Unifying Classical and Quantum Key Distillation

Matthias Christandl[1], Artur Ekert[1,2], Michał Horodecki[3], Paweł Horodecki[4], Jonathan Oppenheim[1], and Renato Renner[1]

[1] Centre for Quantum Computation, University of Cambridge, United Kingdom
{m.christandl,jono,r.renner}@damtp.cam.ac.uk
[2] Department of Physics, National University of Singapore, Singapore
artur.ekert@qubit.org
[3] Institute of Theoretical Physics and Astrophysics, University of Gdańsk, Poland
fizmh@univ.gda.pl
[4] Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Poland pawel@mif.pg.gda.pl

Abstract. Assume that two distant parties, Alice and Bob, as well as an adversary, Eve, have access to (quantum) systems prepared jointly according to a tripartite state ρ_{ABE}. In addition, Alice and Bob can use local operations and authenticated public classical communication. Their goal is to establish a key which is unknown to Eve. We initiate the study of this scenario as a unification of two standard scenarios: (i) key distillation (agreement) from classical correlations and (ii) key distillation from pure tripartite quantum states.

Firstly, we obtain generalisations of fundamental results related to scenarios (i) and (ii), including upper bounds on the key rate, i.e., the number of key bits that can be extracted per copy of ρ_{ABE}. Moreover, based on an embedding of classical distributions into quantum states, we are able to find new connections between protocols and quantities in the standard scenarios (i) and (ii).

Secondly, we study specific properties of key distillation protocols. In particular, we show that every protocol that makes use of pre-shared key can be transformed into an equally efficient protocol which needs no pre-shared key. This result is of practical significance as it applies to quantum key distribution (QKD) protocols, but it also implies that the key rate cannot be locked with information on Eve's side. Finally, we exhibit an arbitrarily large separation between the key rate in the standard setting where Eve is equipped with quantum memory and the key rate in a setting where Eve is only given classical memory. This shows that assumptions on the nature of Eve's memory are important in order to determine the correct security threshold in QKD.

1 Introduction

Many cryptographic tasks such as message encryption or authentication rely on *secret keys*,[5] i.e., random strings only known to a restricted set of parties.

[5] In the sequel, we will use the term *key* instead of *secret key*.

In *information-theoretic cryptography*, where no assumptions on the adversary's resources[6] are made, distributing keys between distant parties is impossible if only public classical communication channels are available [1, 2]. However, this situation changes dramatically if the parties have access to additional devices such as noisy channels (where also a wiretapper is subject to noise), a noisy source of randomness, a quantum channel, or a pre-shared quantum state. As shown in [2–6], these devices allow the secure distribution of keys.[7]

This work is concerned with information-theoretic key distillation from pre-distributed noisy data. More precisely, we consider a situation where two distant parties, *Alice* and *Bob*, have access to (not necessarily perfectly) correlated pieces of (classical or quantum) information, which might be partially known to an adversary, *Eve*. The goal of Alice and Bob is to *distill* virtually perfect key bits from these data, using only an authentic (but otherwise insecure) classical communication channel.

Generally speaking, key distillation is possible whenever Alice and Bob's data are sufficiently correlated and, at the same time, Eve's uncertainty on these data is sufficiently large. It is one of the goals of this paper to exhibit the properties pre-shared data must have in order to allow key distillation.

In practical applications, the pre-distributed data might be obtained from realistic physical devices such as noisy (classical or quantum) channels or other sources of randomness. Eve's uncertainty on Alice and Bob's data might then be imposed by inevitable noise in the devices due to thermodynamic or quantum effects.

Quantum key distribution (QKD) can be seen as a special case of key distillation where the pre-shared data is generated using a quantum channel. The laws of quantum physics imply that the random values held by one party, say Alice, cannot at the same time be correlated with Bob and Eve. Hence, whenever Alice and Bob's values are strongly correlated (which can be checked easily) then Eve's uncertainty about them must inevitably (by the laws of quantum mechanics) be large, hence, Alice and Bob can distil key. Because of this close relation between key distillation and QKD, many of the results we give here will have direct implications to QKD.

Furthermore, the theory of key distillation has nice parallels with the theory of *entanglement distillation*, where the goal is to distil maximally entangled states (also called *singlets*) from (a sequence of) bipartite quantum states. In fact, the two scenarios have many properties in common. For example, there is a gap between the *key rate* (i.e., the amount of key that can be distilled from some given noisy data) and the *key cost* (the amount of key that is needed to simulate the noisy data, using only public classical communication) [7]. This gap can be seen as the classical analogue of a gap between *distillable entanglement* (the

[6] In this context, the term *resources* typically refers to computational power and memory space.

[7] In certain scenarios, including the one studied in this paper, an authentic classical channel is needed in addition.

amount of singlets that can be distilled from a given bipartite quantum state) and *entanglement cost* (the amount of singlets needed to generate the state).

1.1 Related work

The first and basic instance of an information-theoretic key agreement scenario is Wyner's wiretap channel [8]. Here, Alice can send information via a noisy classical channel to Bob. Eve, the eavesdropper, has access to a degraded version of Bob's information. Wyner has calculated the rate at which key generation is possible if only Alice is allowed to send public classical messages to Bob. Wyner's work has later been generalised by Csiszár and Körner, relaxing the restrictions on the type of information given to Eve [3]. Based on these ideas, Maurer and Ahlswede and Csiszár have proposed an extended scenario where key is distilled from arbitrary correlated classical information (specified by a tripartite probability distribution) [2, 4]. In particular, Maurer has shown that two-way communication can lead to a strictly positive key rate even though the key rate in the one-way communication scenario might be zero [2].

In parallel to this development quantum cryptography emerged: in 1984 Bennett and Brassard devised a QKD scheme in which quantum channels could be employed in order to generate a secure key without the need to put a restriction on the eavesdropper [5]. In 1991, Ekert discovered that quantum cryptographic schemes could be based on entanglement, that is, on quantum correlations that are strictly stronger than classical correlations [6]. Clearly, this is key distillation from quantum information.

The first to spot a relation between the classical and the quantum development were Gisin and Wolf; in analogy to *bound entanglement* in quantum information theory, they conjectured the existence of *bound information*, namely classical correlation that can only be created from key but from which no key can be distilled [9]. Their conjecture remains unsolved, but has stimulated the community in search for an answer.

To derive lower bounds on the key rate, we will make repeated use of results by Devetak and Winter, who derived a bound on the key rate if the tripartite quantum information consists of many identical and mutually independent pieces, and by Renner and König, who derived privacy amplification results which also hold if this independence condition is not satisfied [10, 11].

