Diploma Thesis

Secret-Key Agreement Information-Theoretically Secure Against Active Adversaries

Christian Schaffner

Supervisors:
Prof. Dr. Ueli M. Maurer
Renato Renner

Institute for Theoretical Computer Science
ETH Zürich, Switzerland

August 29, 2003

Abstract

In the setting of information-theoretically secure secret-key agreement, two parties, Alice and Bob, want to extract a secret key from independent realisations of a given distribution by communication over a public channel in such a way that only minimal information about the key is leaked to the adversary Eve. Considering this process as a transformation of distributions, the secret-key rate of a distribution is redefined in a new way.

This new formalism proves to be convenient to generalise this setting to different active adversaries. These adversaries are able to choose the initial distributions from a given set of distributions but have no influence on the public channel. The corresponding secret-key rates of sets of distributions are defined, and various relations between them are proved and illustrated by examples. In particular, it is shown that an adaptive adversary is not more powerful than an non-adaptive one.

Contents

Chapter 1

Introduction

A main goal of cryptography is to establish a secret communication between two parties Alice and Bob over an insecure channel overheard by the adversary Eve. Symmetric cryptographic schemes have been used since Roman times to encrypt messages (e.g., the one-time pad) and authenticate the communication, but all these schemes require an initial secret key shared by Alice and Bob.

In 1976, Whitfield Diffie and Martin Hellman gave a solution for the problem of secret-key agreement by introducing the revolutionary concept of Public-Key Cryptography [DH76]. Since then, Public-Key Cryptography has been extensively studied, improved, and become very popular. Its security is based on the computational hardness of such mathematical problems as factoring large numbers or finding discrete logarithms. These problems are believed to have no efficient solutions, i.e., a computationally bounded adversary cannot solve them in reasonable time. However, since a sufficiently powerful adversary can solve any computational problem, and the non-existence of efficient algorithms for these problems has not been proven so far, computational security is always conditional, and computationally-secure schemes could be broken by future progress in complexity theory and hardware engineering (e.g., quantum computing).

Unconditionally-secure cryptographic schemes are called information-theoretically secure. The security can be proven using Information Theory, a mathematical theory based on probability theory and statistics, introduced by Claude Shannon [Sha48]. This thesis deals with information-theoretically secure secret-key agreement by public discussion from common information. In this setting first studied by Maurer [Mau93], Alice and Bob start with some correlated information not fully known to Eve. By discussion over a public channel completely susceptible to eavesdropping by the adversary, they extract a mutual secret key in such a way that only minimal information is leaked to Eve.

A protocol specifies, based on the correlated information, which messages are exchanged by Alice and Bob over the public channel and how they calculate the secret key. This process can be seen as a transformation of distributions. The initial joint distribution of the information known to each party Alice, Bob, and Eve is transformed into another joint distribution which is nearly an ideal secret-key distribution, i.e., Alice and Bob's strings are equal as well as uniformly distributed over the key space, and Eve's knowledge is statistically independent.

In order to formally define protocols and quantities related to secret-key agreement, we introduce in this thesis a new formalism which uses distributions instead of information-theoretical measures like (Shannon) entropy and mutual information. This formalism makes it easy to deal with more general settings like secret-key agreement secure against active adversaries as described below or the reversed process of generating a joint distribution from secret-key bits by public discussion. Studying the reversed process has been recently contributed to better insights on how many secret-key bits can be extracted from a given distribution [RW03].

1.1 Motivating Example: The Extended Satellite Scenario

One realistic way to obtain correlated information is the following satellite scenario introduced in [Mau93] and completely analysed in [MW96]. Alice, Bob, and Eve use antennas to receive random bits broadcasted by a satellite. The received bits are subject to various transmission errors depending, among other things, on the quality and size of the antennas. Surprisingly, it could be shown that an information-theoretically-secure secret key can be extracted from the received bits by public discussion even if Eve's equipment is much more sophisticated than Alice's and Bob's, i.e., Eve's error probability is much smaller than the error rate of Alice's or Bob's bits.

Extending the scenario, assume that the adversary Eve uses a jamming transmitter to disturb the transmission of the satellite's bit stream. In this way she actively influences the chances of transmission errors and hence "chooses" the initial joint distribution of the information from which Alice and Bob want to extract a secret key.

In all scenarios studied so far, Alice and Bob have access to many independent realisations of the same distribution. The property of the distribution specifying at which rate secret-key bits can be extracted is called *secret-key rate*. In this thesis analogous quantities are defined for a set of distributions. In the most general setting, the adversary Eve acts adaptively: she chooses a distribution from the given set based on the outcome of her previous variables. This enables her to generate dependent distributions. In a more restricted scenario, she chooses independently (possibly different) distributions from the set. In a third setting, she fixes only one distribution from the set, and the parties have access to independent realisations of this distribution.

1.2 Contributions

A new formalism is introduced to define good protocols which yields a definition of the secret-key rate of a distribution that is equivalent to the common definition but deals with distributions rather than with information-theoretical quantities. In this formalism a well-known upper bound on the secret-key rate is reproved, and known theorems are adapted to the new form.

The formalism turns out to be suitable to define, for a given set of distributions, the secret-key rate in the three scenarios of an active adversary[1] described above. Relations between these secret-key rates are proved. It is shown in particular that the generalised secret-key rate of a set of distributions equals the secret-key rate for a fixed distribution from a set which

[1] It should be pointed out that in this thesis, contrary to the active adversaries considered in [Wol99, Chapter 6], an "active" adversary is only able to choose distributions but is *not allowed* to disturb the public discussion by inserting, modifying, or deleting messages. Hence, the public channel remains the same as in the passive model.

is derived from the original one and that an adaptive adversary is not more powerful than a non-adaptive one. Examples are given to illustrate the facts.

1.3 Outline of the Thesis

In Sections 2.1–2.3 of Chapter 2, the necessary definitions and notation used in the thesis are presented, basic facts are restated, and some lemmata derived. Section 2.4 contains a definition of good protocols based on the distance of distributions.

In Chapter 3, Section 3.1 gives the new definition of the secret-key rate of one distribution, and basic properties are proved in Section 3.2. The reproof of an upper bound can be found in Section 3.3. Section 3.4 adapts to the new formalism known theorems that are used in the proofs later on.

Chapter 4 is concerned with sets of distributions. In the first Section 4.1, good protocols for the different scenarios and the related secret-key rates of sets of distributions are defined, and basic properties are shown in Section 4.2. In the remaining sections of the chapter, relations between the different secret-key rates are proved.

The first Section 5.1 of Chapter 5 summarises the results from the previous chapters and gives illustrating examples. Section 5.2 lists suggestions for further research.

The appendix contains two technical calculations which prove more precise results about the continuity of mutual information used in Section 3.3 and the difference between drawing with and without replacement discussed in Section 4.3.

Chapter 2

Notation, Definitions and Basic Facts

2.1 Random Variables, Distributions, Distances

Notation 2.1. *Random variables are denoted by capital letters A, B, C, $\ldots$, X, Y, Z. Their ranges (or target sets) $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$ are always finite.*

We denote with $X^N = [X_1, \ldots, X_N]$ and $X^{NK} = [X_1, \ldots, X_{NK}]$ the first N and NK random variables of the sequence $X_1, X_2, X_3, \ldots$. If we are handling blocks of random variables, the following notation is used: $X_1^N = [X_1, \ldots, X_N]$, $X_2^N = [X_{N+1}, \ldots, X_{2N}], \ldots,$ $X_K^N = [X_{(K-1)N+1}, \ldots, X_{NK}]$

Notation 2.2. *For X and Y random variables with the same range $\mathcal{X}$, we use $P_X = P_Y$ as short notation for the equality $\forall x \in \mathcal{X} : P_X(x) = P_Y(x)$.*

In this thesis we often handle joint distributions of random variables X, Y, and Z with finite ranges $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, respectively. For these probability distributions, we will use a representation of the form given by the table below.

X Y (Z)	x_1	x_2	$\ldots$	x_n
y_1	$(z_1)\ p_{1,1,1}$ $(z_2)\ p_{1,1,2}$ $\vdots$ $(z_p)\ p_{1,1,p}$	$(z_1)\ p_{2,1,1}$ $(z_2)\ p_{2,1,2}$ $\vdots$ $(z_p)\ p_{2,1,p}$	$\ldots$	$(z_1)\ p_{n,1,1}$ $(z_2)\ p_{n,1,2}$ $\vdots$ $(z_p)\ p_{n,1,p}$
y_2	$(z_1)\ p_{1,2,1}$ $(z_2)\ p_{1,2,2}$ $\vdots$ $(z_p)\ p_{1,2,p}$	$(z_1)\ p_{2,2,1}$ $(z_2)\ p_{2,2,2}$ $\vdots$ $(z_p)\ p_{2,2,p}$	$\ldots$	$(z_1)\ p_{n,2,1}$ $(z_2)\ p_{n,2,2}$ $\vdots$ $(z_p)\ p_{n,2,p}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
y_m	$(z_1)\ p_{1,m,1}$ $(z_2)\ p_{1,m,2}$ $\vdots$ $(z_p)\ p_{1,m,p}$	$(z_1)\ p_{2,m,1}$ $(z_2)\ p_{2,m,2}$ $\vdots$ $(z_p)\ p_{2,m,p}$	$\ldots$	$(z_1)\ p_{n,m,1}$ $(z_2)\ p_{n,m,2}$ $\vdots$ $(z_p)\ p_{n,m,p}$

The table entries are numbers $p_{i,j,k} := P_{XYZ}(x_i, y_j, z_k)$ where $\mathcal{X} = \{x_1, \ldots, x_n\}$, $\mathcal{Y} = \{y_1, \ldots, y_m\}$ and $\mathcal{Z} = \{z_1, \ldots, z_p\}$ are the ranges of X, Y, and Z, respectively. We usually scratch all zero probabilities. Let for example $\mathcal{X} = \mathcal{Y} = \{0, 1, 2\}$, $\mathcal{Z} = \{0, 1, 2, 3\}$ and the joint distribution P_{XYZ} of X, Y, and Z be given by the following table.

Z (X, Y)	0	1	2	3
$(0, 0)$	$\frac{2}{14}$	0	0	0
$(0, 1)$	0	$\frac{1}{14}$	0	0
$(1, 0)$	0	$\frac{4}{14}$	$\frac{3}{14}$	0
$(1, 1)$	0	0	0	$\frac{4}{14}$

Since there are a lot of zero entries in this table our new representation is more compact.

X Y (Z)	0	1
0	(0) $\frac{2}{14}$	(1) $\frac{4}{14}$ (2) $\frac{3}{14}$
1	(1) $\frac{1}{14}$	(3) $\frac{4}{14}$

Notation 2.3. *We call a distribution of a random variable X* trivial *if X is constant, i.e.,* $\exists x_o \in \mathcal{X} : P_X(x) = \delta_{x_0 x} = \begin{cases} 1 & \text{if } x = x_0, \\ 0 & \text{if } x \neq x_0. \end{cases}$

Definition 2.4. *The L_1-*distance*, or just* distance*, between two distributions of discrete random variables X and Y with the same range $\mathcal{X}$ is defined as*

$$d\left(P_X, P_Y\right) := \sum_{x \in \mathcal{X}} \left|P_X(x) - P_Y(x)\right|.$$

The L_1-distance between the distribution of a random variable X and the uniform distribution P_U over $\mathcal{X}$ can be interpreted as follows. Assume that $d(P_X, P_U) \leq \varepsilon$. Then there is a refinement of the probability space underlying X in which an event $\mathcal{E}$ exists that has probability at least $1-\varepsilon$ such that $P_{X|\mathcal{E}} = P_U$, i.e., with probability at least $1-\varepsilon$, X behaves like a uniformly distributed random variable.

In [CT91, Page 299] it is shown that the L_1-distance equals the variational distance $\|P_X - P_Y\|$:

$$d\left(P_X, P_Y\right) = 2 \sup_{A \subseteq \mathcal{X}} \left|P_X(A) - P_Y(A)\right| = \|P_X - P_Y\|.$$

We take a closer look at the distances of joint distributions.

Lemma 2.5. *The distance of two joint distributions P_{AB} and P_{CD} is larger than the the distances of the marginal distributions. Formally, $d\left(P_{AB}, P_{CD}\right) \geq d(P_A, P_C)$, and $d\left(P_{AB}, P_{CD}\right) \geq d\left(P_B, P_D\right)$.*

Proof.

$$
\begin{aligned}
d\left(P_{AB}, P_{CD}\right) &= \sum_{a,b} \left|P_{AB}(a,b) - P_{CD}(a,b)\right| \\
&\geq \sum_{a} \Big|\sum_{b} \left(P_{AB}(a,b) - P_{CD}(a,b)\right)\Big| \\
&= \sum_{a} \left|P_A(a) - P_C(a)\right| \\
&= d(P_A, P_C).
\end{aligned}
$$

The other inequality $d\left(P_{AB}, P_{CD}\right) \geq d(P_B, P_D)$ follows in the same way. □

The triangle inequality yields the following upper bound:

$$
d\left(P_{AB}, P_{CD}\right) \leq d\left(P_{AB}, P_C P_B\right) + d\left(P_C P_B, P_{CD}\right).
$$

Note that $d(P_{AB}, P_C P_B)$ can only be further upper bounded by $d(P_A, P_C)$ if A and B are independent.

$$
\begin{aligned}
d\left(P_{AB}, P_C P_B\right) &= \sum_{a,b} \left|P_{AB}(a,b) - P_C(a) P_B(b)\right| \\
&= \sum_{a,b} \left|P_A(a) P_B(b) - P_C(a) P_B(b)\right| \\
&= \sum_{a} \underbrace{\sum_{b} P_B(b)}_{=1} \left|P_A(a) - P_C(a)\right| \\
&= d(P_A, P_C).
\end{aligned}
$$

These two ideas are used to prove the following useful

Lemma 2.6. *Let $\varepsilon > 0$ and $X^N = [X_1, X_2, \ldots, X_N]$ be independent random variables with the property that for all i holds: $d(P_{X_i}, P_Y) < \varepsilon$. If the random variables $Y^N = [Y_1, Y_2, \ldots, Y_N]$ are all independent and P_Y-distributed, it is true that $d\left(P_{X^N}, P_{Y^N}\right) < N \cdot \varepsilon$.*

Proof. From above follows that

$$
\begin{aligned}
& d\left(P_{X_1 X_2 X_3 \ldots X_N}, P_{Y_1 Y_2 Y_3 \ldots Y_N}\right) \\
&\leq d\left(P_{X_1 X_2 X_3 \ldots X_N}, P_{Y_1} P_{X_2 X_3 \ldots X_N}\right) + d(P_{Y_1} P_{X_2 X_3 \ldots X_N}, P_{Y_1 Y_2} P_{X_3 \ldots X_N}) + \\
&\qquad + d\left(P_{Y_1 Y_2} P_{X_3 \ldots X_N}, P_{Y_1 Y_2 Y_3} P_{X_4 \ldots X_N}\right) + \ldots + d\left(P_{Y_1 Y_2 Y_3 \ldots Y_{N-1}} P_{X_N}, P_{Y_1 Y_2 Y_3 \ldots Y_{N-1} Y_N}\right) \\
&= d(P_{X_1}, P_{Y_1}) + d(P_{X_2}, P_{Y_2}) + \ldots + d(P_{X_N}, P_{Y_N}) \\
&< N \cdot \varepsilon.
\end{aligned}
$$

□

If the variables X_1 and X_2 are both nearly P_Y-distributed but dependent, the distance between the joint distributions cannot be bounded in terms of the distance between the marginal distributions.

For example, consider for $0 < \delta \leq 1/4$ the following distribution:

X_1 / X_2	0	1
0	$\frac{1}{4}+\delta$	$\frac{1}{4}-\delta$
1	$\frac{1}{4}-\delta$	$\frac{1}{4}+\delta$

The marginal distributions are both uniform $P_{X_1}(0) = P_{X_1}(1) = P_{X_2}(0) = P_{X_2}(1) = 1/2$. If Y is another uniform binary random variable independent of X_1 and X_2, we have $d(P_{X_1}, P_Y) = 0$ and $d(P_{X_2}, P_Y) = 0$ but $d(P_{X_1X_2}, P_Y P_Y) = 4 \cdot \delta > 0$.

2.2 Entropy, Mutual Information

We refer to [CT91] and [Bla90] for general introductions to all information-theoretical quantities treated in this section and repeat only those facts that are used later on in this thesis or might help to understand how these measures behave.

In this thesis the binary logarithm (to base 2) of a real number $x \in \mathbb{R}$ is denoted by $\log(x)$, the natural logarithm (to base e) by $\ln(x)$. We denote the (Shannon) entropy of a random variable with $H(X)$ and the conditional entropy with $H(X|Z)$. It is easy to see that conditioning reduces entropy [CT91, Theorem 2.6.5]

$$H(X|Y) \leq H(X).$$

Lemma 2.7. *If the random variable A completely determines B, i.e., $H(B|A) = 0$, it follows that for all X $H(B|AX) = 0$, $H(ABX) = H(AX)$, and $H(X|AB) = H(X|A)$ holds.*

Proof.

$$\begin{aligned} 0 \leq H(B|AX) &\leq H(B|A) = 0 \\ H(AX) + \underbrace{H(B|AX)}_{=0} &= H(ABX) \\ H(X|AB) = H(ABX) - H(AB) &= H(AX) - H(A) = H(X|A). \end{aligned}$$

□

Definition 2.8. *The* mutual information *between X and Y and the* conditional mutual information *between X and Y given Z are defined by*

$$\begin{aligned} I(X;Y) &:= H(X) - H(X|Y), \\ I(X;Y|Z) &:= H(X|Z) - H(X|YZ). \end{aligned}$$

It can be shown [CT91, Theorem 2.4.1] that

$$I(X;Y) = I(Y;X).$$

As $H(Z|XY) \leq H(Z|Y)$, it follows from above that

$$I(XY;Z) \geq I(Y;Z). \tag{2.1}$$

2.3 Markov Chains

Definition 2.9. *A sequence of random variables $X_1, X_2, \ldots, X_N$ is called a* Markov chain, *denoted by*

$$X_1 \leftrightarrow X_2 \leftrightarrow \ldots \leftrightarrow X_N$$

if for all $i > 1$,

$$P_{X_i|X_1 X_2 \cdots X_{i-1}} = P_{X_i|X_{i-1}}. \tag{2.2}$$

See Notation 2.2 for the correct interpretation of equation (2.2).

