ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Information Security
& Cryptography

Thesis to the Semester Project

Information-Theoretically Secure Key Agreement from Arbitrarily Correlated Information

Andreas Meier and Simon Heimlicher

Supervision: Renato Renner, Prof. Dr. Ueli M. Maurer
Publication: 11th July 2004

Contents

List of Figures

Abstract

The agreement of two parties on a secret, for instance to enable confidential communication, is a fundamental problem in cryptography. In this thesis, interactive information-theoretic secret key agreement is discussed for both noisy and quantum channels.

Non-interactive settings for secret key agreement based on the assumption that the adversary's channel is inferior to the legitimate channel were introduced by Wyner and later Csiszár and Körner. Interactive scenarios were discussed by Maurer and subsequently Ahlswede and Csiszár. In the latter settings, the adversary is not constrained by the above assumption, but the correlated information is assumed to consist of independent and identical parts.

In the first part of this text, recent results about smooth entropy by Renner and Wolf are used to derivate a lower bound for the secret key rate in an interactive scenario without constraints on the correlation.

In the second part, a quantum channel is discussed and it is shown how the secret key rate of the BB84 protocol can be increased substantially by replacing the sender's random variable with a noisy copy before performing the error correction in the Information Reconciliation phase.

1 Introduction

In many cryptographic applications, for example confidential communication, the agreement of both partners on a secret value is a fundamental problem.

It was shown by Shannon in his classic paper in 1948 [1], that perfect secrecy is only possible among communication partners who share a secret which is at least as long as the transmitted message. This effectively implies that any perfectly secret cipher cannot be more practical than Vernam's one-time pad [2].

However, in most practical cases the adversary's access to the ciphertext is not perfect. Often, it is bound by physical laws, e. g. by the inevitable noise on classical channels or the uncertainty principle when a quantum channel is used. Both these scenarios will be discussed.

Non-interactive settings for key agreement were introduced by Wyner in 1975 [3] and Csiszár and Körner in 1978 [4]. These models are based on the assumption that the adversary's channel is incurred by more noise than the one of the legitimate recipient. Interactive scenarios were proposed by Maurer in 1993 [5] and in the same year by Ahlswede and Csiszár [6]. In the above settings, the adversary's access to the channel is not required to be inferior to the access of the designated recipient, but the correlation of the information is assumed to comprise independent and identical parts.

Recent publications by Renner and Wolf [7], [8] and others [9] indicate that this assumptions can be done away with and generalisation to arbitrarily correlated information is possible. This will be discussed in the first part of the text. In the second part, key agreement over a quantum channel is studied and it is shown, how the secret key rate can be increased by replacing the sender's random variable with a noisy copy before performing the error correction in the Information Reconciliation phase.

This thesis is structured as follows: In Section 2, a short breakdown of the essential information-theoretic concepts is given. Section 3 comprises the application of results obtained by Renner and Wolf to derive a lower bound for the secret key rate in a scenario with arbitrarily correlated information. Section 4 discusses a recent idea in quantum cryptography which allows to increase the secret key rate using artificial noise. We conclude in Section 5. Appendix A provides excerpts from the Matlab code used to analyse the quantum channel of Section 4 and the task formulation is given in Appendix B.

2 Background Information

Among the fundamental problems in cryptography, the agreement of two parties on a common shared secret is of prime interest. In one of the basic cryptographic settings, where one party—usually called *Alice*—wants to transmit a message to another—*Bob*—without the eavesdropper *Eve* gaining a non-negligible amount of knowledge, this shared secret might be used as the key for a symmetric cipher.

Alice needs to give the secret key to Bob previously to, during, or after the transmission of the encrypted message via a communication channel to which Eve has no access that allows her to gain more than a negligible amount of information. Often, such a channel is very expensive or unavailable, especially in online contexts like e-commerce applications.

2.1 Computational Security

The above problem has been addressed by cryptographers around the world for ages. It was only in 1976 that Whitfield Diffie and Martin Hellman published a seminal paper [10] with a usable solution for this paradox problem. Their *Diffie-Hellman Key Agreement Protocol* allows two parties to agree on a shared secret via an authentic two-way communication channel which may be entirely public. However, the secrecy of this secret is based on the assumed yet unproven hardness of a mathematical problem—computing discrete logarithms—and it is thus called only *computationally-secure.* Its attributed security is based on complexity theory. The numbers involved in the key agreement protocol need to be chosen carefully to make it hard for an eavesdropper to compute the shared secret. In the case of the Diffie-Hellman Key Agreement, it suffices to compute the discrete logarithm of one of the exchanged numbers. As soon as a more efficient algorithm or a faster implementation for this problem is found, previously believed to be secure keys might be broken by an attacker with the right amount of time and money.

2.2 Information-Theoretical Security

In stark contrast, the security of *information-theoretically secure* cryptosystems can be proven based on information theory (cf. [1] and [11]). The success probability of an unlimited adversary can be made arbitrarily small by choosing the parameters of the protocol adequately. In this text, we only consider information-theoretically secure key agreement.

2.3 Information Measures

The amount of information contained in a random variable can be specified by information measures. The three measures we use are discussed in the rest of the section.

2.3.1 Shannon Entropy

Definition 2.1 (Shannon Entropy) *The* Shannon entropy $H(X)$ *of a random variable* X *with probability distribution* P_X *is defined as*

$$H(P_X) := \sum_{x \in \mathcal{X}} -P_X(x) \cdot \log_2 P_X(x) = \mathrm{E}[-\log_2 P_X] =: H(X)$$

where $0 \log_2 0 := 0$.

The conditional entropy $H(X|Y = y)$ of a random variable X conditioned on an event $\mathcal{A} = \{Y = y\}$ is given by

$$H(X|Y = y) := H(P_{X|Y=y}).$$

The binary entropy function is

$$h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x). \tag{2.1}$$

The Shannon Entropy is a suitable measure when many independent realisations of the same random variable can be assumed. In the context of Information Reconciliation or Privacy Amplification this is not assured and therefore other entropy measures like the (smoothed) Rényi entropy are appropriate.

2.3.2 Rényi Entropy

Definition 2.2 (Rényi Entropy) *The* Rényi entropy of order $\alpha \in \mathbb{R}^+ \setminus \{0, 1\}$ $H_\alpha(X)$ *of a probability distribution* P_X *with range* $\mathcal{X}$ *is given by*

$$H_\alpha(X) := \begin{cases} \hat{H}_\alpha(X) & \text{if } \alpha \notin \{0, 1, \infty\} \\ lim_{\alpha \to 0} \hat{H}_\alpha(X) & \text{if } \alpha = 0 \\ lim_{\alpha \to 1} \hat{H}_\alpha(X) & \text{if } \alpha = 1 \\ lim_{\alpha \to \infty} \hat{H}_\alpha(X) & \text{if } \alpha = \infty, \end{cases}$$

where

$$\hat{H}_\alpha(X) := \frac{1}{1 - \alpha} \log_2 \left(\sum_{x \in \mathcal{X}} P_X(x)^\alpha \right).$$