1.2 Contributions

We initiate the study of a unified key distillation scenario, which includes key distillation from pre-shared *classical* and *quantum* data (Section 2). We then derive a variety of quantitative statements related to this scenario. These unify and extend results from both the quantum and classical world.

There are numerous upper bounds available in the specific scenarios and it is our aim to provide the bigger picture that will put order into this zoo by employing the concept of a *secrecy monotone*, i.e., a function that decreases under local operations and public communication (Section 3), as introduced in [12]. The upper bounds can then roughly be subdivided into two categories: (i) the ones based on classical key distillation [13] and (ii) the ones based on quantum communication or entanglement measures [14].

The unified scenario that we develop does not stop at an evaluation of the key rate but lets us investigate intricate connections between the two extremes. We challenge the viewpoint of Gisin and Wolf who highlight the relation between key distillation from classical correlation and entanglement distillation from this very correlation *embedded* into quantum states [9]: we prove a theorem that relates key distillation from certain classical correlation and key (and not entanglement) distillation from their embedded versions (Section 4). This ties in with recent work which established that key distillation can be possible even from quantum states from which no entanglement can be distilled [15].

A fruitful concept that permeates this work is the concept of *locking of classical information in quantum states*: let Alice choose an n-bit string $x = x_1 \ldots x_n$ with uniform probability and let her either send the state $|x_1\rangle \ldots |x_n\rangle$ or the state $H^{\otimes n}|x_1\rangle \ldots |x_n\rangle$ to Bob, where H is the Hadamard transformation. Not knowing if the string is sent in the computational basis or in the Hadamard basis, it turns out that the optimal measurement that Bob can do in order to maximise the mutual information between the measurement outcome y and Alice's string x is with respect to a randomly chosen basis, in which case he will obtain $I(X;Y) = \frac{n}{2}$. If, however, he has access to the single bit which determines the basis, he will have $I(X;Y) = n$. A *single bit* can therefore *unlock* an arbitrary amount of information. This effect has been termed *locking of classical information in quantum states* or simply *locking* and was first described in [16]. In this paper, we will discuss various types of locking effects and highlight their significance for the design and security of QKD protocols (Section 5).

Finally, we demonstrate that the amount of key that can be distilled from given pre-shared data strongly depends on whether Eve is assumed to store her information in a classical or in a quantum memory. This, again, has direct consequences for the analysis of protocols in quantum cryptography (Section 6).

For a more detailed explanation of the contributions of this paper, we refer to the introductory paragraphs of Sections 3–6.

2 The unified key distillation scenario

In classical information-theoretic cryptography one considers the problem of distilling key from correlated data specified by a tripartite probability distribution p_{ijk} ($p_{ijk} \geq 0$, $\sum_{i,j,k} p_{ijk} = 1$). Alice and Bob who wish to distil the key have access to i and j, respectively, whereas the eavesdropper Eve knows the value k (see, e.g., [17]). Typically, it is assumed that many independently generated copies of the triples (i,j,k) are available[8]. The *key rate* or *distillable key* of a distribution p_{ijk} is the rate at which key bits can be obtained per realisation of

[8] Using de Finetti's representation theorem, this assumption can be weakened to the assumption that the overall distribution of all triples is invariant under permutations (see [18] for more details including a treatment of the quantum case).

this distribution, if Alice and Bob are restricted to local operations and public but authentic classical communication.

Before we continue to introduce the quantum version of the key distillation scenario described above, let us quickly note that it will be convenient to regard probability distributions as *classical states*, that is, given probabilities p_i, we consider $\rho = \sum_{i=1}^{d} p_i |i\rangle\langle i|$, where $|i\rangle$ is an orthonormal basis of a d-dimensional Hilbert space; we will assume that $d < \infty$. In the sequel we will encounter not only classical or quantum states, but also states that are distributed over several systems which might be partly classical and partly quantum-mechanical. To make this explicit, we say that a bipartite state ρ_{AB} is *cq (classical-quantum)* if it is of the form $\rho_{AB} = \sum_i p_i |i\rangle\langle i|_A \otimes \rho_B^i$ for quantum states ρ_B^i and a probability distribution p_i. This definition easily extends to three or more parties, for instance:

- a *ccq (classical-classical-quantum) state* ρ_{ABE} is of the form $\sum_{i,j} p_{ij} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes \rho_E^{ij}$, where p_{ij} is a probability distribution and ρ_E^{ij} are arbitrary quantum states.
- the distribution p_{ijk} corresponds to a *ccc (classical-classical-classical) state* $\rho_{ABE} = \sum_{i,j,k} p_{ijk} |ijk\rangle\langle ijk|_{ABE}$, where we use $|ijk\rangle_{ABE}$ as a short form for $|i\rangle_A \otimes |j\rangle_B \otimes |k\rangle_E$ (as above, the states $|i\rangle_A$ for different values of i, and likewise $|j\rangle_B$ and $|k\rangle_k$, are normalised and mutually orthogonal).

We will be concerned with key distillation from arbitrary tripartite quantum states ρ_{ABE} shared by Alice, Bob, and an adversary Eve, assisted by *local quantum operations and public classical communication (LOPC)* [10, 19, 15]. A local quantum operation on Bob's side is of the form

$$\rho_{ABE} \mapsto (I_{AE} \otimes \Lambda_B)(\rho_{ABE}) \ .$$

Public classical communication from Alice to Bob can be modelled by copying a local classical register, i.e., any state of the form $\rho_{AA'BE} = \sum_i \rho_{ABE}^i \otimes |i\rangle\langle i|_{A'}$ is transformed into $\rho'_{AA'BB'EE'} = \sum_i \rho_{ABE}^i \otimes |iii\rangle\langle iii|_{A'B'E'}$. Similarly, one can define these operations with the roles of Alice and Bob interchanged.

The goal of a key distillation protocol is to transform copies of tripartite states ρ_{ABE} into a state which is close to

$$\tau_{ABE}^{\ell} = \frac{1}{2^\ell} \sum_{i=1}^{2^\ell} |ii\rangle\langle ii|_{AB} \otimes \tau_E \tag{1}$$

for some arbitrary τ_E. τ_{ABE}^{ℓ} (also denoted τ^ℓ for short) corresponds to a perfect *key of length* ℓ, i.e., uniform randomness on an alphabet of size 2^ℓ shared by Alice and Bob and independent of Eve's system. We measure *closeness* of two states ρ and σ in terms of the trace norm $\|\rho - \sigma\| := \frac{1}{2}\mathrm{Tr}|\rho - \sigma|$. The trace norm is the natural quantum analogue of the variational distance to which it reduces if ρ and σ are classical.