The following lemmata state some basic facts about Markov chains.

Lemma 2.10. *The following three statements are equivalent:*

1. *$P_{Z|XY} = P_{Z|Y}$, i.e., $X \leftrightarrow Y \leftrightarrow Z$.*
2. *$P_{X|YZ} = P_{X|Y}$, i.e., $Z \leftrightarrow Y \leftrightarrow X$.*
3. *$P_{X|Y} \cdot P_{Z|Y} = P_{XZ|Y}$, i.e., X and Z are independent given Y.*

Proof. $1. \Rightarrow 2.: P_{X|YZ} = \frac{P_{XYZ}}{P_{YZ}} = \frac{P_{XYZ}}{P_{XY}} \cdot \frac{P_{XY}}{P_{YZ}} \stackrel{1.}{=} \frac{P_{YZ}}{P_Y} \cdot \frac{P_{XY}}{P_{YZ}} = P_{X|Y}$.

$2. \Rightarrow 3.: P_{XZ|Y} = \frac{P_{XYZ}}{P_Y} = \frac{P_{XYZ}}{P_{YZ}} \cdot \frac{P_{YZ}}{P_Y} \stackrel{2.}{=} P_{X|Y} \cdot P_{Z|Y}$.

$3. \Rightarrow 1.: P_{Z|XY} = \frac{P_{XYZ}}{P_{XY}} = \frac{P_{XYZ}}{P_Y} \cdot \frac{P_Y}{P_{XY}} \stackrel{3.}{=} \frac{P_{XY}}{P_Y} \cdot \frac{P_{YZ}}{P_Y} \cdot \frac{P_Y}{P_{XY}} = P_{Z|Y}$. □

From Lemma 2.10 follows that if $X \leftrightarrow Y \leftrightarrow Z \leftrightarrow W$ is a Markov chain, the reversed chain $W \leftrightarrow Z \leftrightarrow Y \leftrightarrow X$ is also Markov which justifies the arrows in both directions. Since $P_{W|X(YZ)} = P_{W|Z} = P_{W|(YZ)}$, $X \leftrightarrow YZ \leftrightarrow W$ is a Markov chain as well, and in a similar way $XY \leftrightarrow Z \leftrightarrow W$ and $X \leftrightarrow Y \leftrightarrow ZW$ are Markov chains.

Note that $P_{W|XYZ} = P_{W|YZ}$ does *not* imply $P_{W|XY} = P_{W|Y}$. For $X = Z = W$ and Y statistically independent of $Z = W$, $P_{W|XY}$ is trivial, and $P_{W|Y} = P_W$ can be nontrivial.

Lemma 2.11. *Let A, B, C, and Z be random variables with ranges $\mathcal{A}, \mathcal{B}, \mathcal{C}$, and $\mathcal{Z}$, respectively.*

1. *If $AZ \leftrightarrow B \leftrightarrow C$ is a Markov chain, then $A \leftrightarrow BZ \leftrightarrow C$, $A \leftrightarrow B \leftrightarrow C$, and $Z \leftrightarrow B \leftrightarrow C$ are also Markov chains.*
2. *If $A \leftrightarrow BZ \leftrightarrow C$ and $Z \leftrightarrow B \leftrightarrow C$ are Markov chains, then $AZ \leftrightarrow B \leftrightarrow C$ is a Markov chain as well.*

Proof.
1. $P_{C|ABZ} = P_{C|B} \Rightarrow P_{C|ABZ} = P_{C|BZ}$. By summing the equality $P_{AZ|BC} = P_{AZ|B}$ over $z \in \mathcal{Z}$ and $a \in \mathcal{A}$, respectively, we obtain $P_{A|BC} = P_{A|B}$ and $P_{Z|BC} = P_{Z|B}$.
2. $P_{C|ABZ} = P_{C|BZ} = P_{C|B}$.

□

Lemma 2.12. *If $A \leftrightarrow BZ \leftrightarrow C$ is a Markov chain, the following inequality holds*

$$I(A;B|Z) \geq I(A;B|ZC).$$

Proof.

$$\begin{aligned} I(A;B|Z) &= H(A|Z) - H(A|BZ) = H(A|Z) - H(A|BZC) \\ &\geq H(A|ZC) - H(A|BZC) = I(A;B|ZC) \end{aligned}$$

where the first and last equalities are the definitions of conditional mutual information, and the second follows by Markovity. The inequality is due to the fact that conditioning on further random variables cannot increase entropy. □

If a random variable Y is send over a channel c to obtain $\widetilde{Y}$, the channel c is completely specified by the conditional probability $P_{\widetilde{Y}|Y}$. Conditioning on further variables does not change this probability. Therefore, we use the following

Notation 2.13. *We write* $\ldots \leftrightarrow Y \stackrel{c}{\leftrightarrow} \widetilde{Y}$ *if the random variable* $\widetilde{Y}$ *is obtained by sending* Y *over a channel* c*.*

The ellipsis $\ldots$ stands for any random variable(s) different from Y and $\widetilde{Y}$.

Lemma 2.14. *If* Y *and* Z *are sent over the same channel* c *to obtain* $\widetilde{Y}$ *and* $\widetilde{Z}$*, i.e.,* $\ldots \leftrightarrow Y \stackrel{c}{\leftrightarrow} \widetilde{Y}$ *and* $\ldots \leftrightarrow Z \stackrel{c}{\leftrightarrow} \widetilde{Z}$ *with* $P_{\widetilde{Y}|Y} = P_{\widetilde{Z}|Z}$*. Then it holds*

$$d\left(P_{Y\widetilde{Y}}, P_{Z\widetilde{Z}}\right) = d\left(P_Y, P_Z\right).$$

Proof.

$$\begin{aligned} d\left(P_{Y\widetilde{Y}}, P_{Z\widetilde{Z}}\right) &= \sum_{y,\widetilde{y}} \left|P_{Y\widetilde{Y}}(y,\widetilde{y}) - P_{Z\widetilde{Z}}(y,\widetilde{y})\right| \\ &= \sum_{y,\widetilde{y}} \left|P_{\widetilde{Y}|Y} \cdot P_Y - P_{\widetilde{Z}|Z} \cdot P_Z\right| \\ &= \sum_{y,\widetilde{y}} \left|P_{\widetilde{Y}|Y} \cdot P_Y - P_{\widetilde{Y}|Y} \cdot P_Z\right| \qquad (2.3) \\ &= \sum_{y} \underbrace{\sum_{\widetilde{y}} P_{\widetilde{Y}|Y}}_{=1} \left|P_Y - P_Z\right| \\ &= d\left(P_Y, P_Z\right). \end{aligned}$$

Equation (2.3) holds as the channel c is the same. □

The channel c from the previous lemma can be extended to a channel c' whose output is still $\widetilde{Y}$ and $\widetilde{Z}$ if XY and WZ are sent. This channel ignores the first variable and sends the second over c. The lemma above then assures that $d\left(P_{XY\widetilde{Y}}, P_{WZ\widetilde{Z}}\right) = d\left(P_{XY}, P_{WZ}\right)$ which proves the following lemma.

Lemma 2.15. *If* $\ldots \leftrightarrow Y \stackrel{c}{\leftrightarrow} \widetilde{Y}$ *and* $\ldots \leftrightarrow Z \stackrel{c}{\leftrightarrow} \widetilde{Z}$*, it holds for arbitrary random variables* X *and* W *that*

$$d\left(P_{XY\widetilde{Y}}, P_{WZ\widetilde{Z}}\right) = d\left(P_{XY}, P_{WZ}\right).$$

2.4 Protocols

In the setting of secret-key agreement by public discussion from common information [Mau93], the two *players Alice and Bob* and the *adversary Eve* get realisations of random variables X, Y, and Z with ranges $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, respectively and joint distribution P_{XYZ}. Then Alice and Bob communicate over an authentic but insecure channel. Eve reads all messages sent over this public channel, but she is not able to alter, delete, or insert messages. After the communication Alice and Bob calculate output random variables $\bar{X}$ and $\bar{Y}$ in the key space $\mathcal{S}$.

A protocol specifies, for each $N \in \mathbb{N}$, the messages $C_1, C_2, \ldots, C_t$ exchanged over the public channel. The first message C_1 is sent by Alice to Bob and calculated by Alice knowing only her realisation of X^N, Bob sends to Alice the second message C_2 which he calculates based on Y^N and C_1 etc. We assume that the number of messages, denoted by t, is even, i.e., the last message C_t is sent by Bob. Having sent C_t to Alice, Bob calculates his output $\bar{Y}^M$ consisting of M values from a target set $\mathcal{S}$. After having received the last message C_t from Bob, Alice calculates $\bar{X}^M \in \mathcal{S}^M$. In the following scheme we write for $1 \leq i \leq t : C^i = [C_1, C_2, \ldots, C_i]$.

Alice		**Bob**
knows X^N		knows Y^N
calculates C_1 based on X^N	$\xrightarrow{C_1}$	receives C_1
receives C_2	$\xleftarrow{C_2}$	calculates C_2 based on $Y^N C_1$
calculates C_3 based on $X^N C^2$	$\xrightarrow{C_3}$	receives C_3
$\vdots$		$\vdots$
receives C_t	$\xleftarrow{C_t}$	calculates C_t based on $Y^N C^{t-1}$
calculates $\bar{X}^M$ based on $X^N C^t$		calculates $\bar{Y}^M$ based on $Y^N C^t$

This process can be understood as a transformation of distributions and be formally defined as follows.

Definition 2.16. *A* protocol $\mathcal{P}$ *is a set of conditional probability distributions which specify, for all N, how to transform the distribution $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ where $M \in \mathbb{N}$ is a function of N. The conditional probabilities define the second steps of the following Markov chains:*

$$Y^N Z^N \leftrightarrow X^N \leftrightarrow C_1, \tag{2.4}$$

$$X^N Z^N \leftrightarrow Y^N C^1 \leftrightarrow C_2, \tag{2.5}$$

$$Y^N Z^N \leftrightarrow X^N C^2 \leftrightarrow C_3, \tag{2.6}$$

$$\ldots$$

$$Y^N Z^N \leftrightarrow X^N C^{t-2} \leftrightarrow C_{t-1}, \tag{2.7}$$
$$X^N Z^N \leftrightarrow Y^N C^{t-1} \leftrightarrow C_t, \tag{2.8}$$
$$X^N Z^N \leftrightarrow Y^N C^* \leftrightarrow \bar{Y}^M, \tag{2.9}$$
$$\bar{Y}^M Y^N Z^N \leftrightarrow X^N C^* \leftrightarrow \bar{X}^M \tag{2.10}$$

where $C^i = [C_1, C_2, \ldots, C_i]$ for all $1 \leq i \leq t$, and $C^* := C^t$ denotes the whole communication over the public channel.

Definition 2.17. *The* rate *of a protocol $\mathcal{P}$ is defined as* $\mathrm{Rate}(\mathcal{P}) = \lim_{N\to\infty} \frac{M(N)}{N}$.

We want to study protocols that fulfill a certain task, i.e., that asymptotically transform a given distribution P_{XYZ} into another $P_{\hat{X}\hat{Y}\hat{Z}}$ in such a way that after the transformation the adversary does not know more than $\hat{Z}$. The allowed knowledge of the adversary can be formalized by a random variable U which is obtained by sending $\hat{Z}$ over a channel. This yields a set of "ideal distributions" $\{P_{\hat{X}^M\hat{Y}^M U} : \ldots \leftrightarrow \hat{Z}^M \leftrightarrow U\}$. We say that a protocol is good if the distance between the obtained distribution $P_{\bar{X}^M\bar{Y}^M Z^N C^*}$ and the set of ideal distributions $P_{\hat{X}^M\hat{Y}^M U}$ tends to zero for large N. Formally, we make the following definition.

Definition 2.18. *The set of all* good protocols *with respect to P_{XYZ} and $P_{\hat{X}\hat{Y}\hat{Z}}$ is denoted by $\Gamma\left(P_{XYZ} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ and consists of those protocols that specify for all N a $M(N)$ and transform the distribution $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M\bar{Y}^M Z^N C^*}$ in such a way that*

$$\min_{P_{U|\hat{Z}^M}} d\left(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{\hat{X}^M\hat{Y}^M U}\right) \overset{(N\to\infty)}{\longrightarrow} 0.$$

Note that $\Gamma\left(P_{XYZ} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ is not the empty set as trivial protocols without output, i.e., with $M = 0$, are always good.

We can use protocols in $\Gamma\left(P_{XYZ} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ as well for a distribution $P_{\tilde{X}\tilde{Y}\tilde{Z}}$ whose distance to P_{XYZ} is small. The following proposition assures that the distributions generated by the protocol do not differ more than the input distributions.

Proposition 2.19. *Let $\mathcal{P}$ be a protocol which transforms $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M\bar{Y}^M Z^N C^*}$, and let $\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}$ be random variables with the same range as $X^N Y^N Z^N$. Then $\mathcal{P}$ transforms $P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}}$ into $P_{\widetilde{\bar{X}^M}\widetilde{\bar{Y}^M}\widetilde{Z^N}\widetilde{C^*}}$ such that*

$$d\left(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{\widetilde{\bar{X}^M}\widetilde{\bar{Y}^M}\widetilde{Z^N}\widetilde{C^*}}\right) \leq d\left(P_{X^N Y^N Z^N}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}}\right).$$

Proof. Using the Markov chains (2.4) – (2.10) from the definition of a protocol and Lemma 2.11, we see that the following are all Markov chains:

$$\bar{Y}^M \leftrightarrow X^N Y^N Z^N C^t \leftrightarrow \bar{X}^M, \tag{2.11}$$
$$X^N \leftrightarrow Z^N Y^N C^t \leftrightarrow \bar{Y}^M, \tag{2.12}$$
$$X^N \leftrightarrow Y^N Z^N C^{t-1} \leftrightarrow C_t, \tag{2.13}$$
$$Y^N \leftrightarrow X^N Z^N C^{t-2} \leftrightarrow C_{t-1}, \tag{2.14}$$
$$\ldots$$
$$Y^N \leftrightarrow X^N Z^N \leftrightarrow C_1. \tag{2.15}$$

We use Lemma 2.5 for the first inequality and make repeated use of Lemma 2.15 for the remaining steps.

$$
\begin{aligned}
d\left(P_{\bar{X}^M\bar{Y}^M Z^N C^t}, P_{\widetilde{\bar{X}^M}\widetilde{\bar{Y}^M}\widetilde{Z^N}\widetilde{C^t}}\right) &\leq d\left(P_{\bar{X}^M\bar{Y}^M X^N Y^N Z^N C^t}, P_{\widetilde{\bar{X}^M}\widetilde{\bar{Y}^M}\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^t}}\right) \\
&\stackrel{(2.11)}{=} d\left(P_{\bar{Y}^M X^N Y^N Z^N C^t}, P_{\widetilde{\bar{Y}^M}\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^t}}\right) \\
&\stackrel{(2.12)}{=} d\left(P_{X^N Y^N Z^N C^t}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^t}}\right) \\
&\stackrel{(2.13)}{=} d\left(P_{X^N Y^N Z^N C^{t-1}}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^{t-1}}}\right) \\
&\stackrel{(2.14)}{=} d\left(P_{X^N Y^N Z^N C^{t-2}}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^{t-2}}}\right) \\
&= \ldots \\
&= d\left(P_{X^N Y^N Z^N C^1}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}\widetilde{C^1}}\right) \\
&\stackrel{(2.15)}{=} d\left(P_{X^N Y^N Z^N}, P_{\widetilde{X^N}\widetilde{Y^N}\widetilde{Z^N}}\right)
\end{aligned}
$$

□

Chapter 3

Secret-Key Rate of a Distribution

3.1 Definition of the Secret-Key Rate

In the scenario of secret-key agreement, we want to attain the distribution $P_{S_A S_B \perp}$ where $\perp$ denotes a constant random variable, the key space $\mathcal{S} = \{0, 1\}$ is binary and S_A, S_B have key-bit distribution:

$$P_{S_A S_B}(x, y) = \begin{cases} 1/2 & \text{if } x = y = 0, \\ 1/2 & \text{if } x = y = 1, \\ 0 & \text{if } x \neq y. \end{cases} \tag{3.1}$$

A constant variable is always independent. Hence, $P_{S_A S_B \perp} = P_{S_A S_B} \cdot P_\perp$. The set $\Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)$ consists of all protocols $\mathcal{P}$ that transform, for all N, the distribution $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ in such a way that

$$\begin{aligned} & \min_{P_{U|\perp}} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) \stackrel{(N\to\infty)}{\longrightarrow} 0 \\ \iff \quad & \min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) \stackrel{(N\to\infty)}{\longrightarrow} 0. \end{aligned} \tag{3.2}$$

As the random variables U and $\perp$ are independent, equivalence (3.2) holds.

Definition 3.1. *The* secret-key rate *of a distribution P_{XYZ} is defined as*

$$S(P_{XYZ}) = \sup_{\mathcal{P} \in \Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)} \mathrm{Rate}(\mathcal{P}).$$

It should be pointed out that this definition of the secret-key rate of a distribution is equivalent to the earlier definition introduced in [Mau93]. It can be shown that

$$S(X; Y||Z) \leq S(P_{XYZ}) \leq S_w(X; Y||Z)$$

where $S_w(X; Y||Z)$ denotes the weak secret-key rate and $S(X; Y||Z)$ the earlier definition of the secret-key rate. These two quantities are defined and showed to be equal in [Wol99] which gives the equivalence of the definitions.

3.2 Properties of the Secret-Key Rate

The following proposition states that the secret-key rate increases as Eve's knowledge decreases.

Proposition 3.2. *Let P_{XYZ} be the joint distribution of random variables X, Y, and Z. By sending Z over a channel c, the random variable $\widehat{Z}$ is obtained, i.e., $\ldots \leftrightarrow Z \overset{c}{\leftrightarrow} \widehat{Z}$. Then $S(P_{XYZ}) \leq S(P_{XY\widehat{Z}})$.*

Proof. Let $\mathcal{P}$ be a protocol in $\Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)$. Thus, $\mathcal{P}$ transforms $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ in such a way that

$$\min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) \overset{(N\to\infty)}{\longrightarrow} 0. \tag{3.3}$$

We show that the same protocol is secure and can be used if Eve gets random variables $\widehat{Z}^N$ instead of Z^N.

