Robustness of Optimal Basis Transformations to Secure Entanglement Swapping Based QKD Protocols

Stefan Schauer and Martin Suda

Digital 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 as well as the robustness of these basis transformations considering an imperfect physical apparatus. 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. Nevertheless, these optimal angles for the basis transformations have to be precisely configured in the laboratory to achieve the minimum amount for the adversary's information. Since we can not be sure that the physical apparatus is perfect, we will look at the robustness of the optimal choice for the angles. 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. Further, we will show that the optimal angles to achieve these results are very robust such that an imperfect configuration does only have an insignificant effect on the security of the protocol.**

Keywords–quantum key distribution; optimal basis transformations; imperfect apparatus; Gaussian distribution of angles; security analysis; entanglement swapping

I. Introduction

In a recent article [1], the authors have shown that in a quantum key distribution (QKD) protocol based on entanglement swapping the Hadamard operation is not the optimal choice to secure the protocol against an adversary. Moreover, a combination of basis transformations will reduce the amount of the adversary's information drastically when using general basis transformations. Additionally, we want to show in this article that these general basis transformations are also robust against an imperfect configuration of the physical apparatus.

QKD is one of the major applications of quantum mechanics and, in the last three decades, QKD protocols have been studied at length in theory and in practical implementations [2]–[9]. 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 [10]–[12]. In addition to these prepare and measure protocols, several protocols based on the phenomenon of entanglement swapping have been introduced [13]–[18], where entanglement swapping is used to obtain correlated measurement results between the legitimate communication parties, Alice and Bob.

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 share two Bell states of the form $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ (cf. picture (1) in Figure 1) in such a way that Alice sends qubit 2 to Bob and Bob sends qubit 3 to Alice. Hence, afterwards Alice is in possession of qubits 1 and 3 and Bob of qubits 2 and 4 (cf. picture (2) in Figure 1). The state of the overall system can thus be described as

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

Next, Alice performs a complete Bell state measurement on the two qubits in her possession. After this measurement, the qubits 2 and 4 at Bob's side collapse into a Bell state although both qubits originated at completely different sources (cf. picture (4) in Figure 1). Moreover, the state of Bob's qubits fully depends on Alice's measurement result. As presented in (1), Bob always obtains the same result as Alice when performing a Bell state measurement on his qubits. In the aforementioned QKD protocols based on entanglement swapping, Alice and Bob use these correlated measurement results to establish a secret key among them.

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 [2] and [4] but also in QKD schemes based on entanglement swapping (e.g., [14] [17] [22]). Nevertheless, this security measure has just been discussed on the surface so far when it comes to QKD protocols based on entanglement swapping. It has only been shown that these protocols are secure against intercept-resend attacks and basic collective attacks (cf. for example, [13] [14] [17]).

In this article, we will analyze the security of QKD protocols based on entanglement swapping against the *simulation attack*, a general version of a collective attack [23]. As a security measure we will analyze the application of a general

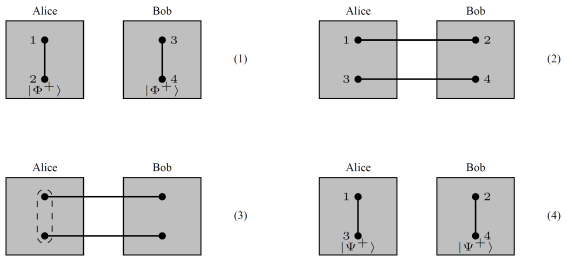

Figure 1. Illustration of entanglement swapping where Alice and Bob share two Bell states each of the form $|\Phi^+\rangle$. The dashed line indicates a measurement in the Bell basis.

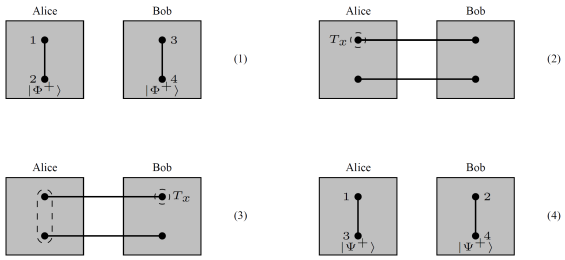

Figure 2. Sketch of a standard setup for an entanglement swapping based QKD protocol. Qubits 2 and 3 are exchanged (cf. picture (2)) and a basis transformation T_x is applied on qubit 1 and inverted by using T_x on qubit 2.

basis transformation T_x, defined by the angles θ and ϕ (cf. (4) and picture (2) in Figure 2). 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. Furthermore, we will look at the robustness of these optimal values for θ and ϕ, i.e., how much the expected error probability and the adversary's information change if Alice and Bob are not able to precisely adjust their apparatus to the optimal values for θ and ϕ.

In the following section, the simulation attack is described in detail and it is explained how an adversary is able to perfectly eavesdrop on a protocol where no basis transformations are applied. In Section III, 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 IV and at the application of two different basis transformations by each of the communication parties in Section V. In Section VI, we will analyze how these results change if the physical apparatus is not configured precisely and the choice of angles can be described by a Gaussian distribution. In the end, we sum up the implications of the results on the security of entanglement based QKD protocols.

II. The Simulation Attack Strategy

In entanglement swapping based QKD protocols like [13]–[15], [17], [18] Alice and Bob rest their security check onto the correlations between their respective measurement results coming from the entanglement swapping (cf. (1)). If these correlations are violated, Alice and Bob have to assume that an adversary is present. In other words, an adversary stays undetected if these correlations are not violated. 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 (cf. also Figure 3).

In a previous article [23], we already described such a collective attack called *simulation attack* for a specific protocol [18]. The attack implements the strategy described in the previous paragraph, i.e., the correlations are preserved (or "simulated") such that the Eve stays undetected. The generalization from the version presented in [23] is straight forward as described in the following paragraphs.