With α equal to zero, $H_0(X)$ leads to a measure for the maximal amount of uniform randomness that can be extracted from the random variable X and can also be written as:

$$H_0(X) = \log_2 \left(|\{x \in \mathcal{X} : P(x) > 0\}| \right).$$

With $\alpha = 1$, we get $H_1(X)$, which corresponds to the Shannon entropy:

$$H_1(X) = H(P).$$

Finally, $H_\infty(X)$ is a measure for the minimal length of an encoding of a random variable X, and is also known as *min-entropy*. Evaluating the limes leads to:

$$H_\infty(X) = -\log_2\left(\max_{x\in\mathcal{X}} P_X(x)\right).$$

These special cases of the Rényi entropy are related to each other as follows:

$$H_\infty(X) \leq H_1(X) \leq H_0(X).$$

In the special but common case, where many independent realisations of the same random variable X are considered, Rényi entropy converges to Shannon entropy:

$$H_\infty(X) = H_1(X) = H_0(X) = H(X).$$

The conditional Rényi entropy of order α of a random variable X conditioned on W is thus given by

$$H_\alpha(X|W) := \begin{cases} \min_{w\in\mathcal{W}} H_\alpha\left(X|W=w\right) & \text{if } \alpha > 1 \\ \max_{w\in\mathcal{W}} H_\alpha\left(X|W=w\right) & \text{if } \alpha < 1. \end{cases}$$

2.3.3 Smooth Rényi Entropy

Definition 2.3 (Smooth Rényi Entropy) *The* ε-smooth Rényi entropy of order α $H_\alpha^\varepsilon(X)$ *of a probability distribution* P_X *with range* $\mathcal{X}$ *and* $\alpha \in \mathbb{R}^\infty \setminus \{1\}$ *is*

$$H_\alpha^\varepsilon(X) := \begin{cases} \hat{H}_\alpha^\varepsilon(X) & \text{if } \alpha \notin \{0,\infty\} \\ lim_{\alpha\to 0}\hat{H}_\alpha^\varepsilon(X) & \text{if } \alpha = 0 \\ lim_{\alpha\to\infty}\hat{H}_\alpha^\varepsilon(X) & \text{if } \alpha = \infty, \end{cases}$$

where

$$\hat{H}_\alpha^\varepsilon(X) := \frac{1}{1-\alpha}\inf_{Q:\delta(P,Q)\leq\varepsilon}\log_2\left(\sum_{x\in\mathcal{X}} P_Q(x)^\alpha\right)$$

and Q *ranges over the set of probability distributions with alphabet* $\mathcal{X}$.

As with Rényi entropy, $H_0^\varepsilon(X)$ corresponds to the maximal uniform randomness that can be extracted from X, and $H_\infty^\varepsilon(X)$—the min-entropy—is a measure for the minimal encoding length of X. The additional parameter ε determines the maximal sum of the probabilities of realisations of X that are ignored. Note, that the smooth Rényi entropy is a powerful tool to analyse problems in the area of this thesis, but it is often infeasible to calculate this entropy within a reasonable amount of time.

The conditional smooth Rényi entropy for the special case of $\alpha = \infty$ is

$$H_\infty^\varepsilon(X|W) := \max_{P_{X'W'}:\delta(P'_XW',P_XW)<\varepsilon} H_\infty\left(X|W=w\right).$$

As a direct consequence, we have the following inequalities for a random variable X and $\mathcal{W} \subset \mathcal{X}$ and $\varepsilon \geq 0$:

$$H_0^\varepsilon(X) \leq \log_2|\mathcal{W}|, H_0^{\varepsilon+\varepsilon'}(XW) \qquad \leq H_0^\varepsilon(X) + H_0^{\varepsilon'}(W).$$

Since the min-entropy of a random variable X conditioned on W cannot decrease more than the Rényi entropy of order zero of W, we have:

$$H_\infty^{\varepsilon'+\varepsilon+\hat{\varepsilon}}(X|W) \geq H_\infty^{\varepsilon'}(XW) - H_0^\varepsilon(W) - \log_2\left(\frac{1}{\hat{\varepsilon}}\right). \tag{2.2}$$

For proofs of the above inequalities and further discussion of the smooth Rényi entropy measure, please refer to [8] and [9].

3 Information-Theoretic Secret Key Agreement

3.1 Introduction

3.1.1 Overview of the Protocol

In a setting commonly referred to as the *Satellite Scenario [5],* Alice, Bob and Eve each receive a string consisting of truly random bits disseminated by a communication satellite. It can be shown that Eve's channel has to be incurred by an error rate greater than zero (if she is listening) in order for the following protocol to work.

In a three-step protocol (cf. [7]), Alice and Bob agree on a secret key of which the eavesdropper, Eve, has arbitrarily little information, even if her error rate is considerably lower than the error rates of Alice and Bob.

In the first step, *Advantage Distillation,* Alice and Bob utilize an authentic public two-way channel to determine, which of their received bits are correct with high probability. This gives them an advantage over Eve.

Information Reconciliation, the next step, is essentially an error correction protocol between Alice and Bob. At the end of this phase, the strings of Alice and Bob are equal with overwhelming probability.

In the last step, *Privacy Amplification,* Alice and Bob extract a small part of information from their very insecure strings and get a highly secure, shared secret key, again with overwhelming probability.

Since this text is aimed at a scenario with a quantum cryptographic channel (see Section 4 for details), we will only discuss Information Reconciliation (IR) and Privacy Amplification (PA) further. In such an environment, Alice and Bob can measure an upper bound of the information Eve has about their communication. If this amount is too large for IR and PA to appear promising, it makes much more sense to start again with the protocol instead of performing Advantage Distillation.

3.1.2 Setting and Assumptions

The initial random variables from Alice, Bob and Eve, X, Y and Z, respectively, are given by the joint probability distribution P_{XYZ}. From Alice to Bob, an authentic, unidirectional channel is available, but wiretapped by Eve with an error rate potentially as low as zero (cf. Figure 1). We assume Alice to have access to a perfect random number generator.

3.2 Information Reconciliation

In this phase, Alice and Bob perform an error-correction protocol in order to make their strings equal with overwhelming probability, while minimising the information Eve gets in the process.

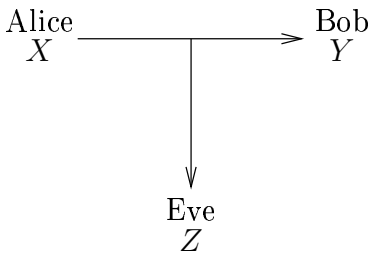

Figure 1: *Secret Key Agreement Setting:* Alice, Bob and Eve, one-way channels Alice$\rightarrow$ *Bob*, *Alice* $\rightarrow$ *Eve*, and the respective random variables X, Y, and Z.

3.2.1 Description of IR

Bob conceptually maintains a set Q of specific realisations Y_i' of X given by

$$\{Q : \delta(X, Y_i') \leq \varepsilon\},$$

where ε is a security paramter. The uncertainty of Bob, i.e. the length of this list is given by $b := H_0^{\varepsilon}(X|Y)$.

Alice sends error-correction information C to Bob which allows him to reduce this list to one Y' which is identical to her X with high probability. This is visualized in Figure 2.

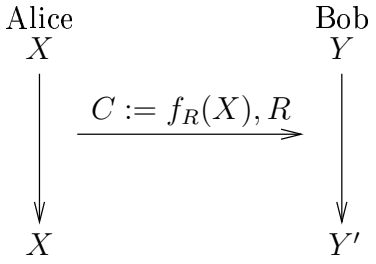

Figure 2: *Information Reconciliation:* Alice sends error-correction information C to Bob to allow him to determine, which Y_i' is the correct one with high probability.

The error-correction information C is computed from X using a *two-universal* random function f_R often referred to as two-universal function. A two-universal function is defined as follows:

Definition 3.1 (Two-Universal (Random) Function)

$$\begin{aligned} f_R &: \mathcal{F} \to \mathcal{G} \\ &x \mapsto f_R(x) \\ \forall x' \neq x &: \mathrm{P}\left[f_R(x) = f_R(x')\right] \leq \frac{1}{|G|}, \end{aligned} \tag{3.1}$$

where R specifies, which particular instance of this class of functions is used.

