that only the angle θ can be chosen freely.

In this section and the next one, we want to extend the results from [24] [25] by applying general basis transformations, which means Alice and Bob are able to choose both angles θ and ϕ in (2) freely. We are at first looking only on one party performing a basis transformation on the respective qubits and in the next section on two different basis transformations performed by each of the parties. For each scenario we will show, which values for θ and ϕ are optimal to give an adversary the least information about the raw key bits. In the course of the two scenarios, we will denote Alice's operation as $T_x\big(\theta_A, \phi_A\big)$ and, accordingly, Bob's operation as $T_x\big(\theta_B, \phi_B\big)$.

As already pointed out above, the application of the basis transformation occurs at random and Eve is able to obtain full information about Alice's and Bob's secret due to the structure of the state $|\delta\rangle$, if the two parties do not apply any basis transformation at all [24] [25]. Therefore, we look at first at the effects of a basis transformation at Alice's side. Her initial application of the general basis transformation $T_x\big(\theta_A, \phi_A\big)$ does alter the state $|\delta\rangle_{1QR4TU}$ introduced by Eve such that it is changed to

$$|\delta'\rangle_{1QR4TU} = T_x^{(1)}\big(\theta_A, \phi_A\big)|\delta\rangle_{1QR4TU} \tag{8}$$

After a little algebra, we see that Alice obtains all four Bell states with equal probability and after her measurement the state of the remaining qubits is

$$\begin{aligned} &e^{i\phi_A}\cos\frac{\theta_A}{2}\cos\phi_A\ |\Phi^+\rangle_{Q4}|\varphi_1\rangle_{TU} \\ -&ie^{i\phi_A}\cos\frac{\theta_A}{2}\sin\phi_A\ |\Phi^-\rangle_{Q4}|\varphi_2\rangle_{TU} \\ -&ie^{i\phi_A}\sin\frac{\theta_A}{2}\ |\Psi^+\rangle_{Q4}|\varphi_3\rangle_{TU} \end{aligned} \tag{9}$$

assuming Alice obtained $|\Phi^+\rangle_{1R}$. We are presenting just the state for this particular result in detail because it would be simply too complex to present the representation of the whole state for all possible outcomes here. Nevertheless, for the other three possible results the remaining qubits end up in a similar state, where only Bob's Bell states of the qubits Q and 4 as well as Eve's auxiliary states of the qubits T and U change accordingly to Alice's measurement result.

Before Bob performs his Bell state measurement, he has to reverse Alice's basis transformation. This can be achieved by applying $T_x^{-1}\big(\theta_A, \phi_A\big)$ on qubit Q in his possession. Whereas this would reverse the effect of Alice's basis transformation if no adversary is present, the structure of Eve's state $|\delta\rangle$ makes this reversion impossible, as already pointed out in the previous section. Therefore, Bob obtains the correlated state $|\Phi^+\rangle_{Q4}$ only with probability

$$P_{\Phi^+} = \frac{1}{4}\Big(3 + \cos\big(4\phi_A\big)\Big)\cos^4\frac{\theta_A}{2} + \sin^4\frac{\theta_A}{2} \tag{10}$$

Hence, due to Eve's intervention Bob obtains a result uncorrelated to Alice's outcome with probability

$$P_e = \frac{1}{2}\Big(\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\big(2\phi_A\big)\Big). \tag{11}$$

Assuming that Bob obtains $|\Phi^+\rangle_{Q4}$, i.e., the expected result based on Alice's measurement outcome, Eve obtains either $|\varphi_1\rangle$, $|\varphi_2\rangle$ or $|\varphi_3\rangle$ from her measurement on qubits T and U with the respective probabilities

$$\begin{aligned} P_{\varphi_1} &= \frac{\cos^4\frac{\theta_A}{2}\cos^4\phi_A}{\frac{1}{4}(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + \sin^4\frac{\theta_A}{2}} \\ P_{\varphi_2} &= \frac{\cos^4\frac{\theta_A}{2}\sin^4\phi_A}{\frac{1}{4}(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + \sin^4\frac{\theta_A}{2}} \\ P_{\varphi_3} &= \frac{-\sin^2\frac{\theta_A}{2}}{(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + 4\sin^4\frac{\theta_A}{2}} \end{aligned} \tag{12}$$

Furthermore, in case Bob measures an uncorrelated result, Eve obtains two out of the four auxiliary states $|\varphi_i\rangle$ at random. Hence, due to the basis transformation $T_x\big(\theta_A, \phi_A\big)$, Eve's auxiliary systems are less correlated to Bob's result compared to the application of a simple basis transformation as described in [24] [25]. In other words, Eve's information on Alice's and Bob's result is further reduced compared to the scenarios described therein.