It has been pointed out in detail in [23] that Eve uses four qubits in a state similar to (1) to simulate the correlations between Alice and Bob. Further, she introduces additional systems $|\varphi_i\rangle$ 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 [23]. From (2) it is easy to see that after a Bell measurement on qubits P and R the state of qubits Q and S collapses into a correlated state. Hence, the state $|\delta\rangle$ preserves the correlation of Alice's and Bob's measurement results coming from the entanglement swapping (cf. (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 they are pairwise orthogonal, i.e.,

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

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 (cf. picture (1) and (2) in Figure 2). 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 equations (1) and (2) as well as pictures (3) and (4) in Figure 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 the respective 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. Nevertheless, Eve's second possibility is to intercept the qubits 2 and 3 flying from Alice to Bob and vice versa and

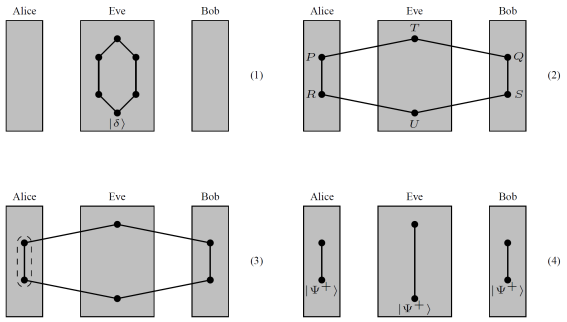

Figure 3. Illustration of the simulation attack for an entanglement swapping based QKD protocol where no basis transformation is applied. It is assumed that Eve directly distributes the state $|\delta\rangle$ between Alice and Bob.

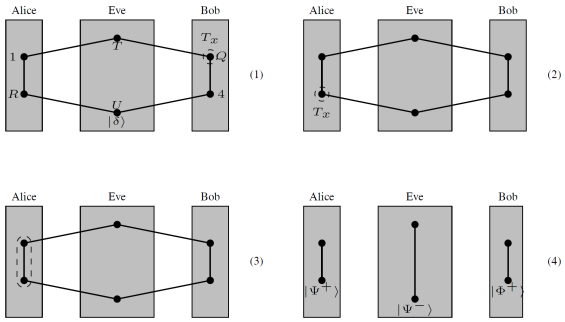

Figure 4. Illustration of the simulation attack for an entanglement swapping based QKD protocol where the basis transformation T_x is applied by Bob. Eve's intervention destroys the correlation between Alice and Bob.

to perform entanglement swapping to distribute the state $|\delta\rangle$. This is a straight forward method as already described in [23].

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 [13]. As already pointed out in [23], 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. 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 recurrently found in prepare and measure protocols (e.g., in [2] or [4]) as well as entanglement swapping based protocols (e.g., in [14] [17] or the improved version of the protocol in [18]). The idea for Alice or Bob (or both parties) is to choose at random whether to apply a basis transformation on one of their qubits. This randomly alters the initial state and makes it impossible for an adversary to eavesdrop the transmitted information without introducing a certain error rate, i.e., without being detected. The basis transformation 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.,

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

The rotations about the X- or Z-axis are described in the most general way by the operators (cf. for example, [24] for further details on rotation operators)

$$\begin{aligned} \mathrm{R}_x\big(\theta\big) &= \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ \mathrm{R}_z\big(\theta\big) &= \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \end{aligned} \tag{5}$$

Based on these operators, we directly obtain the matrix representation for $T_x(\theta,\phi)$ as

$$T_x\big(\theta,\phi\big) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\,e^{i\phi}\sin\frac{\theta}{2} \\ -i\,e^{i\phi}\sin\frac{\theta}{2} & e^{2i\phi}\cos\frac{\theta}{2} \end{pmatrix} \tag{6}$$

and the effect of $T_x(\theta,\phi)$ on the computational basis

$$\begin{aligned} T_x\big(\theta,\phi\big)|0\rangle &= \cos\frac{\theta}{2}|0\rangle - i\,e^{i\phi}\sin\frac{\theta}{2}|1\rangle \\ T_x\big(\theta,\phi\big)|1\rangle &= -i\,e^{i\phi}\sin\frac{\theta}{2}|0\rangle + e^{2i\phi}\cos\frac{\theta}{2}|1\rangle. \end{aligned} \tag{7}$$

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 (4) into account, the Bell state $|\Phi^+\rangle$ changes into

$$\begin{aligned} T_x^{(1)}\big(\theta,\phi\big)|\Phi^+\rangle_{12} = \cos\frac{\theta}{2}\,\frac{1}{\sqrt{2}}\Big(|00\rangle + e^{2i\phi}|11\rangle\Big) \\ -i\,e^{i\phi}\sin\frac{\theta}{2}\,\frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \end{aligned} \tag{8}$$

and accordingly for the other Bell states. The superscript "(1)" in (8) 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, after the application of the basis transformation on qubit 1, the overall state of Alice's and Bob's qubits is (cf. picture (2) in Figure 2)

$$\begin{aligned} T_x^{(1)}\big(\theta,\phi\big)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \\ \frac{1}{2}\Big(|\Phi^+\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Phi^+\rangle_{24} \\ +|\Phi^-\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Phi^-\rangle_{24} \\ +|\Psi^+\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Psi^+\rangle_{24} \\ +|\Psi^-\rangle_{13}T_x^{(2)}\big(\theta,\phi\big)|\Psi^-\rangle_{24}\Big) \end{aligned} \tag{9}$$

Next, Alice performs her Bell state measurement on qubits 1 and 3 of this state and obtains one of the four Bell states (cf. picture (3) in Figure 2). The superscripts "(1)" and "(2)" in (9) 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. Thus, when Bob performs his Bell state measurement on qubits 2 and 4, he will not obtain a result correlated to Alice's measurement outcome any more. In detail, assuming that Alice obtained $|\Phi^+\rangle_{13}$ from her measurement we can

directly see from (8) that Bob will obtain $|\Phi^+\rangle_{24}$ only with probability (cf. also (9) above)

$$\begin{aligned} P_{corr} &= T_x^{(2)}\big(\theta,\phi\big)\ \langle\Phi^+||\Phi^+\rangle\langle\Phi^+|\ T_x^{(2)}\big(\theta,\phi\big)|\Phi^+\rangle \\ &= \frac{1}{4}\cos^2\frac{\theta}{2}\Big(2+e^{2i\phi}+e^{-2i\phi}\Big) \\ &= \cos^2\frac{\theta}{2}\ \cos^2(\phi). \end{aligned} \tag{10}$$