Here, the domain $\mathcal{F}$ is equal to $\mathcal{X}$. The range $\mathcal{G}$ depends on the length of the desired key and will be discussed in detail later.

Alice randomly selects one instance of such a function and computes

$$D := f_R(X).$$

The information she then sends to Bob consists of her selection of the random function, R, and D, the result of this function applied to X:

$$C := D \| R.$$

It is now shown, how the probability that Bob succeeds in determining an unambiguous value Y' can be made arbitrarily high, depending on a security parameter s. For the purpose of the following discussion and without loss of generality, we set

$$r := \log_2 |G|.$$

Bob will only keep those Y_i' which satisfy $f_R(Y_i') = D$. We first calculate the probability that Bob fails to eliminate *one specific* value Y_{i^*}'. Therefore, this probability is upper bounded by the collision probability of the two-universal function f_R as defined in (3.1):

$$\mathrm{P}[\text{Bob keeps } Y_{i^*}' \neq X'] \leq \frac{1}{|G|} = 2^{-r}.$$

The sum of the probabilities for all Y_i' is an upper bound for the probability that Bob fails to eliminate *any* of them:

$$\mathrm{P}[\text{Bob keeps any } Y' \neq X'] \leq \underbrace{2^{-r} + 2^{-r} + \cdots + 2^{-r}}_{H_0^\varepsilon(X|Y) \text{ addends}}. \tag{3.2}$$

The security parameter s allows to control the success probability as follows:

$$\begin{aligned} s &:= -H_0^\varepsilon(X|Y) + r, \\ \therefore \quad r &= H_0^\varepsilon(X|Y) + s. \end{aligned}$$

Hence,

$$\mathrm{P}[\text{Bob keeps any } Y_i' \neq X'] \leq 2^{H_0^\varepsilon(X|Y)} \cdot 2^{-r} = 2^{-s}. \tag{3.3}$$

Using (3.2) and (3.3), $|G|$ can now be determined:

$$\log_2 |G| = r = s + H_0^{\varepsilon}(X|Y). \tag{3.4}$$

It follows from this, that the amount of error-correction information which Alice needs to send to Bob is

$$|G| = 2^r = 2^{H_0^{\varepsilon}(X|Y)+s}.$$

Note, that R, the information, which particular instance of the class of two-universal functions Alice has used, is sent to Bob, but does not give any additional information to Eve. Since Eve is assumed to be computationally unlimited, she might have computed all outcomes of $f_R(Z)$ to all possible values of R previously.

3.2.2 Discussion of IR

Two kinds of failures can occur in the process of information reconciliation. Firstly, Bob's list of values might not contain the value of Alice, i.e. $X \notin \{Y_1', Y_2', \ldots, Y_b'\}$. This probability is controlled by ε as follows: The sum of the probabilities of all neglected values is at most ε, as defined in Definition 2.3. Secondly, Bob might not end up with a unique Y' because his list contains two different values Y_i', Y_j', $i \neq j$, with $f_R(Y_i') = f_R(Y_j')$. The probability that Y' can be determined uniquely is determined by s and is at least $1 - 2^{-s}$. In both cases, Y', Bob's notion of X, is essentially useless.

3.3 Privacy Amplification

The Privacy Amplification phase allows Alice and Bob to extract a key about which a potential eavesdropper has arbitrarily little information from an only marginally secure string.

We assume Alice and Bob to share a common value of length l bits, i.e. $Y' = X$, about which Eve has considerable, but not complete knowledge. How big Eve's amount of information is needs to be estimated by Alice and Bob and directly determines the length k of the secure key they can negotiate in the process of PA. It is shown in [8] that the $\bar{\varepsilon}$-smooth min-entropy of X given W, $H_{\infty}^{\bar{\varepsilon}}(X|W)$, appropriately measures Eve's knowledge about X after the IR phase. Furthermore it is shown that a lower bound for the secret key length is given by:

$$k = |S| \geq H_{\infty}^{\bar{\varepsilon}}(X|W) - s', \tag{3.5}$$

where $\bar{\varepsilon}$ and s' are security parameters.

3.3.1 Description of PA

To generate the highly-secret key S of length k from the only marginally secure string X with length l, Alice and Bob both apply a random function g (e.g. a two-universal function) to their notion of X:

$$g : \{0,1\}^l \to \{0,1\}^k$$

This is depicted in Figure 3. The function is chosen by Alice from a large set of random functions and sent authentically to Bob.

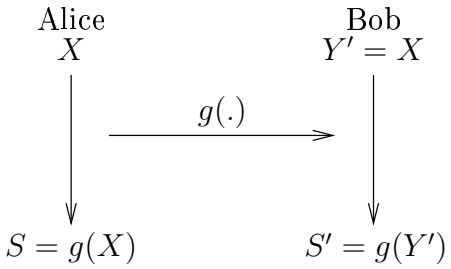

Figure 3: *Privacy Amplification:* Alice and Bob extract a highly secure string S from the only marginally secure string X. It is assumed that the information reconciliation phase has been successful, i.e. $Y' = X$.

3.3.2 Discussion of PA

Eve may overhear g, but does not gain any additional information about X from it because g is statistically independent from X and she might as well just compute all results for all possible random functions $g'(Z)$ in advance. The lower bound for the secret key length $|S|$ given in inequality (3.5) can be expanded by means of equation (2.2) as follows:

$$|S| \geq H_\infty^{\varepsilon'+\hat{\varepsilon}}(X|Z,C) - s' \geq H_\infty^{\varepsilon'}(X|Z) - H_0(C) - \log_2\left(\frac{1}{\hat{\varepsilon}}\right) - s', \quad (3.6)$$

where $H_0(C)$ is $H_0^\varepsilon(X|Y) + s$.

When a large number n of independent realisations of X are considered, i.e. n approaches positive infinity and ε goes to zero, the right-hand side of equation (3.6) can be reduced to the following equation, which is often referred to as *Csiszár-Körner Bound:*

$$\text{CKB} := H(X|Z) - H(C) = H(X|Z) - H(X|Y).$$

The Privacy Amplification results in a string S. Its secrecy is determined by its distance from a uniformly random string U as follows:

$$\mathrm{d}(S,U) \leq \varepsilon' + \hat{\varepsilon} + 2^{-s'}.$$

3.4 Discussion of the Protocol

We have shown, under which conditions secret key agreement is possible. The efficiency of the protocol can be specified by the secret key rate SKR:

$$\mathrm{SKR} := \frac{|S|}{|X|}.$$

In the Information Reconciliation phase, the parameters s and ε determine the probability that Alice and Bob end up with the same key:

$$\mathrm{P}[S \neq S'] = \varepsilon + 2^{-s}.$$

The secrecy of this key is determined by $\hat{\varepsilon}$, ε' and s' in the Privacy Amplification phase:

$$d(S,U) = \hat{\varepsilon} + \varepsilon' + 2^{-s'}, \quad \text{where } U \text{ is the uniform distribution.}$$

These parameters can be chosen at discretion in a way to make the secrecy and correctness arbitrarily high at the cost of a lower secret key rate.

In the next section, the special case of secret key agreement using a quantum channel is analysed.

