# Universally Composable Privacy Amplification Against Quantum Adversaries[*]

Renato Renner Robert König

Computer Science Department
ETH Zürich; Switzerland
renner@inf.ethz.ch rkoenig@inf.ethz.ch

March, 2004

**Abstract**

Privacy amplification is the art of shrinking a partially secret string $Z$ to a highly secret key $S$. We introduce a universally composable security definition for secret keys in a context where an adversary holds quantum information and show that privacy amplification by two-universal hashing is secure with respect to this definition. Additionally, we give an asymptotically optimal lower bound on the length of the extractable key $S$ in terms of the adversary's (quantum) knowledge about $Z$.

## 1 Introduction

Consider two parties having access to a common string $Z$ about which an adversary might have some partial information $W$. *Privacy amplification* is the art of transforming this partially secure string $Z$ into a highly secret key $S$ by public discussion. A good technique is to compute $S$ as the output of a publicly chosen two-universal hash function[1] $F$ applied to $Z$. Indeed, it has been shown [4, 3] that this method essentially allows to exploit the whole uncertainty of the adversary about $Z$. For instance, if both the initial string $Z$ and the adversary's knowledge $W$ consist of many independent and identically distributed parts, the number of extractable key bits is asymptotically equal to the conditional Shannon entropy $H(Z|W)$.

The analysis of privacy amplification can be extended to a situation where the adversary might hold quantum instead of only classical information about $Z$. It has been shown [11] that two-universal hashing allows for the extraction of a secure key $S$ whose length roughly equals the difference between the entropy of $Z$ and the number of qubits stored by the adversary. This can be applied for proving the security of quantum key distribution protocols where privacy amplification is used for the classical post-processing of the (only partially secure) raw key [7].

The contribution of this paper is two-fold. First, we introduce a new universally composable security definition for classical secret keys in the context of quantum adversaries. Roughly speaking, a cryptographic scheme is said to be *universally composable* if it remains secure in any

[*] This work was partially supported by the Swiss National Science Foundation, project No. 20-66716.01.

[1] See Section 2.1 for a definition of two-universal functions.

arbitrary context (cf. Section 3). For a secret key $S$, this means that $S$ can be used as if it were an independent and uniformly distributed string. We show that the key obtained by privacy amplification using two-universal hash functions is secure according to this security definition (Section 4). Since privacy amplification is applied in many quantum key distribution protocols to generate the final key out of a raw key, universal composability immediately carries over to the security of quantum key distribution.

Second, we improve the lower bound on the length of the extractable key $S$ given in [11]. If the initial string $Z$ as well as the adversary's (quantum) knowledge consists of $n$ independent pieces, the bound is asymptotically tight, for $n$ approaching infinity. In particular, for the case where the adversary holds purely classical information $W$, this reproduces the classical result of $H(Z|W)$ for the length of the extractable key (cf. Section 4.2).

# 2 Preliminaries

## 2.1 Random functions and two-universal functions

A *random function* from $\mathcal{X}$ to $\mathcal{Y}$ is a random variable taking values from the set of functions with domain $\mathcal{X}$ and range $\mathcal{Y}$. A random function $F$ from $\mathcal{X}$ to $\mathcal{Y}$ is called *two-universal* if

$$\Pr[F(x) = F(x')] \leq \frac{1}{|\mathcal{Y}|}$$

holds for any distinct $x, x' \in \mathcal{X}$.[2] In particular, $F$ is two-universal if, for any distinct $x, x' \in \mathcal{X}$, the random variables $F(x)$ and $F(x')$ are independent and uniformly distributed. For instance, the random function chosen uniformly from the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is two-universal. Non-trivial examples of two-universal functions can, e.g., be found in [6] and [18].

## 2.2 Density operators and random states

Let $\mathcal{H}$ be a Hilbert space. We denote by $\mathcal{S}(\mathcal{H})$ the set of *density operators* on $\mathcal{H}$, i.e., $\mathcal{S}(\mathcal{H})$ is the set of positive operators $\rho$ on $\mathcal{H}$ with $\mathrm{tr}(\rho) = 1$. A density operator $\rho \in \mathcal{S}(\mathcal{H})$ is called *pure* if it has rank 1, i.e., $\rho = |\phi\rangle\langle\phi|$ for some $|\phi\rangle \in \mathcal{H}$.