Since Alice applies the basis transformation at random, i.e., with probability 1/2, the average error probability $\langle P_e\rangle$ can be directly computed using (11) and its variations based on Alice's measurement result as

$$\langle P_e\rangle = \frac{1}{4}\left[\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\Big(2\phi_A\Big)\right]. \tag{13}$$

Keeping in mind that Eve does not introduce any error when Alice does not use the basis transformation $T_x\big(\theta_A, \phi_A\big)$, the average collision probability $\langle P_c\rangle$ can be computed as (cf. also (12))

$$\begin{aligned} \langle P_c\rangle = \frac{1}{64}\Big(&53 - 4\cos\theta_A + 7\cos\big(2\theta_A\big) \\ &+ 8\cos^4\frac{\theta_A}{2}\cos\big(4\phi_A\big)\Big). \end{aligned} \tag{14}$$

In further consequence this leads to the Shannon entropy H of the raw key, i.e.,

$$H = \frac{1}{2}\left[h\Big(\cos^2\frac{\theta_A}{2}\Big) + \cos^2\frac{\theta_A}{2}\ h\Big(\cos^2\phi_A\Big)\right]. \tag{15}$$

As we can directly see from Figure 3, the average error probability $\langle P_e\rangle$ has its maximum at 1/3 with $\theta_A \simeq 0.39183\pi$ and $\phi_A = \pi/4$ or $\phi_A = 3\pi/4$. For this choice of θ_A and ϕ_A we see from Figure 4 that the Shannon entropy is also maximal with $H \simeq 0.79248$. Hence, the adversary Eve is left with a mutual information of

$$I_{AE} = 1 - H = 0.20752 \tag{16}$$

This value for the mutual information is less than half of Eve's information on the raw key compared to the application of a Hadamard operation (cf. [1] [3] [21] [13]) or the application of a simplified basis transformation (cf. [24] [25]).

Unfortunately, the angle for $\theta_A \simeq 0.39183\pi$ to reach the maximum value is rather odd and difficult to realize in a practical implementation. In contrast, an angle $\theta_A = 3\pi/8$ is more convenient and much easier to realize. For this scenario we can compute from (13) an average error rate of $\langle P_e\rangle \simeq 0.33288$ and from (15) the respective Shannon entropy $H \simeq 0.79148$ (cf. also Figure 3 and Figure 4), which are both just insignificantly lower than their maximum values.

ISBN: 978-1-61208-380-3

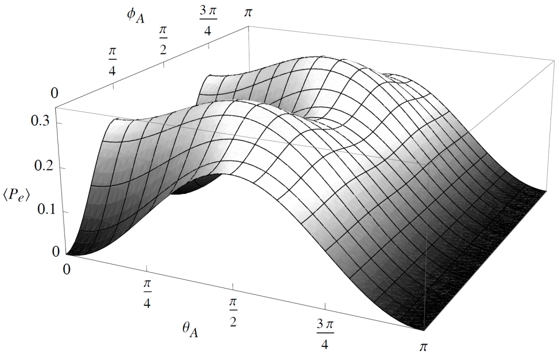

Figure 3. Error probability $\langle P_e \rangle$ depending on θ_A and ϕ_A

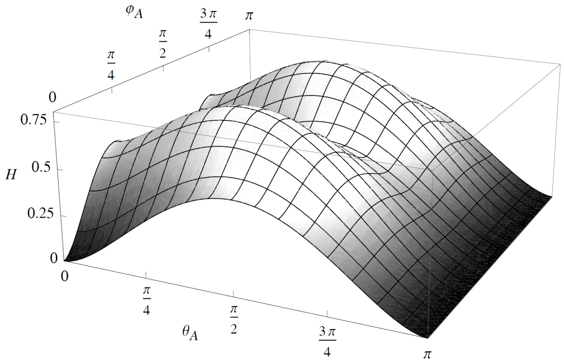

Figure 4. Shannon entropy H of the raw key depending on θ_A and ϕ_A

Accordingly, Eve's mutual information on the raw key is slightly above 20%, i.e., $I_{AE} \simeq 0.20852$. Hence, the security of the protocol is drastically increased using a general basis transformation compared to the application of a Hadamard operation.