We will now give the formal definition of an LOPC protocol and of the key rate.

Definition 1. *An* LOPC protocol $\mathcal{P}$ *is a family* $\{\Lambda_n\}_{n\in\mathbb{N}}$ *of completely positive trace preserving (CPTP) maps*

$$\Lambda_n : (\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes n} \to \mathcal{H}_A^n \otimes \mathcal{H}_B^n \otimes \mathcal{H}_E^n$$

which are defined by the concatenation of a finite number of local operation and public communication steps.

Definition 2. *We say that an LOPC protocol* $\mathcal{P}$ *distills key at rate* $\mathcal{R}_\mathcal{P}$ *if there exists a sequence* $\{\ell_n\}_{n\in\mathbb{N}}$ *such that*

$$\limsup_{n\to\infty} \frac{\ell_n}{n} = R_\mathcal{P}$$
$$\lim_{n\to\infty} \|\Lambda_n(\rho_{ABE}^{\otimes n}) - \tau_{ABE}^{\ell_n}\| = 0$$

where $\tau_{ABE}^{\ell_n}$ *are the ccq states defined by (1). The* key rate *or* distillable key *of a state* ρ_{ABE} *is defined as* $K_D(\rho_{ABE}) := \sup_\mathcal{P} \mathcal{R}_\mathcal{P}$.

The quantity K_D obviously depends on the partition of the state given as argument into the three parts controlled by Alice, Bob, and Eve, respectively. We thus indicate the assignment of subsystems by semicolons if needed. For instance, we write $\rho_{AD;B;E}$ if Alice holds an additional system D.

It can be shown that the maximisation in the definition of K_D can be restricted to protocols whose communication complexity grows at most linearly in the number of copies of ρ_{ABE}. Hence, if $d = \dim \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E < \infty$ then the dimension of the output of the protocol is bounded by $\log \dim \mathcal{H}_A^n \otimes \mathcal{H}_B^n \otimes \mathcal{H}_E^n \leq cn \log d$, for some constant c. (The proof of this statement will appear in a full version of this paper.)

The above security criterion is (strictly) weaker than the one proposed in [10][9], hence $K_D(\rho_{ABE})$ is lower bounded by a lower bound derived in [10]:

$$K_D(\rho_{ABE}) \geq I(A:B)_\rho - I(A:E)_\rho \ . \tag{2}$$

This expression can be seen as a quantum analogue of the well-known bound of Csiszár, Körner, and Maurer [3, 17]. Here $I(A:B)_\rho$ denotes the mutual information defined by $I(A:B)_\rho := S(A)_\rho + S(B)_\rho - S(AB)_\rho$ where $S(A)_\rho := S(\rho^A)$ is the von Neumann entropy of system A (and similarly for B and E). For later reference we also define the *conditional mutual information* $I(A:B|E)_\rho := S(AE)_\rho + S(BE)_\rho - S(ABE)_\rho - S(E)_\rho$.

Note also that the criterion for the quality of the distilled key used in Definition 2 implies that the key is both uniformly distributed and independent of the adversary's knowledge, just as in [11]. Previous works considered uniformity and security separately. Note that, even though weaker than certain alternative

[9] The security criterion of [10] implies that, conditioned on *any* value of the key, Eve's state is almost the same. In contrast, according to the above definition, Eve's state might be arbitrary for a small number of values of the key.

criteria such as the one of [10], the security measure of Definition 2 is universally composable [11].

In [20], the question was posed whether the security condition also holds if the accessible information is used instead of the criterion considered here. Recently, it has been shown that this is not the case [21]. More precisely, an example of a family of states was exhibited such that Eve has exponentially small knowledge in terms of accessible information but constant knowledge in terms of the Holevo information. This implies that in this context, security definitions based on the accessible information are problematic. In particular, a key might be insecure even though the accessible information of an adversary on the key is exponentially small (in the key size).

3 Upper bounds for the key rate

In this section, we first derive sufficient conditions that a function has to satisfy in order to be an upper bound for the key rate (Section 3.1). We focus on functions that are *secrecy monotones* [12], i.e., they are monotonically decreasing under LOPC operations. Our approach therefore parallels the situation in classical and quantum information theory where resource transformations are also bounded by monotonic functions; examples include the proofs of converses to coding theorems and entanglement measures (see, e.g., [14]). As a corollary to our characterisation of secrecy monotones, we show how to turn entanglement monotones into secrecy monotones.

In a second part (Section 3.2), we provide a number of concrete secrecy monotones that satisfy the conditions mentioned above. They can be roughly divided into two parts: (i) functions derived from the intrinsic information and (ii) functions based on entanglement monotones. Finally, we will compare different secrecy monotones (Section 3.3) and study a few particular cases in more detail (Section 3.4).

3.1 Secrecy monotones

Theorem 1. *Let $M(\rho)$ be a function mapping tripartite quantum states $\rho \equiv \rho_{ABE}$ into the positive numbers such that the following holds:*

1. *Monotonicity: $M(\Lambda(\rho)) \leq M(\rho)$ for any LOPC operation Λ.*
2. *Asymptotic continuity: for any states ρ^n, σ^n on $\mathcal{H}_A^n \otimes \mathcal{H}_B^n \otimes \mathcal{H}_E^n$, the condition $\|\rho^n - \sigma^n\| \to 0$ implies $\frac{1}{\log r_n}\big|M(\rho^n) - M(\sigma^n)\big| \to 0$ where $r_n = \dim(\mathcal{H}_A^n \otimes \mathcal{H}_B^n \otimes \mathcal{H}_E^n)$.*
3. *Normalisation: $M(\tau^\ell) = \ell$.*

Then the regularisation *of the function M given by $M^\infty(\rho) = \limsup_{n\to\infty} \frac{M(\rho^{\otimes n})}{n}$ is an upper bound on K_D, i.e., $M^\infty(\rho_{ABE}) \geq K_D(\rho_{ABE})$ for all ρ_{ABE} with $\dim \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E < \infty$. If in addition M satisfies*

4. *Subadditivity on tensor products: $M(\rho^{\otimes n}) \leq nM(\rho)$,*

then M is an upper bound for K_D.