Let $(\Omega, P)$ be a discrete probability space. A *random state* $\boldsymbol{\rho}$ on $\mathcal{H}$ is a random variable with range $\mathcal{S}(\mathcal{H})$, i.e., a function from $\Omega$ to $\mathcal{S}(\mathcal{H})$. Let $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ be two random states on $\mathcal{H}$ and $\mathcal{H}'$, respectively. The *tensor product* $\boldsymbol{\rho} \otimes \boldsymbol{\rho}'$ of $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ is the random state on $\mathcal{H} \otimes \mathcal{H}'$ defined by

$$(\boldsymbol{\rho} \otimes \boldsymbol{\rho}')(\omega) := \boldsymbol{\rho}(\omega) \otimes \boldsymbol{\rho}'(\omega)$$

for any $\omega \in \Omega$.

To describe settings involving both classical and quantum information, it is often convenient to represent classical information as a state of a quantum system. Let $X$ be a random variable with range $\mathcal{X}$ and let $\mathcal{H}$ be a $|\mathcal{X}|$-dimensional Hilbert space with orthonormal basis $\{|x\rangle\}_{x \in \mathcal{X}}$. The *random state representation* of $X$, denoted $\{X\}$, is the random state on $\mathcal{H}$ defined by $\{X\} := |X\rangle\langle X|$, i.e., for any $\omega \in \Omega$,

$$\{X\}(\omega) = |X(\omega)\rangle\langle X(\omega)| \ .$$

[2] In the literature, two-universality is usually defined for families $\mathcal{F}$ of functions: A family $\mathcal{F}$ is called two-universal if the random function $F$ with uniform distribution over $\mathcal{F}$ is two-universal.

Let $\boldsymbol{\rho}$ be a random state. For an observer which is ignorant of the randomness of $\boldsymbol{\rho}$, the density operator of the quantum state described by $\boldsymbol{\rho}$ is given by

$$[\boldsymbol{\rho}] := E_{\boldsymbol{\rho}}[\boldsymbol{\rho}] = \sum_{\omega \in \Omega} P(\omega) \boldsymbol{\rho}(\omega) \ .$$

More generally, for any event $\mathcal{E}$, the *density operator of* $\boldsymbol{\rho}$ *conditioned on* $\mathcal{E}$, denoted $[\boldsymbol{\rho}|\mathcal{E}]$, is defined by

$$[\boldsymbol{\rho}|\mathcal{E}] := E_{\boldsymbol{\rho}}[\boldsymbol{\rho}|\mathcal{E}] = \frac{1}{\Pr[\mathcal{E}]} \sum_{\omega \in \mathcal{E}} P(\omega) \boldsymbol{\rho}(\omega) \ .$$

Let $\boldsymbol{\rho} \otimes \{X\}$ be a random state consisting of a classical part $\{X\}$ specified by a random variable $X$. It is easy to see that the corresponding density operator $[\boldsymbol{\rho} \otimes \{X\}]$ is given by

$$[\boldsymbol{\rho} \otimes \{X\}] = E_X \left[ \rho_X \otimes |X\rangle\langle X| \right] \tag{1}$$

where $\rho_x := [\boldsymbol{\rho}|X = x]$. In particular, if $X$ is independent of $\boldsymbol{\rho}$, then

$$[\boldsymbol{\rho} \otimes \{X\}] = [\boldsymbol{\rho}] \otimes [\{X\}] \ . \tag{2}$$

### 2.3 Distance measures and non-uniformity

The *variational distance* between two probability distributions $P$ and $Q$ over the same range $\mathcal{X}$ is defined by

$$\delta(P, Q) := \frac{1}{2} \sum_{x \in \mathcal{X}} |P(x) - Q(x)| \ .$$

The variational distance between two probability distributions $P$ and $Q$ can be interpreted as the probability that two random experiments described by $P$ and $Q$, respectively, are different. This is formalized by the following lemma.

**Lemma 2.1.** *Let $P$ and $Q$ be two probability distributions. Then there exists a pair of random variables $X$ and $X'$ with joint probability distribution $P_{XX'}$ such that $P_X = P$, $P_{X'} = Q$, and*

$$\Pr[X \neq X'] = \delta(P, Q) \ .$$

The *trace distance* between two density operators $\rho$ and $\sigma$ on the same Hilbert space $\mathcal{H}$ is defined by

$$\delta(\rho, \sigma) := \frac{1}{2} \mathrm{tr}(|\rho - \sigma|) \ .$$

The trace distance is a metric on the set of density operators $\mathcal{S}(\mathcal{H})$. We say that $\rho$ is $\varepsilon$*-close* to $\sigma$ if $\delta(\rho, \sigma) \leq \varepsilon$, and denote by $\mathcal{B}^\varepsilon(\rho)$ the set of density operators which are $\varepsilon$-close to $\rho$, i.e., $\mathcal{B}^\varepsilon(\rho) = \{\sigma : \delta(\rho, \sigma) \leq \varepsilon\}$.