4 Secret Key Agreement Over a Quantum Channel

In the previous section, a classical cryptographic protocol has been given which enables Alice and Bob to agree on a shared secret using only an authentic public channel. In this section, we analyse a quantum cryptographic protocol. In a classical scheme, Eve can eavesdrop the public channel without being noticed. This stands in contrast to a quantum channel where any such behaviour is limited by virtue of physical laws and can in most cases be detected.

A wide range of models exist to analyse eavesdropping on a quantum channel. In the introduction, we will give a brief description of the basic approach for secret key agreement over a quantum channel and discuss a very simple model to estimate Eve's knowledge. We will later use an accurate model to study the maximal achievable secret key rate and see how it can be increased with artificial noise. However, the quantum physical background of this model is beyond the scope of this text. For a thorough introduction into the field please refer to [14], [15] and [16].

4.1 Introduction

The fundamental idea was first introduced in a protocol by C. H. Bennett and G. Brassard in 1984 [12]. It is referred to as *BB84* and is summarised below.

4.1.1 Setting and Assumptions

The setting is as follows: There is a quantum channel between Alice and Bob which allows Alice to send photons to Bob. The eavesdropper, Eve, has access to this channel and can remove and add photons without a perceivable time delay. In addition, there is a public authentic channel between Alice and Bob.

Alice and Bob need access to a perfect random number generator. Alice has a generator for photons to create photons polarised in any specific direction. She uses this device to inject photons polarised in one of four directions (0°, 45°, 90° or 135°) into the quantum channel. Bob at the other end of the channel uses a polarisation detector which allows him to measure the polarisation of the photons. Eve is assumed to have unlimited computing power, in particular she has access to a quantum computer.

4.1.2 Overview of the Protocol

To arrange for a potential secret key, Alice first has to generate a random bit string. She then sends this bit sequence over the quantum channel to Bob, using one single photon for every bit, encoding the value in its polarisation. Alice has two possibilities to encode the value of the bit: The protocol uses

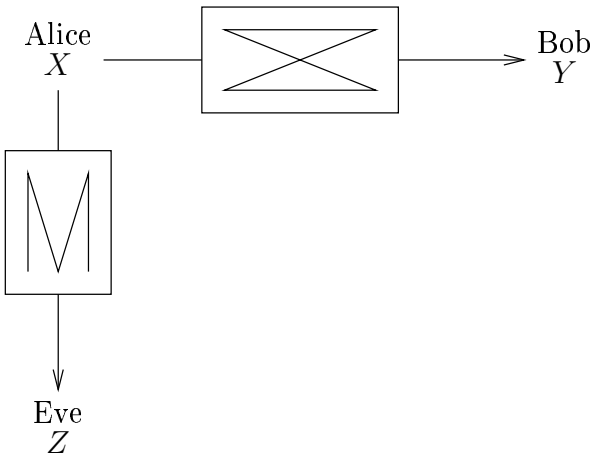

Figure 4: *Quantum Channel Setting:* Between Alice and Bob there is a binary symmetric channel whilst Eve is connected by a three-valued channel.

two different bases, *rectilinear* and *diagonal,* and Alice selects one of these randomly. If Alice uses the rectilinear basis, she sends the photon with a polarisation of either 0° or 90° and if she uses the diagonal basis, she selects either 45° or 135°. Which of the two possible polarisations in the chosen basis Alice selects is determined by the value of the bit she is about to send.

When Bob receives a photon, there is no way of knowing the basis Alice has used and therefore he chooses one of the two bases randomly for the measurement. Since the random number generators of Bob and Alice are assumed to be perfect, the chosen bases will match on average for every second photon. If the bases are the same, Bob will correctly detect the bit sent by Alice. Otherwise, the result of the measurement will be completely random and will not provide any information about the bit sent by Alice. Even though polarisation is a continuous variable, it is not possible to gain more than one bit of information, as stipulated by the uncertainty principle.

For the rest of the protocol, only bits which have been measured in the correct basis by Bob can be used. To this end, Alice sends her choice of the basis for every bit to Bob who answers "match" or "no match" over the public channel. Doing so, both can determine exactly which bits of the original sequence have been detected correctly. An example of this protocol is shown in Table 1.

Eve's access is not constrained by the protocol, but the physical laws proof to be very limiting. It is physically impossible to copy a photon with its polarisation intact [17]. If Eve decides to measure the polarisation of a photon, she has to remove it from the channel, store it and wait for Alice to send the information about its basis on the public channel. But as soon as Alice announces the basis to Bob, they will notice that a photon is missing.

Alice's string	1	1	0	1	0	0	1	0	0	0	1	1
Alice's basis	+	×	+	+	×	×	+	×	×	+	×	+
Alice sends	→	↘	↑	→	↗	↗	→	↗	↗	↑	↘	→
Bob's basis	+	+	+	×	+	×	+	×	+	×	×	×
Bob's result	→	↑	↑	↗	→	↗	→	↗	→	↘	↘	↗
Compare bases	√	–	√	–	–	√	√	√	–	–	√	–
Secret key	1		0			0	1	0			1	

Table 1: *Quantum Protocol Example:* The arrows describe the polarisation of the photons (↑ 0°, ↗ 45°, → 90°, ↘ 135°), while the basis is described by + (0°/90°) and × (45°/135°).

To avoid this, Eve has to send a photon to Bob immediately after removing the photon sent by Alice from the channel. But since she does not know the basis Alice used, Eve cannot determine the polarisation and her best option is to polarise the photon randomly. If Bob measures this fake photon with the same basis as Alice, he will detect Eve's manipulation with a probability of one half. In the case where his basis differs from Alice's, the tampering cannot be detected. Since such bits will be discarded anyway, this has no influence on the success of the protocol.

Even if Alice and Bob have chosen the same basis, a bit error might still occur, for instance caused by noise or if Bob's detector is not perfectly aligned to Alice's generator. In this case they have to assume the worst, namely that every single error has been caused by an adversary. Therefore, if the error rate is too high, the protocol has to be cancelled.

In the following sections, we will determine an upper bound for this error rate ε below which secret key agreement is possible. We will then show how this bound of ε can be increased using artificial noise.

4.2 Quantum Channel Models

For the purpose of the following discussion, we will now introduce the model for the quantum channel from Alice to Bob and two different models for the channel from Alice to Eve.

4.2.1 Model of the Channel from Alice to Bob

In most relevant problems, the quantum channel between Alice and Bob can be modelled by a binary symmetric channel as depicted in Figure 5. This model assumes that the probability of a bit flip is the same for zero- and one-valued bits and can be specified by the parameter ε. Bit slips are assumed not to occur.

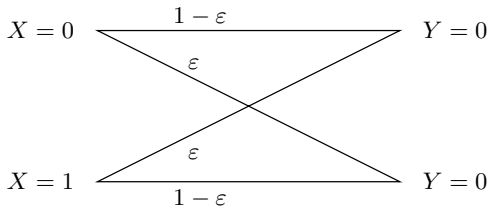

Figure 5: *Binary Symmetric Channel:* Models the quantum channel from Alice to Bob with parameter ε.

4.2.2 Simple Channel Model from Alice to Eve

Several useful models exist for the channel between Alice and Eve. The model discussed in the introduction is shown in Figure 6. Here, it is assumed that Eve measures the polarisation of the photon with a probability of $1 - \delta$ and therefore knows the bit sent by Alice. Otherwise, Eve does not interfere with the photon and hence will not get any information about the value of the bit.