Alice and Bob start with the same random variables as before. So, the protocol generates the same output $\bar{X}^M \bar{Y}^M$ and communication C^* with distribution $P_{\bar{X}^M \bar{Y}^M \widehat{Z}^N C^*}$. Let V be the random variable that minimises $d\big(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_V\big)$ and denote by $\widehat{V}$ the random variable obtained by sending the Z-part of V over the same channel as Z, i.e., $\ldots \leftrightarrow V \overset{c'}{\leftrightarrow} \widehat{V}$ where the channel c' sends the Z-part of V over c and leaves the C^*-part unchanged. It follows

$$\begin{aligned}
\min_{P_{\widehat{U}}} d\left(P_{\bar{X}^M \bar{Y}^M \widehat{Z}^N C^*}, P_{S_A^M S_B^M} P_{\widehat{U}}\right) &\leq d\left(P_{\bar{X}^M \bar{Y}^M \widehat{Z}^N C^*}, P_{S_A^M S_B^M} P_{\widehat{V}}\right) \\
&\leq d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^* \widehat{Z}^N C^*}, P_{S_A^M S_B^M} P_{V\widehat{V}}\right) && (3.4) \\
&= d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_V\right) && (3.5) \\
&= \min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right). && (3.6)
\end{aligned}$$

Inequality (3.4) is due to Lemma 2.5 and equality 3.5 follows from Lemma 2.15. The last term (3.6) tends to zero according to (3.3). Hence, the protocol $\mathcal{P}$ is in $\Gamma\left(P_{XY\widehat{Z}} \to P_{S_A S_B \perp}\right)$ which shows that $\Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right) \subseteq \Gamma\left(P_{XY\widehat{Z}} \to P_{S_A S_B \perp}\right)$, and the proposition follows by taking the suprema over the rates of the protocols in these two sets. □

Alice cannot gain any advantage by sending her variables over a channel.

Proposition 3.3. *For a joint distribution P_{XYZ}, let $P_{\widehat{X}YZ}$ be the distribution where $\widehat{X}$ is obtained by sending X over a channel, i.e., $\ldots \leftrightarrow X \leftrightarrow \widehat{X}$. Then $S(P_{\widehat{X}YZ}) \leq S(P_{XYZ})$.*

Proof. Let $\widehat{\mathcal{P}}$ be a protocol in $\Gamma\left(P_{\widehat{X}YZ} \to P_{S_A S_B \perp}\right)$. A protocol $\mathcal{P} \in \Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)$ with the same $\mathrm{Rate}\,\widehat{\mathcal{P}} = \mathrm{Rate}\,\mathcal{P}$ is obtained if Alice sends, as a precomputation, her variables X^N over the channel and then applies $\widehat{P}$. The proposition follows like in the previous proof. □

3.3 An Upper Bound on the Secret-Key Rate

In [Mau93] it has been shown that for every secret-key agreement protocol holds

$$S(P_{XYZ}) \leq \min\{I(X;Y), I(X;Y|Z)\}.$$

For the trivial cases where Alice and Bob share no common information, i.e., X and Y are statistically independent, or the adversary gets the same information as one of the players, this bound implies that no secret key can be extracted because one of the quantities $I(X;Y)$ and $I(X;Y|Z)$ vanishes.

As described in [Wol99, Section 5.1], a better bound is given by the *intrinsic (conditional mutual) information* $I(X;Y{\downarrow}Z)$ which is the infimum over all quantities $I(X;Y|\overline{Z})$ where $\overline{Z}$ is obtained by sending Z over a channel.

$$I(X;Y{\downarrow}Z) := \inf\left\{I(X;Y|\overline{Z}) : \ldots \leftrightarrow Z \leftrightarrow \overline{Z}\right\}.$$

Theorem 3.4. *[Wol99, Theorem 5.1] For arbitrary random variables X, Y, and Z, we have*

$$S(P_{XYZ}) \leq I(X;Y{\downarrow}Z). \tag{3.7}$$

In this section we reprove Theorem 3.4 based on the new definition of the secret-key rate introduced in Section 3.1.

For this proof two lemmata are used. The first says that mutual information given Eve's knowledge can only decrease in each step of a protocol. The second formalises the continuity of mutual information.

Lemma 3.5. *Consider a protocol $\mathcal{P}$ which transforms the joint distribution $P_{X^NY^NZ^N}$ into $P_{\bar{X}^M\bar{Y}^MZ^NC^*}$. In each step of the protocol, the mutual information given Eve's knowledge cannot increase. Formally,*

$$\begin{aligned}
I\left(X^N;Y^N|Z^N\right) &\geq I\left(X^N;Y^N|Z^NC^1\right) && (3.8)\\
&\geq I\left(X^N;Y^N|Z^NC^2\right) && (3.9)\\
&\geq \ldots\\
&\geq I\left(X^N;Y^N|Z^NC^*\right) && (3.10)\\
&\geq I\left(\bar{X}^M;\bar{Y}^M|Z^NC^*\right) && (3.11)
\end{aligned}$$

Proof. From Definition 2.16 of a protocol, we know that $Y^NZ^N \leftrightarrow X^N \leftrightarrow C^1$ is Markov and by Lemma 2.11, $Y^N \leftrightarrow Z^NX^N \leftrightarrow C^1$ is Markov as well. Hence, Lemma 2.12 implies (3.8).

For the next step in the protocol, we obtain similarly

$$X^NZ^N \leftrightarrow Y^NC^1 \leftrightarrow C_2 \Longrightarrow X^N \leftrightarrow Z^NY^NC^1 \leftrightarrow C_2.$$

Again, Lemma 2.12 implies (3.9). The same reasoning applies to all communication steps of the protocol, therefore (3.10).

Using (2.9) and (2.10) and Lemma 2.11 again, we see that the following are all Markov chains:

$$\begin{aligned}
X^N &\leftrightarrow Z^NY^NC^* \leftrightarrow \bar{Y}^M && (3.12)\\
\bar{Y}^M &\leftrightarrow X^NY^NZ^NC^* \leftrightarrow \bar{X}^M && (3.13)\\
Y^N &\leftrightarrow X^NZ^NC^* \leftrightarrow \bar{X}^M && (3.14)
\end{aligned}$$

From this we can conclude

$$
\begin{aligned}
I\left(X^N;Y^N|Z^N C^*\right) &= H\left(X^N|Z^N C^*\right) - H\left(X^N|Y^N Z^N C^*\right) \\
&\stackrel{(3.12)}{=} H\left(X^N|Z^N C^*\right) - H\left(X^N|\bar{Y}^M Y^N Z^N C^*\right) \\
&= I\left(X^N;Y^N \bar{Y}^M|Z^N C^*\right) \\
&= H\left(Y^N \bar{Y}^M|Z^N C^*\right) - H\left(Y^N \bar{Y}^M|X^N Z^N C^*\right) \\
&= H\left(Y^N \bar{Y}^M|Z^N C^*\right) - H\left(Y^N \bar{Y}^M|X^N \bar{X}^M Z^N C^*\right) \qquad (3.15) \\
&= I\left(X^N \bar{X}^M;Y^N \bar{Y}^M|Z^N C^*\right) \\
&\geq I\left(\bar{X}^M;Y^N \bar{Y}^M|Z^N C^*\right) \qquad (3.16) \\
&\geq I\left(\bar{X}^M;\bar{Y}^M|Z^N C^*\right). \qquad (3.17)
\end{aligned}
$$

Inequalities (3.16) and (3.17) are due to (2.1) and (3.15) follows from

$$
\begin{aligned}
H\left(Y^N \bar{Y}^M|X^N Z^N C^*\right) &= H\left(\bar{Y}^M|X^N Y^N Z^N C^*\right) + H\left(Y^N|X^N Z^N C^*\right) \\
&\stackrel{(3.13)}{=} H\left(\bar{Y}^M|X^N \bar{X}^M Y^N Z^N C^*\right) + H\left(Y^N|X^N Z^N C^*\right) \\
&\stackrel{(3.14)}{=} H\left(\bar{Y}^M|X^N \bar{X}^M Y^N Z^N C^*\right) + H\left(Y^N|X^N \bar{X}^M Z^N C^*\right) \\
&= H\left(Y^N \bar{Y}^M|X^N \bar{X}^M Z^N C^*\right).
\end{aligned}
$$

□

Lemma 3.6. *The conditional mutual information is a continuous function of the distribution with respect to the L_1-distance. Formally, let ABZ and CDU be random variables with joint range $\mathcal{A} \times \mathcal{B} \times \mathcal{Z}$. Then it holds*

$$\forall \varepsilon > 0\, \exists \delta > 0 : d\left(P_{ABZ}, P_{CDU}\right) < \delta \Rightarrow |I(A;B|Z) - I(C;D|U)| < \varepsilon. \qquad (3.18)$$

Proof. According to [CT91, Equation 2.61] the conditional mutual information $I(A;B|Z)$ can be explicitly written as

$$
\begin{aligned}
I(A;B|Z) &= \sum_{z\in\mathcal{Z}} P_Z(z) \sum_{\substack{a\in\mathcal{A}\\ b\in\mathcal{B}}} P_{AB|Z}(a,b|z) \log \frac{P_{AB|Z}(a,b|z)}{P_{A|Z}(a|z)\cdot P_{B|Z}(b|z)} \\
&= \sum_{\substack{a\in\mathcal{A}\\ b\in\mathcal{B}\\ z\in\mathcal{Z}}} P_{ABZ}(a,b,z)\cdot \log \frac{P_{AB|Z}(a,b|z)}{P_{A|Z}(a|z)\cdot P_{B|Z}(b|z)}.
\end{aligned}
$$

The distributions $P_{AB|Z}$, $P_{A|Z}$, and $P_{B|Z}$ can be written as sums in terms of P_{ABZ}, e.g.,

$$P_{AB|Z}(a,b|z) = \frac{P_{ABZ}(a,b,z)}{P_Z(z)} = \frac{P_{ABZ}(a,b,z)}{\sum_{a,b} P_{ABZ}(a,b,z)}.$$

As summing, dividing and taking logarithms are continuous operations and the composition of continuous functions is a continuous function, the conditional mutual information is a continuous function of the distribution. □

Lemma A.1 in the Appendix proves a more precise relation between $I(A;B|Z)$ and the distribution P_{ABZ}.

With the help of the two lemmata, we show the upper bound $S(P_{XYZ}) \leq I(X;Y\!\downarrow Z)$ stated by Theorem 3.4.

Proof of Theorem 3.4. Let $\mathcal{P} \in \Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)$ be a protocol that transforms $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ in such a way that

$$\min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) \overset{(N\to\infty)}{\longrightarrow} 0. \tag{3.19}$$

We denote by V the random variable that minimises $d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_V\right)$. From the definition of the secret-key-bit distribution (3.1) follows

$$I(S_A^M; S_B^M | V) = I(S_A^M; S_B^M) = M.$$

We claim that Alice's and Bob's mutual information given Eve's knowledge after the protocol tends to M if N approaches infinity. Fix $\varepsilon > 0$. Lemma 3.6 assures the existence of a $\delta > 0$ such that

$$\begin{aligned} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_V\right) < \delta \Rightarrow & \left| I(\bar{X}^M; \bar{Y}^M | Z^N C^*) - I(S_A^M; S_B^M | V) \right| \\ &= \left| I(\bar{X}^M; \bar{Y}^M | Z^N C^*) - M \right| < \varepsilon. \end{aligned} \tag{3.20}$$

Because of (3.19) we can choose $N_0(\delta) \in \mathbb{N}$ such that

$$\forall N \geq N_0 : d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_V\right) < \delta \text{ which implies (3.20).}$$

As ε can be arbitrary small, this shows

$$I(\bar{X}^M; \bar{Y}^M | Z^N C^*) \overset{(N\to\infty)}{\longrightarrow} M.$$

It follows that

$$I(X;Y|Z) = \frac{1}{N} \cdot I(X^N; Y^N | Z^N) \geq \frac{1}{N} \cdot I(\bar{X}^M; \bar{Y}^M | Z^N C^*) \overset{(N\to\infty)}{\longrightarrow} \lim_{N\to\infty} \frac{M}{N} = \mathrm{Rate}(\mathcal{P})$$

where the inequality is due to Lemma 3.5. This shows $S(P_{XYZ}) \leq I(X;Y|Z)$. According to Proposition 3.2 the secret-key rate can only increase if Eve sends her Z-values over a channel to obtain $\overline{Z}$. Hence,

$$S(P_{XYZ}) \leq S(P_{XY\overline{Z}}) \leq I(X;Y|\overline{Z}).$$

and Theorem 3.4 follows. □

3.4 A Lower Bound on the Secret-Key Rate

In this section more general entropy measures than the common Shannon entropy are used. We refer to [Cac97, Chapters 2 and 3] for an introduction to these measures and repeat only the definitions.

Definition 3.7. *The* min-entropy *of a random variable X with range $\mathcal{X}$ is defined as*

$$H_\infty(X) := -\log \max_{x \in \mathcal{X}} P_X(x).$$

The Rényi entropy of order 0 *is defined as*

$$H_0(X) = \log |\mathcal{X}'|$$

where $\mathcal{X}' := \{x \in \mathcal{X} : P_X(x) > 0\}$ denotes the set of all values the random variable X takes on with positive probability.

Even more general is

Definition 3.8. *For a fixed $\varepsilon > 0$ the* ε-min entropy *and* ε-Rényi entropy of order 0 *are defined as*

$$\begin{aligned} H_\infty^\varepsilon(X) &:= \inf_{X' : d(P_{X'}, P_X) < \varepsilon} H_\infty(X'), \\ H_0^\varepsilon(X) &:= \sup_{X' : d(P_{X'}, P_X) < \varepsilon} H_0(X'). \end{aligned}$$

The following theorem states a well-known lower bound on the secret-key rate.

Theorem 3.9. *[Wol99, Theorem 4.7] For all distributions P_{XYZ} there is a protocol $\mathcal{P} \in \Gamma(P_{XYZ} \to P_{S_A S_B \perp})$ with*

$$\mathrm{Rate}(\mathcal{P}) \geq \max\bigl\{I(X;Y) - I(X;Z), I(Y;X) - I(Y;Z)\bigr\}. \tag{3.21}$$

This lower bound has been generalised by Renner and Wolf as follows:[1]

Theorem 3.10. *Let X, Y, and Z be random variables with joint distribution P_{XYZ} and $\varepsilon > 0$. With probability $1 - \varepsilon$, a secret key of size*

$$\max\bigl\{H_\infty^\varepsilon(X|Z) - H_0^\varepsilon(X|Y), H_\infty^\varepsilon(Y|Z) - H_0^\varepsilon(Y|X)\bigr\} \tag{3.22}$$

can be extracted.

It can be shown that for any fixed $\varepsilon > 0$ and for enough independent realisations of the random variables XYZ, (3.22) gets equal to the right hand side of (3.21).

The following proposition gives bounds on these entropies for K blocks which have nearly secret-key distribution. Using Notation 2.1, consider blocks of random variables $\bar{X}_1^M \bar{Y}_1^M Z_1^N$, $\bar{X}_2^M \bar{Y}_2^M Z_2^N$, ..., $\bar{X}_K^M \bar{Y}_K^M Z_K^N$. We denote by Z^{NK} all Z-variables and by $\bar{X}_{-i}^{MK} \bar{Y}_{-i}^{MK} Z_{-i}^{NK}$ all random variables except the ones from the ith block.

Proposition 3.11. *Let $\varepsilon > 0$. If for each i we have*

$$\min_{P_U} d\left(P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N \bar{X}_{-i}^{MK} \bar{Y}_{-i}^{MK} Z_{-i}^{NK}}, P_{S_A^M S_B^M} \cdot P_U\right) \leq \varepsilon, \tag{3.23}$$

it holds that $H_\infty^{\sqrt{\varepsilon}}(\bar{X}^{MK}|Z^{NK}) \geq (1 - \sqrt{\varepsilon})MK$ and $H_0^{\sqrt{\varepsilon}}(\bar{X}^{MK}|\bar{Y}^{MK}) \leq \sqrt{\varepsilon}MK$.

[1] This result has not yet been published.

Proof. According to the remark after Definition 2.4, there exist events $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_K$ that all have probabilities smaller than ε with the property that whenever the complementary event $\overline{\mathcal{E}_i}$ occurs, $\bar{X}_i^M \bar{Y}_i^M$ is uniformly distributed and statistically independent of Eve's knowledge Z_i^N and all other blocks, hence a perfect secret key.

We claim that the probability that L or more events occur is upper bounded by $\frac{K}{L}\varepsilon$. To prove this claim, let S be the set of all 0-1-vectors of length K with L or more 1's:

$$S := \{\vec{s} = (s_1, s_2, \ldots, s_K) \in \{0,1\}^K : w(\vec{s}) \geq L\}$$

where $w(\vec{s})$ denotes the number of 1's in $\vec{s}$ or the *weight of* $\vec{s}$. We denote by $\vec{\mathcal{E}}$ the characteristic vector of the events $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_K$, i.e., $\vec{\mathcal{E}}_i = 1$ if the event $\mathcal{E}_i$ occurs and $\vec{\mathcal{E}}_i = 0$ otherwise. It holds that

$$\begin{aligned}
K \cdot \varepsilon &\geq \sum_{i=1}^{K} P[\mathcal{E}_i] && (3.24)\\
&= \sum_{i=1}^{K} P\left[\bigcup_{\vec{s}\in\{0,1\}^K : \vec{s}_i = 1} \vec{\mathcal{E}} = \vec{s}\right] \\
&\geq \sum_{i=1}^{K} P\left[\bigcup_{\vec{s}\in S : \vec{s}_i = 1} \vec{\mathcal{E}} = \vec{s}\right] \\
&= \sum_{i=1}^{K} \sum_{\vec{s}\in S : \vec{s}_i = 1} P\left[\vec{\mathcal{E}} = \vec{s}\right] && (3.25)\\
&\geq L \cdot \sum_{\vec{s}\in S} P\left[\vec{\mathcal{E}} = \vec{s}\right] && (3.26)\\
&= L \cdot P[L \text{ or more events occur}].
\end{aligned}$$

The probability that the event $\mathcal{E}_i$ occurs is smaller than ε, hence (3.24). Equation (3.25) holds because the events $\{\vec{\mathcal{E}} = \vec{s}\}$ and $\{\vec{\mathcal{E}} = \vec{t}\}$ are disjoint for $\vec{s} \neq \vec{t}$. As every $\vec{s} \in S$ has weight at least L, (3.26) follows by double counting. This proves the claim.