The trace distance is subadditive with respect to the tensor product, i.e., for any $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ and $\rho', \sigma' \in \mathcal{S}(\mathcal{H}')$,

$$\delta(\rho \otimes \rho', \sigma \otimes \sigma') \leq \delta(\rho, \sigma) + \delta(\rho', \sigma') \ , \tag{3}$$

with equality if $\rho' = \sigma'$, i.e.,

$$\delta(\rho \otimes \rho', \sigma \otimes \rho') = \delta(\rho, \sigma) \ . \tag{4}$$

The trace distance between two density operators $\rho$ and $\sigma$ can not increase when the same quantum operation $\mathcal{E}$ is applied to both $\rho$ and $\sigma$, i.e.,

$$\delta(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \delta(\rho, \sigma) \ . \tag{5}$$

Similarly, the trace distance between two density operators $\rho$ and $\sigma$ is an upper bound for the variational distance between the probability distributions $P$ and $Q$ of the outcomes when applying the same measurement to $\rho$ and $\sigma$, respectively, i.e.,

$$\delta(P, Q) \leq \delta(\rho, \sigma) \ . \tag{6}$$

The variational distance can be seen as a (classical) special case of the trace distance. Let $X$ and $Y$ be random variables. Then the variational distance between the probability distributions of $X$ and $Y$ equals the trace distance between the corresponding density matrices $[\{X\}]$ and $[\{Y\}]$, i.e.,

$$\delta(P_X, P_Y) = \delta([\{X\}], [\{Y\}]) \ .$$

The trace distance between two density operators containing a representation of the same classical random variable $X$ can be written as the expectation over the values of $X$.

**Lemma 2.2.** *Let $X$ be a random variable and let $\boldsymbol{\rho}$ and $\boldsymbol{\sigma}$ be random states. Then*

$$\delta([\boldsymbol{\rho} \otimes \{X\}], [\boldsymbol{\sigma} \otimes \{X\}]) = E_X[\delta(\rho_X, \sigma_X)]$$

*where $\rho_x := [\boldsymbol{\rho}|X = x]$ and $\sigma_x := [\boldsymbol{\sigma}|X = x]$).*

*Proof.* Using (1) and the orthogonality of the vectors $|x\rangle$, we have

$$\delta([\boldsymbol{\rho} \otimes \{X\}], [\boldsymbol{\sigma} \otimes \{X\}]) = \frac{1}{2}\mathrm{tr}\Big|E_X\left[(\rho_X - \sigma_X) \otimes |X\rangle\langle X|\right]\Big| = \frac{1}{2}\mathrm{tr}\Big(E_X\Big[\big|(\rho_X - \sigma_X) \otimes |X\rangle\langle X|\big|\Big]\Big) \ .$$

The assertion then follows from the linearity of the trace and the fact that $\mathrm{tr}\big|(\rho_x - \sigma_x) \otimes |x\rangle\langle x|\big| = \mathrm{tr}|\rho_x - \sigma_x|$. □

In Section 3, we will see that a natural measure for characterizing the secrecy of a key is its trace distance to a uniform distribution.

**Definition 2.3.** Let $X$ be a random variable with range $\mathcal{X}$ and let $\boldsymbol{\rho}$ be a random state. The *non-uniformity* of $X$ *given* $\boldsymbol{\rho}$ is defined by

$$d(X|\boldsymbol{\rho}) := \delta([\{X\} \otimes \boldsymbol{\rho}], [\{U\}] \otimes [\boldsymbol{\rho}])$$

where $U$ is a random variable uniformly distributed on $\mathcal{X}$.

Note that $d(X|\boldsymbol{\rho}) = 0$ if and only if $X$ is uniformly distributed and independent of $\boldsymbol{\rho}$.