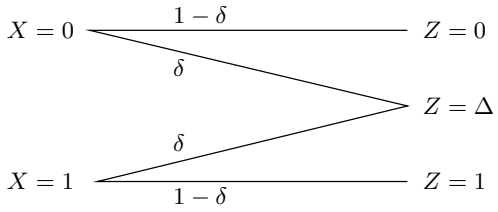

Figure 6: *Simple Adversary Channel:* This simple model corresponds to the attack strategy sketched in the introduction.

4.2.3 Accurate Channel Model from Alice to Eve

A more complex model uses four values at Eve's end and it can be shown (cf. [14]) that it allows to model the optimal attack of Eve. As illustrated in Figure 7, Eve can distinguish 0, 1, Δ_0 and Δ_1. The intuition behind this model is as follows: Eve inputs every photon into her quantum computer. She can perform an accurate measurement with an error rate of δ, but has to send a randomly polarised photon to Bob and thus her tampering is detectable as mentioned in the description of the BB84 protocol. Even if she does not store the photon for measuring, she can still extract a little bit of information from it (Δ_0 or Δ_1). But this pseudo measurement is susceptible to errors, wich is indicated by the parameter μ.

In the comparison of the two adversary channel models in Figure 8, it is

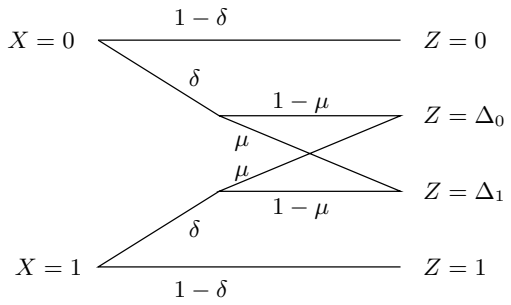

Figure 7: *Accurate Adversary Channel:* To model the optimal attack of Eve, this complex model with four values at Eve's end is necessary.

clearly visible that the simplified model is too optimistic from Alice's and Bob's point of view. Its key rate is positive until the error rate ε crosses the value 0.17054, whereas the accurate model indicates a non-positive key rate beginning from $\varepsilon \approx 0.12619$.

The entropy calculations in the following section are based on a channel which can be modeled by the accurate model.

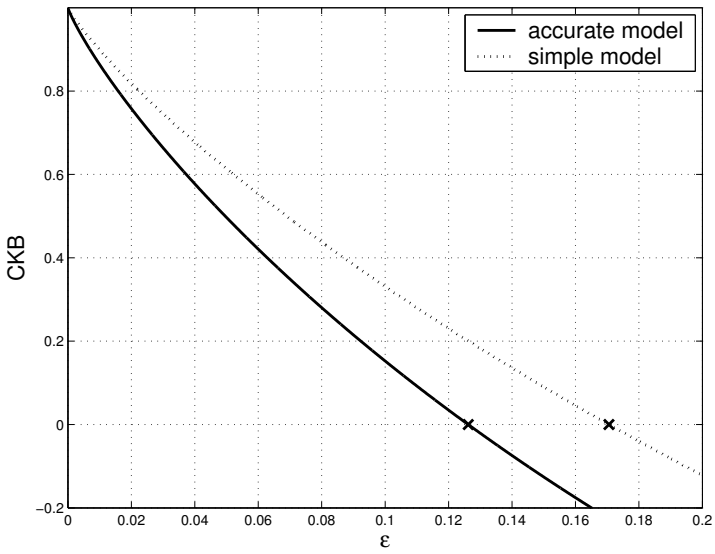

Figure 8: *Comparison of the Adversary Channel Models:* The simple model indicates that secret key agreement is possible at a value of the error rate ε where, according to the accurate model, secret key agreement is not feasible anymore.

4.3 Increasing the Secret Key Rate

Astonishingly, it is possible to increase the key rate derived in the previous section using artificial noise. The protocol begins as before, but upon entering the Information Reconciliation phase, Alice replaces her random variable by a noisy version $\hat{X}$ of X to perform the error correction. If the IR phase succeeds, both Alice and Bob end up with $\hat{X}$.

The artificial noise is described by the binary random variable N which is defined as

$$N := \begin{cases} 0 & \textit{with probability} \quad 1-p \\ 1 & \textit{with probability} \quad p. \end{cases}$$

The new random variable $\hat{X}$ is derived form X by applying the XOR operation to X and N:

$$\hat{X} := X \oplus N.$$

This addition of noise can be modelled by the binary symmetric channel shown in Figure 9. The artificial noise parameter p determines the probability that a bit is flipped on this channel. If p is equal to zero, no noise is added, whereas with $p = 0.5$, this channel has the effect of eliminating any relation between X and $\hat{X}$. Hence Information Reconciliation is not possible.

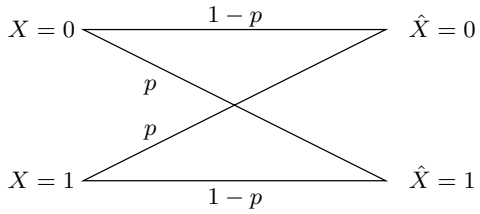

Figure 9: *Binary Symmetric Channel to Model Noise:* Models Alice's addition of noise to X. The probability of a bit flip is controlled by the artificial noise parameter p.

4.3.1 Entropy of the Channel Models

We will now present results obtained by Renner which we will use for the analysis of the scenario.

The amount of information Bob receives over the binary symmetric channel concerning the noise Alice adds to her bit string before performing the Information Reconciliation is

$$H(X|Y)(\varepsilon, p) := h((1-p)\varepsilon + p(1-\varepsilon)) = h(\varepsilon + p - 2\varepsilon p),$$

where ε is the (symmetric) error rate between Alice and Bob and p is the probability of a bit flip when adding the noise. This can be seen directly by concatenating Figure 9 and Figure 5, e.g. prepending the channel modelling the bit flipping of Alice to the quantum channel from Alice to Bob.

In the present protocol, there are many independent realisations of the random variables $\hat{X}$, Y and Z, and therefore, Shannon entropy can be used. With the additional parameter p describing the added noise, the lower bound for the secret key rate given in equation (3.6) of the previous section becomes

$$\mathrm{SKR}_{accurate}(\varepsilon, p) \geq H(\hat{X}|Z)(\varepsilon, p) - H(\hat{X}|Y)(\varepsilon, p), \tag{4.1}$$

where

$$H(\hat{X}|Z)(\varepsilon, p) := H(\hat{X}Z)(\varepsilon, p) - H(Z)(\varepsilon, p)$$

with

$$H(\hat{X}Z)(\varepsilon, p) = \varepsilon \bar{h}(\frac{1}{2}, p) + (1-\varepsilon)\bar{h}(\frac{1-\frac{3}{2}\varepsilon}{1-\varepsilon}, p) + h(p) + 1$$

$$H(Z)(\varepsilon, p) = h(\varepsilon) + \varepsilon + (1-\varepsilon)h(\frac{1-\frac{3}{2}\varepsilon}{1-\varepsilon}).$$

The binary quantum entropy $\bar{h}$ is given by

$$\bar{h}(q, p) := h\left(\frac{1}{2}\left(1 - \sqrt{1 + 16qp(p-1)(1-q)}\right)\right),$$

where $h(.)$ is the binary entropy function from equation (2.1). Refer to [14] for additional information concerning this derivation.

4.3.2 Discussion

The secret key rate SKR can be increased by adding the appropriate amount of noise as shown in equation (4.1). The optimal amount of artificial noise varies depending on the detected error rate ε of the quantum channel from Alice to Bob. Figure 10 shows the secret key rate SKR in function of the artificial noise parameter p for two specific values of the error rate ε, $\varepsilon = 0.12$ and $\varepsilon = 0.13$.