Proof. Consider a key distillation protocol $\mathcal{P}$ that produces output states σ^n such that $\|\sigma^n - \tau^{\ell_n}\| \to 0$. We will show that $M^\infty(\rho) \geq R_{\mathcal{P}}$. Let us assume without loss of generality that $R_{\mathcal{P}} > 0$. Indeed, by monotonicity we have $M(\rho^{\otimes n}) \geq M(\sigma^n)$, which is equivalent to

$$\frac{1}{n} M(\rho^{\otimes n}) \geq \frac{\ell_n}{n} \left(\frac{M(\sigma^n) - M(\tau^{\ell_n})}{\ell_n} + 1 \right) , \tag{3}$$

where we have used the normalisation condition. As remarked in Definition 2 there is a constant $c > 0$ such that $\log r_n \leq cn$ and by definition of $R_{\mathcal{P}}$ there exists a $c' > 0$ and n_0 such that for all $n \geq n_0$, $\log d_n \geq c'n$. Hence $\ell_n \geq c'n \geq \frac{c'}{c} \log r_n$, therefore asymptotic continuity implies

$$\lim_{n\to\infty} \frac{1}{\ell_n} \big| M(\sigma^n) - M(\tau^{\ell_n}) \big| = 0 .$$

Taking the limsup on both sides of (3) gives $M^\infty(\rho) \geq \limsup_n \frac{\ell_n}{n} = R_{\mathcal{P}}$. Thus we have shown that M^∞ is an upper bound for the rate of an arbitrary protocol, so that it is an also upper bound for K_D. □

If we restrict our attention to the special case of key distillation from bipartite states ρ_{AB}, we can immediately identify a well-known class of secrecy monotones, namely entanglement monotones. A convenient formulation is in this case not given by the distillation of states τ^ℓ with help of LOPC operations, but rather by the distillation of states γ^ℓ via local operations and classical communication (LOCC), where $\gamma^\ell = U|\psi\rangle\langle\psi|_{AB}^{\otimes \ell} \otimes \rho_{A'B'} U^\dagger$, for some unitary $U = \sum_{i=1}^{2^\ell} |ii\rangle\langle ii|_{AB} \otimes U_{A'B'}^{(i)}$ and $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ [15, 22]. Note that measuring the state γ^ℓ with respect to the computational bases on Alice and Bob's subsystems results in ℓ key bits.

Corollary 1. *Let $E(\rho)$ be a function mapping bipartite quantum states $\rho \equiv \rho_{AB}$ into the positive numbers such that the following holds:*

1. *Monotonicity: $E(\Lambda(\rho)) \leq E(\rho)$ for any LOCC operation Λ.*
2. *Asymptotic continuity: for any states ρ^n, σ^n on $\mathcal{H}_A^n \otimes \mathcal{H}_B^n$, the condition $\|\rho^n - \sigma^n\| \to 0$ implies $\frac{1}{\log r_n} \big| E(\rho^n) - E(\sigma^n) \big| \to 0$ where $r_n = \dim(\mathcal{H}_A^n \otimes \mathcal{H}_B^n)$.*
3. *Normalisation: $E(\gamma^\ell) \geq \ell$.*

Then the regularisation of the function E given by $E^\infty(\rho) = \limsup_{n\to\infty} \frac{E(\rho^{\otimes n})}{n}$ is an upper bound on K_D, i.e., $E^\infty(\rho_{AB}) \geq K_D(|\psi\rangle\langle\psi|_{ABE})$ where $|\psi\rangle\langle\psi|_{ABE}$ is a purification of ρ_{AB}. If in addition E satisfies

4. *Subadditivity on tensor products: $E(\rho^{\otimes n}) \leq nE(\rho)$,*

then E is an upper bound for K_D.

The analogue of this result in the realm of *entanglement* distillation has long been known: namely, every function E satisfying LOCC monotonicity, asymptotic continuity near maximally entangled states as well as normalisation on maximally entangled states ($E(|\psi\rangle\langle\psi|) = \log d$ for $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$) can be shown to provide an upper bound on distillable entanglement E_D [23, 24], that is, $E^\infty(\rho) \geq E_D(\rho)$. Additionally, if E is subadditive, the same inequality holds with E^∞ replaced by E. Indeed this result can be seen as a corollary to Corollary 1 by restricting from distillation of states τ^ℓ to distillation of $|\psi\rangle\langle\psi|^{\otimes\ell}$ and noting that $|\psi\rangle\langle\psi|^{\otimes\ell}$ is of the form τ^ℓ with trivial $A'B'$.

In the above corollary, we have identified asymptotic continuity on *all* states as well as normalisation on the states γ^ℓ (rather than on singlets) as the crucial ingredients in order for an entanglement measure to bound distillable key from above. Note also that we require those additional conditions as, for instance, the *logarithmic negativity* as defined in [25] satisfies the weaker conditions, therefore being an upper bound on distillable entanglement, but fails to be an upper bound on distillable key.

We will now show how to turn this bound for bipartite states (or tripartite pure states) into one for arbitrary tripartite states. The recipe is simple: for a given state ρ_{ABE}, consider a purification $|\psi\rangle\langle\psi|_{AA'BB'E}$ where the purifying system is denoted by $A'B'$ and is split between Alice and Bob. Clearly, for any splitting, $K_D(|\psi\rangle\langle\psi|_{AA'BB'E}) \geq K_D(\rho_{ABE})$. This inequality combined with the previous corollary applied to $|\psi\rangle\langle\psi|_{AA'BB'E}$ proves the following statement.

Corollary 2. *If E satisfies the conditions of Corollary 1 then*

$$K_D(\rho_{ABE}) \leq E^\infty(\rho_{AA'BB'}) ,$$

where $\rho_{AA'BB'} = \mathrm{Tr}_E|\psi\rangle\langle\psi|_{AA'BB'E}$ and $\rho_{ABE} = \mathrm{Tr}_{A'B'}|\psi\rangle\langle\psi|_{AA'BB'E}$. If E is subadditive, the same inequality holds with E replacing E^∞.

3.2 Examples of secrecy monotones

We will now introduce a number of secrecy monotones. We will only briefly comment on the relations between them. A more detailed analysis of how the different bounds on the key rate compare is given in Section 3.3.

Intrinsic information The *intrinsic information* of a probability distribution p_{ijk} is given by

$$I(A : B \downarrow E) := \inf I(A : B|E')_\rho \tag{4}$$

where ρ_{ABE} is the ccc state corresponding to p_{ijk}. The infimum is taken over all channels from E to E' specified by a conditional probability distributions $p_{l|m}$. $\rho_{ABE'}$ is the state obtained by applying the channel to E. This quantity has been defined by Maurer and Wolf and provides an upper bound on the key rate from classical correlations [13]. We can extend it in the following way to arbitrary tripartite quantum states ρ_{ABE}.