### 2.4 (Smooth) Rényi entropy

Let $\rho \in \mathcal{S}(\mathcal{H})$ be a density operator and let $\alpha \in [0, \infty]$. The *Rényi entropy of order $\alpha$ of $\rho$* is defined by

$$S_\alpha(\rho) := \frac{1}{1-\alpha} \log_2\bigl(\mathrm{tr}(\rho^\alpha)\bigr)$$

with the convention $S_\alpha(\rho) := \lim_{\beta \to \alpha} S_\beta(\rho)$ for $\alpha \in \{0, 1, \infty\}$. In particular, for $\alpha = 0$, $S_0(\rho) = \log_2\bigl(\mathrm{rank}(\rho)\bigr)$ and, for $\alpha = \infty$, $S_\infty(\rho) = -\log_2\bigl(\lambda_{\max}(\rho)\bigr)$ where $\lambda_{\max}(\rho)$ denotes the maximum eigenvalue of $\rho$. For $\alpha = 1$, $S_\alpha(\rho)$ is equal to the von Neumann entropy $S(\rho)$. Moreover, for $\alpha, \beta \in [0, \infty]$,

$$\alpha \leq \beta \implies S_\alpha(\rho) \geq S_\beta(\rho) \ . \tag{7}$$

Note that, for a classical random variable $X$, the Rényi entropy $S_\alpha([\{X\}])$ of the quantum representation of $X$ corresponds to the Rényi entropy $H_\alpha(X)$ of $X$ as defined in classical information theory [17].

The definition of Rényi entropy for density operators can be generalized to the notion of smooth Rényi entropy as introduced in [16] for the classical case.

**Definition 2.4.** Let $\rho \in \mathcal{S}(\mathcal{H})$, let $\alpha \in [0, \infty]$, and let $\varepsilon \geq 0$. The *$\varepsilon$-smooth Rényi entropy of order $\alpha$ of $\rho$* is defined by

$$S_\alpha^\varepsilon(\rho) := \frac{1}{1-\alpha} \log_2 \left( \inf_{\sigma \in \mathcal{B}^\varepsilon(\rho)} \mathrm{tr}(\sigma^\alpha) \right)$$

with the convention $S_\alpha^\varepsilon(\rho) := \lim_{\beta \to \alpha} S_\beta^\varepsilon(\rho)$ for $\alpha \in \{0, 1, \infty\}$.

In particular, for $\alpha = 0$,

$$S_0^\varepsilon(\rho) = \inf_{\sigma \in \mathcal{B}^\varepsilon(\rho)} S_0(\sigma) \tag{8}$$

and, for $\alpha = \infty$,

$$S_\infty^\varepsilon(\rho) = \sup_{\sigma \in \mathcal{B}^\varepsilon(\rho)} S_\infty(\sigma) \ . \tag{9}$$

The following lemma is a direct generalization of the corresponding classical statement in [16], saying that, for any $\alpha$, the smooth Rényi entropy $H_\alpha^\varepsilon(W)$ of a random variable $W$ consisting of many independent and identically distributed pieces asymptotically equals its Shannon entropy $H(W)$.

**Lemma 2.5.** *Let $\rho$ be a density operator. Then, for any $\alpha \in [0, \infty]$,*

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{S_\alpha^\varepsilon(\rho^{\otimes n})}{n} = S(\rho) \ .$$

## 3 Secret keys and composability

Cryptographic security definitions are often required to be *universally composable*. This means that a cryptographic primitive (e.g., a secret key) which is secure according to such a definition remains secure even if it is used as a component in any (arbitrarily complex) cryptographic scheme. For instance, the universal composability of a secret key $S$ guarantees that any bit of $S$ remains secret even if some other part of $S$ is given to an adversary.[3]

In the past few years, composable security has attracted a lot of interest and lead to important new definitions and proofs (see, e.g., [5] or [15]). Recently, the notion of universal composability has been generalized to the quantum case [13]. Universally composable security definitions are usually based on the idea of characterizing the security of a cryptographic scheme by its distance to an ideal system which (by definition) is perfectly secure.

Our security definition for classical secret keys with respect to quantum mechanical adversaries follows the same lines. Informally, a key $S$ is secure if it is close to a uniformly distributed bitstring which is independent of any (quantum) information that an adversary might possess. This is formalized by the notion of non-uniformity.

**Definition 3.1.** Let $S$ be a random variable and let $\boldsymbol{\rho}$ be a random state. $S$ is said to be an *$\varepsilon$-secure secret key with respect to $\boldsymbol{\rho}$* if $d(S|\boldsymbol{\rho}) \leq \varepsilon$.