This first result looks very promising. On the left hand side of the graph—where p is equal to zero—the secret key rate without adding noise can be seen. The curves arise very steeply when p is increased and after passing the maximum, the secret key rate lowers again and converges to zero as p approaches one half. As mentioned before, this particular value of p has the effect of a perfect random number generator, and therefore $\hat{X}$ is statistically independent from X, Y and Z. This means that neither Bob nor Eve get any information about the string Alice performs the Information Reconciliation with. The most interesting points in the plot are of course the maxima and marked by crosses on the curves. The corresponding values

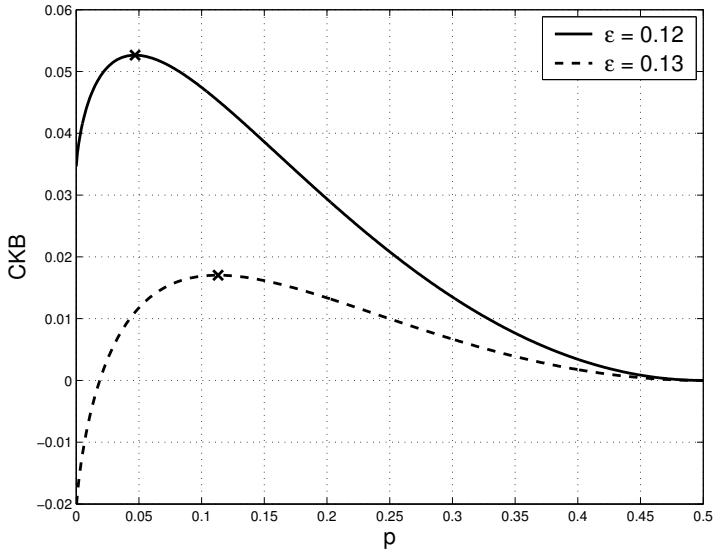

Figure 10: *Optimal Amount of Noise:* For fixed values $\varepsilon = 0.12$ and $\varepsilon = 0.13$, the resulting Csiszár-Körner Bound CKB is shown for every p in the range $[0, 0.5]$.

ϵ	$\text{SKR}_{noNoise}$	$\text{SKR}_{optimal}$	p
0	1	1	0
0.05	0.49682	0.49682	$3.8858{\cdot}10^{-16}$
0.1	0.15242	0.15521	0.0071875
0.11	0.092343	0.10002	0.019297
0.12	0.03463	0.052639	0.046953
0.12619	$1.7036{\cdot}10^{-5}$	0.028856	0.080391
0.13	-0.020882	0.017028	0.11313
0.14	-0.074325	0.0002077	0.34883
0.141	-0.07956	$2.3902{\cdot}10^{-6}$	0.44953
0.1411	-0.080082	$5.9737{\cdot}10^{-8}$	0.47992

Table 2: *Numerical Results:* Numerical evaluation of the Csiszár-Körner Bound and the corresponding artificial noise parameter p for two specific values of ε.

for the optimal secret key rate $\mathrm{SKR}_{optimal}$ represent the lower bounds of the secret key rate for the specific error rate ε measured by Alice and Bob.

It is now interesting to determine how much the secret key rate can be increased by adding artificial noise depending on ε. This is shown in Figure 11, where the secret key rate SKR is plotted versus the error rate ε. It is no surprise that the artificial noise has virtually no effect on the achievable secret key rate for a small ε. In this case, the artificial noise parameter p is close to zero and is indicated by the dotted line. More accurate values can be extracted from Table 2, where some specific numeric values are evaluated. The interesting area is around the point where the secret key rate approaches zero, which is shown in Figure 12. While the unaltered secret key rate decays more or less linearly, the optimized key rate approaches the decisive zero line much slower. In the normal protocol, the secret key rate $\mathrm{SKR}_{noNoise}$ crosses zero where $\varepsilon \approx 0.12619$. For the same error rate, the noise adding protocol still allows secret key agreement at a rate of $\mathrm{SKR}_{optimal} \approx 0.02886$ by setting the artificial noise parameter p to $p \approx 0.08039$.

The crucial range of the error rate ε is around $\varepsilon \approx 0.14$. In this area the secret key rate $\mathrm{SKR}_{optimal}$ of the noise adding protocol approaches the zero line and the corresponding optimal artificial noise parameter p rises very steeply. While a value of $\varepsilon = 0.14$ still allows to use every 5000^{th} sent bit for the secret key, an error rate $\varepsilon = 0.1411$ only allows to use every one billionth bit. The upper bound for the error rate in the quantum channel between Alice and Bob that allows secret key agreement is:

$$\varepsilon_{upperBound} \lesssim 0.14111875.$$

The dotted line in the graph is really steep just before this value of ε. As the error rate ε approaches the upper bound indicated above, the optimal artificial noise parameter p gets arbitrarily close to one half. As soon as the error rate ε is higher than this upper bound, the optimal value for p is 0.5, which means as mentioned already, that neither Bob nor Eve get any information about Alice's string and therefore the secret key rate is equal to zero. Note that this is still better than without artificial noise as the secret key rate never turns negative. The optimal value for the artificial noise parameter p is one half for all error rates greater than $\varepsilon_{upperBound}$.

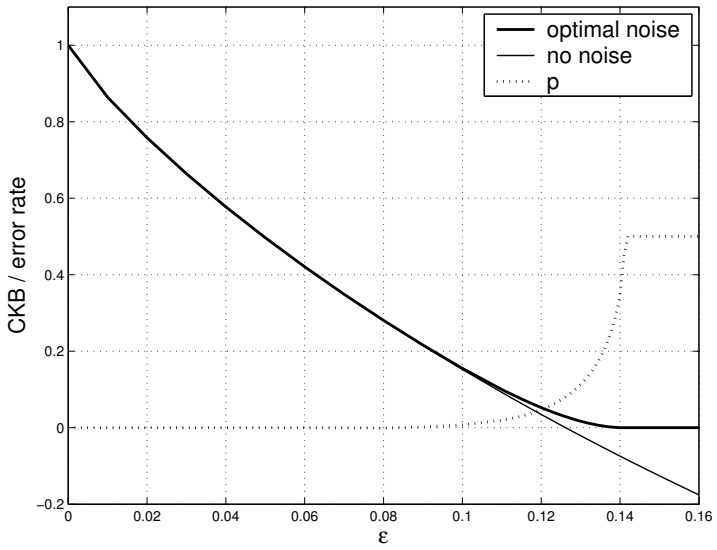

Figure 11: *Csiszár-Körner Bound* CKB *vs. Error Rate* ε*:* The Csiszár-Körner Bound CKB for both, the case without noise and the case with the optimal amount of noise, is plotted versus the error rate ε on the quantum channel from Alice to Bob. The optimal value for the artificial noise parameter p is indicated by the dotted line.