If L events occur, the remaining $K - L$ blocks are independent and perfect secret keys according to (3.23). Hence, with probability at least $1 - \frac{K}{L}\varepsilon$ holds

$$\begin{aligned}
H_\infty(\bar{X}^{MK} | Z^{NK}) &\geq (K - L)M,\\
H_0(\bar{X}^{MK} | \bar{Y}^{MK}) &\leq L \cdot \log|\mathcal{S}|^M = LM \cdot \log(2) = LM.
\end{aligned}$$

By setting $L := \sqrt{\varepsilon} \cdot K$, it follows that

$$\begin{aligned}
H_\infty^{\sqrt{\varepsilon}}(\bar{X}^{MK} | Z^{NK}) &\geq \left(1 - \sqrt{\varepsilon}\right) MK,\\
H_0^{\sqrt{\varepsilon}}(\bar{X}^{MK} | \bar{Y}^{MK}) &\leq \sqrt{\varepsilon} MK.
\end{aligned}$$

□

Theorem 3.10 and Proposition 3.11 can be combined to yield the following useful proposition.

Proposition 3.12. *Given a protocol which is applied to each block and transforms for each i the distribution of the ith block $P_{X_i^N Y_i^N Z_i^N}$ into $P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N C_i^*}$ in such a way that*

$$\min_{P_U} d\left(P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N C_i^* \bar{X}_{-i}^{MK} \bar{Y}_{-i}^{MK} Z_{-i}^{NK} C_{-i}^{*K}}, P_{S_A^M S_B^M} \cdot P_U\right) \stackrel{(N\to\infty)}{\longrightarrow} 0, \tag{3.27}$$

there is a protocol which extracts at the same rate a secret key from the K blocks. Formally, it transforms the distribution $P_{X^{NK} Y^{NK} Z^{NK}}$ into $P_{\bar{X}^{MK} \bar{Y}^{MK} Z^{NK} C^*}$ such that

$$\min_{P_U} d\left(P_{\bar{X}^{MK} \bar{Y}^{MK} Z^{NK} C^*}, P_{S_A^{MK} S_B^{MK}} P_U\right) \stackrel{(K,N\to\infty)}{\longrightarrow} 0.$$

Proof. Given $\varepsilon > 0$, N can be chosen large enough that inequality (3.23) is fulfilled. Proposition 3.11 then assures that

$$H_\infty^{\sqrt{\varepsilon}}(\bar{X}^{MK}|Z^{NK}) - H_0^{\sqrt{\varepsilon}}(\bar{X}^{MK}|\bar{Y}^{MK}) \geq \left(1 - 2\sqrt{\varepsilon}\right)MK.$$

Hence, by Theorem 3.10, we can extract with probability at least $1 - \sqrt{\varepsilon}$ a secret key of length at least $\left(1 - 2\sqrt{\varepsilon}\right)MK$. As $\sqrt{\varepsilon}$ is arbitrarily small for large K and N, this proves the proposition. □

For independent blocks follows

Corollary 3.13. *Given a protocol which transforms the distribution $P_{X^N Y^N Z^N}$ (not necessarily identically nor independently distributed) into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ in such a way that*

$$\min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) \stackrel{(N\to\infty)}{\longrightarrow} 0, \tag{3.28}$$

there is a protocol with the same rate which transforms K independent blocks *of $P_{X^N Y^N Z^N}$ into $P_{\bar{X}^{MK} \bar{Y}^{MK} Z^{NK} C^{*K}}$ such that*

$$\min_{P_U} d\left(P_{\bar{X}^{MK} \bar{Y}^{MK} Z^{NK} C^{*K}}, P_{S_A^{MK} S_B^{MK}} P_U\right) \stackrel{(K,N\to\infty)}{\longrightarrow} 0.$$

Proof. As the blocks are independent, (3.28) implies (3.27) and Proposition 3.12 yields the protocol. □

Chapter 4

Secret-Key Rate of a Set of Distributions

4.1 Definitions

4.1.1 Good Protocols for Different Scenarios

Let us consider the setting in which Eve can choose the distributions $P_{X_iY_iZ_i}$ from a set of distributions $\mathcal{D}$. In the most general case, Eve acts adaptively, i.e., she chooses $P_{X_1Y_1Z_1}$, looks at her realisation of Z_1, then chooses $P_{X_2Y_2Z_2}$ and so on. On the same lines as in Section 2.4, we define what a good protocol for this scenario is:

Definition 4.1. *Let $\mathcal{D}$ be a set of distributions P_{XYZ}, and let $X^NY^NZ^N$ be random variables with distributions in $\mathcal{D}$. The distribution $P_{X_iY_iZ_i}$ might depend on $Z_1, Z_2, \ldots, Z_{i-1}$. We denote by $\Gamma_d\left(\mathcal{D} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ the set of all good protocols that transform, for all N, this distribution $P_{X^NY^NZ^N}$ into $P_{\bar{X}^M\bar{Y}^MZ^NC^*}$ in such a way that*

$$\min_{P_{U|\hat{Z}^M}} d\left(P_{\bar{X}^M\bar{Y}^MZ^NC^*}, P_{\hat{X}^M\hat{Y}^MU}\right) \stackrel{(N\to\infty)}{\longrightarrow} 0. \tag{4.1}$$

In a more restricted scenario of independent distributions, Eve is not allowed to look at her realisations while choosing. We define in analogy:

Definition 4.2. *The set $\Gamma\left(\mathcal{D} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ consists of all good protocols that transform, for all N, the distribution $P_{X^NY^NZ^N} = \prod_{i=1}^N P_{X_iY_iZ_i}$ with (possibly different) $P_{X_iY_iZ_i} \in \mathcal{D}$ into $P_{\bar{X}^M\bar{Y}^MZ^NC^*}$ in such a way that* (4.1) *holds.*

If we consider only the case of independent random variables with a fixed distribution, we can define in a very similar way:

Definition 4.3. *The set $\Gamma_f\left(\mathcal{D} \to P_{\hat{X}\hat{Y}\hat{Z}}\right)$ consists of all good protocols that transform, for all N, the distribution $P_{X^NY^NZ^N} = \prod_{i=1}^N P_{XYZ}$ for a fixed (but possibly unknown) $P_{XYZ} \in \mathcal{D}$ into $P_{\bar{X}^M\bar{Y}^MZ^NC^*}$ in such a way that* (4.1) *holds.*

4.1.2 Secret-Key Rates

Having defined good protocols in each case, we define the *secret-key rates* belonging to these settings.

Definition 4.4. *The* secret-key rate for dependent distributions *is*

$$S_d(\mathcal{D}) := \sup_{\mathcal{P}\in\Gamma_d(\mathcal{D}\to P_{S_A S_B \perp})} \mathrm{Rate}(\mathcal{P}).$$

The generalised secret-key rate *of a set of distributions $\mathcal{D}$ is defined as*

$$S(\mathcal{D}) := \sup_{\mathcal{P}\in\Gamma(\mathcal{D}\to P_{S_A S_B \perp})} \mathrm{Rate}(\mathcal{P}).$$

The secret-key rate for a fixed distribution *is*

$$S_f(\mathcal{D}) := \sup_{\mathcal{P}\in\Gamma_f(\mathcal{D}\to P_{S_A S_B \perp})} \mathrm{Rate}(\mathcal{P}).$$

As Eve's options are more restricted from scenario to scenario, it follows immediately that

$$S_d(\mathcal{D}) \leq S(\mathcal{D}) \leq S_f(\mathcal{D}) \tag{4.2}$$

because every protocol in $\Gamma_d(\mathcal{D} \to P_{S_A S_B \perp})$ can in particular handle the situation of independent distributions and is therefore in $\Gamma(\mathcal{D} \to P_{S_A S_B \perp})$, and in the same way holds $\Gamma(\mathcal{D} \to P_{S_A S_B \perp}) \subseteq \Gamma_f(\mathcal{D} \to P_{S_A S_B \perp})$. By taking the suprema over the rates of the protocols in these sets, the inequalities 4.2 follow. The main goal of this chapter is to study the properties of the generalised secret-key rate $S(\mathcal{D})$.

As a first simple fact, we show the following proposition.

Proposition 4.5. *Let $\mathcal{D}$ be a set of distributions. Then*

$$S_f(\mathcal{D}) \leq \inf_{P_{XYZ}\in\mathcal{D}} S(P_{XYZ}). \tag{4.3}$$

Proof. Let $\mathcal{P} \in \Gamma_f(\mathcal{D} \to P_{S_A S_B \perp})$ be a protocol. It is clear from the definitions above that $\forall P_{XYZ} \in \mathcal{D} : \mathcal{P} \in \Gamma(P_{XYZ} \to P_{S_A S_B \perp})$. It follows that $\forall P_{XYZ} \in \mathcal{D} : \Gamma_f(\mathcal{D} \to P_{S_A S_B \perp}) \subseteq \Gamma(P_{XYZ} \to P_{S_A S_B \perp})$. By taking the suprema of the rates over the two sets, we see that $\forall P_{XYZ} \in \mathcal{D} : S_f(\mathcal{D}) \leq S(P_{XYZ})$. Hence, inequality (4.3) holds. □

4.2 Basic Properties

In this section the generalised secret-key rate of a set of distribution $S(\mathcal{D})$ is studied, expressed, and bounded from above in terms of the secret-key rate for a fixed distribution $S_f(\widehat{\mathcal{D}})$ where the set $\widehat{\mathcal{D}}$ is derived from $\mathcal{D}$. We start with two definitions showing how such sets of distributions $\widehat{\mathcal{D}}$ can be derived.

Definition 4.6. *For a set of distributions $\mathcal{D}$, we define*

$$\mathcal{D}' := \left\{P_{XY(ZD)} : P_{XYZ} \in \mathcal{D} \text{ and } D \text{ uniquely determines } P_{XYZ}\right\}$$

the set of distributions with the property that, from her realization of ZD, Eve can learn the joint distribution of XYZ.

Definition 4.7. *Given a set of distributions $\mathcal{D}$, the* convex hull $\overline{\mathcal{D}}$ *of $\mathcal{D}$ is the intersection of all convex sets containing $\mathcal{D}$.*

Note that for a finite set of distributions $\mathcal{D} = \left\{P^{(1)}_{XYZ}, P^{(2)}_{XYZ}, \ldots, P^{(n)}_{XYZ}\right\}$, the convex hull can be expressed as follows

$$\overline{\mathcal{D}} := \left\{\sum_{j=1}^{n} \alpha_j P^{(j)}_{XYZ} : \forall j : \alpha_j \in \mathbb{R}, 0 \leq \alpha_j \leq 1, \sum_j \alpha_j = 1\right\}.$$

Some basic properties of derived sets are given by

Proposition 4.8. *Let $\mathcal{D}$, $\mathcal{D}_1$, and $\mathcal{D}_2$ be sets of distributions. Then the following three statements hold.*

1. $\forall \mathcal{D}_1 \subseteq \mathcal{D}_2 : S_f(\mathcal{D}_2) \leq S_f(\mathcal{D}_1)$ *and* $S(\mathcal{D}_2) \leq S(\mathcal{D}_1)$.
2. $\forall \mathcal{D} : S_f(\mathcal{D}') = S_f(\mathcal{D})$ *and* $S(\mathcal{D}') = S(\mathcal{D})$.
3. $\forall \mathcal{D} : S_f(\overline{\mathcal{D}'}) \leq S_f(\overline{\mathcal{D}})$ *and* $S(\overline{\mathcal{D}'}) \leq S(\overline{\mathcal{D}})$.

Proof. We prove only the statements about $S(\cdot)$, the reasoning for $S_f(\cdot)$ is the same.

1. follows from $\Gamma\left(\mathcal{D}_2 \to P_{S_A S_B \perp}\right) \subseteq \Gamma\left(\mathcal{D}_1 \to P_{S_A S_B \perp}\right)$.
2. $\geq$: Eve knows the the distributions of XYZ already because she chooses them from $\mathcal{D}$. $\leq$: Eve can "forget" the additional information by sending ZD over a channel which eliminates D. Proposition 3.2 assures that this can only increase the secret-key rate.
3. Using the same argument, Eve can "forget" her additional information.

□

Proposition 4.9. *For a set of distributions $\mathcal{D}$ holds that $S(\overline{\mathcal{D}'}) = S(\mathcal{D})$.*

Proof. $\leq$: $S(\overline{\mathcal{D}'}) \leq S(\mathcal{D}') = S(\mathcal{D})$ by Proposition 4.8, points 1 and 2.

$\geq$: For a probabilistic adversary Eve, let R be the random tape determining all of Eve's probabilistic choices. For a fixed randomness R, Eve's strategy to choose N distributions from $\overline{\mathcal{D}'}$ is deterministic. According to Carathéodory's Fundamental Theorem [Eck93], each point in the convex hull $\overline{\mathcal{D}'}$ can be expressed as convex combination of n distributions from $\mathcal{D}'$ where n depends on the dimension of the joint range $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$. Therefore, Eve's deterministic strategy can be described by at most nN distributions $P^{(j)}_{XY(ZD)} \in \mathcal{D}'$ and real numbers $\alpha^{(i)}_j \in \mathbb{R}$ for $1 \leq i \leq N, 1 \leq j \leq nN$ with the property that $\forall i : 0 \leq \alpha^{(i)}_j \leq 1$, $\sum_{j=1}^{nN} \alpha^{(i)}_j = 1$ and $P_{X_i Y_i Z_i} = \sum_{j=1}^{nN} \alpha^{(i)}_j P^{(j)}_{XY(ZD)}$.

We consider another adversary George. Contrary to the deterministic Eve (remember that R is fixed), George makes probabilistic choices, i.e., for a fixed strategy $\alpha^{(i)}_j$, George chooses with probability $\alpha^{(i)}_j$ $P^{(j)}_{XYZ}$ as distribution of $P_{X_i Y_i Z_i}$. After his choice George forgets the probabilities $\alpha^{(i)}_j$ and keeps in mind only which distributions from the set $\mathcal{D}$ he has chosen. George's resulting distributions $P_{X_1 Y_1 Z_1}, P_{X_2 Y_2 Z_2}, \ldots$ are the same as Eve's as long as they use the same strategy.

We claim that George's knowledge about the distributions $P_{X_1 Y_1 Z_1}, P_{X_2 Y_2 Z_2}, \ldots$ is the same as Eve's. For every i, Eve can derive from $Z_i D_i$ "from which corner in $\mathcal{D}$ the realisations of $X_iY_iZ_i$ come", i.e., which of the distributions in $\mathcal{D}$ the distribution of $X_iY_iZ_i$ is. George has kept exactly this information in mind after his probabilistic choice.

Hence, we have shown that the two kind of adversaries are equally powerful, and without loss of generality, we can assume George (instead of Eve) as adversary. This results in a situation where we can apply a protocol $\mathcal{P} \in \Gamma\left(\mathcal{D} \to P_{S_AS_B\perp}\right)$. Therefore, $\Gamma\left(\overline{\mathcal{D}'} \to P_{S_AS_B\perp}\right) \supseteq \Gamma\left(\mathcal{D} \to P_{S_AS_B\perp}\right)$ and the inequality follows by taking the suprema over the rates of the protocols in these two sets. □

Corollary 4.10. *For all sets of distributions $\mathcal{D}$, $S(\mathcal{D}) = S(\overline{\mathcal{D}})$ holds.*

Proof. $S(\mathcal{D}) \geq S(\overline{\mathcal{D}})$ follows from the first point of Proposition 4.8. The proposition above assures $S(\mathcal{D}) = S(\overline{\mathcal{D}'})$, and $S(\overline{\mathcal{D}'}) \leq S(\overline{\mathcal{D}})$ holds true by Proposition 4.8, point 3. □

4.3 Relation Between $S(\mathcal{D})$ and $S_f(\mathcal{D})$

Having given the relations between the secret-key rate of a set $\mathcal{D}$ and its derivatives in the last section, this section investigates the relation between $S(\mathcal{D})$ and $S_f(\cdot)$. The goal is to prove

Theorem 4.11. *Let $\mathcal{D}$ be a set of distributions. Then it is true that*

$$S(\mathcal{D}) = S_f(\overline{\mathcal{D}'}).$$

We first give the key ideas that lead to the proof presented at the end of this section. The relation $S(\mathcal{D}) = S(\overline{\mathcal{D}'}) \leq S_f(\overline{\mathcal{D}'})$ follows from Proposition 4.9 and (4.2). For the other inequality $S(\mathcal{D}) \geq S_f(\overline{\mathcal{D}'})$, Eve independently chooses distributions $P_{X_1Y_1Z_1}, P_{X_2Y_2Z_2}, \ldots, P_{X_NY_NZ_N}$ from a finite set $\mathcal{D}$. Alice and Bob want to use a protocol $\mathcal{P} \in \Gamma_f\left(\overline{\mathcal{D}} \to P_{S_AS_B\perp}\right)$ which handles only random variables with a fixed distribution in $\overline{\mathcal{D}}$.

A first idea Alice and Bob can have is to draw $\widetilde{X_1}\widetilde{Y_1}$ uniformly at random from their random variables $\{X_1Y_1,\ X_2Y_2, \ldots, X_NY_N\}$. It is easy to see that $P_{\widetilde{X_1}\widetilde{Y_1}} = \frac{1}{N}\sum_{i=1}^N P_{X_iY_i}$ which is an element of the convex set $\overline{\mathcal{D}}$. They might continue to independently draw (with replacement) N times from $\{X_1Y_1, X_2Y_2, \ldots, X_NY_N\}$ with the idea to obtain $P_{\widetilde{X^N}\widetilde{Y^N}} \stackrel{?}{=} \left(\frac{1}{N}\sum_{i=1}^N P_{X_iY_i}\right)^N$ and apply $\mathcal{P}$, but this works only if no variable is drawn twice as otherwise $\widetilde{X^N}\widetilde{Y^N}$ are not independent. It is well-known that the first time an element is drawn twice when drawing uniformly and independently with replacement from a set with N elements is around the $\sqrt{N}$th try which disables the proposed procedure.

