Effects of Noise on the Security of Entanglement Swapping Based QKD Protocols

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

***Abstract*—In this article, we discuss the effects of noise in a quantum channel on the security of quantum key distribution protocols based on entanglement swapping. Therefore, we look at two different models of quantum noise, the depolarization channel and the decoherence channel. Based on these models, we examine at first the effects on entanglement swapping and further the implications on the security parameters in quantum cryptography. We are able to show that a fidelity of at least 0.9428 is necessary to guarantee the security of the protocol. Additionally, we take the exponential decrease of entanglement over the distance between the communication parties into account. Using the photonic channel with coherence lengths from 10 km to 50 km as a reference model, we find that in this scenario the maximum length of a quantum channel for secure communication based on entanglement swapping lies between 1.19 km and 6.12 km.**

***Keywords*—quantum key distribution; entanglement swapping; noisy channels; security analysis.**

I. INTRODUCTION

Quantum key distribution (QKD) is an important application of quantum mechanics and QKD protocols have been studied at length in theory and in practical implementations [1], [2], [3], [4], [5], [6], [7], [8]. Most of these protocols focus on prepare and measure schemes, where single qubits are in transit between the communication parties Alice and Bob. The security of these protocols has been discussed in depth and security proofs have been given for example in [9], [10], [11]. In addition to these prepare and measure protocols, several protocols based on the phenomenon of entanglement swapping have been introduced [12], [13], [14], [15], [16]. In these protocols, entanglement swapping is used to obtain correlated measurement results between the legitimate communication parties, Alice and Bob. In other words, each party performs a Bell state measurement and due to entanglement swapping their results are correlated and further on used to establish a secret key.

Entanglement swapping has been introduced by Bennett et al. [17], Zukowski et al. [18] as well as Yurke and Stolen [19], respectively. It provides the unique possibility to generate entanglement from particles that never interacted in the past. In detail, Alice and Bob share two Bell states of the form $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ such that afterwards Alice is in possession of qubits 1 and 3 and Bob of qubits 2 and 4 (cf. (2) in Figure 1). The overall state can now be written as

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

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

The effects of noise on entangled states have already been discussed in detail in literature. It has been pointed out that the fidelity is reduced due to the noise in a quantum channel and entanglement purification methods have been developed to overcome this problem [20], [21], [22], [23]. In principle, entanglement purification can be used to bring a tempered entangled state arbitrarily close to a pure stated given the required resources. This is one of the reasons why the security of QKD protocols based on entanglement swapping has been discussed on the surface so far. They have only been analyzed using pure states in an idealistic environment (loss-free quantum channels, perfect devices, etc.) not considering the noise in a real-world environment. In this article, we are going to look at the security of QKD protocols based on entanglement swapping in a noisy environment. Using the *depolarizing channel* as well as the *dephasing channel* as reference models, the effect of the natural noise on entanglement swapping is described. Further, threshold values on the fidelity of the entanglement of the initial states are given, below which a secure communication is possible. Additionally, we look at the impact of the distance between Alice and Bob on the fidelity of entanglement and also estimate threshold values for the security of entanglement swapping QKD protocols in connection with the length of a quantum channel.

In the following section, we are going to shortly review the two most common noisy channel models, the depolarizing channel and the dephasing channel. In Section III, the effect of the noisy channels on entanglement swapping are described. In detail, the probabilities for uncorrelated results coming from entanglement swapping are computed. In the following Sections IV and V, we discuss the effects of noise on the security parameters and the maximal channel length for secure communication using these models. Here, we are relating the

 ISBN: 978-1-61208-303-2

fidelity of the initial states as well as the length of the quantum channel to upper bounds coming from current QKD protocols. In the end, we summarize the results and give a short outlook on the next steps into this topic.

II. Noisy Channel Models

In a classical communication, the only type of errors that occur are bit flip errors, i.e., a change from 0 to 1 and vice versa. Since qubits are more sophisticated systems than classical bits, two major types of errors can occur: bit flip and phase flip errors. Further, any linear combination of these two errors is possible. A bit flip and phase flip of a qubit is described by the Pauli operations σ_x and σ_z, respectively. Consequently, if both errors occur at the same time this can be described by the Pauli operation σ_y.