(and similarly for Alice's other possible results). Otherwise, he obtains an uncorrelated result, which results in 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 of qubits 2 and 4 back into its original form before he performs his Bell state measurement. Following (9), where Alice performs $T_x\big(\theta,\phi\big)$ on qubit 1, he achieves that by applying the inverse of the basis transformation, i.e.,

$$T_x^{-1}\big(\theta,\phi\big) = \begin{pmatrix} \cos\frac{\theta}{2} & i\,e^{-i\phi}\sin\frac{\theta}{2} \\ i\,e^{-i\phi}\sin\frac{\theta}{2} & e^{-2i\phi}\cos\frac{\theta}{2} \end{pmatrix} \tag{11}$$

on qubit 2 in his possession. Afterwards, he will obtain a correlated result from his measurement on qubits 2 and 4.

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 (9) 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.

IV. Single Application of General Basis Transformations

Previous works [25] [26] 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 [25], 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 [25] [26] by applying general basis transformations, which means Alice and Bob are able to choose both angles θ and ϕ in (4) freely. At first, we are 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, due to the structure of the state $|\delta\rangle$, Eve is able to obtain full information about Alice's and Bob's secret, if the two parties do not apply any basis transformation at all (cf. [25] [26]). 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

$$|\delta'\rangle_{1QR4TU} = T_x^{(1)}\big(\theta_A,\phi_A\big)|\delta\rangle_{1QR4TU} \tag{12}$$

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

$$\begin{aligned} &e^{i\phi_A}\cos\frac{\theta_A}{2}\cos\phi_A\ |\Phi^+\rangle_{Q4}|\varphi_1\rangle_{TU} \\ -&ie^{i\phi_A}\cos\frac{\theta_A}{2}\sin\phi_A\ |\Phi^-\rangle_{Q4}|\varphi_2\rangle_{TU} \\ &-ie^{i\phi_A}\sin\frac{\theta_A}{2}\ |\Psi^+\rangle_{Q4}|\varphi_3\rangle_{TU} \end{aligned} \tag{13}$$

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 describe 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. As already pointed out in the previous section, 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. Hence, the application of $T_x^{-1}\big(\theta_A,\phi_A\big)$ on qubit Q changes the state in (13) into

$$\begin{aligned} &e^{i\phi_A}\cos\frac{\theta_A}{2}\cos\phi_A\Bigg[\cos\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|00\rangle_{Q4}+e^{-2i\phi_A}|11\rangle_{Q4}\Big) \\ &\qquad +ie^{-i\phi_A}\sin\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|01\rangle_{Q4}+|10\rangle_{Q4}\Big)\Bigg]|\varphi_1\rangle_{TU} \\ -&ie^{i\phi_A}\cos\frac{\theta_A}{2}\sin\phi_A\Bigg[\cos\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|00\rangle_{Q4}-e^{-2i\phi_A}|11\rangle_{Q4}\Big) \\ &\qquad +ie^{-i\phi_A}\sin\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|01\rangle_{Q4}+|10\rangle_{Q4}\Big)\Bigg]|\varphi_2\rangle_{TU} \\ -&ie^{i\phi_A}\sin\frac{\theta_A}{2}\Bigg[\cos\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|01\rangle_{Q4}+e^{-2i\phi_A}|10\rangle_{Q4}\Big) \\ &\qquad +ie^{-i\phi_A}\sin\frac{\theta_A}{2}\frac{1}{\sqrt{2}}\Big(|00\rangle_{Q4}+|11\rangle_{Q4}\Big)\Bigg]|\varphi_3\rangle_{TU} \end{aligned} \tag{14}$$

Therefore, Bob obtains the correlated state $|\Phi^+\rangle_{Q4}$ only with probability

$$P_{\Phi^+} = \frac{1}{4}\Big(3+\cos\big(4\phi_A\big)\Big)\cos^4\frac{\theta_A}{2}+\sin^4\frac{\theta_A}{2} \tag{15}$$

and the other results with the respective probabilities

$$\begin{aligned} P_{\Phi^-} &= 2\cos^4\frac{\theta_A}{2}\cos^2\phi_A\sin^2\phi_A \\ P_{\Psi^+} &= \frac{1}{2}\sin^2\theta_A\cos^2\phi_A \\ P_{\Psi^-} &= \frac{1}{2}\sin^2\theta_A\sin^2\phi_A. \end{aligned} \tag{16}$$

Hence, due to Eve's intervention Bob obtains a result uncor-

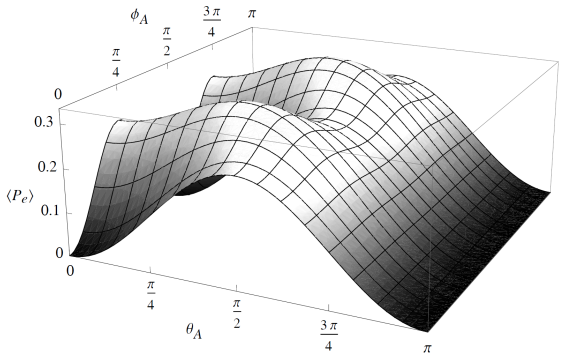

Figure 5. Error probability $\langle P_e \rangle$ depending on θ_A and ϕ_A

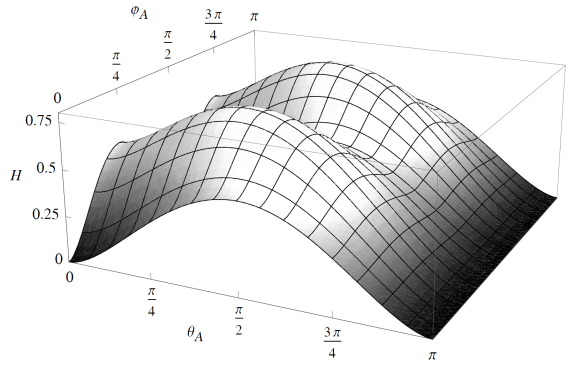

Figure 6. Shannon entropy H of the raw key depending on θ_A and ϕ_A

related to Alice's outcome with probability

$$\begin{aligned} P_e &= P_{\Phi^-} + P_{\Psi^+} + P_{\Psi^-} \\ &= \frac{1}{2}\Big(\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\big(2\phi_A\big)\Big). \end{aligned} \tag{17}$$