Alice and Bob have to make sure that their random variables remain independent. They draw from $\{X_1Y_1, X_2Y_2, \ldots, X_NY_N\}$ *without replacement* which is the same as permuting their variables. The distribution of the first element drawn $P_{\widetilde{X_1}\widetilde{Y_1}}$ is the average distribution $\frac{1}{N}\sum_{i=1}^N P_{X_iY_i}$ just like above, but with every element that is drawn, the distribution differs more from the average distribution.

This problem can be eased by drawing (without replacement) only a few elements from a large set of variables which results in permuting NK variables and processing them in K blocks of size N. It is shown in Appendix A.2 that the resulting distribution $P_{\widetilde{X_i^N}\widetilde{Y_i^N}}$ of one block tends to the average distribution as K goes to infinity. Lemma A.2 can be used to prove Theorem 4.11 as alternative to the proof presented below.

The adversary Eve chooses the distributions and learns the permutation sent over the public channel. Hence she knows the exact distributions of all random variables. When considering a protocol for a fixed distribution from $\overline{\mathcal{D}}$, we have to take care that none of the adversary's information is lost. That is why we take a protocol from $\Gamma_f\left(\overline{\mathcal{D}'} \to P_{S_A S_B \perp}\right)$.

For the proof of Theorem 4.11, a result from [DF80] that formalises the above ideas is used. Let $\mathcal{S}$ be a set of finite cardinality c. Let $\mathcal{S}^k$ be the set of k-tuples of elements of $\mathcal{S}$. A probability P on $\mathcal{S}^k$ is said to be *exchangeable* provided it is invariant under permutations. More precisely, if π is a permutation of $\{1, 2, \ldots, k\}$, then

$$P(s_1, \ldots, s_k) = P(s_{\pi(1)}, \ldots s_{\pi(k)}).$$

Let $\mathcal{S}^*$ be the set of probabilities on $\mathcal{S}$; geometrically, $\mathcal{S}^*$ is the unit simplex in $\mathbb{R}^c$. For a probability $Q \in \mathcal{S}^*$, let $Q^k = \prod_{i=1}^k Q$ be the distribution of k independent picks from Q. If μ is a probability on the Borel subsets of $\mathcal{S}^*$, we define the probability $P_{\mu k}$ on $\mathcal{S}^k$ as follows: Choose Q from $\mathcal{S}^*$ at random with probability μ, then make k independent picks from Q. Formally,

$$P_{\mu k}(A) = \int_{\mathcal{S}^*} Q^k(A)\, \mu(dQ).$$

If P is a probability on $\mathcal{S}^n$ and $k \leq n$, let P_k be the projection of P onto $\mathcal{S}^k$. More formally, P_k is the distribution of $(s_1, \ldots, s_k)$ when the n-tuple $(s_1, \ldots, s_k, s_{k+1}, \ldots, s_n)$ is distributed according to P. Clearly, $(P_{\mu n})_k = P_{\mu k}$.

Theorem 4.12. *[DF80, Theorem 3] Let $\mathcal{S}$ be a set of finite cardinality $c \in \mathbb{N}$. For $n \in \mathbb{N}$, let P be an exchangeable probability on $\mathcal{S}^n$. Then there exists a probability μ on the Borel subsets of $\mathcal{S}^*$ such that*

$$\|P_k - P_{\mu k}\| \leq 2c\frac{k}{n} \qquad \textit{for all } k \leq n.$$

Proof of Theorem 4.11. As stated above, it follows from Proposition 4.9 and (4.2) that $S(\mathcal{D}) = S(\overline{\mathcal{D}'}) \leq S_f(\overline{\mathcal{D}'})$. As $S(\mathcal{D}) = S(\mathcal{D}')$ it remains to prove $S(\mathcal{D}') \geq S_f(\overline{\mathcal{D}'})$ which is done by giving for each protocol $\mathcal{P}_f \in \Gamma_f\left(\overline{\mathcal{D}'} \to P_{S_A S_B \perp}\right)$ a protocol with the same rate in $\Gamma\left(\mathcal{D}' \to P_{S_A S_B \perp}\right)$.

Fix $\varepsilon > 0$ and $\mathcal{P}_f \in \Gamma_f\left(\overline{\mathcal{D}'} \to P_{S_A S_B \perp}\right)$. The protocol $\mathcal{P}_f$ transforms $P^N_{XYZ} = \prod_{i=1}^N P_{XYZ}$ for $P_{XYZ} \in \overline{\mathcal{D}'}$ into $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ so that for large enough N holds

$$\min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) < \varepsilon. \tag{4.4}$$

Let Eve independently choose distributions $P_{X_1 Y_1 (Z_1 D_1)}, P_{X_2 Y_2 (Z_2 D_2)}, \ldots$ from $\mathcal{D}'$.

For $K \in \mathbb{N}$ which will be chosen later on, the protocol $\mathcal{P}$ consists of the following steps:

1. Alice chooses uniformly at random a permutation π from the set of all permutations of NK elements. She sets for all $i = 1, 2, \ldots, NK : \widetilde{X}_i := X_{\pi(i)}$.

2. Alice sends as first message $C_0 := \pi$ to Bob. Bob sets $\widetilde{Y}_i := Y_{\pi(i)} \quad \forall i = 1, 2, \ldots, NK$.

3. Alice and Bob partition their random variables into K blocks of size N:

$$\underbrace{\widetilde{X}_1\widetilde{Y}_1, \ldots, \widetilde{X}_N\widetilde{Y}_N}_{\widetilde{X}_1^N\widetilde{Y}_1^N}, \underbrace{\widetilde{X}_{N+1}\widetilde{Y}_{N+1}, \ldots, \widetilde{X}_{2N}\widetilde{Y}_{2N}}_{\widetilde{X}_2^N\widetilde{Y}_2^N}, \ldots, \underbrace{\widetilde{X}_{N(K-1)+1}\widetilde{Y}_{N(K-1)+1}, \ldots, \widetilde{X}_{NK}\widetilde{Y}_{NK}}_{\widetilde{X}_K^N\widetilde{Y}_K^N}$$

   To each block $\widetilde{X}_i^N\widetilde{Y}_i^N$ they apply the protocol $\mathcal{P}_f$.

We claim that $\mathcal{P}$ fulfills condition (3.28). Then Corollary 3.13 yields a protocol in $\Gamma(\mathcal{D}' \to P_{S_A S_B \perp})$. For an arbitrary joint distribution $P_{X^{NK}Y^{NK}Z^{NK}}$ of NK discrete random variables and a randomly chosen permutation π, the "permuted" probability $P_{\widetilde{X^{NK}}\widetilde{Y^{NK}}\widetilde{Z^{NK}}}$ is exchangeable because it is invariant under permutations. According to Theorem 4.12 there exists a probability μ such that

$$d\left(P_{\widetilde{X^n}\widetilde{Y^n}\widetilde{Z^n}}, P^n_{XYZ,\mu}\right) \leq 2c\frac{n}{NK} \quad \text{for all } n \leq NK \tag{4.5}$$

where $c = |\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}|$ and $P_{XYZ,\mu}$ does not depend on n and is defined as follows: choose P_{XYZ} at random with probability μ, then make n independent picks from P_{XYZ}. Formally,

$$P^n_{XYZ,\mu}(x,y,z) = \int P^n_{XYZ}(x,y,z)\,\mu(dP_{XYZ}).$$

For $n = 1$ follows from (4.5) that $P_{XYZ,\mu}$ lies in $\overline{\mathcal{D}}$ for large N and K because $P_{\widetilde{X_1}\widetilde{Y_1}\widetilde{Z_1}} \in \mathcal{D}$ and

$$d\left(P_{\widetilde{X_1}\widetilde{Y_1}\widetilde{Z_1}}, P_{XYZ,\mu}\right) \leq 2c\frac{1}{NK} \overset{(N,K\to\infty)}{\longrightarrow} 0.$$

We choose K large enough such that in each block i, the real distribution is nearly identically distributed. Formally,

$$d\left(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P^N_{XYZ,\mu}\right) \leq 2c\frac{N}{NK} = 2c\frac{1}{K} < \varepsilon. \tag{4.6}$$

Eve chooses the distributions from $\mathcal{D}$ and learns π from the first message C_0. Hence, she knows the distribution of each random variable $P_{\widetilde{X_i}\widetilde{Y_i}\widetilde{Z_i}}$. As the random variables are independent, only $\widetilde{Z_i}\widetilde{D_i} = Z_{\pi(i)}D_{\pi(i)}$ gives information about $\widetilde{X_i}\widetilde{Y_i}$. By Definition 4.6 $\widetilde{D_i}$ uniquely determines the distribution $P_{\widetilde{X_i}\widetilde{Y_i}\widetilde{Z_i}}$. Hence, we can assume without loss of generality that Eve only knows $\widetilde{Z_1}\widetilde{D_1}, \widetilde{Z_2}\widetilde{D_2}, \ldots, \widetilde{Z_{NK}}\widetilde{D_{NK}}$, i.e., she forgets the original distributions $P_{X_1Y_1(Z_1D_1)}, P_{X_2Y_2(Z_2D_2)}, \ldots, P_{X_{NK}Y_{NK}(Z_{NK}D_{NK})}$ as well as the permutation π.

Considering the ith block, the same argument yields that we can assume Eve to know only $\widetilde{Z_i^N}\widetilde{D_i^N}$. Hence, the protocol $\mathcal{P}_f$ can be applied to this block. It transforms $P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}$ into $P_{\widetilde{X_i^M}\widetilde{Y_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}$ and $P^N_{XYZ,\mu}$ into $P_{\bar{X}^M\bar{Y}^M Z^N C^*}$. We conclude

$$\begin{aligned}
&\min_{P_U} d\Big(P_{\widetilde{X_i^M}\widetilde{Y_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M}P_U\Big) &(4.7)\\
&\leq \min_{P_U}\Big(d\Big(P_{\widetilde{X_i^M}\widetilde{Y_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{\bar{X}^M\bar{Y}^M Z^N C^*}\Big) + d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M}P_U\Big)\Big)\\
&= d\Big(P_{\widetilde{X_i^M}\widetilde{Y_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{\bar{X}^M\bar{Y}^M Z^N C^*}\Big) + \min_{P_U} d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M}P_U\Big)\\
&\leq d\Big(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P^N_{XYZ,\mu}\Big) + \min_{P_U} d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M}P_U\Big) &(4.8)\\
&< 2\varepsilon. &(4.9)
\end{aligned}$$

Inequality (4.8) follows from Proposition 2.19 and (4.9) from (4.4) and (4.6). Therefore (4.7) can be made arbitrarily small and Corollary 3.13 be applied to obtain a protocol with the same rate as $\mathcal{P}_f$ in $\Gamma(\mathcal{D}' \to P_{S_A S_B \perp})$. □

4.4 Recognition of a Distribution

4.4.1 Groups of Similar Distributions

Alice and Bob can try to find out which distribution(s) the adversary Eve has chosen. If Eve chooses independently from an infinite set $\mathcal{D}$, and we assume that the players Alice and Bob can deduce the distributions from their random variables, they are able to form groups of random variables with similar distributions. A protocol suitable for each group can then be applied.

Alice and Bob are also allowed to communicate over the public channel in order to determine the joint distribution as long as the conversation does not reveal more information about the realisations to the adversary than Eve already has from the joint distribution.

Theorem 4.13. *Let $\mathcal{D}$ be a set of distributions P_{XYZ} so that, for all i, Alice and Bob are able to find out from their random variables X_iY_i and by restricted public discussion described above the joint distribution $P_{X_iY_iZ_i}$. Then*

$$S(\mathcal{D}) = \inf_{P_{XYZ}\in\mathcal{D}} S(P_{XYZ}).$$

Proof. From relation (4.2) and Proposition 4.5 follows $S(\mathcal{D}) \leq S_f(\mathcal{D}) \leq \inf_{P_{XYZ}\in\mathcal{D}} S(P_{XYZ})$. To show the other inequality, consider random variables $X_1Y_1Z_1, X_2Y_2Z_2, \ldots$ with given distributions $P_{X_1Y_1Z_1}$, $P_{X_2Y_2Z_2}, \ldots \in \mathcal{D}$.

Let $\varepsilon > 0$ and N large enough that for all protocols $\mathcal{P} \in \bigcup_{P_{XYZ}\in\mathcal{D}} \Gamma\left(P_{XYZ} \to P_{S_AS_B\perp}\right)$ holds

$$\min_{P_U} d\left(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) < \varepsilon. \tag{4.10}$$

In a first step Alice and Bob communicate over the public channel to determine all joint distributions $P_{X_iY_iZ_i}$. By assumption this is done in a such way that no new information is revealed to Eve. After this step all players involved know all distributions.

Alice and Bob want to partition $P_{X_1Y_1Z_1}, P_{X_2Y_2Z_2}, \ldots$ into a finite number of classes. In each class, the maximal distance between pairs of distributions should be ε/N.

From a geometric point of view, a distribution P_{XYZ} can be seen as a point of the unit simplex in $\mathbb{R}^c$ where $c = |\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}|$ denotes the dimension of the joint range of XYZ. $\mathcal{D}$ is a subset of this simplex.

Recall that the L_1-distance of two points $a, b \in \mathbb{R}^c$ is defined as $\sum_{i=1}^{c} |a_i - b_i|$. Hence, the maximal L_1-distance between two points in a two-dimensional square with side length δ is 2δ. In a three-dimensional cube with side length δ, the maximal distance is 3δ. In the c-dimensional hypercube it is $c\cdot\delta$. To cover the unit simplex in $\mathbb{R}^c$ in such a way that the maximal distance in one class is at most ε/N, we need therefore a c-dimensional $\frac{\varepsilon}{Nc}$-grid. Hence, the number of classes to cover the unit simplex in this way is upper bounded by $\left(\frac{Nc}{\varepsilon}\right)^c < \infty$.

By partitioning the infinitely many distributions $P_{X_1Y_1Z_1}, P_{X_2Y_2Z_2}, \ldots$ into this finite number of classes, we consider only those classes that get infinitely many elements when more and more distributions are divided up into the classes.

Let us denote the distributions in one of these classes with $P_{\widetilde{X}_1\widetilde{Y}_1\widetilde{Z}_1}, P_{\widetilde{X}_2\widetilde{Y}_2\widetilde{Z}_2}, \ldots$. Alice and Bob arbitrarily fix one of these distributions, denote it by P_{XYZ}, and choose a protocol

$\mathcal{P} \in \Gamma\left(P_{XYZ} \to P_{S_A S_B \perp}\right)$. All other distributions of this class have distance at most ε/N from P_{XYZ}. They form blocks of length N with the realisations of the random variables: $\widetilde{X_1}\widetilde{Y_1}\widetilde{Z_1}, \ldots, \widetilde{X_N}\widetilde{Y_N}\widetilde{Z_N}$, $\widetilde{X_{N+1}}\widetilde{Y_{N+1}}\widetilde{Z_{N+1}}, \ldots, \widetilde{X_{2N}}\widetilde{Y_{2N}}\widetilde{Z_{2N}}$, ... In each block i Lemma 2.6 assures that

$$d\left(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P_{XYZ}^N\right) \leq \varepsilon \quad \forall i = 1, 2, \ldots. \tag{4.11}$$

The protocol $\mathcal{P}$ is applied to each block. It transforms $P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}$ into $P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}$ and P_{XYZ}^N into $P_{S_A^M S_B^M Z^N C^*}$. It follows like in the previous proof that

$$\begin{aligned}
&\min_{P_U} d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M} P_U\Big) &(4.12)\\
&\leq \min_{P_U}\Big(d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{\bar{X}^M\bar{Y}^M Z^N C^*}\Big) + d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big)\Big)\\
&= d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{\bar{X}^M\bar{Y}^M Z^N C^*}\Big) + \min_{P_U} d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big)\\
&\leq d\Big(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P_{XYZ}^N\Big) + \min_{P_U} d\Big(P_{\bar{X}^M\bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big)\\
&\leq 2\varepsilon \qquad \text{by (4.11) and (4.10).}
\end{aligned}$$

Hence, (4.12) can be made arbitrarily small. Applying Corollary 3.13, Alice and Bob obtain a secret key at rate $S(P_{XYZ})$ from this class. The same thing can be done for all infinite classes. After another step of Privacy Amplification[1], i.e., application of Corollary 3.13 to minimise Eve's knowledge about the keys from different classes, Alice and Bob share a secret key. As only protocols with rates larger than $\inf_{P_{XYZ}\in\mathcal{D}} S(P_{XYZ})$ have been used, this yields an overall secret-key rate which is larger or equal to $\inf_{P_{XYZ}\in\mathcal{D}} S(P_{XYZ})$. □

4.4.2 Estimate a Distribution

The scenario of the previous section is based on the quite strong assumption that Alice and Bob are able to directly deduce the joint distribution P_{XYZ} from a single representation of their variables. Motivated by the bounds of $S(\mathcal{D})$ in terms of $S_f(\cdot)$ from Section 4.3, we restrict ourselves in this section to a fixed distribution from $\mathcal{D}$ which Alice and Bob want to estimate based on independent realisations. They use some of their variables to estimate this distribution and apply a protocol intended for the estimated distribution to extract a secret key from the rest of their variables. We have to make sure that they can somehow deduce the joint distribution P_{XYZ} from their estimate $\widehat{P}_{XY}$. This is done by the following definition of a continuous set $\mathcal{D}$.

For a set of distributions $\mathcal{D}$, let f be the function which gives for every marginal distribution P_{XY} from $\mathcal{D}$ the set of all possible original distributions. Formally,

$$f(P_{XY}) := \Big\{P_{XYZ} \in \mathcal{D} : P_{XY} = \sum_z P_{XYZ}\Big\}.$$

[1] See [Wol99] for a definition of Privacy Amplification.