A very common way to characterize a noisy quantum channel is to use the *depolarizing channel* [24], [25]. This model takes both bit flip and phase flip errors on the qubit in transit into account and is therefore described by the application of all three Pauli operations σ_x, σ_y and σ_z. If the qubit transmitted over the noisy channel is part of an entangled state, the whole system is affected by the noisy channel. In case of a Bell state, e.g., $|\Phi^+\rangle$, the system of the two qubits after the effect of the depolarizing channel can be described by a Werner state [26]

$$\begin{aligned} W_F &= \mathrm{F}|\Phi^+\rangle\langle\Phi^+| \\ &+\frac{1-\mathrm{F}}{3}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big) \end{aligned} \tag{2}$$

with fidelity $\langle\Phi^+|W_F|\Phi^+\rangle = F$. A more common way to look at the Werner state is to describe it in connection with white noise, i.e.,

$$\rho = (1-p)|\Phi^+\rangle\langle\Phi^+| + p\frac{\mathbb{1}}{4} \tag{3}$$

where p is the error probability. In this case the fidelity can be easily computed as $\mathrm{F} = 1 - 3p/4$.

A more specialized model for a noisy quantum channel is the phase damping or also called *dephasing channel* [27]. This is a phase scrambling and energy preserving mechanism described by the two operators

$$\sqrt{\frac{1+e^{-p}}{2}}\mathbb{1} \qquad \text{and} \qquad \sqrt{\frac{1-e^{-p}}{2}}\sigma_z \tag{4}$$

with p again the probability that an error is introduced by the quantum channel. Looking at the scenario where one qubit of the Bell state $|\Phi^+\rangle$ is transmitted over the noisy channel, the resulting state can be described as

$$\chi = \frac{1+e^{-p}}{2}|\Phi^+\rangle\langle\Phi^+| + \frac{1-e^{-p}}{2}|\Phi^-\rangle\langle\Phi^-| \tag{5}$$

III. Entanglement Swapping in a Noisy Environment

As a consequence of the transmission of qubits over a noisy channel the operations on those qubits are affected, too. In the protocols we are dealing with in this article the most interesting operation is entanglement swapping. Following eq. (1) and Figure 1 we assume Alice prepares the Bell state $|\Phi^+\rangle\langle\Phi^+|_{12}$ and Bob prepares $|\Phi^+\rangle\langle\Phi^+|_{34}$ in their respective laboratories.

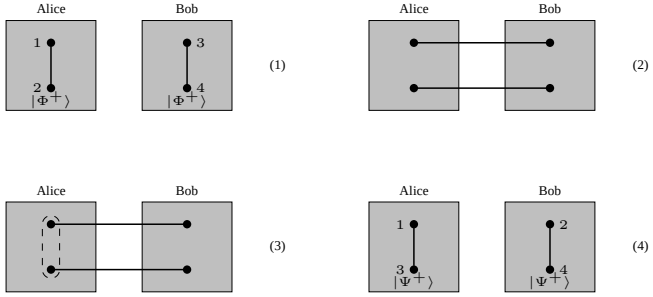

Fig. 1. Illustration of a standard setup for an entanglement swapping based QKD protocol.

They send qubits 2 and 3 to the other party over a depolarizing channel such that the overall system is described by $\rho \otimes \rho$. After Alice's Bell state measurement on qubits 1 and 3 in her possession the system of qubits 2 and 4 is (assuming Alice obtains $|\Phi^+\rangle\langle\Phi^+|_{13}$)

$$\begin{aligned} \rho_{24} =& \frac{4-6p+3p^2}{4}|\Phi^+\rangle\langle\Phi^+|_{24} \\ &+\frac{2p-p^2}{4}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big)_{24} \end{aligned} \tag{6}$$

which is again a Werner state (cf. eq. (2) above). Comparing this equation with eq. (1) describing entanglement swapping with pure states we directly see that Alice and Bob obtain correlated results only with probability