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

$$\begin{aligned} P_{\varphi_1} &= \frac{\cos^4\frac{\theta_A}{2}\cos^4\phi_A}{\frac{1}{4}(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + \sin^4\frac{\theta_A}{2}} \\ P_{\varphi_2} &= \frac{\cos^4\frac{\theta_A}{2}\sin^4\phi_A}{\frac{1}{4}(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + \sin^4\frac{\theta_A}{2}} \\ P_{\varphi_3} &= \frac{-\sin^2\frac{\theta_A}{2}}{(3+\cos 4\phi_A)\cos^4\frac{\theta_A}{2} + 4\sin^4\frac{\theta_A}{2}} \end{aligned} \tag{18}$$

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 [25] [26]. 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 $\langle P_e \rangle_A$ can be directly computed using (17) and its variations based on Alice's measurement result as

$$\langle P_e \rangle_A = \frac{1}{4}\left[\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\Big(2\phi_A\Big)\right]. \tag{19}$$

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 (18))

$$\begin{aligned} \langle P_c \rangle_A = \frac{1}{64}\Big(&53 - 4\cos\theta_A + 7\cos\big(2\theta_A\big) \\ &+ 8\cos^4\frac{\theta_A}{2}\cos\big(4\phi_A\big)\Big). \end{aligned} \tag{20}$$

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

$$H_A = \frac{1}{2}\left[h\Big(\cos^2\frac{\theta_A}{2}\Big) + \cos^2\frac{\theta_A}{2}\; h\Big(\cos^2\phi_A\Big)\right]. \tag{21}$$

Here, the function $h(x)$ describes the binary entropy, i.e.,

$$h\big(x\big) = -x\log_2 x - \big(1-x\big)\log_2\big(1-x\big) \tag{22}$$

with $\log_2$ the binary logarithm.

As we can directly see from Figure 5, the average error probability $\langle P_e \rangle_A$ has its maximum at 1/3 with

$$\theta_{A_0} \simeq 0.39183\pi \qquad \phi_{A_0} \in \Big\{\frac{\pi}{4}, \frac{3\pi}{4}\Big\}. \tag{23}$$

For this choice of θ_A and ϕ_A we see from Figure 6 that the Shannon entropy is also maximal with $H_A \simeq 0.79248$. Hence, the adversary Eve is left with a mutual information of

$$I_{AE} = 1 - H_A = 0.20752 \tag{24}$$

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. [2] [4] [22] [14]) or the application of a simplified basis transformation (cf. [25] [26]).

Unfortunately, the angle for $\theta_{A_0} \simeq 0.39183\pi$ to reach the maximum value is rather odd and might be difficult to realize in a practical implementation. In this context, difficult to realize in a physical implementation means that a transformation about an angle of $\pi/4$ or $3\pi/8$ is easier to implement in a laboratory than an angle of 0.39183π. Therefore, choosing an angle $\theta_A = 3\pi/8$ for this scenario we can compute from (19) an average error rate of $\langle P_e \rangle_A \simeq 0.33288$ and from (21) the respective Shannon entropy $H_A \simeq 0.79148$ (cf. also Figure 5 and Figure 6), which are both just insignificantly lower than their maximum values. Accordingly, Eve's mutual information on the raw key is $I_{AE} \simeq 0.20852$, which is slightly above the maximum given in (24). Hence, the security of the protocol is drastically increased using a general basis transformation compared to the application of a Hadamard operation.

V. 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 (19) as well as the Shannon entropy H in (21) 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.

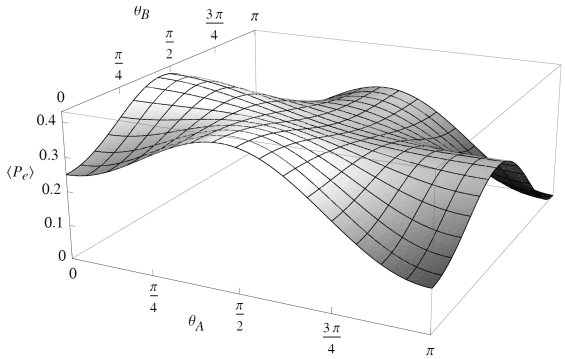

Figure 7. Error probability $\langle P_e \rangle$ depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$.

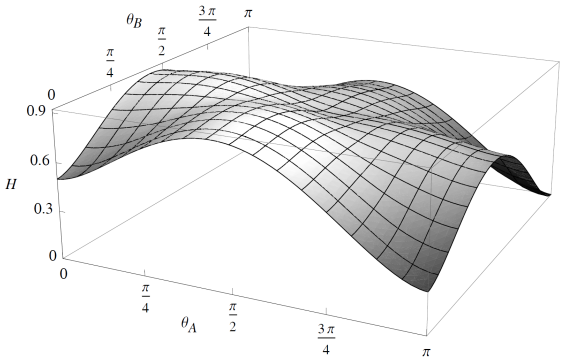

Figure 8. Shannon entropy H of the raw key depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$.