In particular, if the adversary's information is represented by a random state $\boldsymbol{\rho}$, the $\varepsilon$-security of a key $S$ with respect to $\boldsymbol{\rho}$ implies that the real situation $[\boldsymbol{\rho} \otimes \{S\}]$ where $S$ is used as a key is $\varepsilon$-close (with respect to the trace distance) to an ideal situation $[\boldsymbol{\rho} \otimes \{U\}]$ where $S$ is replaced by a perfect key $U$ which is uniformly distributed and independent of $\boldsymbol{\rho}$.

The universal composability of Definition 3.1 follows directly from the fact that the trace distance does not increase when appending an additional quantum system (cf. (4)) or when applying any arbitrary quantum operation (cf. (5)): Even if the secret key $S$ is used in any arbitrary context, the density operator describing the whole setting including the key $S$ and the adversary's state $\boldsymbol{\rho}$ does not differ by more than $\varepsilon$ from the density operator of an ideal setting where $S$ is replaced by $U$. In particular, if follows from (6) and Lemma 2.1 that the real and the ideal setting can be considered to be identical with probability at least $1 - \varepsilon$.

# 4 Main result

## 4.1 Theorem and proof

**Theorem 4.1.** *Let $Z$ be a random variable with range $\mathcal{Z}$, let $\boldsymbol{\rho}$ be a random state, and let $F$ be a two-universal function on $\mathcal{Z}$ with range $\mathcal{S} = \{0,1\}^s$ which is independent of $Z$ and $\boldsymbol{\rho}$. Then*

$$d(F(Z)|\{F\} \otimes \boldsymbol{\rho}) \leq \frac{1}{2} 2^{-\frac{1}{2}(S_2([\{Z\}\otimes\boldsymbol{\rho}]) - S_0([\boldsymbol{\rho}]) - s)} .$$

The following corollary is a consequence of property (7), expressions (8) and (9), and the triangle inequality for the trace distance.

**Corollary 4.2.** *Let $Z$ be a random variable with range $\mathcal{Z}$, let $\boldsymbol{\rho}$ be a random state, let $F$ be a two-universal function on $\mathcal{Z}$ with range $\mathcal{S} = \{0,1\}^s$ which is independent of $Z$ and $\boldsymbol{\rho}$, and let $\varepsilon \geq 0$. Then*

$$d(F(Z)|\{F\} \otimes \boldsymbol{\rho}) \leq \frac{1}{2} 2^{-\frac{1}{2}(S^\varepsilon_\infty([\{Z\}\otimes\boldsymbol{\rho}]) - S^\varepsilon_0([\boldsymbol{\rho}]) - s)} + 2\varepsilon .$$

[3] Note that this is not necessarily the case for many widely used security definitions where, e.g., only the mutual information between the key $S$ and the outcome of an arbitrary measurement of the adversary's quantum state is required to be small (for a formal definition, see, e.g., [14] or [9]).

Let us first state some technical lemmas to be used for the proof of Theorem 4.1.

**Lemma 4.3.** *Let $Z$ be a random variable with range $\mathcal{Z}$, let $\boldsymbol{\rho}$ be a random state, and let $F$ be a random function with domain $\mathcal{Z}$ which is independent of $Z$ and $\boldsymbol{\rho}$. Then*

$$d(F(Z)|\{F\} \otimes \boldsymbol{\rho}) = E_F[d(F(Z)|\boldsymbol{\rho})].$$

*Proof.* Let $U$ be a random variable uniformly distributed on $\mathcal{Z}$ and independent of $F$ and $\boldsymbol{\rho}$. Then

$$d(F(Z)|\boldsymbol{\rho} \otimes \{F\}) = \delta\left([(\{F(Z)\} \otimes \boldsymbol{\rho}) \otimes \{F\}], [([\{U\}] \otimes \boldsymbol{\rho}) \otimes \{F\}]\right),$$