$$P_{corr} = \frac{4-6p+3p^2}{4} \tag{7}$$

and Bob's measurement yields an arbitrary state not correlated to Alice's measurement with probability

$$P_{err} = \frac{6p-3p^2}{4} \tag{8}$$

For QKD protocols based on entanglement swapping this means that an error is detected during the communication between Alice and Bob. Considering Figure 2 we see that performing entanglement swapping over a noisy channel gives reasonable results, i.e., it is more likely to obtain correlated results than uncorrelated, only if $P_{err} < P_{corr}$. The maximum error probability to achieve that is $(3-\sqrt{3})/3$, which is the point where $P_{err} = P_{corr}$, corresponding to a fidelity of the initial states of at least $F = 0.683$. This value indicates a lower bound on the initial states to make entanglement swapping possible.

Taking at a dephasing channel instead of a depolarizing channel into account, we obtain a different error rate. If Alice and Bob again prepare the states $|\Phi^+\rangle\langle\Phi^+|_{12}$ and $|\Phi^+\rangle\langle\Phi^+|_{34}$, the overall system after they sent their qubits over the quantum channel is described by $\chi \otimes \chi$. Alice performs a Bell state measurement on qubits 1 and 3 in her possession, which leads to the state (assuming again that Alice's result is $|\Phi^+\rangle\langle\Phi^+|_{13}$)

$$\begin{aligned} \chi_{24} =& \frac{1+e^{-2p}}{2}|\Phi^+\rangle\langle\Phi^+|_{24} \\ &+\frac{1-e^{-2p}}{2}|\Phi^-\rangle\langle\Phi^-|_{24} \end{aligned} \tag{9}$$

 ISBN: 978-1-61208-303-2

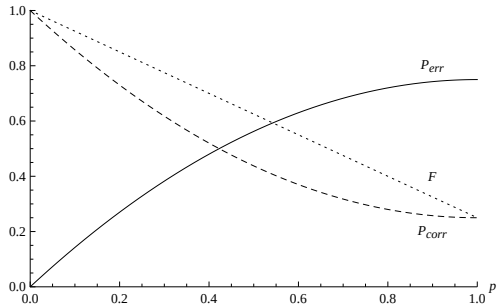

Fig. 2. The probabilities P_{corr} (dashed line) and P_{err} (solid line) from entanglement swapping in a depolarizing channel.

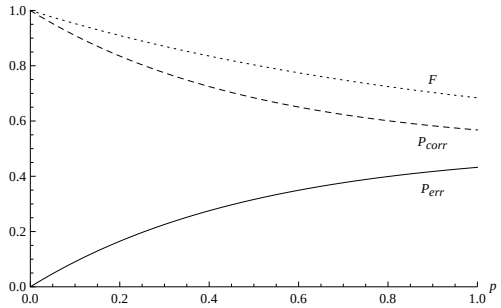

Fig. 3. The probabilities P_{corr} (dashed line) and P_{err} (solid line) from entanglement swapping in a dephasing channel.

Analogous to the depolarizing channel, Alice and Bob obtain correlated results only with probability

$$P_{corr} = \frac{1 + e^{-2p}}{2} \tag{10}$$

and they obtain different results with probability

$$P_{err} = \frac{1 - e^{-2p}}{2} \tag{11}$$

In contrary to the depolarizing channel, we see from Figure 3 that P_{corr} and P_{err} never intersect, i.e., it is always $P_{err} < P_{corr}$. This is a huge advantage, since the maximum probability that Alice and Bob obtain uncorrelated results is $P_{err} = 0.4323$ for $p = 1$, which is much smaller compared to the the error probability for the depolarizing channel defined in eq. (8) above. Nevertheless, this leads to almost the same minimal fidelity $\mathrm{F} = 0.6839$ compared to the required fidelity in the depolarizing channel described above, indicating that the dephasing channel has a much higher error tolerance.