Definition 4.14. *The set $\mathcal{D}$ and the function f are called* continuous *if*

$$\forall \varepsilon > 0 \, \exists \delta > 0 \, \forall P_{XY}, \widehat{P}_{XY} \in \mathcal{D} : d\left(P_{XY}, \widehat{P}_{XY}\right) \leq \delta \Rightarrow \max_{\substack{P_{XYZ} \in f(P_{XY}) \\ \widehat{P}_{XYZ} \in f(\widehat{P}_{XY})}} d\left(P_{XYZ}, \widehat{P}_{XYZ}\right) \leq \varepsilon.$$

Theorem 4.15. *For a continuous set $\mathcal{D}$ holds*

$$S_f(\mathcal{D}) = \inf_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ}).$$

For the proof of this theorem, two statistical tools from [CT91] are used. The *relative entropy* $D(P||Q)$ of two probabilities P and Q is another measure of the distance between P and Q. It behaves like the square of the Euclidean distance:

Lemma 4.16. *[CT91, Lemma 12.6.1]*

$$D(P||Q) \cdot 2 \ln 2 \geq d(P,Q)^2.$$

Definition 4.17. *[CT91] The* type *or* empirical probability distribution $P_{\mathbf{x}}$ *of a sequence $\mathbf{x} = (x_1, x_2, \dots, x_n)$ is the relative proportion of occurrences of each symbol of $\mathcal{X}$, i.e., $P_{\mathbf{x}}(a) = N(a|\mathbf{x})/n$ for all $a \in \mathcal{X}$, where $N(a|\mathbf{x})$ is the number of times the symbol a occurs in the sequence $\mathbf{x} \in \mathcal{X}^n$.*

The following theorem gives the key estimate.

Theorem 4.18. *[CT91, Theorem 12.2.1] Let $X_1, X_2, \dots, X_n$ be random variables independently and identically distributed according to $Q(x)$. Then*

$$P_{X^n}\left[D\left(P_{x^n}||Q\right) > \varepsilon\right] \leq 2^{-n\left(\varepsilon - |\mathcal{X}|\frac{\log(n+1)}{n}\right)}.$$

Proof of Theorem 4.15. Proposition 4.5 states $S_f(\mathcal{D}) \leq \inf_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ})$. For the other inequality fix a distribution P_{XYZ} from $\mathcal{D}$ and let $X_1Y_1Z_1, X_2Y_2Z_2, \dots$ be independently P_{XYZ}-distributed. For a fixed $\varepsilon > 0$, we choose N large enough that for all protocols $\mathcal{P} \in \bigcup_{\widetilde{P}_{XYZ} \in \mathcal{D}} \Gamma\left(\widetilde{P}_{XYZ} \to P_{S_A S_B \perp}\right)$ holds

$$\min_{P_U} d\Big(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big) < \varepsilon. \tag{4.13}$$

The idea of the proof is that, for a $L \in \mathbb{N}$ which is determined later on, Alice and Bob use L of their random variables to determine a distribution $\widehat{P}_{XYZ}$ which is an estimate of the true distribution P_{XYZ}. They then partition the remaining variables into K blocks of size N and apply a protocol in $\Gamma\left(\widehat{P}_{XYZ} \to P_{S_A S_B \perp}\right)$ to each block.

For $K, L \in \mathbb{N}$ the following protocol processes $NK + L$ variables:

1. Alice and Bob exchange the first L variables over the public channel. From the sequence $\mathbf{xy} = (x_1y_1, \dots, x_Ly_L)$ they both determine the empirical distribution

$$\widehat{P}_{\mathbf{xy}}(x,y) = \frac{N\left(xy|X^LY^L\right)}{L}.$$

2. They agree on a distribution $\widehat{P}_{XY} \in \mathcal{D}$ with minimal L_1-distance to $\widehat{P}_{\mathbf{xy}}$.
3. They further agree on $\widehat{P}_{XYZ} \in f(\widehat{P}_{XY})$ and a protocol $\mathcal{P} \in \Gamma\left(\widehat{P}_{XYZ} \to P_{S_A S_B \perp}\right)$. After partitioning the remaining variables into K blocks of size N, $\mathcal{P}$ is applied to each block.

Since $\mathcal{D}$ is continuous, there exists a $\delta(\varepsilon, N) > 0$ such that

$$d\left(P_{XY}, \widehat{P}_{XY}\right) \leq \delta \Rightarrow d\left(P_{XYZ}, \widehat{P}_{XYZ}\right) \leq \frac{\varepsilon}{N}.$$

The probability that $d(P_{XY}, \widehat{P}_{XY}) \geq d(P_{XY}, \widehat{P}_{\mathbf{xy}}) > \delta$ is bound as follows

$$\begin{aligned}
P_{X^L Y^L}\left[d(\widehat{P}_{\mathbf{xy}}, P_{XY}) > \delta\right] &= P_{X^L Y^L}\left[d(\widehat{P}_{\mathbf{xy}}, P_{XY})^2 > \delta^2\right] \\
&\leq P_{X^L Y^L}\left[D(\widehat{P}_{\mathbf{xy}} || P_{XY}) \cdot 2\ln 2 > \delta^2\right] \qquad (4.14) \\
&= P_{X^L Y^L}\left[D(\widehat{P}_{\mathbf{xy}} || P_{XY}) > \frac{\delta^2}{2\ln 2}\right] \\
&\leq 2^{-L\left(\frac{\delta^2}{2\ln 2} - |\mathcal{X}|\cdot|\mathcal{Y}|\frac{\log(L+1)}{L}\right)}. \qquad (4.15)
\end{aligned}$$

Inequality (4.14) is due to Lemma 4.16, and the last inequality is given by Theorem 4.18. Depending on δ, i.e., on N and ε, we choose $L \in \mathbb{N}$ large enough that the last term (4.15) is smaller than ε.

This shows that with probability $1 - \varepsilon$ Alice and Bob can estimate the true distribution P_{XYZ} by $\widehat{P}_{XYZ}$ which is good enough that in each block holds:

$$d\left(P^N_{XYZ}, \widehat{P}^N_{XYZ}\right) \leq N \cdot \underbrace{d\left(P_{XYZ}, \widehat{P}_{XYZ}\right)}_{\leq \varepsilon/N} \leq \varepsilon \qquad (4.16)$$

where Lemma 2.6 is used for the first inequality. For the rest of the proof, we denote with $P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N C_i^*}$ the distribution generated by the protocol $\mathcal{P}$ when applied to the ith block and by $P_{\widehat{\bar{X}^M}\widehat{\bar{Y}^M}\widehat{Z^N}\widehat{C^*}}$ the generated distribution if the processed variables had distribution $\widehat{P}_{XYZ}$ and conclude as usual:

$$\begin{aligned}
&\min_{P_U} d\left(P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N C_i^*}, P_{S_A^M S_B^M} P_U\right) \\
&\leq d\left(P_{\bar{X}_i^M \bar{Y}_i^M Z_i^N C_i^*}, P_{\widehat{\bar{X}^M}\widehat{\bar{Y}^M}\widehat{Z^N}\widehat{C^*}}\right) + \min_{P_U} d\left(P_{\widehat{\bar{X}^M}\widehat{\bar{Y}^M}\widehat{Z^N}\widehat{C^*}}, P_{S_A^M S_B^M} P_U\right) \\
&\leq d\left(P^N_{XYZ}, \widehat{P}^N_{XYZ}\right) + \min_{P_U} d\left(P_{\widehat{\bar{X}^M}\widehat{\bar{Y}^M}\widehat{Z^N}\widehat{C^*}}, P_{S_A^M S_B^M} P_U\right) \\
&\leq 2\varepsilon \qquad \text{by (4.16) and (4.13).}
\end{aligned}$$

The blocks are independent, Corollary 3.13 applies. We showed that with probability $1 - \varepsilon$, we can extract a secret key at rate

$$\frac{KM}{KN + L} = \frac{M(N)}{N + \frac{L(N)}{K}}. \qquad (4.17)$$

As L is independent of K, we let K grow faster than $L(N)$ for $N \to \infty$. Hence, we have obtained a protocol in $\Gamma_f\left(D \to P_{S_A S_B \perp}\right)$ whose rate (4.17) tends to $\lim_{N\to\infty} \frac{M(N)}{N} = \mathrm{Rate}(\mathcal{P}) = S(\widehat{P}_{XYZ}) \geq \inf_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ})$ with probability at least $1 - \varepsilon$. □

4.5 Adaptive Eve: Dependent Distributions

In this section we show that the generalised secret-key rate $S(\mathcal{D})$ is equal to the secret-key rate of dependent distributions $S_d(\mathcal{D})$.

Theorem 4.19. *For all sets of distributions $\mathcal{D}$, it holds*

$$S_d(\mathcal{D}) = S(\mathcal{D}).$$

4.5.1 Examples and Ideas

We start with an example to illustrate the problems that occur if Eve can adaptively choose the distributions and give the idea how these problems can be solved. Consider the set $\mathcal{D} = \{P^{(1)}_{XYZ}, P^{(2)}_{XYZ}\}$ consisting of the two following distributions:

$P^{(1)}_{XYZ}$

X / Y (Z)	0	1	2
0	(0) 1/3		
1		(0) 1/3	
2			(1) 1/3

$P^{(2)}_{XYZ}$

X / Y (Z)	3	4
3	(2) 1/2	
4		(2) 1/2

It is easy to give a protocol in $\Gamma\left(\mathcal{D} \to P_{S_A S_B \perp}\right)$ with $S(\mathcal{D}) > 0$: Alice and Bob discard the random variables X and Y whose realisations take on the value 2, map values $\{3, 4\}$ to $\{0, 1\}$, and after a uniformation step, they share a perfect secret key. We slightly modify this protocol to obtain a protocol $\mathcal{P}'$. The modified protocol $\mathcal{P}'$ does exactly the same as $\mathcal{P}$ but "fails", i.e., outputs the all-zero string of length M if the following three conditions hold:

- The first distribution $P_{X_1Y_1Z_1}$ is $P^{(1)}_{XYZ}$.
- For all $i = 1, \ldots, N-1$ holds: If $X_i \in \{0, 1, 3, 4\}$ then $P_{X_{i+1}Y_{i+1}Z_{i+1}} = P^{(1)}_{XYZ}$.
- For all $i = 1, \ldots, N-1$ holds: If $X_i = 2$ then $P_{X_{i+1}Y_{i+1}Z_{i+1}} = P^{(2)}_{XYZ}$.

Note that the protocol $\mathcal{P}'$ is also in $\Gamma\left(\mathcal{D} \to P_{S_A S_B \perp}\right)$ because the probability that the protocol fails, i.e., that the distributions are independently chosen in such a way that all three conditions hold tends to zero as N grows infinitely.

The protocol $\mathcal{P}'$ illustrates the advantage of an adaptive adversary.[2] If Eve can look at her Z-realisations before choosing the next distribution, she can always cause the protocol $\mathcal{P}'$ to fail. Hence, $\mathcal{P}' \notin \Gamma_d\left(\mathcal{D} \to P_{S_A S_B \perp}\right)$. If Eve wants to *independently*—without looking at her Z-realisations—choose the distributions in such a way that the protocol fails, she has to guess correctly for every $P^{(1)}_{XYZ}$-distributed variable whether $X = 2$ or not, but the probability of correct guessing vanishes exponentially in N.

In this example there is a way for Alice and Bob to prevent an adaptive Eve from causing the protocol $\mathcal{P}'$ to fail. Alice randomly permutes her X-variables, and sends the permutation to Bob who does the same with his Y-variables. Eve learns the permutation as it is sent over the public channel, but she has no control of the order the variables have after the

[2] Of course, $\mathcal{P}'$ is a "pathological" protocol constructed only for illustration purposes and of less practical use than $\mathcal{P}$.

permutation. However Eve (adaptively) chooses the distributions, the probability that the three conditions hold for the permuted variables tends to zero for large N. This illustrates the fact that permuting the variables can help Alice and Bob to prevent adaptive attacks of the adversary, but the next example shows that permuting is not sufficient.

Let $\mathcal{D}$ and $\mathcal{P}$ be like above. This time, the modified protocol $\widehat{\mathcal{P}}$ is identical to $\mathcal{P}$ except it fails whenever the following is true:

- Of the N distributions the protocol has to handle, the number of occurrences of the distribution $P^{(2)}_{XYZ}$ equals exactly the number of times X takes on the value 2.

It is easy to verify that like $\mathcal{P}'$ from the first example, the protocol $\widehat{\mathcal{P}}$ is in $\Gamma\left(\mathcal{D} \to P_{S_A S_B \perp}\right)$ but not in $\Gamma_d\left(\mathcal{D} \to P_{S_A S_B \perp}\right)$. Of course, in this case permuting the variables does not help. Alice and Bob cannot prevent an adaptive Eve from choosing exactly as many distributions $P^{(2)}_{XYZ}$ as occurrences of $X = 2$.

Another "countermeasure" can be used instead: after the random permutation from above, Alice and Bob partition their random variables in K blocks of size N. For large K it is unlikely that the condition above is fulfilled in each block. It is intuitive and can be shown that for large enough K and N, the protocol $\widehat{\mathcal{P}}$ can be applied to each block and fails only for a negligible number of blocks. Hence, a secret key can be extracted at rate $\text{Rate}(\widehat{\mathcal{P}})$.

The concepts of permuting the random variables and partitioning them into blocks have already been formalised in Section 4.3 and are used as well in the next section to prove Theorem 4.19.

4.5.2 Proof of Theorem 4.19

$S_d(\mathcal{D}) \leq S(\mathcal{D})$ is already stated in (4.2). For the other inequality $S_d(\mathcal{D}) \geq S(\mathcal{D}) = S(\overline{\mathcal{D}})$, let Eve adaptively choose distributions of $X_1Y_1Z_1, X_2Y_2Z_2, \ldots$ from $\mathcal{D}$ as described in Definition 4.1. We fix $\varepsilon > 0$ and $\mathcal{P} \in \Gamma\left(\overline{\mathcal{D}} \to P_{S_A S_B \perp}\right)$ which generates $P_{\bar{X}^M \bar{Y}^M Z^N C^*}$ from N independent random variables. Let N be large enough such that

$$\min_{P_U} d\left(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\right) < \varepsilon. \tag{4.18}$$

For $K \in \mathbb{N}$ the protocol $\mathcal{P}'$ is exactly the same as in the proof of Theorem 4.11. For the sake of completeness, it is repeated here:

1. Alice chooses uniformly at random a permutation π from the set of all permutations of NK elements. She sets for all $i = 1, 2, \ldots, NK : \widetilde{X}_i := X_{\pi(i)}$.

2. Alice sends as first message $C_0 := \pi$ to Bob. Bob sets $\widetilde{Y}_i := Y_{\pi(i)} \quad \forall i = 1, 2, \ldots, NK$.

3. Alice and Bob partition their random variables into K blocks of size N:

$$\underbrace{\widetilde{X}_1\widetilde{Y}_1, \ldots, \widetilde{X}_N\widetilde{Y}_N}_{\widetilde{X}_1^N\widetilde{Y}_1^N}, \underbrace{\widetilde{X}_{N+1}\widetilde{Y}_{N+1}, \ldots, \widetilde{X}_{2N}\widetilde{Y}_{2N}}_{\widetilde{X}_2^N\widetilde{Y}_2^N}, \ldots, \underbrace{\widetilde{X}_{N(K-1)+1}\widetilde{Y}_{N(K-1)+1}, \ldots, \widetilde{X}_{NK}\widetilde{Y}_{NK}}_{\widetilde{X}_K^N\widetilde{Y}_K^N}$$

To each block $\widetilde{X}_i^N\widetilde{Y}_i^N$ they apply the protocol $\mathcal{P}$.

The idea is to apply Proposition 3.12 to obtain a protocol in $\Gamma_d\left(\mathcal{D} \rightarrow P_{S_A S_B \perp}\right)$. Therefore, it is shown like in the proof of Theorem 4.11 that there exist μ and $P_{XYZ,\mu} \in \overline{\mathcal{D}}$, and K can be chosen large enough such that in each block i, the real distribution is nearly independent. Formally,

$$d\left(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P_{XYZ,\mu}^N\right) \leq 2c\frac{N}{NK} = 2c\frac{1}{K} < \varepsilon. \tag{4.19}$$

The protocol $\mathcal{P} \in \Gamma\left(\overline{\mathcal{D}} \rightarrow P_{S_A S_B \perp}\right)$ can handle independent distributions known to (and chosen independently by) the adversary. Therefore, we can apply $\mathcal{P}$ to each block and claim that (3.27) is fulfilled. Recall the block notation from Proposition 3.12 for the following.

The adversary Eve can choose the distributions adaptively from $\mathcal{D}$ and knows the permutation π from the first message C_0 sent over the public channel. Hence, Eve knows the exact distributions of all random variables. We assume for the rest of the proof that this knowledge is contained in her Z-variables. After the adaptive choice is made, the distributions and Z-realisations other than from block i give no more information about the ith block than she already has knowing the exact distributions and Z-realisations of the ith block. Hence,

$$\widetilde{X_i^N}\widetilde{Y_i^N} \leftrightarrow \widetilde{Z_i^N} \leftrightarrow \widetilde{X_{-i}^{NK}}\widetilde{Y_{-i}^{NK}}\widetilde{Z_{-i}^{NK}}$$

is a Markov chain. As the protocol $\mathcal{P}$ processes the $\widetilde{X}\widetilde{Y}$-variables of the ith block independently from Z^{NK} and the $\widetilde{X}\widetilde{Y}$-variables of the other blocks,

$$\begin{aligned} \widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{C_i^*} \leftrightarrow \widetilde{Z_i^N} \leftrightarrow \widetilde{\bar{X}_{-i}^{NK}}\widetilde{\bar{Y}_{-i}^{NK}}\widetilde{Z_{-i}^{NK}}\widetilde{C_{-i}^{*K}} \quad &\text{and} \\ \widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M} \leftrightarrow \widetilde{Z_i^N}\widetilde{C_i^*} \leftrightarrow \widetilde{\bar{X}_{-i}^{NK}}\widetilde{\bar{Y}_{-i}^{NK}}\widetilde{Z_{-i}^{NK}}\widetilde{C_{-i}^{*K}} & \end{aligned} \tag{4.20}$$

are Markov chains as well. The random variable $\widetilde{C_i^*}$ denotes the communication of protocol $\mathcal{P}$ for block i. We assume the first message of the outer protocol $\mathcal{P}'$, the permutation $C_0 = \pi$, as part of $\widetilde{C_i^*}$ for all i.