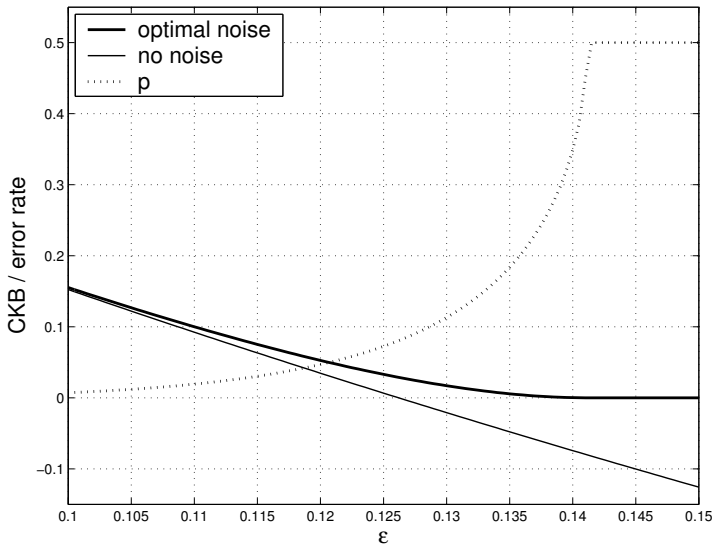

Figure 12: *Csiszár-Körner Bound Close to Zero:* If Alice does not add artificial noise, i.e. $p = 0$, the upper bound for the error rate ε where secret key agreement is possible is $\varepsilon \approx 0.12619$. This limit can be increased up to $\varepsilon \approx 0.14112$ by adding noise.

5 Conclusion

In this thesis, information-theoretic secret key agreement was first discussed in a very general setting. Then it was shown how artifical noise can be used to increase the lower bound of the secret key rate in a specific quantum channel scenario.

5.1 Information-Theoretic Secret Key Agreement

In Section 3, a protocol was studied which enables secret key agreement under the assumption that a certain amount of correlated information is available to both communication partners and the eavesdropper. In contrast to previous papers by Maurer [5], Ahlswede and Csiszár [6] and several others, the correlation of the initial information was not required to comprise independent and identical parts. The discussion was aimed at the scenario of Section 4 where a quantum channel is used to establish the initial conditions. In such a setting, Alice and Bob can determine whether they have an initial advantage over Eve with high probability. Hence, the first phase of secret key agreement protocols (usually called Advantage Distillation) was not discussed and the description began with the Information Reconciliation (IR) step, followed by the Privacy Amplification (PA) phase.

Employing recent publications of Renner and Wolf about an information measure called *smooth Rényi entropy,* a lower bound on the secret key rate was adapted to the setting outlined above, depending on the security parameters ε, ε', $\hat{\varepsilon}$, s and s' as follows:

$$|S| \geq H_\infty^{\varepsilon'+\hat{\varepsilon}}(X|Z,C) - s' \geq H_\infty^{\varepsilon'}(X|Z) - H_0(C) - \log_2\left(\frac{1}{\hat{\varepsilon}}\right) - s'.$$

The parameters allow the legitimate partners to control the following properties of the secret key:

Correctness The probability that Alice and Bob end up with the same value $X = Y'$ after the Information Reconciliation phase is determined by two security parameters, ε and s, as summarized in the following equation about the complementary event:

$$\mathrm{P}[Y' \neq X] = \varepsilon + 2^{-s}.$$

Secrecy The secrecy of the resulting key is determined by the security parameters $\hat{\varepsilon}$, ε' and s' in the Privacy Amplification phase. The secrecy of the key which is extracted in the PA phase was given as its statistical distance from the uniform distribution U:

$$d(S,U) = \hat{\varepsilon} + \varepsilon' + 2^{-s'}.$$

The security parameters can be chosen at discretion so as to increase the secrecy and correctness as desired at the cost of a lower secret key rate. To provide for maximal generality, the initial amount of information Bob has was not required to be superior over Eve's, but if this is not the case, secret key agreement is inherently impossible with the described protocol because no Advantage Distillation is performed.

5.2 Secret Key Agreement Over a Quantum Channel

In the second part, a quantum channel was analysed and it was shown, how the secret key rate can be increased using artificial noise. This was studied on the basis of the *BB84* protocol with the following modification: As in BB84, Alice sends her initial random sequence X to Bob encoded in the polarisation angle of photons, randomly alternating between the rectilinear and the diagonal basis. But after the transmission, she replaces her bit string X with a noisy version $\hat{X}$, which is derived from X by adding white noise. The amount of noise is controlled by the artificial noise parameter p, which determines the probability that Alice flips a bit when deriving $\hat{X}$ from X.

For certain values of this parameter p, the lower bound of the secret key rate SKR increases by a substantial amount. It was shown, that for every value of the error rate ε on the channel from Alice to Bob, there exists an optimal value of p which maximises the lower bound of the secret key rate. Furthermore, plots of the secret key rate SKR versus the error rate ε visualised that the addition of artifical noise can increase the secret key rate considerably.

The upper bound of the error rate ε where secret key agreement becomes possible is approximately $\varepsilon \approx 0.12619$. This limit can be increased up to

$$\varepsilon_{upperBound} \lesssim 0.14111875,$$

by adding the optimal amount of white noise. For values greater than $\varepsilon_{upperBound}$, the optimal value of the artificial noise parameter p is 0.5. In this case, the addition of noise removes the entire correlation between X and $\hat{X}$. Hence, any information about Alice's new bit sequence $\hat{X}$ she makes public in the IR and PA phase is statistically independent from the string she has transmitted to Bob initially. Thus, any information Bob and Eve have about Alice's new random variable $\hat{X}$ stems from the error correction in the IR phase. This results in Eve and Bob gaining exactly the same amount of information about $\hat{X}$ and secret key agreement is impossible because the secret key rate is equal to zero.

5.3 Open Problems

We used white noise to increase the secret key rate on the quantum channel. However, we showed neither whether white noise is the optimal kind of noise, nor if there exist other possibilities to further increase the secret key rate.

From our results, it seems plausible that white noise is indeed optimal. The reasoning for this supposition is as follows: The optimal value of the artificial noise parameter p is $p = 0.5$ for any error rate ε greater than $\varepsilon_{upperBound}$, the value where the secret key rate turns zero. In this range, the addition of white noise has exactly the effect of one-time pad encryption of Alice's random variable X to $\hat{X}$, thus eliminating any relation between X and $\hat{X}$. Since it is desirable not to expose any information about X if secret key agreement is impossible, this means that white noise is optimal in this region.

It appears reasonable to conjecture from the above discussion that the desired effect of the noise is to invalidate a certain amount of information about X which Eve received when Alice transmitted X to Bob by continuing the protocol with a noisy version $\hat{X}$. This elimination of information can be achieved symmetrically for zeros and ones in a controllable fashion by adding white noise.

References

[1] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal,* Vol. 27, pp. 379–423, 623–656, 1948.

[2] G. S. Vernam. Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications. *Journal of the American Institute for Electrical Engineers,* Vol. 55, pp. 109–115, 1926.

[3] A. D. Wyner. The Wire-Tap Channel. *Bell System Technical Journal,* Vol. 54, No. 8, pp. 1355–1387, 1975.

[4] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *Proceedings of IEEE Transactions on Information Theory,* Vol. IT-24, pp. 339–348, 1978.

[5] U. Maurer. Secret Key Agreement by Public Discussion from Common Information. *IEEE Transactions on Information Theory,* Vol. 39, No. 3, pp. 733–742, 1993.

[6] R. Ahlswede and I. Csiszár. Common Randomness in Information Theory and Cryptography – Part 1: Secret Sharing. *IEEE Transactions on Information Theory,* Vol. 39, No. 4, pp. 1121–1132, 1993.

[7] S. Wolf. Information-Theoretically and Computationally Secure Key Agreement in Cryptography. Ph. D. dissertation No. 13138, Department of Computer Science, Swiss Federal Institute of Technology, Zurich, 1999.

[8] R. Renner and S. Wolf. Smooth Rényi Entropy and Applications. *Proceedings of IEEE International Symposium on Information Theory (ISIT),* p. 233, June 2004.