IV. Effects on Security Parameters

To guarantee perfect security in quantum cryptography all noise – introduced naturally or by an adversary – is treated as it is caused by an eavesdropper. In particular, this leads to the rather paranoid but very useful assumption that Eve is able to exchange the noisy channel between Alice and Bob by a perfect quantum channel, i.e., a lossless channel where the polarization and phase are preserved. Hence, Eve can use the error Alice and Bob expect to come from their noisy channel to disguise her eavesdropping attempt. Additionally, in a realistic environment errors can also occur from the physical apparatus itself, affecting, e.g., the detector efficiency [28]. Since we are dealing with a theoretical model of the noisy quantum channel in this article, we are excluding the physical apparatus from our discussions limiting ourselves solely to errors coming from the noisy channel.

The first direct consequence for Alice and Bob when using noisy channels is that they can not allow an error rate larger than the error usually introduced by an adversary. For example, as it is described in most of the protocols based on entanglement swapping [12], [13], [14], [15], [16], the error rate due to Eve's intervention is 25%. If the natural error caused by a noisy channel is equal or larger than 25%, Alice and Bob will not detect Eve's presence. From eq. (8) we know that in case of a depolarizing channel Alice and Bob expect an error rate $P_{err} = 3(2 - p^2)/4$ from entanglement swapping such that $p < 0.1835$. This means, for a fidelity of the initial states $\mathrm{F} > 0.8624$ the natural error introduced by the depolarizing channel is always smaller than 25%, i.e., the error introduced by Eve. Similarly, due to the higher error tolerance of the dephasing channel Alice and Bob can handle a higher error probability compared to the depolarizing channel (cf. eq. (11) and eq. (8)). In this case $p < 0.3466$ and, accordingly, the fidelity of the initial states has to satisfy $\mathrm{F} > 0.8535$ such that the natural error introduced by dephasing is always smaller than 25%.

As discussed in detail in the following paragraphs, Eve has the opportunity to attack only a fraction of all qubits in transit between Alice and Bob. This reduces the error rate coming from her intervention but leaves Eve also with a smaller amount of information about the sifted key. To react on this threat, Alice and Bob perform error correction (EC) and privacy amplification (PA). A basic idea on how these two building blocks of quantum cryptography work and which methods are involved therein is given in [29] and [30]. We just want to stress that using these two primitives Eve's information about the key can be reduced to an arbitrary small amount. Furthermore, as pointed out in [31], to successfully perform error correction and privacy amplification based on one-way classical communication the error rate is bounded above by

$$P_{EC} = \frac{1 - \frac{1}{\sqrt{2}}}{2} \simeq 0.1465 \tag{12}$$

to be achievable [28]. Since the error correction still leaks some information to an adversary, privacy amplification is applied to the key to lower Eve's information to an arbitrary small amount. For a maximum error rate of $P_{PA} \simeq 0.11$ Eve's information can be reduced to at most one bit of the whole key (cf. [11], [32]). Therefore, in the following paragraphs, we define lower bounds on the fidelity of the initial states to achieve these two thresholds P_{EC} and P_{PA}.

Considering entanglement swapping in a noisy channel, we obtain the corresponding lower bounds p_{EC} and F_{EC} for an error rate $P_{err} \simeq 0.1465$ using eq. (8) from above (cf. also Figure 2)

$$p_{EC} \simeq 0.1029 \qquad \mathrm{F}_{EC} \simeq 0.9228. \tag{13}$$

Hence, the fidelity of the initial states has to be over 92% to make one-way error correction feasible. The final bounds p_{PA} and F_{PA} to achieve a maximum error rate of $\simeq 0.11$ and thus secure communication are then

$$p_{PA} \simeq 0.0762 \qquad \mathrm{F}_{PA} \simeq 0.9428, \tag{14}$$

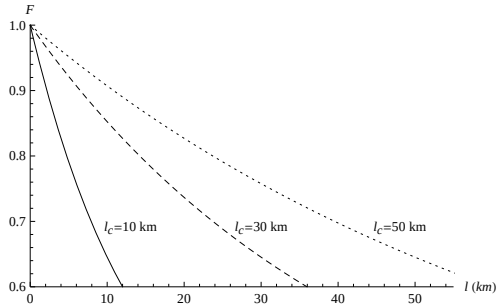

Fig. 4. Correlation between the fidelity F and the length l of a noisy quantum channel.

i.e., the fidelity has to be an additional 2% higher compared to eq. (13) to achieve the maximal tolerable error rate of $\simeq 11\%$.