Considering the ith block, the inner protocol $\mathcal{P}$ transforms $P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}$ into $P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}$ and $P_{XYZ,\mu}^N$ into $P_{\bar{X}^M\bar{Y}^M Z^N C^*}$. In the following we use the same idea as in the proof of Proposition 3.2. Let V be the random variable that minimises $d\big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M} P_V\big)$. Let c be the channel that gives $\widetilde{\bar{X}_{-i}^{NK}}\widetilde{\bar{Y}_{-i}^{NK}}\widetilde{Z_{-i}^{NK}}\widetilde{C_{-i}^{*K}}$ on input $\widetilde{Z_i^N}\widetilde{C_i^*}$ defined by the Markov chain (4.20). We denote by $\widetilde{V}_i$ the random variable obtained by sending V over the same channel c. It then follows that

$$\begin{aligned} &\min_{P_{U'}} d\left(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}\widetilde{\bar{X}_{-i}^{MK}}\widetilde{\bar{Y}_{-i}^{MK}}\widetilde{Z_{-i}^{NK}}\widetilde{C_{-i}^{*K}}}, P_{S_A^M S_B^M} P_{U'}\right) && (4.21) \\ &\leq d\left(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}\widetilde{\bar{X}_{-i}^{MK}}\widetilde{\bar{Y}_{-i}^{MK}}\widetilde{Z_{-i}^{NK}}\widetilde{C_{-i}^{*K}}}, P_{S_A^M S_B^M} P_{V\widetilde{V}_i}\right) && \\ &= d\left(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M} P_V\right) && (4.22) \\ &= \min_{P_U} d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M} P_U\Big). && \end{aligned}$$

Equality (4.22) is due to Lemma 2.15.

We conclude as usual that

$$\begin{aligned}
&\min_{P_U} d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{S_A^M S_B^M} P_U\Big) \\
&\quad \leq d\Big(P_{\widetilde{\bar{X}_i^M}\widetilde{\bar{Y}_i^M}\widetilde{Z_i^N}\widetilde{C_i^*}}, P_{\bar{X}^M \bar{Y}^M Z^N C^*}\Big) + \min_{P_U} d\Big(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big) \\
&\quad \leq d\Big(P_{\widetilde{X_i^N}\widetilde{Y_i^N}\widetilde{Z_i^N}}, P_{XYZ,\mu}^N\Big) + \min_{P_U} d\Big(P_{\bar{X}^M \bar{Y}^M Z^N C^*}, P_{S_A^M S_B^M} P_U\Big) \\
&\quad < 2\varepsilon
\end{aligned}$$

where the last inequality follows from (4.18) and (4.19). Hence, (4.21) can be made arbitrarily small which proves the claim that (3.27) is fulfilled. Proposition 3.12 eventually yields a protocol in $\Gamma_d\left(\mathcal{D} \rightarrow P_{S_A S_B \perp}\right)$. $\square$

Chapter 5

Concluding Remarks

5.1 Conclusions

In the context of secret-key agreement from common information, the secret-key rate is the most interesting property of a distribution. In this thesis we have redefined it in an intuitive way as supremum over the rates of all protocols that transform the distribution into a secret-key distribution. The resulting formalism has proved to be suitable to define and study secret-key agreement information-theoretically secure against an active adversary who chooses distributions from a set. The use of the new formalism is suggested to study other transformations of distributions or further generalisations of known settings.

Summarizing the results of Chapter 4, we have seen that for an arbitrary set of distributions $\mathcal{D}$ the generalized secret key rate $S(\mathcal{D})$ can be expressed and bounded in terms of $S_f(\cdot)$ as follows

$$S_f(\overline{\mathcal{D}'}) = S(\mathcal{D}) = S(\overline{\mathcal{D}}) \leq S_f(\overline{\mathcal{D}}). \tag{5.1}$$

The last inequality cannot be replaced by an equality as shown by the following example:

Consider the set of distributions $\mathcal{D} = \{P^{(1)}_{XYZ}, P^{(2)}_{XYZ}\}$ consisting of the two following distributions:

$P^{(1)}_{XYZ}$

X / Y (Z)	0	1
0	(0) 1/3	
1		(0) 1/3
2	(1) 1/3	
3		

$P^{(2)}_{XYZ}$

X / Y (Z)	0	1
0		(0) 1/3
1	(0) 1/3	
2		
3		(1) 1/3

For this set $\mathcal{D}$ we claim that $S(\mathcal{D}) = S_f(\overline{\mathcal{D}'}) = 0$ and $S_f(\overline{D}) > 0$.

X / Y (Z)	0	1
0	(0) 1/6	(0') 1/6
1	(0') 1/6	(0) 1/6
2	(1) 1/6	
3		(1') 1/6

$\in \overline{\mathcal{D}'}$

If Eve chooses both distributions with probability 1/2, the distribution on the left is obtained. It is easy to see that the intrinsic information of this distribution is zero. Hence, no secret key can be extracted, and $S_f(\overline{\mathcal{D}'}) = 0$ follows.

If Eve cannot distinguish where the distribution comes from, it can be shown that, for all $0 \leq \alpha \leq 1$, the distribution on the left has a positive secret-key rate. Intuitively, if α equals 0 or 1, the realisations where $Y \in \{0, 1\}$ can be transformed into a secret key, otherwise the ones with $Y \in \{2, 3\}$.

X / Y (Z)	0	1
0	(0) $\frac{\alpha}{3}$	(0) $\frac{1-\alpha}{3}$
1	(0) $\frac{1-\alpha}{3}$	(0) $\frac{\alpha}{3}$
2	(1) $\frac{\alpha}{3}$	
3		(1) $\frac{1-\alpha}{3}$

$\in \overline{\mathcal{D}}$

From relation (5.1) the question arises for which sets $\mathcal{D}$ the secret-key rate for a fixed distribution $S_f(\mathcal{D})$ equals the infimum of the secret-key rates of all distributions in the set $\inf_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ})$. Theorem 4.15 shows that this is the case for continuous sets $\mathcal{D}$ where the joint distribution P_{XYZ} can be deduced from the marginal distribution P_{XY}. This is not possible in the following example.

For $N \in \mathbb{N}$ and range $\mathcal{X} = \mathcal{Y} = \{1, \ldots, N\}$, let

$$P_{XY}(x, y) = \begin{cases} \frac{2}{N(N+1)} & \text{for } 1 \leq x \leq y \leq N, \\ 0 & \text{otherwise,} \end{cases}$$

be the marginal distribution of P_{XYZ}. The random variable Z uniquely informs the adversary about X and Y except for two values $1 \leq x_0 < y_0 \leq N$. The adversary gets a dummy symbol $\heartsuit$ in the three following cases $X = Y = x_0$, $X = Y = y_0$, and $X = x_0 \wedge Y = y_0$. For example, for $N = 5$, $x_0 = 2$, $y_0 = 4$ we have the following distribution:

X / Y (Z)	1	2	3	4	5
1	(1,1) 1/15				
2	(1,2) 1/15	($\heartsuit$) 1/15			
3	(1,3) 1/15	(2,3) 1/15	(3,3) 1/15		
4	(1,4) 1/15	($\heartsuit$) 1/15	(3,4) 1/15	($\heartsuit$) 1/15	
5	(1,5) 1/15	(2,5) 1/15	(3,5) 1/15	(4,5) 1/15	(5,5) 1/15

For a fixed N, let $\mathcal{D}$ be the set of all distributions of this form. The cardinality $|\mathcal{D}| = \binom{N}{2}$ is the number of ways the two elements $x_0 < y_0$ can be chosen from $\mathcal{X} = \{1, \ldots, N\}$.

Although Alice and Bob know (or easily estimate from some of their realisations) the marginal distribution P_{XY}, they cannot deduce the joint distribution P_{XYZ} from it as P_{XY} is the same for all elements of $\mathcal{D}$. If they knew the two values x_0 and y_0, they could discard all realisations different from those values and apply protocols for Information Reconciliation and Privacy Amplification to obtain a secret key.[1]

We believe that for this set of distributions holds $S_f(\mathcal{D}) < \inf_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ})$, because the chances of correctly guessing x_0, y_0 are very small for large N, and the known protocols for Information Reconciliation do not work if Alice and Bob do not know x_0, y_0. It seems that in this case, Alice has to send Bob so much information about her realisations that Eve is in a better position compared to the situation where Alice and Bob know x_0, y_0.

We have shown that an adaptive adversary is not more powerful than a non-adaptive one. The examples in Section 4.5.1 show that the tools of "permuting the variables" and

[1] See, for example, [Wol99] for such protocols and the notions of Information Reconciliation and Privacy Amplification.

"partitioning into blocks" are necessary to prove the statement. It is astonishing at first sight that the same tool (Theorem 4.12) can be used to prove different things like both Theorems 4.11 and 4.19. It is a sign of the power of randomisation that both proofs are based on a permutation of the variables.

Processing blocks instead of single variables is the second tool strongly used in this thesis. In the context of secret-key agreement, it is often sufficient to control the adversary's knowledge about every single block because a subsequent step of Privacy Amplification (Proposition 3.12) gives control over the adversary's whole knowledge.

5.2 Suggestions for Further Research

An (incomplete) list of suggestions for further research follows:

- Apply the obtained results to concrete examples, e.g. from quantum cryptography.
- Find more sets of distributions $\mathcal{D}$ with interesting and provable properties. Besides the difficulty to find good examples with certain interesting properties, it is often hard to *formally prove* conjectured properties due to, among other reasons, the lack of tight upper and lower bounds on the secret-key rate.
- We extended the standard model of secret-key agreement to an active adversary who chooses distributions from a set. Investigate the scenario in which Alice (or Bob or both) chooses the distributions from a set $\mathcal{D}$. Can the secret-key rate (which has to be defined) be strictly larger than $\max_{P_{XYZ} \in \mathcal{D}} S(P_{XYZ})$?
- Using the new formalism, study other transformations of distributions or different generalisations of secret-key agreement.

5.3 Acknowledgments

I would like to thank everyone who supported me in writing this diploma thesis. Great thanks is dedicated to my supervisors Prof. Dr. Ueli M. Maurer and his PhD student Renato Renner for offering me the possibility to carry out this thesis in the crypto research group. Special thanks go to Renato whose door has always been open for me. His patience in introducing me to the world of cryptographic information theory and his great guidance and support were a big help for me.

I would finally like to give my warmest thanks to my family, particularly to my parents for loving and supporting me at all times of my life.

Appendix A

Technical Calculations

A.1 Continuity of Conditional Mutual Information

Lemma 3.6 from Section 3.3 states the continuity of conditional mutual information. In this section a more explicit expression for the continuity of the mutual information conditioned on the same variable is given.

Lemma A.1. *Let A and C be random variables with range $\mathcal{A}$; B and D random variables with range $\mathcal{B}$ and Z a random variable with range $\mathcal{Z}$. Then it holds for $d\left(P_{ABZ}, P_{CDZ}\right) \to 0$ that*

$$\big|I(A;B|Z) - I(C;D|Z)\big| = O\big(\sqrt{d\left(P_{ABZ}, P_{CDZ}\right)}\big). \tag{A.1}$$

Proof. The proof is divided into two steps. In a first step we prove the lemma for distributions that slightly differ in two points only. In the second step we decompose the general case in many of these special cases.

Let us assume, for the first step, a small $\delta > 0$, two points $(a_0, b_0, z_0), (a_1, b_1, z_1) \in \mathcal{A}\times\mathcal{B}\times\mathcal{Z}$ and two distributions P_{ABZ}, P_{CDZ} such that

$$P_{ABZ}(a_0, b_0, z_0) = P_{CDZ}(a_0, b_0, z_0) + \delta, \tag{A.2}$$

$$P_{ABZ}(a_1, b_1, z_1) = P_{CDZ}(a_1, b_1, z_1) - \delta,$$

$$P_{ABZ}(a, b, z) = P_{CDZ}(a, b, z) \qquad \text{for all other } (a, b, z). \tag{A.3}$$

Assume for a contradiction that $z_0 \neq z_1$. It would follow that $P_Z(z_0) = \sum_{a,b} P_{ABZ}(a, b, z_0) = \sum_{a,b} P_{CDZ}(a, b, z_0) + \delta = P_Z(z_0) + \delta$ which is not possible. That is why the distribution can only differ in two points with identical Z-components.

According to [CT91, equation (2.61)] the conditional mutual information $I(A;B|Z)$ can be explicitly written as

$$I(A;B|Z) = \sum_{z\in\mathcal{Z}} P_Z(z) \sum_{\substack{a\in\mathcal{A}\\ b\in\mathcal{B}}} P_{AB|Z}(a, b|z) \log \frac{P_{AB|Z}(a, b|z)}{P_{A|Z}(a|z)\cdot P_{B|Z}(b|z)}.$$

From this, we derive the inequality

$$
\begin{aligned}
|I(A;B|Z) - I(C;D|Z)| &\leq \sum_{a,b,z} \left| P_{ABZ} \cdot \log \frac{P_{AB|Z}}{P_{A|Z} \cdot P_{B|Z}} - P_{CDZ} \cdot \log \frac{P_{CD|Z}}{P_{C|Z} \cdot P_{D|Z}} \right| && \text{(A.4)} \\
&= \sum_{\substack{a \neq a_0 \\ b = b_0 \\ z = z_o}} \cdots + \sum_{\substack{a \neq a_1 \\ b = b_1 \\ z = z_o}} \cdots + \sum_{\substack{b \neq b_0 \\ a = a_0 \\ z = z_o}} \cdots + \sum_{\substack{b \neq b_1 \\ a = a_1 \\ z = z_o}} \cdots + \sum_{\substack{a = a_0 \\ b = b_0 \\ z = z_o}} \cdots + \sum_{\substack{a = a_1 \\ b = b_1 \\ z = z_o}} \cdots && \text{(A.5)} \\
&= S_1 + S_2 + S_3 + S_4 + S_5 + S_6
\end{aligned}
$$

where the first two sums in (A.5) run over a, the next two over b, and the last two have only one addend. These are all nonzero addends of the right hand side of (A.4). If $P_Z(z_0) = 0$, all sums vanish, and there is nothing to prove. We suppose $P_Z(z_0) > 0$, define $\delta' := \frac{\delta}{P_Z(z_0)}$, and calculate

$$
P_{A|Z}(a|z_0) = \sum_{b' \in \mathcal{B}} \frac{P_{ABZ}(a, b', z_0)}{P_Z(z_0)} = \begin{cases} P_{C|Z}(a_0|z_0) + \delta' & \text{if } a = a_0, \\ P_{C|Z}(a_1|z_0) - \delta' & \text{if } a = a_1, \\ P_{C|Z}(a|z_0) & \text{otherwise,} \end{cases} \tag{A.6}
$$

$$
P_{B|Z}(b|z_0) = \sum_{a' \in \mathcal{A}} \frac{P_{ABZ}(a', b, z_0)}{P_Z(z_0)} = \begin{cases} P_{D|Z}(b_0|z_0) + \delta' & \text{if } b = b_0, \\ P_{D|Z}(b_1|z_0) - \delta' & \text{if } b = b_1, \\ P_{D|Z}(b|z_0) & \text{otherwise.} \end{cases} \tag{A.7}
$$

To upper bound S_1, we make use of equations (A.2), (A.3), (A.6), and (A.7):

$$
\begin{aligned}
S_1 &= \sum_{\substack{a \neq a_0 \\ b = b_0 \\ z = z_o}} \left| P_{ABZ}(a,b,z) \cdot \log \frac{P_{AB|Z}}{P_{A|Z} \cdot P_{B|Z}} - P_{CDZ}(a,b,z) \cdot \log \frac{P_{CD|Z}}{P_{C|Z} \cdot P_{D|Z}} \right| \\
&= \sum_{a \neq a_0} P_{CDZ}(a, b_0, z_0) \cdot \left| \log \frac{P_{CD|Z} \cdot P_{C|Z} \cdot P_{D|Z}}{P_{C|Z} \cdot (P_{D|Z} + \delta') \cdot P_{CD|Z}} \right| \\
&= \underbrace{\sum_{a \neq a_0} P_{CDZ}(a, b_0, z_0) \cdot}_{\leq 1} \left| -\log \left(1 + \frac{\delta'}{P_{D|Z}(b_0|z_0)} \right) \right| && \text{(A.8)} \\
&\leq O(\delta') = O(\delta) = O(\sqrt{\delta}) \quad \text{for } \delta \to 0
\end{aligned}
$$

where the last inequality follows from the Taylor Series of the logarithm: $\log(1 + x) = \frac{\ln(1+x)}{\ln(2)} = \frac{1}{\ln(2)}\left(x - \frac{x^2}{2} + \ldots\right) = O(x)$ for small x. Note that $P_{D|Z}(b_0|z_0) = 0$ implies that $\forall a \; P_{CDZ}(a, b_0, z_0) = 0$ and S_1 vanishes. If otherwise $P_{D|Z}(b_0|z_0) > 0$, the fraction in (A.8) is well defined. The sums S_2, S_3, and S_4 can be upper bounded in the same way by $O(\sqrt{\delta})$.