Definition 3. *The* intrinsic information *of a tripartite quantum state ρ_{ABE} is given by*

$$I(A:B\downarrow E)_\rho := \inf I(A:B|E')_\rho$$

where the infimum is taken over all CPTP maps $\Lambda_{E\to E}$ from E to E' where $\rho_{ABE'} = (I_{AB}\otimes\Lambda_{E\to E})(\rho_{ABE})$.

This definition is compatible with the original definition since it reduces to (4) if the systems A, B and E are classical.

It is straightforward to show that the intrinsic information satisfies the requirements of Theorem 1. Hence we have proved the following theorem.

Theorem 2. *The intrinsic information is an upper bound on distillable key, i.e., $K_D(\rho_{ABE}) \leq I(A:B\downarrow E)_\rho$.*

Let us note that this bound differs from the bound proposed in [26, 19] where instead of all quantum channels, arbitrary measurements were considered. Our present bound can be tighter, as it can take into account Eve's quantum memory.

In the case where ρ_{ABE} is pure, this bound can be improved by a factor of two because $I(A:B\downarrow E)_\rho = 2E_{sq}(\rho_{AB})$, where E_{sq} is the squashed entanglement defined below and because squashed entanglement is an upper bound for the key rate.

Squashed entanglement

Definition 4. *Squashed entanglement is defined as*

$$E_{sq}(\rho_{AB}) = \frac{1}{2}\inf_{\substack{\rho_{ABE}:\\ \rho_{AB}=\mathrm{Tr}_E\rho_{ABE}}} I(A:B|E)_\rho$$

Squashed entanglement can be shown to be a LOCC monotone, additive [27], and asymptotically continuous [28]. In [29, Proposition 4.19] it was shown to satisfy the normalisation condition and is therefore an upper bound on distillable key according to Corollary 1.

Theorem 3. *Squashed entanglement is an upper bound on distillable key, i.e., $K_D(\rho_{ABE}) \leq E_{sq}(\rho_{AA'BB'})$ where $\rho_{AA'BB'} = \mathrm{Tr}_E|\psi\rangle\langle\psi|_{AA'BB'E}$ and $\rho_{ABE} = \mathrm{Tr}_{A'B'}|\psi\rangle\langle\psi|_{AA'BB'E}$.*

Reduced intrinsic information There is another way in which we can find a bound on the key rate which is tighter than the intrinsic information. In [30] it was shown that the classical intrinsic information is *E-lockable*, i.e., it can increase sharply when a single bit is taken away from Eve. Since (classical) distillable key is not E-lockable, the bound that the intrinsic information provides cannot be tight. This was the motivation for defining the *reduced intrinsic information* by $I(AB\downarrow\downarrow E) = \inf I(AB\downarrow EE') + S(E')$ where the infimum is taken over arbitrary classical values E' [30]. We now define the quantum extension of this function.

Definition 5. *Let $a = 1, 2$. The* reduced intrinsic information (with parameter *a*) *is given by*

$$I(A : B \downarrow\downarrow E)^{(a)}_{\rho} = \inf\{I(AB \downarrow EE')_{\rho} + aS(E')_{\rho}\}$$

where the infimum is taken over all extensions $\rho_{ABEE'}$ with a classical register E' if $a = 1$ and over arbitrary extensions $\rho_{ABEE'}$ if $a = 2$.

The parameter a reflects the different behaviour of the intrinsic information subject to loss of a single bit (qubit). The reduced intrinsic information is an upper bound on distillable key since

$$K_D(\rho_{ABE}) \leq K_D(\rho_{ABEE'}) + aS(E') \leq I(AB \downarrow EE') + aS(E') \ .$$

The first inequality corresponds to Corollary 4 below.

Theorem 4. *The reduced intrinsic information is an upper bound on distillable key, i.e., $K_D(\rho_{ABE}) \leq I(A : B \downarrow\downarrow E)^{(a)}_{\rho}$, for $a = 1, 2$.*

Relative entropy of entanglement The relative entropy of entanglement and its regularised version are well-known entanglement measures that serve as important tools in entanglement theory.

Definition 6. *The relative entropy of entanglement is given by [31, 32]*

$$E_R(\rho_{AB}) = \inf_{\sigma_{AB}} S(\rho_{AB} \| \sigma_{AB})$$

where $S(\rho_{AB}\|\sigma_{AB}) = \mathrm{Tr}\rho_{AB}[\log \rho_{AB} - \log \sigma_{AB}]$ and the minimisation is taken over all separable states σ_{AB}, i.e. $\sigma_{AB} = \sum_i p_i \rho^i_A \otimes \rho^i_B$.

The relative entropy of entanglement was the first upper bound that has been provided for $K_D(|\psi\rangle\langle\psi|_{ABE})$ [15, 22]. We now extend this result to all tripartite quantum states ρ^{ABE}.

Theorem 5. *The relative entropy of entanglement is an upper bound on distillable key, i.e., $K_D(\rho_{ABE}) \leq E^{\infty}_R(\rho_{AA'BB'}) \leq E_R(\rho_{AA'BB'})$ where $\rho_{AA'BB'} = \mathrm{Tr}_E|\psi\rangle\langle\psi|_{AA'BB'E}$ and $\rho_{ABE} = \mathrm{Tr}_{A'B'}|\psi\rangle\langle\psi|_{AA'BB'E}$.*

It is a particular advantage of E_R in its function as an upper bound that it is not lockable [33].

3.3 Comparison of secrecy monotones

Pure versus mixed For entangled states, bounds derived from entanglement measures are usually tighter than the intrinsic information and its reduced version. Consider for example the state $\rho_{ABE} = |\psi\rangle\langle\psi|_{AB} \otimes \rho_E$ where $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Here we have

$$E_R(\rho_{ABE}) = E^{\infty}_R(\rho_{ABE}) = E_{sq}(\rho_{ABE}) = K_D(\rho_{ABE}) = 1 \ ,$$

while

$$I(A:B\downarrow E)_\rho = I(A:B\downarrow\downarrow E)^{(a)}_\rho = 2\ ,$$

for $a=1,2$. In general, for tripartite pure states, squashed entanglement is a tighter bound on the key rate than the intrinsic information by at least a factor of two:

$$2E_{sq}(|\psi\rangle\langle\psi|_{ABE}) = I(A:B\downarrow E)_{|\psi\rangle\langle\psi|}.$$