Now, applying Lemma 2.2 to the random states $\{F(Z)\} \otimes \boldsymbol{\rho}$ and $\{U\} \otimes \boldsymbol{\rho}$ gives the desired result, since

$$\begin{aligned}[\{F(Z)\} \otimes \boldsymbol{\rho}|F = f] &= [\{f(Z)\} \otimes \boldsymbol{\rho}] \\ [\{U\} \otimes \boldsymbol{\rho}|F = f] &= [\{U\}] \otimes [\boldsymbol{\rho}]\end{aligned}$$

which holds because $F$ is independent of $Z$, $\boldsymbol{\rho}$, and $U$. □

The following lemmas can most easily be formalized in terms of the square of the Hilbert-Schmidt distance. For two density operators $\rho$ and $\sigma$, let

$$\Delta(\rho, \sigma) := \mathrm{tr}\big((\rho - \sigma)^2\big) .$$

Moreover, for a random variable $X$ with range $\mathcal{X}$ and a random state $\boldsymbol{\rho}$, we define

$$D(X|\boldsymbol{\rho}) := \Delta([\{X\} \otimes \boldsymbol{\rho}], [\{U\}] \otimes [\boldsymbol{\rho}])$$

where $U$ is a random variable uniformly distributed on $\mathcal{X}$.

**Lemma 4.4.** *Let $\rho$ and $\sigma$ be two density operators on $\mathcal{H}$. Then*

$$\delta(\rho, \sigma) \leq \frac{1}{2}\sqrt{\mathrm{rank}(\rho - \sigma) \cdot \Delta(\rho, \sigma)} .$$

*Proof.* The assertion follows directly from Lemma A.2 and the definition of the distance measures $\delta(\cdot, \cdot)$ and $\Delta(\cdot, \cdot)$. □

**Lemma 4.5.** *Let $X$ be a random variable with range $\mathcal{X}$ and let $\boldsymbol{\rho}$ be a random state. Then*

$$d(X|\boldsymbol{\rho}) \leq \frac{1}{2} 2^{\frac{S_0([\boldsymbol{\rho}])}{2}} \sqrt{|\mathcal{X}| \cdot D(X|\boldsymbol{\rho})}.$$

*Proof.* This is an immediate consequence of the definitions and Lemma 4.4. □

**Lemma 4.6.** *Let $X$ be a random variable with range $\mathcal{X}$ and let $\boldsymbol{\rho}$ be a random state. Then*

$$D(X|\boldsymbol{\rho}) = \mathrm{tr}\left( (\sum_{x \in \mathcal{X}} P_X(x)^2 \rho_x^2) - \frac{1}{|\mathcal{X}|}[\boldsymbol{\rho}]^2 \right)$$

*where $\rho_x := [\boldsymbol{\rho}|X = x]$ for $x \in \mathcal{X}$.*

*Proof.* From (1), we have

$$\begin{aligned} D(X|\boldsymbol{\rho}) &= \operatorname{tr}\left(\left(\sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x|\otimes\rho_x - \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}|x\rangle\langle x|\otimes[\boldsymbol{\rho}]\right)^2\right) \\ &= \operatorname{tr}\left(\sum_{x\in\mathcal{X}}\left(P_X(x)\rho_x - \frac{1}{|\mathcal{X}|}[\boldsymbol{\rho}]\right)^2\right) \\ &= \operatorname{tr}\left(\sum_{x\in\mathcal{X}} P_X(x)^2\rho_x^2 - \frac{2}{|\mathcal{X}|}[\boldsymbol{\rho}]\sum_{x\in\mathcal{X}} P_X(x)\rho_x + \frac{1}{|\mathcal{X}|}[\boldsymbol{\rho}]^2.\right) . \end{aligned}$$

Inserting the identity

$$[\boldsymbol{\rho}] = \sum_{x\in\mathcal{X}} P_X(x)\rho_x$$

concludes the proof. □

**Lemma 4.7.** *Let $Z$ be a random variable with range $\mathcal{Z}$, let $\boldsymbol{\rho}$ be a random state, and let $F$ be a two-universal function on $\mathcal{Z}$ chosen independently of $Z$ and $\boldsymbol{\rho}$. Then*

$$E_F\left[D(F(Z)|\boldsymbol{\rho})\right] \leq 2^{-S_2([\{Z\}\otimes\boldsymbol{\rho}])} .$$

*Proof.* Let us define $\rho_z := [\boldsymbol{\rho}|Z = z]$ for every $z\in\mathcal{Z}$ and let $\mathcal{S}$ be the range of $F$. With Lemma 4.6, we obtain

$$E_F\left[D(F(Z)|\boldsymbol{\rho})\right] = \operatorname{tr}\left(E_F\left[\sum_{s\in\mathcal{S}}\Pr[F(Z)=s]^2[\boldsymbol{\rho}|F(Z)=s]^2\right]\right) - \frac{1}{|\mathcal{S}|}\operatorname{tr}([\boldsymbol{\rho}]^2) , \qquad (10)$$

using the linearity of the expectation value and the trace. Note that

$$\Pr[f(Z)=s]\cdot[\boldsymbol{\rho}|f(Z)=s] \;=\; \sum_{z\in f^{-1}(\{s\})} P_Z(z)\rho_z .$$