IV. Combined Application of General Basis Transformations

In the previous section, we discussed the application of one general basis transformation $T_x\big(\theta_A, \phi_A\big)$ on Alice's side. It is easy to see that the results for the average error probability $\langle P_e \rangle$ in (13) as well as the Shannon entropy H in (15) are the same if only Bob randomly applies the basis transformation $T_x\big(\theta_B, \phi_B\big)$ on his side.

Hence, a more interesting scenario is the combined random application of two different basis transformations, i.e., $T_x\big(\theta_A, \phi_A\big)$ on Alice's side and $T_x\big(\theta_B, \phi_B\big)$ on Bob's side. The application of these two different basis transformations alters the state introduced by Eve accordingly to

$$|\delta'\rangle_{1QR4TU} = T_x^{(1)}\big(\theta_A, \phi_A\big)\, T_x^{(4)}\big(\theta_B, \phi_B\big)\, |\delta\rangle_{1QR4TU} \quad (17)$$

where again the superscripts "(1)" and "(4)" indicate that $T_x\big(\theta_A, \phi_A\big)$ is applied on qubit 1 and $T_x\big(\theta_B, \phi_B\big)$ on qubit 4, respectively. Following the protocol, Alice has to undo Bob's transformation using $T_x^{-1}\big(\theta_B, \phi_B\big)$ before she can perform her Bell state measurement. Similar to the application of one basis transformation described above, Alice obtains all four Bell states with equal probability from her measurement. The state of the remaining qubits changes in a way analogous to (9) above and Bob has to reverse Alice's transformation using $T_x^{-1}\big(\theta_A, \phi_A\big)$. Hence, when Bob performs his measurement on qubits Q and 4, he does not only obtain a result correlated to Alice's outcome, but all four possible Bell states with different probabilities such that an error is introduced in the protocol. As already discussed in the previous section, the results from Eve's measurement on qubits T and U are not fully correlated to Alice's and Bob's results and therefore Eve's information on the raw key bits is further reduced compared to the application of only one transformation.

Due to the fact that Alice as well as Bob choose at random whether they apply their respective basis transformation, the average error probability is calculated over all scenarios, i.e., no transformation is applied, either Alice or Bob applies $T_x\big(\theta_A, \phi_A\big)$ or $T_x\big(\theta_B, \phi_B\big)$, respectively, or both transformations are applied. Therefore, using the results from (13) above, the overall error probability can be computed as

$$\begin{aligned}\langle P_e \rangle = &\frac{1}{8}\Big[\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\Big(2\phi_A\Big)\Big] \\ &+\frac{1}{8}\Big[\sin^2\theta_B + \cos^4\frac{\theta_B}{2}\sin^2\Big(2\phi_B\Big)\Big] \\ &+\frac{1}{16}\Big[\sin^2\Big(\theta_A + \theta_B\Big) \\ &\qquad + \cos^4\frac{\theta_A + \theta_B}{2}\sin^2\Big(2\big(\phi_A + \phi_B\big)\Big)\Big] \\ &+\frac{1}{16}\Big[\sin^2\Big(\theta_A - \theta_B\Big) \\ &\qquad + \cos^4\frac{\theta_A - \theta_B}{2}\sin^2\Big(2\big(\phi_A - \phi_B\big)\Big)\Big]\end{aligned} \quad (18)$$

having its maximum at $\langle P_e \rangle \simeq 0.41071$. One possibility to reach the maximum is to choose the angles

$$\begin{aligned}\theta_A &= 0 \qquad \theta_B \simeq 0.45437\pi \\ \phi_A &= \frac{\pi}{4} \qquad \phi_B = \frac{\pi}{4}.\end{aligned} \quad (19)$$

In fact, as long as $\phi_A = \pi/4$ or $\phi_A = 3\pi/4$ the value of ϕ_B can be chosen freely to reach the maximum. Hence, the average error probability is plotted in Figure 5 taking $\phi_A = \phi_B = \pi/4$.