The locking effect We will now give a concrete example which shows that there is a purification $|\psi\rangle_{AA'BB'E}$ of ρ_{ABE} such that

$$K_D(\rho_{ABE}) = E_R(\rho_{AA'BB'}) < I(AA':BB'\downarrow E)_\rho\ .$$

Consider the distribution p_{ijkl} defined by the following distribution for p_{ij}

i j	0	1	2	3
0	$\frac{1}{8}$	$\frac{1}{8}$	0	0
1	$\frac{1}{8}$	$\frac{1}{8}$	0	0
2	0	0	$\frac{1}{4}$	0
3	0	0	0	$\frac{1}{4}$

and where k and l are uniquely determined by (i,j),

$$\begin{aligned} &k = i+j(\text{mod } 2) \quad \text{for} \quad i,j\in\{0,1\} \\ &k = i(\text{mod } 2) \qquad \text{for} \quad i\in\{2,3\} \\ &l = \lfloor i/2 \rfloor \end{aligned}$$

for all (i,j) with $p_{ij}>0$. We denote the corresponding cccc state by $\rho_{ABEF} = \sum_{ijkl} p_{ijkl}|ijkl\rangle\langle ijkl|$. Clearly $K_D(\rho_{A;B;EF})=0$, as Eve can factorise Alice and Bob, by keeping k when $l=1$ and forgetting it when $l=0$. In the former case, when $l=0$, then Alice and Bob have $(i,j)=(2,2)$, and when $l=1$, then Alice and Bob have $(i,j)=(3,3)$. In the latter case, both Alice and Bob have at random 0 or 1 and they are not correlated.

On the other hand, when Eve does not have access to l, then the key rate is equal to 1, i.e., $K_D(\rho_{A;B;E})$=1. Indeed, it cannot be greater, as key cannot increase more than the entropy of the variable that was taken out from Eve. However one finds that the intrinsic information is equal to 3/2, i.e., $I(A:B\downarrow E)_\rho = 3/2$ [30].

Let us consider the purification of the above state,

$$\begin{aligned} |\psi_{A'ABEF}\rangle = \frac{1}{2}\big(&|0\rangle_{A'}|22\rangle_{AB}|0\rangle_E|0\rangle_F + |0\rangle_{A'}|33\rangle_{AB}|1\rangle_E|0\rangle_F \\ &+|\psi\rangle_{A'AB}|0\rangle_E|1\rangle_F + |\phi\rangle_{A'AB}|1\rangle_E|1\rangle_F\big), \end{aligned}$$

where

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A'}|00\rangle_{AB} + |1\rangle_{A'}|11\rangle_{AB})$$

and

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{A'}|01\rangle_{AB} + |1\rangle_{A'}|10\rangle_{AB}) \ .$$

Thus when E and F are with Eve, the state $\rho_{AA';B}$ of Alice and Bob is a mixture of four states: $|0\rangle|22\rangle$, $|0\rangle|33\rangle$, $|\phi\rangle$ and $|\psi\rangle$. This state is separable state, hence $E_R(\rho_{AA';B}) = 0$.

Consider now the state $\rho_{AA'F;B}$ where F is controlled by Alice instead of Eve. Measuring F makes the state separable and in [33] it was shown that measuring a single qubit cannot decrease the relative entropy of entanglement by more than 1, thus we obtain

$$E_R(\rho_{AA'F;B}) \leq 1.$$

By Theorem 5 we then have $K_D(\rho_{ABE}) \leq 1$, but indeed one can distil one bit of key from ρ_{ABE}, therefore

$$K_D(\rho_{ABE}) = E_R(\rho_{AA'F;B}) = 1.$$

In [30] the considered distribution was generalised to make the gap between intrinsic information and distillable key arbitrarily large. It is not difficult to see that E_R is still bounded by one. This shows that the bound based on relative entropy of entanglement, though perhaps more complicated in use, can be significantly stronger than intrinsic information bound. We leave it open, whether or not the intrinsic information bound is weaker in general when compared to the relative entropy bound. This parallels the challenge to discover a relation between the relative entropy of entanglement and squashed entanglement. Here it has also been observed that squashed entanglement can exceed the relative entropy of entanglement by a large amount, due to a *locking effect* [34].

3.4 Upper and lower bounds when $\rho_{ABE} = \rho_{AB} \otimes \rho_E$

In this section we focus on states of the form $\rho_{ABE} = \rho_{AB} \otimes \rho_E$. Since distillable key cannot increase under Eve's operations, the form of the state ρ_E is not important and we conclude that $K_D(\rho_{AB} \otimes \rho_E)$ is a function of ρ_{AB} only. If the state ρ_{AB} is classical on system A, then it is known that distillable key is equal to the quantum mutual information, $K_D(\rho_{AB} \otimes \rho_E) = I(A:B)_\rho$ [10]. Indeed, we know from Theorem 2 that the key rate can never exceed $I(A:B)_\rho$. For separable quantum states ρ_{AB} we were able to further improve this bound. The upper bounds are summarised in the following theorem. (Its proof will appear in a full version of this paper.)

Theorem 6. *For all states $\rho_{AB} \otimes \rho_E$,*

$$K_D(\rho_{AB} \otimes \rho_E) \leq I(A:B)_\rho$$

with equality if ρ_{AB} is classical on system A. If ρ_{AB} is separable, i.e., $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$, then

$$K_D(\rho_{AB} \otimes \rho_E) \leq I_{\mathrm{acc}}^{\mathrm{LOPC}}(\mathcal{E}) \leq I_{\mathrm{acc}}(\mathcal{E})$$

where $\mathcal{E} = \{p_i, \rho_A^i \otimes \rho_B^i\}$ and $I_{\mathrm{acc}}^{\mathrm{LOPC}}(\mathcal{E})$ is the maximal mutual information that Alice and Bob can obtain about i using LOPC operations (see e.g. [35, 36]), whereas $I_{\mathrm{acc}}(\mathcal{E})$ denotes the usual accessible information, i.e. maximal mutual information about i obtained by joint measurements.

We will now derive a general lower bound on the key rate in terms of the distillable common randomness.

Definition 7. *We say that an LOPC protocol $\mathcal{P}$ distills* common randomness *at rate $\mathcal{R}_{\mathcal{P}}$ if there exists a sequence $\{\ell_n\}_{n\in\mathbb{N}}$ such that*

$$\limsup_{n\to\infty} \frac{\ell_n - m_n}{n} = R_{\mathcal{P}}$$
$$\lim_{n\to\infty} \|\Lambda_n(\rho_{AB}^{\otimes n}) - \tau^{\ell_n}\| = 0$$

where m_n is the number of communicated bits. The distillable common randomness *of a state ρ^{AB} is defined as $D_R(\rho_{AB}) := \sup_{\mathcal{P}} \mathcal{R}_{\mathcal{P}}$.*

For some protocols the rate may be negative. However it is immediate that $D_R(\rho_{AB})$ is nonnegative for all ρ_{AB}. The following statement is a direct consequence of the results in [10, 11].