The application of these two different basis transformations alters the state introduced by Eve accordingly to

$$|\delta'\rangle_{1QR4TU} = T_x^{(1)}\big(\theta_A, \phi_A\big)\; T_x^{(4)}\big(\theta_B, \phi_B\big)\; |\delta\rangle_{1QR4TU} \quad (25)$$

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 (13) 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 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 four scenarios: 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 (19) above, the overall error probability can be computed as

$$\begin{aligned}
\langle P_e \rangle_{AB} = &\frac{1}{8}\left[\sin^2\theta_A + \cos^4\frac{\theta_A}{2}\sin^2\Big(2\phi_A\Big)\right] \\
&+\frac{1}{8}\left[\sin^2\theta_B + \cos^4\frac{\theta_B}{2}\sin^2\Big(2\phi_B\Big)\right] \\
&+\frac{1}{16}\left[\sin^2\Big(\theta_A + \theta_B\Big)\right. \\
&\qquad\left.+\cos^4\frac{\theta_A + \theta_B}{2}\sin^2\Big(2\big(\phi_A + \phi_B\big)\Big)\right] \\
&+\frac{1}{16}\left[\sin^2\Big(\theta_A - \theta_B\Big)\right. \\
&\qquad\left.+\cos^4\frac{\theta_A - \theta_B}{2}\sin^2\Big(2\big(\phi_A - \phi_B\big)\Big)\right]
\end{aligned} \quad (26)$$

having its maximum at $\langle P_e \rangle_{AB} \simeq 0.41071$. One possibility to reach the maximum is to choose the angles

$$\begin{aligned}
\theta_A &= 0 & \theta_B &\simeq 0.45437\pi \\
\phi_A &= \frac{\pi}{4} & \phi_B &= \frac{\pi}{4}.
\end{aligned} \quad (27)$$

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. Therefore, the graph of the average error probability plotted in Figure 7 uses $\phi_A = \phi_B = \pi/4$.

Following the same argumentation and using (21) from above, the Shannon entropy can be calculated as

$$\begin{aligned}
H_{AB} = &\frac{1}{4}\left[h\Big(\cos^2\frac{\theta_A}{2}\Big) + \cos^2\frac{\theta_A}{2}\; h\Big(\cos^2\phi_A\Big)\right] \\
&+\frac{1}{4}\left[h\Big(\cos^2\frac{\theta_B}{2}\Big) + \cos^2\frac{\theta_B}{2}\; h\Big(\cos^2\phi_B\Big)\right] \\
&+\frac{1}{8}\left[h\Big(\cos^2\frac{\theta_A + \theta_B}{2}\Big)\right. \\
&\qquad\left.+\cos^2\frac{\theta_A + \theta_B}{2}\; h\Big(\cos^2\big(\phi_A + \phi_B\big)\Big)\right] \\
&+\frac{1}{8}\left[h\Big(\cos^2\frac{\theta_A - \theta_B}{2}\Big)\right. \\
&\qquad\left.+\cos^2\frac{\theta_A - \theta_B}{2}\; h\Big(\cos^2\big(\phi_A - \phi_B\big)\Big)\right]
\end{aligned} \quad (28)$$

having its maximum at $H_{AB} \simeq 0.9452$ (cf. Figure 8 for a plot of (28) taking $\phi_A = \phi_B = \pi/4$). This maximum is reached, for example, using

$$\begin{aligned}
\theta_{AB_0} &\simeq -0.18865\pi & \theta_{AB_0} &\simeq 0.42765\pi \\
\phi_{AB_0} &\simeq -0.22405\pi & \phi_{AB_0} &\simeq 0.36218\pi.
\end{aligned} \quad (29)$$

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

$$\begin{aligned}
\theta_A &= -\frac{3\pi}{16} & \theta_B &= \frac{7\pi}{16} \\
\phi_A &= -\frac{\pi}{4} & \phi_B &= \frac{3\pi}{8}
\end{aligned} \quad (30)$$

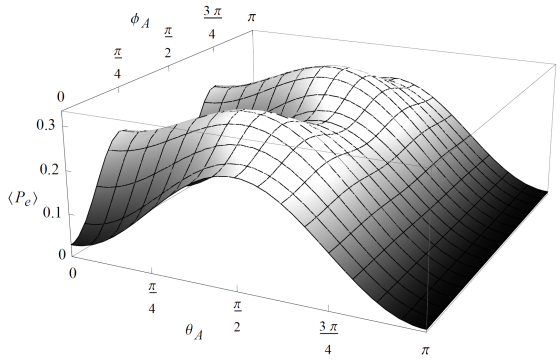

Figure 9. Error probability $\langle P_e \rangle$ depending on θ_A and ϕ_A. Here, a standard deviation $(\delta\varphi) = \pi/20$ of the angles is taken into account.

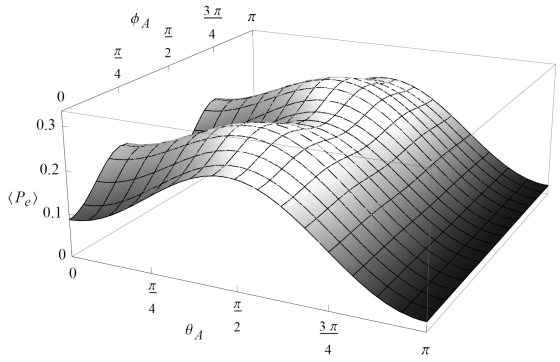

Figure 10. Error probability $\langle P_e \rangle$ depending on θ_A and ϕ_A. Here, a standard deviation $(\delta\varphi) = \pi/10$ of the angles is taken into account.

leading to an almost optimal Shannon entropy $H_{AB} \simeq 0.9399$ and a average respective error probability $\langle P_e \rangle_{AB} \simeq 0.39288$. Keeping ϕ_A and ϕ_B fixed – as already discussed in the previous section – such that

$$\begin{aligned} \theta_A &= \frac{3\pi}{16} \qquad \theta_B = \frac{7\pi}{16} \\ \phi_A &= \frac{\pi}{4} \qquad \phi_B = \frac{\pi}{4} \end{aligned} \tag{31}$$

the same average error probability $\langle P_e \rangle_{AB} \simeq 0.39288$ and a slightly smaller Shannon entropy $H_{AB} \simeq 0.91223$ 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%.

VI. Robustness of the Optimal Angles

As already pointed out above, the optimal values for the angles $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ are rather odd and might not be easy to create in a laboratory. Especially when looking at the combined application of basis transformations at Alice's and Bob's side, it will be very difficult to implement the exact angles given in (29) to achieve the optimal values for $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$. Furthermore, due to physical limitations the apparatus, which is used to adjust the angles $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ in the laboratory can in general not be considered perfect. To model an error introduced by this imperfect apparatus, we will use a Gaussian distribution to describe the angles $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$. In this context, we will look in detail at two rather small standard deviations from the optimal angles, i.e., in the order of 5% and 10% of π, and how this deviation from the optimal angle affects the security of the protocol.