Following the same argumentation and using (15) from above, the Shannon entropy can be calculated as

$$\begin{aligned}H = &\frac{1}{4}\Big[h\Big(\cos^2\frac{\theta_A}{2}\Big) + \cos^2\frac{\theta_A}{2}\, h\Big(\cos^2\phi_A\Big)\Big] \\ &+\frac{1}{4}\Big[h\Big(\cos^2\frac{\theta_B}{2}\Big) + \cos^2\frac{\theta_B}{2}\, h\Big(\cos^2\phi_B\Big)\Big] \\ &+\frac{1}{8}\Big[h\Big(\cos^2\frac{\theta_A + \theta_B}{2}\Big) \\ &\qquad + \cos^2\frac{\theta_A + \theta_B}{2}\, h\Big(\cos^2\big(\phi_A + \phi_B\big)\Big)\Big] \\ &+\frac{1}{8}\Big[h\Big(\cos^2\frac{\theta_A - \theta_B}{2}\Big) \\ &\qquad + \cos^2\frac{\theta_A - \theta_B}{2}\, h\Big(\cos^2\big(\phi_A - \phi_B\big)\Big)\Big]\end{aligned} \quad (20)$$

having its maximum at $H \simeq 0.9452$ (cf. Figure 6 for a plot of (20) taking $\phi_A = \phi_B = \pi/4$). This maximum is reached, for

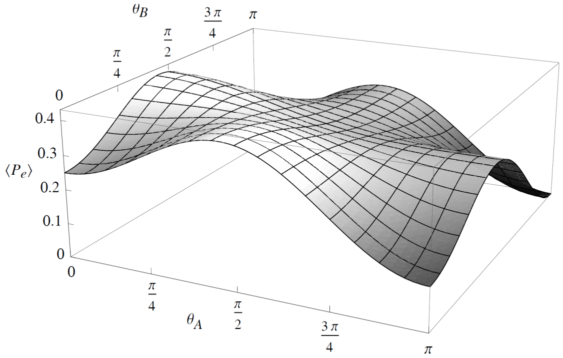

Figure 5. Error probability $\langle P_e \rangle$ depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$.

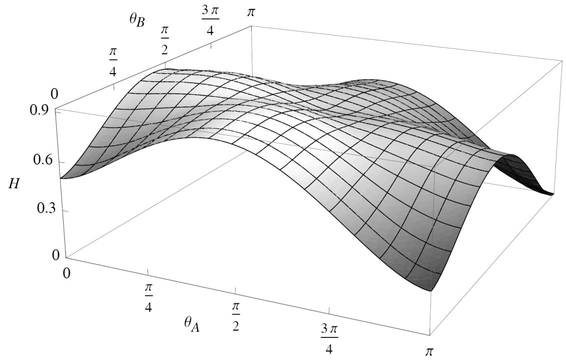

Figure 6. Shannon entropy H of the raw key depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$.

example, using

$$\begin{aligned} \theta_A &\simeq -0.18865\pi & \theta_B &\simeq 0.42765\pi \\ \phi_A &\simeq -0.22405\pi & \phi_B &\simeq 0.36218\pi. \end{aligned} \tag{21}$$

The maximal Shannon entropy can also be reached using other values but they are not as nicely distributed as in the case of the average error probability.