Analogous to the computations above, the threshold values for the dephasing channel can be computed. By inserting into eq. (11) above we obtain

$$p_{EC} \simeq 0.1733 \qquad \mathrm{F}_{EC} \simeq 0.9204. \tag{15}$$

In this case, the error probability P_{EC} can be almost twice as high compared to the depolarizing channel resulting in almost the same fidelity for the initial states. Furthermore, the final bounds p_{PA} and F_{PA} are then

$$p_{PA} \simeq 0.1242 \qquad \mathrm{F}_{PA} \simeq 0.9415. \tag{16}$$

Again, the fidelity of the initial states is almost the same compared to the depolarizing channel, whereas the error probability can be almost twice as high.

V. Effects on the Channel Length

In a realistic environment we also have to take into account that the fidelity F of the entanglement decreases exponentially with the length l of the channel. Modeling our quantum channel as a *photonic channel* [33] it has been shown in [34] that the fidelity is given by

$$\mathrm{F} \simeq \left| \frac{1 + e^{-l/2l_c}}{2} \right|^2 \tag{17}$$

where l_c is the coherence length of an optical fiber. Therefore, we see from Figure 4 that the fidelity of the initial state is below 0.68 for a channel longer than 8.64 km and a coherence length $l_c = 10$ km, which means that entanglement swapping is no longer possible at this distance. For a higher coherence length, the maximum distance is increased accordingly to 25.91 km with $l_c = 30$ km or 43.19 km with $l_c = 50$ km. The decrease of the fidelity of entanglement has a huge impact on the security of quantum cryptography based on entanglement swapping as discussed above. In Figure 4, we used three different values for the coherence length l_c: 10 km, 30 km and 50 km. As we can directly see from Figure 4, a higher coherence length results in a smaller decrease of the fidelity. As shown in Section III, using a depolarization channel Alice and Bob need a fidelity of at least $\mathrm{F}_{EC} = 0.9228$ to perform error correction and a fidelity $\mathrm{F}_{PA} = 0.9428$ to reduce the error rate to 0.11. Furthermore, when using a dephasing channel the respective fidelities do not differ very much from these result, i.e., $\mathrm{F}_{EC} = 0.9204$ and $\mathrm{F}_{PA} = 0.9415$.

TABLE I. Comparison of minimal fidelity and maximal channel length in the depolarizing and dephasing channel.

Channel	**Coherence Length**		
Depolarizing	$l_c = 10$ km	$l_c = 30$ km	$l_c = 50$ km
$\mathrm{F}_{EC} \simeq 0.9228$	1.64 km	4.92 km	8.20 km
$\mathrm{F}_{PA} \simeq 0.9428$	1.19 km	3.59 km	5.98 km
Dephasing	$l_c = 10$ km	$l_c = 30$ km	$l_c = 50$ km
$\mathrm{F}_{EC} \simeq 0.9204$	1.69 km	5.08 km	8.47 km
$\mathrm{F}_{PA} \simeq 0.9415$	1.22 km	3.67 km	6.12 km

Combining our results from the previous section with eq. (17) we can directly see that in a quantum channel with coherence length $l_c = 10$ km F_{EC} limits the length of the quantum channel to 1.64 km when using a depolarizing channel. Moreover, to guarantee a fidelity F_{PA}, the length of the channel has to be at most 1.19 km (cf. Table I). Taking a higher coherence length of $l_c = 30$ km, the distance over which error correction is still possible increases to 4.92 km and the distance for secure communication increases to 3.59 km. In the third scenario where we take $l_c = 50$ km, we still get the fidelity F_{EC} at a distance of 8.20 km and the fidelity F_{PA} at a distance of 5.98 km. Using the dephasing channel the maximal distances do not differ very much from these values (cf. Table I).