Using this identity and rearranging the summation order, we get

$$\sum_{s\in\mathcal{S}}\Pr[f(Z)=s]^2[\boldsymbol{\rho}|f(Z)=s]^2 = \sum_{z,z'\in\mathcal{Z}} P_Z(z)P_Z(z')\rho_z\rho_{z'}\delta_{f(z),f(z')} ,$$

where $\delta_{x,y}$ is the Kronecker delta which equals 1 if $x=y$ and 0 otherwise. Taking the expectation value over the random choice of $F$ then gives

$$E_F\left[\sum_{s\in\mathcal{S}}\Pr[F(Z)=s]^2[\boldsymbol{\rho}|F(Z)=s]^2\right] = \sum_{z,z'\in\mathcal{Z}} P_Z(z)P_Z(z')\rho_z\rho_{z'}\Pr[F(z)=F(z')] .$$

Similarly, we obtain

$$[\boldsymbol{\rho}]^2 = \sum_{z,z'\in\mathcal{Z}} P_Z(z)P_Z(z')\rho_z\rho_{z'} .$$

Inserting this into (10), we get

$$E_F\left[D(F(Z)|\boldsymbol{\rho})\right] = \sum_{z,z' \in \mathcal{Z}} P_Z(z) P_Z(z') \left( \Pr[F(z) = F(z')] - \frac{1}{|\mathcal{S}|} \right) \mathrm{tr}(\rho_z \rho_{z'}) \ .$$

As we assumed that $F$ is two-universal, all summands with $z \neq z'$ are not larger than zero and we are left with

$$E_F\left[D(F(Z)|\boldsymbol{\rho})\right] \leq \sum_{z \in \mathcal{Z}} P_Z(z)^2 \mathrm{tr}(\rho_z^2) = \mathrm{tr}\big([\{Z\} \otimes \boldsymbol{\rho}]^2\big)$$

which concludes the proof. □

*Proof of Theorem 4.1.* Using Lemma 4.3, Lemma 4.5, and the convexity of the square root together with Jensen's inequality, we get

$$\begin{aligned} d(F(Z)|\{F\} \otimes \boldsymbol{\rho}) &= E_F[d(F(Z)|\boldsymbol{\rho})] \\ &\leq \frac{1}{2} 2^{\frac{s+S_0([\boldsymbol{\rho}])}{2}} E_F[\sqrt{D(F(Z)|\boldsymbol{\rho})}] \\ &\leq \frac{1}{2} 2^{\frac{s+S_0([\boldsymbol{\rho}])}{2}} \sqrt{E_F[D(F(Z)|\boldsymbol{\rho})]} \ . \end{aligned}$$

The statement of the theorem now follows from Lemma 4.7. □

## 4.2 Privacy amplification and secret key distribution

Consider two distant parties which are connected by an authentic, but otherwise fully insecure classical communication channel. Additionally, they have access to a common random string $Z$ about which an adversary has some partial information represented by the state $\boldsymbol{\rho}$ of a quantum system. The two legitimate parties can apply the following *privacy amplification protocol* to obtain a secure key $S$: One of the parties chooses an instance of a two-universal function $F$ and announces his choice to the other party using the public communication channel. Then, both parties compute $S = F(Z)$. Since the information of the adversary after the execution of the protocol is given by $\boldsymbol{\rho} \otimes \{F\}$, one wants the final key $S$ to be $\varepsilon$-secure with respect to $\boldsymbol{\rho} \otimes \{F\}$, for some small $\varepsilon \geq 0$. It is an immediate consequence of Corollary 4.2 that this is achieved if the length $s$ of the key $S$ satisfies

$$s \leq S_\infty^{\bar{\varepsilon}}([\{Z\} \otimes \boldsymbol{\rho}]) - S_0^{\bar{\varepsilon}}([\boldsymbol{\rho}]) - 2\log_2(\frac{1}{2\bar{\varepsilon}'}) \ , \tag{11}$$

for $\bar{\varepsilon}, \bar{\varepsilon}' \geq 0$ with $2\bar{\varepsilon} + \bar{\varepsilon}' \leq \varepsilon$.