In detail, a Gaussian distribution for some angle x can be described as

$$f\Big[x, x_0, (\delta x)\Big] = \frac{1}{\sqrt{2\pi}(\delta x)}\, e^{-\frac{(x-x_0)^2}{2(\delta x)^2}} \tag{32}$$

with x_0 the expected value (e.g., the optimal angle for some configuration) and (δx) the standard deviation (the deviation from that optimal angle). Accordingly, the mean value is described by the area under the curve, and is computed by the integral

$$\int_{-\infty}^{\infty} f\Big[x, x_0, (\delta x)\Big] dx = 1. \tag{33}$$

Based on this definition, the mean value for the cosine function $\cos(\lambda x)$ of some angle x and a real number λ can be computed directly as

$$\begin{aligned} \overline{\cos(\lambda x)} &= \int_{-\infty}^{\infty} f\Big[x, x_0, (\delta x)\Big] \cos(\lambda x) dx \\ &= e^{-\lambda^2 \frac{(\delta x)^2}{2}} \cos(\lambda x_0). \end{aligned} \tag{34}$$

Taking this approach into account, we can rephrase the calculations leading to the expected error probability $\langle P_e \rangle_A$ given in (19) and $\langle P_e \rangle_{AB}$ given in (26). This leads to a representation of the expected error probability depending on the deviation from the optimal value for the angles $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$, respectively. The computation of the Shannon entropy H_A described in (21) and H_{AB} described in (28) using this approach is more complex due to the application of the binary logarithm when computing the binary entropy h. Hence, we will not provide it here.

First, we describe this extension with regards to the expected error probability $\langle P_e \rangle_A$ in (19). Therefore, we use the equalities

$$\begin{aligned} \sin^2(x) &= \frac{1}{2}\Big[1 - \cos(2x)\Big] \qquad \text{and} \\ \cos^4(x) &= \frac{1}{8}\Big[\cos(4x) + 4\cos(2x) + 3\Big] \end{aligned} \tag{35}$$

as well as the definition in (34) above. After a few computations we see that

$$\begin{aligned} \overline{\langle P_e \rangle_A} &= \frac{1}{4}\Bigg[\frac{1}{2}\Big(1 - \overline{\cos(2\theta_A)}\Big) \\ &\quad + \frac{1}{8}\Big(\overline{\cos(2\theta_A)} + 4\,\overline{\cos(\theta_A)} + 3\Big) \\ &\quad \times \frac{1}{2}\Big(1 - \overline{\cos(4\phi_A)}\Big)\Bigg] \\ &= \frac{1}{4}\Bigg[\frac{1}{2}\Big(1 - e^{-2(\delta\varphi)^2}\cos(2\theta_{A_0})\Big) \\ &\quad + \frac{1}{8}\Big(e^{-2(\delta\varphi)^2}\cos(2\theta_{A_0}) \\ &\quad + 4\, e^{-\frac{1}{2}(\delta\varphi)^2}\cos(\theta_{A_0}) + 3\Big) \\ &\quad \times \frac{1}{2}\Big(1 - e^{-8(\delta\varphi)^2}\cos(4\phi_{A_0})\Big)\Bigg] \end{aligned} \tag{36}$$

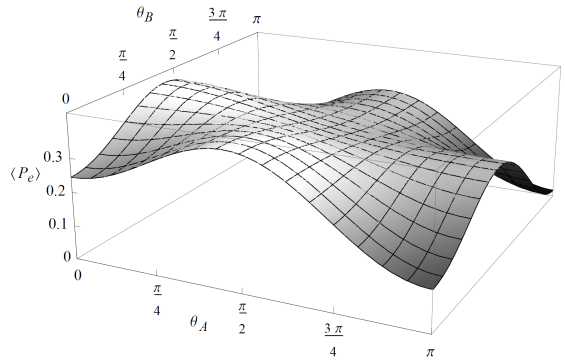

Figure 11. Error probability $\langle P_e \rangle$ depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$. Here, a standard deviation $(\delta\varphi) = \pi/20$ of the angles is taken into account.

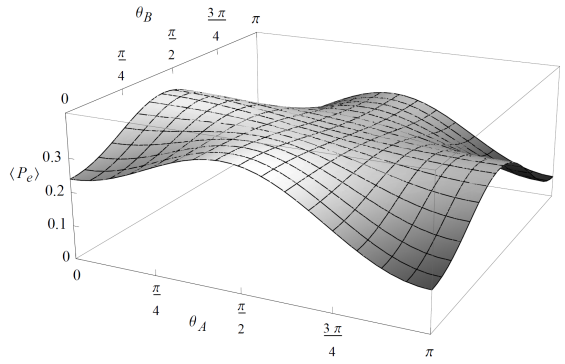

Figure 12. Error probability $\langle P_e \rangle$ depending on θ_A and θ_B. The remaining parameters ϕ_A and ϕ_B are fixed at $\pi/4$. Here, a standard deviation $(\delta\varphi) = \pi/10$ of the angles is taken into account.

For reasons of simplicity, we use the same standard deviation for both angles θ_A and ϕ_A such that $(\delta\theta_A) = (\delta\phi_A) = (\delta\varphi)$.

As we can conclude from (36), a deviation from the optimal angles θ_{A_0} and ϕ_{A_0} results in a reduced expected error probability $\overline{\langle P_e \rangle_A}$ (cf. also Figure 9 and Figure 10). Additionally, the expected error probability does not reach 0 any more due to the attenuation by the Gaussian distribution. Considering, for example, a standard deviation $(\delta\varphi) = \pi/20$, the maximum is slightly reduced by 4% (compared to (19)) from 1/3 to $\overline{\langle P_e \rangle_A} \simeq 0.3194$. This value is achieved using

$$\theta_{A_0} \simeq 0.40108\pi \qquad \phi_{A_0} \in \left\{\frac{\pi}{4}, \frac{3\pi}{4}\right\}. \tag{37}$$

Furthermore, taking a bigger standard deviation $(\delta\varphi) = \pi/10$, the maximum is reduced by almost 14% to $\overline{\langle P_e \rangle_A} \simeq 0.28826$.