These distances are still very low and of minor practical value for quantum communication since, for example, physical implementations of prepare and measure QKD protocols work over larger distances [5], [6], [7], [8]. Hence, Alice and Bob have to increase the fidelity of their entangled states before they can perform entanglement swapping, i.e., start the actual protocol. As already pointed out above, this is achieved using entanglement purification and nested purification protocols [20], [21], [22], [23]. Nevertheless, the fidelity can only be brought to its maximum in theory, since too many resources would be required. Hence, there will always be a certain error coming from entanglement swapping, which Alice and Bob have to deal with.

VI. Conclusion

In this article, we discussed the effect of noise on the security parameters of QKD protocols based on entanglement swapping. Therefore, we used two reference models for a noisy channel, the depolarizing channel and the more specific dephasing channel. Taking these two models into account, we showed that the fidelity of the initial states of a QKD protocol has to be at least $\mathrm{F} \simeq 0.68$ to obtain reasonable results from entanglement swapping. Regarding the security of QKD protocols, we looked at two threshold values often referred to in literature: P_{EC}, which describes the maximum error rate to make one-way classical error correction possible, and P_{PA}, which denotes the maximum error rate such that privacy amplification can be used to reduce the information of an adversary to a minimum. Based on these threshold values the minimal fidelity of the initial states was computed. Here, we showed that a minimal fidelity $\mathrm{F} \simeq 0.9428$ is required to obtain a maximum error rate of 0.11 in a depolarizing channel. Accordingly, in a dephasing channel the fidelity is slightly lower with $\mathrm{F} \simeq 0.9415$ (cf. also Table I).

 ISBN: 978-1-61208-303-2

Additionally, we discussed the exponential decrease of the fidelity when transmitted through a noisy channel. In this case, we looked in detail at the photonic channel as reference model and calculated the maximum length of a channel to achieve the minimal fidelities described above. For different coherence lengths of 10 km, 30 km, and 50 km we obtained maximum distances between 1.19 km and 6.12 km for a fidelity $F \simeq 0.94$.

As pointed out, these values are rather low compared to physical implementations of prepare and measure QKD protocols. Hence, one of our next steps is to refine the model for the decrease of entanglement over distance to a more practical scenario. Further, we want to investigate entanglement purification protocols in context with entanglement swapping based QKD protocols and their respective impacts on the security.

ACKNOWLEDGMENTS

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, 1996.

[21] D. Deutsch, A. Ekert, R. Josza, C. Machiavello, S. Popescu, and A. Sanpera, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," *Phys. Rev. Lett.*, vol. 77, no. 13, pp. 2818–2821, 1996.

[22] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state Entanglement and Quantum Error Correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[23] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum Repeaters Based on Entanglement Purification," *Phys. Rev. A*, vol. 59, no. 1, pp. 169–181, 1999.

[24] C. H. Bennett, C. A. Fuchs, and J. A. Smolin, "Entanglement-Enhanced Classical Communication on a Noisy Quantum Channel," *quant-ph/9611006 v1*, 1996.

[25] D. G. Fischer, M. Mack, M. A. Cirone, and M. Freyberger, "Enhanced Estimation of a Noisy Quantum Channel Using Entanglement," *Phys. Rev. A*, vol. 64, no. 2, p. 022309, 2001.

[26] R. F. Werner, "Quantum States with Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model," *Phys. Rev. A*, vol. 40, no. 8, p. 4277, 1989.

[27] I. Devetak and P. Shor, "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information," *Comm. Math. Phys*, vol. 256, no. 2, pp. 287–303, 2005.

[28] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[29] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *J. Crypt.*, vol. 5, no. 1, pp. 3–28, 1992.

[30] B. Huttner and A. Ekert, "Information Gain in Quantum Eavesdropping," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2455–2466, 1994.

[31] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, 2002.

[32] B. Kraus, N. Gisin, and R. Renner, "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication," *Phys. Rev. Lett.*, vol. 95, no. 8, p. 080501, 2005.

[33] S. J. van Enk, J. I. Cirac, and P. Zoller, "Photonic Channels for Quantum Communication," *Science*, vol. 279, no. 5348, pp. 205–208, 1998.

[34] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, 3rd ed. Springer, 2001.

 ISBN: 978-1-61208-303-2