Theorem 7. *For the states $\rho_{ABE} = \rho_{AB} \otimes \rho_E$ the distillable key is an upper bound on the distillable common randomness, i.e., $K_D(\rho_{AB} \otimes \rho_E) \geq D_R(\rho_{AB})$ for all ρ_{AB} and ρ_E.*

4 Embedding classical into quantum states

The problem of distilling key from a classical tripartite distribution (i.e., ccc states) is closely related to the problem of distilling entanglement from a bipartite quantum state (where the environment takes the role of the adversary), as noted in [9, 30]. It thus seems natural to ask whether, in analogy to *bound entangled* quantum states (which have positive entanglement cost but zero distillable entanglement), there might be classical distributions with *bound information.* These are distributions with zero key rate but positive key cost, i.e., no key can be distilled from them, yet key is needed to generate them. The existence of such distributions, however, is still unproved. (There are, however, some partial positive answers, including an asymptotic result [30] as well as a result for scenarios involving more than three parties [37].)

In [9, 30], it has been suggested that the classical distribution obtained by measuring bound entangled quantum states might have bound information. Such hope, however, was put into question by the results of [15], showing that there are quantum states with positive key rate but no distillable entanglement (i.e., they are bound entangled). However, the examples of states put forward in [15] have a rather special structure. It is thus still possible that distributions with bound information might be obtained by measuring appropriately chosen bound entangled states.

In the following, we consider a special *embedding* of classical distributions into quantum states as proposed in [9]. We then show how statements about key distillation starting from the original state and from the embedded state are related to each other. Let

$$\rho_{ccc} := \sum_{ijk} p_{ijk} |ijk\rangle\langle ijk|_{ABE} \tag{5}$$

be a ccc state defined relative to fixed orthonormal bases on the three subsystems (in the following called *computational bases*). We then consider the *qqq embedding* $\rho_{qqq} = |\psi\rangle\langle\psi|$ of ρ_{ccc} given by

$$|\psi\rangle = \sum_{i} \sqrt{p_{ijk}} |ijk\rangle_{ABE} \ .$$

Note that, if Alice and Bob measure ρ_{qqq} in the computational basis, they end up with a state of the form

$$\rho_{ccq} = \sum_{ij} p_{ij} |ij\rangle\langle ij|_{AB} \otimes |\psi^{ij}\rangle\langle\psi^{ij}|_{E} \tag{6}$$

for some appropriately chosen $|\psi^{ij}\rangle$. We call this state the *ccq embedding* of ρ_{ccc}.

In a similar way as classical distributions can be translated to quantum states, classical protocols have a quantum analogue. To make this more precise, we consider a classical LOPC protocol $\mathcal{P}$ that Alice and Bob wish to apply to a ccc state ρ_{ccc} as in (5). Obviously, $\mathcal{P}$ can equivalently be applied to the corresponding ccq embedding ρ_{ccq} as defined in (6) (because Alice and Bob's parts are the same in both cases). Because Eve might transform the information she has in the ccq case to the information she has in the ccc case by applying a local measurement, security of the key generated by $\mathcal{P}$ when applied to ρ_{ccq} immediately implies security of the key generated by $\mathcal{P}$ when applied to ρ_{ccc}. Note, however, that the opposite of this statement is generally not true.

In general, a classical protocol $\mathcal{P}$ can be subdivided into a sequence of steps of the following form:

1. generating local randomness
2. forgetting information (discarding local subsystems)
3. applying permutations
4. classical communication.

The *coherent version* of $\mathcal{P}$, denoted $\mathcal{P}_q$, is defined as the protocol acting on a qqq state where the above classical operations are replaced by the following quantum operations:

1. attaching subsystems which are in a superposition of fixed basis vectors
2. transferring subsystems to Eve
3. applying unitary transformations that permute fixed basis vectors
4. adding ancilla systems (with fixed initial state) to both the receiver's and Eve's system, and applying controlled not (CNOT) operations to both ancillas, where the CNOTs are controlled by the communication bits.

Consider now a fixed ccc state ρ_{ccc} of the form (5) and let $\mathcal{P}$ be a classical protocol acting on ρ_{ccc}. It is easy to see that the following operations applied to the qqq embedding ρ_{qqq} of ρ_{ccc} result in the same state: (i) measuring in the computational basis and then applying the classical protocol $\mathcal{P}$; or (ii) applying the coherent protocol $\mathcal{P}_q$ and then measuring the resulting state γ^ℓ in the computational basis. This fact can be expressed by a commutative diagram.

$$\begin{tikzcd}
|\psi\rangle\langle\psi|^{\otimes n} \arrow[r, "\mathcal{P}_q"] \arrow[d, "\text{measurement}"'] & \gamma^\ell \arrow[d, "\text{measurement}"] \\
\rho_{ccq}^{\otimes n} \arrow[r, "\mathcal{P}"] & \tau^\ell
\end{tikzcd}$$

Hence, if the coherent version $\mathcal{P}_q$ of $\mathcal{P}$ acting on ρ_{qqq} distills secure key bits at rate R then so does the protocol $\mathcal{P}$ applied to the original ccc state ρ_{ccc}.

It is natural to ask whether there are cases for which the converse of this statement holds as well. This would mean that security of a classical protocol also implies security of its coherent version. In the following, we exhibit a class of distributions for which this is always true. The key rate of any such distribution is thus equal to the key rate of the corresponding embedded qqq state.

Roughly speaking, the class of distributions we consider is characterised by the property that the information known to Eve is completely determined by the joint information held by Alice and Bob.