[9] M. Christiandl, R. Renner and A. Ekert. A Generic Security Proof for Quantum Key Distribution. Available from `http://arxiv.org/abs/quant-ph/0402131` arXiv.org e-Print archive, March 2004.

[10] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory,* Vol. 22, No. 6, pp. 644–654, 1976.

[11] T. M. Cover and J. A. Thomas. Elements of Information Theory. Wiley-Interscience, ISBN: 0471062596, 1991.

[12] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International*

Conference on Computers, Systems and Signal Processing, pp. 175–179, December 1984.

[13] C. H. Bennett, F. Bessett, G. Brassard, L. Salvail, J. Smolin, and J. Cryptol. Experimental Quantum Cryptography. *Journal of Cryptology,* Vol. 5, No. 1, pp. 3–28, 1992.

[14] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, ISBN: 0521635039, September 2000.

[15] J. Preskill. Lecture Notes on Quantum Computation. Available from `http://theory.caltech.edu/people/preskill/ph229/#lecture` California Institute of Technology, 1997.

[16] M. Oskin. Lecture Notes on Quantum Computing. Available from `http://www.cs.washington.edu/education/courses/590mo/02sp/` University of Washington, 2002.

[17] W. K. Wootters and W. H. Zurek. A Single Quantum Cannot Be Cloned. *Nature,* Vol. 299, pp. 802–803, 1982.

A Matlab Code

Main Sequence – quantum.m

```
% main sequence

% parameters
textSize = 16;
mode_wide = false;

% compare simple channel model with accurate model
e=0:0.0001:0.25;
hold off
plot(e,skr_q(0,e),'k-','LineWidth',2)
hold on
plot(e,skr_c(0,e),'k:','LineWidth',2)
handle = legend('accurate model','simple model');
plot(0.17054,0,'kx','LineWidth',2,'MarkerSize',10)
plot(0.12619,0,'kx','LineWidth',2,'MarkerSize',10)
set(handle, 'FontSize', textSize)
handle = xlabel('\epsilon');
set(handle, 'FontSize', textSize)
handle = ylabel('CKB');
set(handle, 'FontSize', textSize)
axis([0 .2 -.2 1])
axis on
grid on
print -deps 'compare_models'

% plot skr(p,e=fix)
e1=0.12;
e2=0.13;
p=0:0.001:0.5;
hold off
plot(p,skr_q(p,e1),'k-','LineWidth',2)
hold on
plot(p,skr_q(p,e2),'k--','LineWidth',2)
x = optimizenoise(e1);
plot(x,skr_q(x,e1),'kx','LineWidth',2,'MarkerSize',10)
x = optimizenoise(e2);
plot(x,skr_q(x,e2),'kx','LineWidth',2,'MarkerSize',10)
handle = xlabel('p');
set(handle, 'FontSize', textSize)
handle = ylabel('CKB');
```

```
set(handle, 'FontSize', textSize)
handle = legend(['\epsilon = ',num2str(e1)],...
                ['\epsilon = ',num2str(e2)]);
set(handle, 'FontSize', textSize)
axis([0 .5 -.02 0.06])
axis on
grid on
print -deps 'fix_epsilon'

% benefit when adding noise
if (mode_wide)
  e=[0:0.01:0.11 .111:0.001:0.16];
else
  e=0.1:0.0005:0.15;
end
p=[];
f=[];
for i = e
  x = optimizenoise(i);
  p=[p,x];
  f=[f,skr_q(x,i)];
end
hold off
plot(e,f,'-k','LineWidth',2)
hold on
plot(e,skr_q(0,e),'-k','LineWidth',1)
plot(e,p,':k','LineWidth',2)
if (mode_wide)
  axis([0 0.16 -.2 1.1])
  posLegend = 1;
else
  axis([.1 .15 -.15 .55])
  posLegend = 2;
end
handle = legend('optimal noise','no noise','p',posLegend);
set(handle, 'FontSize', textSize)
handle = xlabel('\epsilon');
set(handle, 'FontSize', textSize)
handle = ylabel('CKB / error rate');
set(handle, 'FontSize', textSize)
grid on
if (mode_wide)
  print -deps 'opt_noise_wide'
else
```

```
  print -deps 'opt_noise_focus'
end
```

Find $\mathrm{SKR}_{max}(e)$ **– optimizenoise.m**

```
function [p] = optimizenoise(e)
% find optimal noise p according to e

  options = optimset('Display','off');
  % do not show warnings when no solutions are found

  [p, fm,eflag] = fminsearch(@skrq,.2,options,e);
        if (eflag==0)
    % no solution found - try another start value
    [p, fm,eflag] = fminsearch(@skrq,.1,options,e);
                if (eflag==0)
     % no solution found - try another start value
     [p, fm,eflag] = fminsearch(@skrq,.05,options,e);
   end
  end

  if (p>0.5)
    % p is symmetric, use value for p <= 0.5
    p = 1-p
  end
```

SKR **for the Simple Channel Model – skr_c.m**

```
function y = skr_c(p,e)
% secret key rate of the simple channel model
  HXcondY = h(e+p-2.*e.*p);
  HXcondZ = 1-2.*e+2*e.*h(p);

  y = HXcondZ - HXcondY;
```

SKR **for the Accurate Channel Model – skr_q.m**

```
function y = skr_q(p,e)
% secret key rate of the accurate quantum channel
  HXcondY = h(e+p-2.*e.*p);
  HXRZ = e.*hq(1/2,p)+(1-e).*hq((1-3.*e/2)./(1-e),p)+h(e)+1;
  HRZ = h(e)+e+(1-e).*h((1-3.*e/2)./(1-e));

  y = HXRZ - HRZ - HXcondY;
```

Allows to Find Minima instead of Maxima – skrq.m

```
function y = skrq (p,e)
% allows to find maxima by looking for the minima
y=-skr_q(p,e);
```

Binary Quantum Entropy – hq.m

```
function [y] = hq(q,p)
% binary quantum entropy
  y = h(1/2.*(1-sqrt(1+16.*q.*(p-1).*p-16.*q.^2.*(p-1).*p)));
```

Binary Entropy – h.m

```
function [y] = h(x)
% binary entropy
  y = hs(x) + hs(1 - x);
```

Shannon Entropy – hs.m

```
function [y] = hs(x)
% calculates shannon entropy
  a = (x==0) + x; % special case x=0
  y = -a .* log2(a);
```

B Task Formulation

Semesterarbeit

Von Simon Heimlicher und Andreas Meier

Am Institutit für Theoretische Informatik im Departement Informatik
Verantwortlicher Assistent: Renato Renner, Gruppe für
Informationssicherheit und Kryptographie
Professor: Prof. Dr. Ueli Maurer

Informationstheoretisch sichere Schlüsselgenerierung aus beliebiger korrelierter Information

Die Generierung eines Schlüssels aus korrelierter Information ist ein aktuelles Forschungsgebiet im Bereich der informationstheoretischen Kryptographie. Dabei wird oft angenommen, dass diese korrelierte Information aus unabhängingen und identischen Teilen besteht. Diese Voraussetzung ist aber in den meisten praktischen Szenarien nicht erfüllt. Daher wird in aktuelleren Forschungsarbeiten versucht, die vorhandenen Erkenntnisse auf ein allgemeineres Setting zu erweitern.

Die vorliegende Semesterarbeit soll zu dieser Forschung beitragen. Insbesondere ist das Ziel, verschiedenste Ergebnisse, welche für den Fall von unabhängiger und identischer Korrelation gelten, auf den Fall von beliebiger Korrelation zu erweitern.