Looking again at set of values for $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$, which are more suitable for a physical implementation than the values mentioned above, one possibility for Alice and Bob is to choose

$$\begin{aligned} \theta_A &= -\frac{3\pi}{16} & \theta_B &= \frac{7\pi}{16} \\ \phi_A &= -\frac{\pi}{4} & \phi_B &= \frac{3\pi}{8} \end{aligned} \tag{22}$$

leading to an almost optimal Shannon entropy $H \simeq 0.9399$ and a average respective error probability $\langle P_e \rangle \simeq 0.39288$. In this context, more suitable for a physical implementation means that a transformation about an angle of $\pi/4$ or $3\pi/8$ is easier to realize in a laboratory than an angle of 0.42765π. Keeping ϕ_A and ϕ_B fixed – as already discussed in the previous section – such that

$$\begin{aligned} \theta_A &= \frac{3\pi}{16} & \theta_B &= \frac{7\pi}{16} \\ \phi_A &= \frac{\pi}{4} & \phi_B &= \frac{\pi}{4} \end{aligned} \tag{23}$$

the same average error probability $\langle P_e \rangle \simeq 0.39288$ and a slightly smaller Shannon entropy $H \simeq 0.91223$ compared to the previous values are achieved. Hence, we see that using a set of parameters more suitable for a physical implementation still results in a high error rate and leaves Eve's mutual information I_{AE} below 10%.

V. Results and Implications

The results presented in the previous sections have direct implications on the security of QKD protocols based on entanglement swapping. Where in some QKD protocols [13] [16] [17] a random application of a Hadamard operation is used to detect an eavesdropper and secure the protocol, the above results indicate that the Hadamard operation is not the optimal choice. Using the Hadamard operation leaves an adversary with a mutual information $I_{AE} = 0.5$ and an expected error probability $\langle P_e \rangle = 0.25$ (cf. Table I), which is comparable to standard prepare and measure protocols [1]–[3].

Giving Alice an increased degree of freedom, i.e., choosing both θ_A and ϕ_A freely, she is able to further decrease the adversary's information about the raw key bits. By shifting ϕ_A from $\pi/2$ to $\pi/4$ and θ_A from $\pi/2$ or $\pi/4$ to $3\pi/8$, the adversary's information is reduced to $I_{AE} \simeq 0.208$ (cf. (15)). This is a reduction by almost 60% compared to QKD schemes described in [1]–[3] [13] [17] and more than 50% compared to the combined application of two different basis transformations (cf. also [24] [25]). At the same time, the expected error probability is increased by one third to $\langle P_e \rangle \simeq 0.333$ (cf. (13)). Hence, an adversary does not only obtain fewer information about the raw key bits but also introduces more errors and therefore is easier to detect.

Following these arguments, the best strategy for Alice and Bob is to apply different basis transformations at random to reduce the adversary's information to a minimum. As already pointed out above, this minimum of $I_{AE} \simeq 0.0548$ is reached with a rather odd configuration for $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ as described in the previous section. Hence, it is important to look at configurations more suitable for physical implementations, i.e., configurations of $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ described by simpler fractions of π as given in (22) and (23). In this case, we showed that $\phi_{\{A,B\}}$ can be fixed at $\phi_A = \phi_B = \pi/4$ and with $\theta_A = 3\pi/16$ and $\theta_B = 7\pi/16$ almost maximal values can be achieved resulting in $I_{AE} \simeq 0.088$ and $\langle P_e \rangle \simeq 0.393$ (cf. (23) and also Table I).

Regarding physical implementations, another – even simpler – configuration can be found, involving only $\pi/2$ and $\pi/4$ rotations (cf. Table I). In this case, $\theta_A = 0$, $\phi_A = \pi/4$ and $\theta_B = \phi_B = \pi/2$, which leaves the expected error probability at $\langle P_e \rangle \simeq 0.334$. The adversary's information is nowhere near the minimum but still rather low at $I_{AE} = 0.125$.

In terms of security, these results represent a huge advantage over QKD protocols based on entanglement swapping [13], [16], [17] or standard prepare and measure protocols [1]–[3]. As pointed out, such protocols usually have an expected error probability of $\langle P_e \rangle = 0.25$ and a mutual information $I_{AE} = 0.5$. Due to the four degrees of freedom, the error rate is between one third ($\langle P_e \rangle \simeq 0.334$) and more than one half ($\langle P_e \rangle = 0.411$) higher in the scenarios described here than in the standard protocols, which makes it easier to detect an adversary.