It is also easy to see from (36) that the more precise the apparatus works, i.e., the smaller $(\delta\varphi)$ becomes, the closer the values $\overline{\langle P_e \rangle_A}$ and $\langle P_e \rangle_A$ get. Hence, we reach the limit

$$\lim_{(\delta\varphi)\to 0} \overline{\langle P_e \rangle_A} = \frac{1}{4}\left[\sin^2\theta_{A_0} + \cos^4\frac{\theta_{A_0}}{2}\sin^2\Big(2\phi_{A_0}\Big)\right] \tag{38}$$

which directly corresponds to $\langle P_e \rangle_A$ in (19).

Similarly, looking at the expected error probability $\langle P_e \rangle_{AB}$ in (26) when two different basis transformations are applied at Alice's and Bob's side, we can rewrite (26) such that

$$\begin{aligned}\langle P_e \rangle_{AB} = \frac{1}{2}\langle P_e \rangle_A + \frac{1}{2}\langle P_e \rangle_B \\ + \frac{1}{4}\langle P_e \rangle_{A+B} + \frac{1}{4}\langle P_e \rangle_{A-B}\end{aligned} \tag{39}$$

where

$$\begin{aligned}\langle P_e \rangle_{A+B} = \frac{1}{4}\Bigg[\sin^2\Big(\theta_A + \theta_B\Big) + \\ \cos^4\frac{\theta_A + \theta_B}{2}\sin^2\Big(2(\phi_A + \phi_B)\Big)\Bigg]\end{aligned} \tag{40}$$

and $\langle P_e \rangle_{A-B}$ accordingly. Based on these two equations, we can directly calculate the expected error probability $\overline{\langle P_e \rangle_{AB}}$ as

$$\begin{aligned}\overline{\langle P_e \rangle_{AB}} = \frac{1}{2}\overline{\langle P_e \rangle_A} + \frac{1}{2}\overline{\langle P_e \rangle_B} \\ + \frac{1}{4}\overline{\langle P_e \rangle_{A+B}} + \frac{1}{4}\overline{\langle P_e \rangle_{A-B}}.\end{aligned} \tag{41}$$

In this case, we again use the same standard deviation for all angles, such that $(\delta\theta_A) = (\delta\phi_A) = (\delta\theta_B) = (\delta\phi_B) = (\delta\varphi)$. An explicit representation (as we have provided it in (36) for $\overline{\langle P_e \rangle_A}$) of the above expression would be rather lengthy and therefore is not provided here. Nevertheless, the terms are similar to the result in (36) and we can directly compute the new maxima of the expected error probability. Considering again a standard deviation $(\delta\varphi) = \pi/20$, the maximum is slightly reduced by approximately 4% from 0.41071 to $\overline{\langle P_e \rangle_{AB}} \simeq 0.39599$ compared to (26). This value is achieved using

$$\begin{aligned}\theta_{A_0} = 0 \qquad \theta_{B_0} \simeq 0.45264\pi \\ \phi_{A_0} = \frac{\pi}{4} \qquad \phi_{B_0} = \frac{\pi}{4}.\end{aligned} \tag{42}$$

Applying a bigger standard deviation of $(\delta\varphi) = \pi/10$, these values just slightly change, i.e.,

$$\begin{aligned}\theta_{A_0} = 0 \qquad \theta_{B_0} \simeq 0.44703\pi \\ \phi_{A_0} = \frac{\pi}{4} \qquad \phi_{B_0} = \frac{\pi}{4}.\end{aligned} \tag{43}$$

and the maximum is further decreased by approximately 11% to $\overline{\langle P_e \rangle_{AB}} \simeq 0.36444$.

Analogous to (38), it is easy to see that also the expected error probability $\overline{\langle P_e \rangle_{AB}}$ for the combined application of two basis transformations reaches a limit when $(\delta\varphi)$ approaches 0, which corresponds to $\langle P_e \rangle_{AB}$ from (26) above, i.e.,

$$\begin{aligned}\lim_{(\delta\varphi)\to 0} \overline{\langle P_e \rangle_{AB}} = \lim_{(\delta\varphi)\to 0} \frac{1}{2}\overline{\langle P_e \rangle_A} \\ + \lim_{(\delta\varphi)\to 0} \frac{1}{2}\overline{\langle P_e \rangle_B} \\ + \lim_{(\delta\varphi)\to 0} \frac{1}{4}\overline{\langle P_e \rangle_{A+B}} \\ + \lim_{(\delta\varphi)\to 0} \frac{1}{4}\overline{\langle P_e \rangle_{A-B}}.\end{aligned} \tag{44}$$

As already pointed out above, when it comes to the computation of the Shannon entropy H, the terms are rather complex to evaluate symbolically due to the application of the binary entropy. Based on the above computations in (36) and (41) in context with the expected error probability, we can assume that also the graphs describing the Shannon entropy will be similar to Figure 6 and Figure 8. Due to the application of the Gaussian

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 $\phi_{A,B}$.

	$\phi_A = 0$	$\phi_A = \frac{\pi}{2}$	$\phi_A = \frac{\pi}{4}$
$\phi_B = 0$	$\theta_A = 0, \theta_B = 0$ $\langle P_e \rangle = 0$ $I_{AE} = 1$	$\theta_A = \frac{\pi}{2}, \theta_B = 0$ $\langle P_e \rangle = 0.25$ $I_{AE} = 0.5$	$\theta_A = \frac{3\pi}{8}, \theta_B = 0$ $\langle P_e \rangle \simeq 0.333$ $I_{AE} \simeq 0.208$
$\phi_B = \frac{\pi}{2}$		$\theta_A = \frac{\pi}{2}, \theta_B = \frac{\pi}{4}$ $\langle P_e \rangle = 0.25$ $I_{AE} \simeq 0.45$	$\theta_A = 0, \theta_B = \frac{\pi}{2}$ $\langle P_e \rangle \simeq 0.406$ $I_{AE} = 0.125$
$\phi_B = \frac{\pi}{4}$			$\theta_A = \frac{3\pi}{16}, \theta_B = \frac{7\pi}{16}$ $\langle P_e \rangle = 0.393$ $I_{AE} = 0.088$

TABLE II. OVERVIEW OF THE MEAN VALUE OF THE ERROR RATE $\overline{\langle P_E \rangle}$ FOR DIFFERENT STANDARD VARIATIONS ($\delta\varphi$) AND DIFFERENT VALUES OF $\theta_{A,B}$ AND $\phi_{A,B}$.