For the remaining terms we obtain similarly

$$
\begin{aligned}
S_5 &= \left| P_{ABZ}(a_0,b_0,z_0)\cdot\log\frac{P_{AB|Z}}{P_{A|Z}\cdot P_{B|Z}} - P_{CDZ}(a_0,b_0,z_0)\cdot\log\frac{P_{CD|Z}}{P_{C|Z}\cdot P_{D|Z}}\right| \\
&= \left| P_{CDZ}(a_0,b_0,z_0)\cdot\log\frac{(P_{CD|Z}+\delta')\cdot P_{C|Z}\cdot P_{D|Z}}{(P_{C|Z}+\delta')\cdot(P_{D|Z}+\delta')\cdot P_{CD|Z}} + \delta'\cdot\log\frac{P_{AB|Z}}{P_{A|Z}\cdot P_{B|Z}}\right| \\
&= \left| P_{CDZ}(a_0,b_0,z_0)\cdot\left(\log\left(1+\frac{\delta'}{P_{CD|Z}(a_0,b_0|z_0)}\right) - \log\left(1+\frac{\delta'}{P_{C|Z}(a_0|z_0)}\right)\right.\right. \\
&\qquad \left.\left. - \log\left(1+\frac{\delta'}{P_{D|Z}(b_0|z_0)}\right)\right) + \delta'\cdot\log\frac{P_{CD|Z}+\delta'}{(P_{C|Z}+\delta')\cdot(P_{D|Z}+\delta')}\right| \\
&\le P_{CDZ}(a_0,b_0,z_0)\cdot\big(|O(\delta')|+|O(\delta')|+|O(\delta')|\big) + |O(\sqrt{\delta'})| \\
&\le O(\sqrt{\delta}).
\end{aligned} \tag{A.9}
$$

The first three logarithmic terms in (A.9) are treated as in $S_1,\ldots,S_4$, the fourth term must be handled more carefully. Dividing $\delta'\cdot\log\frac{P_{CD|Z}+\delta'}{(P_{C|Z}+\delta')\cdot(P_{D|Z}+\delta')}$ by $\sqrt{\delta'}$, the remaining polynomial power of the factor $\sqrt{\delta'}$ suffices that the term goes to zero for $\delta'\to 0$ even if the probabilities $P_{CD|Z}$, $P_{C|Z}$, and $P_{D|Z}$ are zero. Hence, it is of order $O(\sqrt{\delta'})$.

The relation $S_6 = O(\sqrt{\delta})$ is derived in a similar way. The arguments above simplify if $P_{CDZ}(a_0,b_0,z_0)$ or $P_{ABZ}(a_1,b_1,z_0)$ equals zero, $a_0=a_1$, or $b_0=b_1$.

As $d(P_{ABZ},P_{CDZ}) = \sum_{a,b,z}|P_{ABZ}(a,b,z)-P_{CDZ}(a,b,z)| = 2\delta$, we have shown equation (A.1) in this special case.

For the general scenario consider two distributions P_{ABZ} and P_{CDZ} with small but positive L_1-distance. We will transform in little steps P_{ABZ} into P_{CDZ} using in each step the special-case result from above. As for a fixed $z_0\in\mathcal{Z}$ it must hold that $\sum_{a,b}P_{ABZ}(a,b,z_0) = P_Z(z_0) = \sum_{a,b}P_{CDZ}(a,b,z_0)$, the transformation can be done for each $z\in\mathcal{Z}$ separately.

For a fixed $z_0\in\mathcal{Z}$ consider the set of points in which the distributions differ:

$$M^{z_0} := \big\{(a,b)\in\mathcal{A}\times\mathcal{B} : P_{ABZ}(a,b,z_0)\neq P_{CDZ}(a,b,z_0)\big\}.$$

As a subset of the finite set $\mathcal{A}\times\mathcal{B}$ the set M^{z_0} is finite, and its elements can be enumerated: $M^{z_0} = \{(a_1,b_1),(a_2,b_2),\ldots,(a_n,b_n)\}$. For ease of notation, we abbreviate: $P_{ABz_0}(a,b) := P_{ABZ}(a,b,z_0)$ and $P_{CDz_0}(a,b) := P_{CDZ}(a,b,z_0)$. To transform P_{ABz_0} into P_{CDz_0} in n steps, we start with

$$P^{(0)}_{ABz_0} := P_{ABz_0}.$$

In a first step we set $P^{(1)}_{ABz_0}(a_1,b_1) := P_{CDz_0}(a_1,b_1)$, i.e., we add $-P^{(0)}_{ABz_0}(a_1,b_1)+P_{CDz_0}(a_1,b_1)$ and have to subtract the same from $P^{(0)}_{ABz_0}(a_2,b_2)$. The distributions $P^{(0)}_{ABz_0}$ and $P^{(1)}_{ABz_0}$ are identical in all other points different from (a_1,b_1) and (a_2,b_2). Formally, we define recursively for every $1\le i\le n-1$:

$$
P^{(i)}_{ABz_0}(a,b) := \begin{cases}
P_{CDz_0}(a_i,b_i) & \text{if } (a,b)=(a_i,b_i), \\
P^{(i-1)}_{ABz_0}(a_{i+1},b_{i+1}) - \big(-P^{(i-1)}_{ABz_0}(a_i,b_i)+P_{CDz_0}(a_i,b_i)\big) & \text{if } (a,b)=(a_{i+1},b_{i+1}), \\
P^{(i-1)}_{ABz_0}(a,b) & \text{otherwise.}
\end{cases}
$$

We claim that $P^{(n-1)}_{ABz_0} = P_{CDz_0}$. It is clear from the definitions above that this is true for all points $(a,b) \notin M^{z_0}$ and for the points $(a_1,b_1),(a_2,b_2),\ldots,(a_{n-1},b_{n-1})$. For the last point (a_n,b_n), we calculate

$$\begin{aligned}
P^{(n-1)}_{ABz_0}(a_n,b_n) &= P^{(n-2)}_{ABz_0}(a_n,b_n) + P^{(n-2)}_{ABz_0}(a_{n-1},b_{n-1}) - P_{CDz_0}(a_{n-1},b_{n-1}) \\
&= P_{ABz_0}(a_n,b_n) + P^{(n-2)}_{ABz_0}(a_{n-1},b_{n-1}) - P_{CDz_0}(a_{n-1},b_{n-1}) \\
&= P_{ABz_0}(a_n,b_n) + P^{(n-3)}_{ABz_0}(a_{n-1},b_{n-1}) + P^{(n-3)}_{ABz_0}(a_{n-2},b_{n-2}) \\
&\qquad - P_{CDz_0}(a_{n-2},b_{n-2}) - P_{CDz_0}(a_{n-1},b_{n-1}) \\
&= P_{ABz_0}(a_n,b_n) + P_{ABz_0}(a_{n-1},b_{n-1}) + P^{(n-3)}_{ABz_0}(a_{n-2},b_{n-2}) \\
&\qquad - P_{CDz_0}(a_{n-2},b_{n-2}) - P_{CDz_0}(a_{n-1},b_{n-1}) \\
&= \ldots \\
&= \sum_{i=1}^{n} P_{ABz_0}(a_i,b_i) - \sum_{i=1}^{n-1} P_{CDz_0}(a_i,b_i) \\
&= \sum_{i=1}^{n} P_{ABz_0}(a_i,b_i) - \sum_{i=1}^{n-1} P_{CDz_0}(a_i,b_i) \\
&\qquad + \sum_{(a,b)\notin M^{z_0}} P_{ABz_0}(a,b) - \sum_{(a,b)\notin M^{z_0}} P_{CDz_0}(a,b) \\
&= P_Z(z_0) - P_Z(z_0) + P_{CDz_0}(a_n,b_n) \\
&= P_{CDz_0}(a_n,b_n)
\end{aligned}$$

which proves the claim.

As stated above, this can be done for all $z_0 \in \mathcal{Z}$. By concatenating the transformation steps for all $z_0 \in \mathcal{Z}$, we obtain a finite transformation sequence $P^{(0)}_{ABZ} = P_{ABZ}$, $P^{(1)}_{ABZ}$, $P^{(2)}_{ABZ},\ldots,P^{(m)}_{ABZ} = P_{CDZ}$ with the following properties:

- Two consecutive distributions differ only in two points with the same Z-components.
- The difference between two consecutive distributions of the transformation is at most $d\left(P_{ABZ},P_{CDZ}\right)$. Formally, for all $1 \le i \le m$:
$$d\left(P^{(i)}_{ABZ},P^{(i-1)}_{ABZ}\right) \le d\left(P_{ABZ},P_{CDZ}\right).$$

Using the first part of the proof, we conclude by showing equation (A.1) as follows

$$\begin{aligned}
&\left|I(A;B|Z) - I(C;D|Z)\right| \\
&\quad = \left|I(A^{(0)};B^{(0)}|Z^{(0)}) - I(A^{(m)};B^{(m)}|Z^{(m)})\right| \\
&\quad = \big|I(A^{(0)};B^{(0)}|Z^{(0)}) - I(A^{(1)};B^{(1)}|Z^{(1)}) + I(A^{(1)};B^{(1)}|Z^{(1)}) \\
&\qquad\quad - I(A^{(2)};B^{(2)}|Z^{(2)}) + I(A^{(2)};B^{(2)}|Z^{(2)}) - \ldots - I(A^{(m)};B^{(m)}|Z^{(m)})\big| \\
&\quad \le \left|I(A^{(0)};B^{(0)}|Z^{(0)}) - I(A^{(1)};B^{(1)}|Z^{(1)})\right| + \left|I(A^{(1)};B^{(1)}|Z^{(1)}) - I(A^{(2)};B^{(2)}|Z^{(2)})\right| \\
&\qquad\quad + \ldots + \left|I(A^{(m-1)};B^{(m-1)}|Z^{(m-1)}) - I(A^{(m)};B^{(m)}|Z^{(m)})\right| \\
&\quad = O\left(\sqrt{d(P^{(0)}_{ABZ},P^{(1)}_{ABZ})}\right) + O\left(\sqrt{d(P^{(1)}_{ABZ},P^{(2)}_{ABZ})}\right) + \ldots + O\left(\sqrt{d(P^{(m-1)}_{ABZ},P^{(m)}_{ABZ})}\right) \\
&\quad \le m \cdot O\big(\sqrt{d\left(P_{ABZ},P_{CDZ}\right)}\big) \\
&\quad = O\big(\sqrt{d\left(P_{ABZ},P_{CDZ}\right)}\big).
\end{aligned}$$

□

A.2 Difference Between Drawing With and Without Replacement

This section is concerned with drawing N elements from a set of NK random variables $\{X_1, X_2, \ldots, X_{NK}\}$. The distance between two distributions obtained by drawing in two different ways from this set is calculated. The result is stated in Lemma A.2 and could be used in the context of Section 4.3 to give another proof of Theorem 4.11.

For large $N, K \in \mathbb{N}$ let $X_1, X_2, \ldots, X_{NK}$ be independent random variables with distributions P_{X_i} from a set of distributions $\mathcal{D}$ and range $\mathcal{X}$. The *average distribution* is denoted by $P_X(x) = \frac{1}{NK}\sum_{i=1}^{NK} P_{X_i}(x)$. For $\mathbf{x} = (x_1, x_2, \ldots, x_N)$, the N-fold product of P_X can be written as

$$\begin{aligned} P_X^N(\mathbf{x}) &= \prod_{j=1}^{N} P_X(x_j) \\ &= \frac{1}{(NK)^N} \prod_{j=1}^{N} \sum_{i=1}^{NK} P_{X_i}(x_j) \\ &= \frac{1}{(NK)^N} \sum_{(i_1,\ldots,i_N)\in[NK]^N} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N) \end{aligned}$$

where $[NK] := \{1, 2, \ldots, NK\}$. Note that this distribution cannot be achieved by drawing independently with replacement from the set of realisations of $X_1, X_2, \ldots, X_{NK}$. As explained in Section 4.3, the variables are not independent if a realisation is drawn twice.[1]

Let π be a randomly chosen permutation of NK elements, and set $\forall i : \widetilde{X_i} := X_{\pi(i)}$. This yields for the first N of the NK variables the distribution

$$P_{\widetilde{X^N}}(\mathbf{x}) = \frac{1}{(NK)^{\underline{N}}} \sum_{(i_1,\ldots,i_N)\in[NK]^{\underline{N}}} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N)$$

where $(NK)^{\underline{N}} = (NK)\cdot(NK-1)\cdots(NK-N+1)$ is the number of ways to draw N elements without replacement from a set of NK elements, and the set $[NK]^{\underline{N}} := \{(i_1, \ldots, i_N) \in [NK]^N : i_k \neq i_l \quad \forall k \neq l\}$ consists of the sequences of length N with pairwise different elements from $[NK]$. This distribution is obtained by drawing at random without replacement N elements from the set of realisations of $X_1, X_2, \ldots, X_{NK}$.

Intuitively, a few (N) elements of a much larger (NK) permuted set are nearly identically P_X^N-distributed. This is proved formally in the rest of this section.

---

[1] To indeed obtain the distribution, each realisation drawn would have to be replaced by *another* independent realisation of the same random variable.

We calculate the difference

$$\begin{aligned}
d\left(P_{\widetilde{X^N}}, P_X^N\right) &= \sum_{\mathbf{x}\in\mathcal{X}^N} \left|P_{\widetilde{X^N}}(\mathbf{x}) - P_X^N(\mathbf{x})\right| \\
&= \sum_{\mathbf{x}\in\mathcal{X}^N} \left(\sum_{(i_1,\dots,i_N)\in[NK]^{\underline{N}}} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N) \left|\frac{1}{(NK)^{\underline{N}}} - \frac{1}{(NK)^N}\right| \right. \\
&\quad \left. + \frac{1}{(NK)^N} \sum_{(i_1,\dots,i_N)\in[NK]^N\setminus[NK]^{\underline{N}}} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N) \right) \\
&= \sum_{(i_1,\dots,i_N)\in[NK]^{\underline{N}}} \underbrace{\sum_{\mathbf{x}\in\mathcal{X}^N} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N)}_{=1} \left|\frac{1}{(NK)^{\underline{N}}} - \frac{1}{(NK)^N}\right| \\
&\quad + \frac{1}{(NK)^N} \sum_{(i_1,\dots,i_N)\in[NK]^N\setminus[NK]^{\underline{N}}} \underbrace{\sum_{\mathbf{x}\in\mathcal{X}^N} P_{X_{i_1}}(x_1)\cdots P_{X_{i_N}}(x_N)}_{=1} \\
&= (NK)^{\underline{N}}\left(\frac{1}{(NK)^{\underline{N}}} - \frac{1}{(NK)^N}\right) + \frac{1}{(NK)^N}\left((NK)^N - (NK)^{\underline{N}}\right) \\
&= 2\left(1 - \frac{(NK)^{\underline{N}}}{(NK)^N}\right).
\end{aligned}$$

Using Stirling's formula $k! \approx \sqrt{2\pi k}\left(\frac{k}{e}\right)^k$, it follows

$$k^{\underline{n}} = \frac{k!}{(k-n)!} \approx \frac{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k}{\sqrt{2\pi(k-n)}\left(\frac{k-n}{e}\right)^{k-n}} = \left(\frac{k}{k-n}\right)^{k+1/2}(k-n)^n e^{-n}.$$

Hence, for $k = NK$, $n = N$

$$\begin{aligned}
\frac{(NK)^{\underline{N}}}{(NK)^N} &\approx \left(\frac{NK}{NK-N}\right)^{NK+1/2} \frac{(NK-N)^N}{(NK)^N} e^{-N} \\
&= \left(\frac{K}{K-1}\right)^{NK+1/2-N} e^{-N} \\
&= \exp\left(\big(N(K-1)+1/2\big)\ln\Big(\frac{K}{K-1}\Big) - N\right) \\
&= \exp\left(-N\left(1 + \Big((K-1) + \frac{1}{2N}\Big)\ln\Big(1 - \frac{1}{K}\Big)\right)\right) \\
&= \exp\left(-N\left(1 + \Big(K - 1 + \frac{1}{2N}\Big)\Big(-\frac{1}{K} - \frac{1}{2K^2} - \frac{1}{3K^3} + O\big(\frac{1}{K^4}\big)\Big)\right)\right) \\
&= \exp\left(-N\left(1 - 1 - \frac{1}{2K} - \frac{1}{3K^2} + \frac{1}{K} + \frac{1}{2K^2} - \frac{1}{2KN} - \frac{1}{4K^2N} + O\Big(\frac{1}{K^3}\Big)\right)\right) \\
&= \exp\left(-N\left(\frac{-N+2N-1}{2KN} + \frac{-4N+6N-3}{12NK^2} + O\Big(\frac{1}{K^3}\Big)\right)\right) \\
&= \exp\left(\frac{3-2N}{12K^2} - \frac{N-1}{2K} + O\Big(\frac{N}{K^3}\Big)\right).
\end{aligned}$$

We have shown the following lemma

Lemma A.2. *For large enough $N, K \in \mathbb{N}$ and $P_{\widetilde{X^N}}$, P_X^N as above holds*

$$d\left(P_{\widetilde{X^N}}, P_X^N\right) \approx 2\left(1 - \exp\left(\frac{3-2N}{12K^2} - \frac{N-1}{2K} + O\left(\frac{N}{K^3}\right)\right)\right).$$

If we have, for example, as many blocks as elements in a block, i.e., $N = K$ the distance tends to $2\left(1 - e^{-1/2}\right) > 0$ for $N, K \to \infty$. On the other hand, the intuition given above is proved true: For fixed N, the distance goes to zero as K approaches infinity.

Bibliography

[Bla90] R. E. Blahut. *Principles and Practice of Information Theory.* Addison-Wesley Series in Electrical and Computer Engineering. Addison-Wesley, Reading, Massachusetts, 1990.

[Cac97] Christian Cachin. *Entropy Measures and Unconditional Security in Cryptography.* PhD thesis, Swiss Federal Institute of Technology (ETH Zurich), 1997. ETH dissertation No. 12187.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley Series in Telecommunications. Wiley, New York, 1991.

[DF80] P. Diaconis and D. Freedman. Finite exchangeable sequences. *JSTOR - The Annals of Probability*, 8(4):745–764, 1980.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[Eck93] J. Eckhoff. *Handbook of Convex Geometry*, chapter 2.1: Helly, Radon, and Carathéodory Type Theorems, pages 389–448. North-Holland, Amsterdam, Netherlands, 1993.

[Mau93] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[MW96] Ueli M. Maurer and Stefan Wolf. Towards characterizing when information-theoretic secret key agreement is possible. In *Advances in Cryptology - ASIACRYPT '96*, volume 1163, pages 196–209. Springer-Verlag, 1996.

[RW03] Renato Renner and Stefan Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. In Eli Biham, editor, *Advances in Cryptology — EUROCRYPT '03*, Lecture Notes in Computer Science. Springer-Verlag, 2003.

[Sha48] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[Wol99] Stefan Wolf. *Information-Theoretically and Computationally Secure Key Agreement in Cryptography.* PhD thesis, Swiss Federal Institute of Technology (ETH Zurich), 1999. ETH dissertation No. 13138.