TABLE I. OVERVIEW OF THE ERROR RATE $\langle P_E \rangle$ AND EVE'S INFORMATION I_{AE} ON THE RAW KEY BITS FOR DIFFERENT VALUES OF $\theta_{A,B}$ AND $\phi_{A,B}$.

	$\phi_A = 0$	$\phi_A = \frac{\pi}{2}$	$\phi_A = \frac{\pi}{4}$
$\phi_B = 0$	$\theta_A = 0, \theta_B = 0$ $\langle P_e \rangle = 0$ $I_{AE} = 1$	$\theta_A = \frac{\pi}{2}, \theta_B = 0$ $\langle P_e \rangle = 0.25$ $I_{AE} = 0.5$	$\theta_A = \frac{3\pi}{8}, \theta_B = 0$ $\langle P_e \rangle \simeq 0.333$ $I_{AE} \simeq 0.208$
$\phi_B = \frac{\pi}{2}$		$\theta_A = \frac{\pi}{2}, \theta_B = \frac{\pi}{4}$ $\langle P_e \rangle = 0.25$ $I_{AE} \simeq 0.45$	$\theta_A = 0, \theta_B = \frac{\pi}{2}$ $\langle P_e \rangle \simeq 0.40625$ $I_{AE} = 0.125$
$\phi_B = \frac{\pi}{4}$			$\theta_A = \frac{3\pi}{16}, \theta_B = \frac{7\pi}{16}$ $\langle P_e \rangle = 0.393$ $I_{AE} = 0.088$

VI. Conclusion

In this article, we discussed the effects of basis transformations on the security of quantum key distribution protocols based on entanglement swapping. We showed that the Hadamard operation, a transformation from the Z- into the X-basis often used in prepare and measure protocols, is not optimal in connection with entanglement swapping based protocols. Starting from a general basis transformation described by two angles θ and ϕ, we inspected the effects on the security when the adversary follows a collective attack strategy. We showed that the application of a basis transformation by one of the communication parties decreases the adversary's information to about $I_{AE} \simeq 0.2075$, which is less than half of the information compared to an application of the Hadamard operation. At the same time, the average error probability introduced by the presence of the adversary increases to $\langle P_e \rangle = 1/3$. Hence, the application of one general basis transformation is more effective, i.e., reveals even less information to the adversary, than the application of a simplified basis transformation as given in [24] [25]. A combined application of two different basis transformations further reduces the adversary's information to about $I_{AE} \simeq 0.0548$ at an average error probability of slightly more than 0.41.

Since the configuration of the angles θ and ϕ to reach these maximal values is not very suitable for a physical implementation, we also showed that these maximal values are almost reached with more convenient values for θ and ϕ. In this case, the adversary's information is still $I_{AE} < 0.1$ with an average error rate $\langle P_e \rangle \simeq 0.393$ for a combined application of two basis transformations.

These results have a direct impact on the security of such protocols. Due to the reduced information of an adversary and the high error probability introduced during the attack strategy, Alice and Bob are able to accept higher error thresholds compared to standard entanglement-based QKD protocols.

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, 1984, pp. 175–179.

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

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

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

[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, 1996, pp. 335–339.

[6] A. Poppe et al., "Practical Quantum Key Distribution with Polarization Entangled Photons," Optics Express, vol. 12, no. 16, 2004, pp. 3865–3871.

[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, 2008, pp. 209–218.

[8] M. Peev et al., "The SECOQC Quantum Key Distribution Network in Vienna," New Journal of Physics, vol. 11, no. 7, 2009, p. 075001.

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

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

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

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

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

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

[15] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," Phys. Rev. A, vol. 68, no. 4, 2003, p. 042317.

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

[17] 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, 2006, pp. 899–906.

[18] C. H. Bennett et al., "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels," Phys. Rev. Lett., vol. 70, no. 13, 1993, pp. 1895–1899.

[19] 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, 1993, pp. 4287–4290.

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

[21] 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, 2001, p. 036301.

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

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

[24] 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.

[25] ——, "Application of the Simulation Attack on Entanglement Swapping Based QKD and QSS Protocols," International Journal on Advances in Systems and Measurements, vol. 6, no. 1&2, 2013, pp. 137–148.

ISBN: 978-1-61208-380-3