	$\theta_A = \frac{3\pi}{8}, \theta_B = 0$ $\phi_A = \frac{\pi}{4}, \phi_B = 0$	$\theta_A = 0, \theta_B = \frac{\pi}{2}$ $\phi_A = \frac{\pi}{4}, \phi_B = \frac{\pi}{2}$	$\theta_A = \frac{3\pi}{16}, \theta_B = \frac{7\pi}{16}$ $\phi_A = \frac{\pi}{4}, \phi_B = \frac{\pi}{4}$
$(\delta\varphi) = 0$	$\overline{\langle P_e \rangle} \simeq 0.333$	$\overline{\langle P_e \rangle} \simeq 0.406$	$\overline{\langle P_e \rangle} \simeq 0.393$
$(\delta\varphi) = \frac{\pi}{20}$	$\overline{\langle P_e \rangle} \simeq 0.318$	$\overline{\langle P_e \rangle} \simeq 0.386$	$\overline{\langle P_e \rangle} \simeq 0.381$
$(\delta\varphi) = \frac{\pi}{10}$	$\overline{\langle P_e \rangle} \simeq 0.286$	$\overline{\langle P_e \rangle} \simeq 0.359$	$\overline{\langle P_e \rangle} \simeq 0.355$

distribution (and the respective standard deviation) for the angles $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ the graphs will be attenuated like it is depicted for the error probability in Figure 9 to Figure 12. Thus, the maximum Shannon entropy will also be decreased, which means that the maximum of the adversary's information I_{AE} will be increased. As we have seen above, even if we consider a rather large deviation of $\pi/10$, the variation of the Shannon entropy will be around 15%. Hence, we can assume that the increase of the adversary's information will not become critical in such a way that the protocol becomes insecure.

VII. Security 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 [14] [17] [18] 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 [2]–[4].

Giving Alice an increased degree of freedom, i.e., choosing both angles θ_A and ϕ_A of the basis transformation 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. (21)). This is a reduction by almost 60% compared to QKD schemes described in [2]–[4] [14] [18] and more than 50% compared to the combined application of two different basis transformations (cf. also [25] [26]). At the same time, the expected error probability is increased by one third to $\langle P_e \rangle_A \simeq 0.333$ (cf. (19)). 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, the minimum of $I_{AE} \simeq 0.0548$ is reached with a rather odd configuration for $\theta_{\{A,B\}}$ and $\phi_{\{A,B\}}$ as described Section V. 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 (30) and (31). 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 $\langle P_e \rangle_{AB} \simeq 0.393$ (cf. (31) 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 $\langle P_e \rangle_{AB} \simeq 0.406$. The adversary's information is nowhere near the minimum but still rather low at $I_{AE} = 0.125$.

Although the configurations described above are much simpler with regards to the angles that have to be prepared, we also pointed out that a potential deviation from these angles has to be taken into account. This deviation is coming from the imperfect configuration of the physical apparatus and can be modeled using a Gaussian distribution. Fortunately, the above configurations are very robust in withstanding this variance such that even a large deviation of $\pi/10$ does not cause a large variation in the expected error rate. For example, with a deviation of $(\delta\varphi) = \pi/10$ the error probability $\overline{\langle P_e \rangle_{AB}}$ is decreased only by about 11% compared to the optimal error probability $\langle P_e \rangle_{AB}$. This also holds compared to the simpler configurations above, as described in Table II. Hence, even if the angles can not be configured precisely, the expected error probability is not drastically decreased and the security of the protocol is not jeopardized.

In terms of security, these results represent a huge advantage over existing QKD protocols based on entanglement swapping [14], [17], [18] or standard prepare and measure protocols [2]–[4]. 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 ($\langle P_e \rangle_{AB} \simeq 0.333$) and more than one half ($\langle P_e \rangle_{AB} = 0.411$) higher in the scenarios described here than in the standard protocols, which makes it easier to detect an adversary.

VIII. Conclusion

In this article, we discussed the effects of basis transformations on the security of QKD protocols based on entanglement swapping. Additionally, we looked at the robustness of these QKD protocols against an imperfect preparation of these basis transformations. 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 analyzed 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 $I_{AE} \simeq 0.2075$, 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 [25] [26]. 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 $\langle P_e \rangle \simeq 0.4107$.

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 values for $\langle P_e \rangle$ and I_{AE}, which are almost maximal, can be reached with more convenient values for θ and ϕ. In this case, the adversary's information is still $I_{AE} < 0.1$ with an expected error probability $\langle P_e \rangle \simeq 0.393$ for a combined application of two basis transformations.

To take the effects of an imperfect preparation of these angles into account, the angles are described using a Gaussian distribution. Based on that model, the effects of two certain values for the standard deviation on the expected error probability are analyzed. In this context, we showed that the variation in the expected error probability is with 11% - 14% rather low even for a large deviation of $\pi/10$. With regards to the application of the Gaussian distribution, we showed that also for these more practical values of θ and ϕ the variation of the expected error probability as well as the increase of the adversary's information is rather low. Hence, we can conclude that the protocol is robust against this kind of error and the gain of the adversary's information will not become critical in such a way that the protocol becomes insecure.

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] S. Schauer and M. Suda, "Optimal Choice of Basis Transformations for Entanglement Swapping Based QKD Protocols," in ICQNM 2014, The Eighth International Conference on Quantum, Nano and Micro Technologies. IARIA, 2014, pp. 8–13.

[2] 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.

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

[4] 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.

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

[6] 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.

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

[8] 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.

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

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

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

[12] 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.

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

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

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

[16] 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.

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

[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, 2006, pp. 899–906.

[19] 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.

[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, 1993, pp. 4287–4290.

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

[22] 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.

[23] 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.

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

[25] 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.

[26] ——, "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.