Assume now that both the string $Z$ as well as the adversary's state $\boldsymbol{\rho}$ consist of many independent pieces, i.e., for $n \in \mathbb{N}$, $Z = (Z_1, \ldots, Z_n)$ and $\boldsymbol{\rho} = \boldsymbol{\rho}_1 \otimes \cdots \otimes \boldsymbol{\rho}_n$ where $(Z_i, \boldsymbol{\rho}_i)$ are independent pairs with some fixed joint probability distribution $P_{Z_i \boldsymbol{\rho}_i} := P_{\bar{Z}\bar{\boldsymbol{\rho}}}$, and let $s(n)$ be the length of the key that can be extracted from $Z$. Then (11) together with Lemma 2.5 implies that the rate $R := \lim_{n \to \infty} \frac{s(n)}{n}$ at which secret key bits can be generated is given by

$$R = S([\{\bar{Z}\} \otimes \bar{\boldsymbol{\rho}}]) - S([\bar{\boldsymbol{\rho}}]) \ .$$

In particular, if the information $\boldsymbol{\rho}$ is purely classical, i.e., $\bar{\boldsymbol{\rho}} = \{\bar{W}\}$ for some random variable $\bar{W}$, we obtain a rate of

$$R = H(\bar{Z}\bar{W}) - H(\bar{W}) = H(\bar{Z}|\bar{W})$$

which has been shown to be optimal (see, e.g., [8] or [12]).

Theorem 4.1 has an interesting implication for quantum key distribution. In [7], a general security proof for quantum key distribution based on the result in [11] has been given which implies the security of known protocols such as BB84 [2] or B92 [1]. As Theorem 4.1 extends the result of [11] to the case of universally composable security, it follows immediately that this strong type of security also holds for the generic quantum key distribution protocol presented in [7]. In particular, the secret keys generated by the BB84 and the B92 protocol are universally composable.

## A Some identities

**Lemma A.1 (Schur's inequality).** *Let $A$ be a linear operator on a $d$-dimensional Hilbert space $\mathcal{H}$ and let $\lambda_1, \ldots, \lambda_d$ be its eigenvalues. Then*

$$\sum_{i=1}^{d} |\lambda_i|^2 \leq \mathrm{tr}(AA^\dagger) \ ,$$

*with equality if and only if $A$ is normal (i.e., $AA^\dagger = A^\dagger A$).*

*Proof.* See, e.g., [10]. □

**Lemma A.2.** *Let $A$ be a normal operator with rank $r$. Then*

$$\mathrm{tr}|A| \leq \sqrt{r}\sqrt{\mathrm{tr}(AA^\dagger)} \ .$$

*Proof.* Let $\lambda_1, \ldots, \lambda_r$ be the $r$ nonzero eigenvalues of $A$. Since the square root is concave, we can apply Jensen's inequality leading to

$$\mathrm{tr}|A| = \sum_{i=1}^{r} |\lambda_i| = \sum_{i=1}^{r} \sqrt{|\lambda_i|^2} \leq \sqrt{r}\sqrt{\sum_{i=1}^{r} |\lambda_i|^2} \ .$$

The assertion then follows from Schur's inequality. □

## References

[1] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, 1992.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, 1995.

[4] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[5] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proc. 42nd IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 136–145, 2001.

[6] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.

[7] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution. ePrint archive: `http://arxiv.org/abs/quant-ph/0402131`, February 2004.

[8] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24:339–348, 1978.

[9] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003.

[10] R. A. Horn and C. R. Johnson. *Matrix analysis.* Cambridge University Press, 1985.

[11] R. König, U. Maurer, and R. Renner. On the power of quantum memory. ePrint archive: `http://arxiv.org/abs/quant-ph/0305154`, 2003.

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

[13] D. Mayers. Universal composability for quantum protocols. Personal communication, 2004.

[14] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2000.

[15] B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In *7th ACM Conference on Computer and Communications Security*, pages 245–254. ACM Press, 2000.

[16] R. Renner and S. Wolf. Smooth Rényi entropy and applications. Accepted for ISIT 2004. Available at `http://www.crypto.ethz.ch/~renner/publications.html`, October 2003.

[17] A. Rényi. On measures of entropy and information. In *Proceedings of the 4th Berkeley Symp. on Math. Statistics and Prob.*, volume 1, pages 547–561. Univ. of Calif. Press, 1961.

[18] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.