Theorem 8. *Let ρ_{ccc} be a ccc state of the form* (5) *such that, for any pair of values (i, j) held by Alice and Bob there exists at most one value k of Eve with $p_{ijk} > 0$. If a classical protocol $\mathcal{P}$ applied to ρ_{ccc} produces key at rate R then so does its coherent version $\mathcal{P}_q$ applied to the qqq embedding $|\psi\rangle$ of ρ_{ccc} (and followed by a measurement in the computational basis).*

Proof. The ccq embedding of ρ_{ccc} is given by a state of the form

$$\rho_{ccq} = \sum_{ij} p_{ij} |ij\rangle\langle ij|_{AB} \otimes |\psi^{ij}\rangle\langle\psi^{ij}|_E \ .$$

Since, by assumption, every pair (i, j) determines a unique $k = k(i, j)$, $|\psi^{ij}\rangle\langle\psi^{ij}|_E$ equals $|k(i, j)\rangle\langle k(i, j)|$ and, hence, ρ_{ccq} is identical to the original ccc state ρ_{ccc}. The assertion then follows from the fact that measurements in the computational basis applied to Alice and Bob's subsystems commute with the coherent version $\mathcal{P}_q$ of $\mathcal{P}$. □

Corollary 3. *Let ρ_{ccc} be a ccc state of the form* (5) *such that, for any pair of values (i,j) held by Alice and Bob there exists at most one value k of Eve with $p_{ijk} > 0$. Then, the key rate for the qqq embedding ρ_{qqq} of ρ_{ccc} satisfies*

$$K_D(\rho_{qqq}) = K_D(\rho_{ccc}) \ .$$

Note that the above statements do not necessarily hold for general distributions. To see this, consider the state

$$|\psi\rangle_{ABA'E} = |00\rangle_{AB}|+\rangle_{A'}|+\rangle_E + |11\rangle_{AB}|\psi_+\rangle_{A'E}$$

where $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\psi_+\rangle := \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. Moreover, let ρ_{ccc} be the ccc state obtained by measuring $|\psi\rangle\langle\psi|_{AA';B;E}$ in the computational basis. Because all its coefficient are positive, it is easy to verify that $|\psi\rangle\langle\psi|_{ABA'E}$ can be seen as the qqq embedding of ρ_{ccc}. Observe that, after discarding subsystem A', ρ_{ccc} corresponds to a perfect key bit. However, the ccq state obtained from $|\psi\rangle\langle\psi|_{ABA'E}$ by discarding A' and measuring in the computational basis is of the form $\frac{1}{2}(|00\rangle\langle 00|_{AB} \otimes |+\rangle\langle +|_E + |11\rangle\langle 11|_{AB} \otimes I_E/2)$. This state, of course, does not correspond to a key bit as Eve might easily distinguish the states $|+\rangle\langle +|$ and $I_E/2$.

We continue with a statement on the relation between the intrinsic information of a ccc state and the so-called *entanglement of formation*[10] E_F of its qqq embedding. More precisely, we show that, under the same condition as in Theorem 8, the first is a lower bound for the latter (see also [39, 40]).

Theorem 9. *Let ρ_{ccc} be a ccc state of the form* (5) *such that, for any pair of values (i,j) held by Alice and Bob there exists at most one value k of Eve with $p_{ijk} > 0$, and let ρ_{qqq} be the qqq embedding of this state. Then*

$$I(A : B \downarrow E)_{\rho_{ccc}} \leq E_F(\mathrm{Tr}_E(\rho_{qqq})) \ .$$

Proof. Note first that any decomposition of $\mathrm{Tr}_E(\rho_{qqq})$ into pure states can be induced by an appropriate measurement on the system E. Hence, we have

$$E_F(\mathrm{Tr}_E(\rho_{qqq})) = \min_{\{|\bar{k}\rangle\}} \sum_{\bar{k}} p_{\bar{k}} S(A)_{|\psi_{\bar{k}}\rangle} \tag{7}$$

where the minimum ranges over all families of (not necessarily normalised) vectors $|\bar{k}\rangle$ such that $\sum_{\bar{k}} |\bar{k}\rangle\langle\bar{k}| = I_E$ (this ensures that they form a measurement), $p_{\bar{k}} := |\langle\bar{k}|_E|\psi\rangle_{ABE}|^2$, and $|\psi_{\bar{k}}\rangle := \langle\bar{k}|_E|\psi\rangle_{ABE}/\sqrt{p_{\bar{k}}}$.

For any pair (i,j) of values held by Alice and Bob (with nonzero probability) we have $\mathrm{Tr}_{AB}\left[\rho_{qqq}\left(|ij\rangle\langle ij| \otimes I_E\right)\right] = p_{ij}|k\rangle\langle k|$, where $k = k(i,j)$ is the corresponding (unique) value held by Eve. Hence, the probability distribution of the state $\bar{\rho}_{ccc}$ obtained by applying the above measurement on Eve's system satisfies

$$q_{ij\bar{k}} := \mathrm{Tr}(|\psi\rangle\langle\psi|_{ABE}|ij\bar{k}\rangle\langle ij\bar{k}|) = p_{ijk} q_{\bar{k}|k} \ ,$$

[10] The *entanglement of formation* E_F is an entanglement measure defined for bipartite states by $E_F(\sigma_{AB}) := \min \sum_i p_i S(\mathrm{Tr}_B(\sigma^i_{AB}))$ where the minimum is taken over all ensembles $\{p_i, \sigma^i_{AB}\}$ with $\sum_i p_i \sigma^i_{AB} = \sigma_{AB}$ [38].

where $q_{\bar{k}|k} := \mathrm{Tr}(|\bar{k}\rangle\langle\bar{k}||k\rangle\langle k|)$. The intrinsic information is thus bounded by

$$I(A:B \downarrow E)_{\rho_{ccc}} \leq \min_{\{|\bar{k}\rangle\}} I(A:B|\bar{E})_{\bar{\rho}_{ccc}} \ ,$$

where $\bar{\rho}_{ccc}$ is the state defined above (depending on the choice of the vectors $|\bar{k}\rangle$). Moreover, using Holevo's bound, we find

$$I(A:B|\bar{E})_{\bar{\rho}_{ccc}} \leq \min_{\{|\bar{k}\}\rangle} \sum_{\bar{k}} p_{\bar{k}} S(A)_{|\psi_{\bar{k}}\rangle} \ .$$

The assertion then follows from (7). □

Because the intrinsic information is additive (i.e., it is equal to its regularised version), Theorem 9 also holds if the entanglement of formation E_F is replaced by the entanglement cost E_C.

The discussion above suggests that classical key distillation from ccc states can indeed by analysed by considering the corresponding qqq embedding of the state, but the original ccc state has to satisfy certain properties. This relation might be particularly useful for the study of bound information as discussed at the beginning of this section. In fact, there exist bound entangled states which satisfy the property required by Theorem 8 above [41].

5 On locking and pre-shared keys

In [30] it was observed that, by adding one bit of information to Eve, the (classical) intrinsic information can decrease by an arbitrarily large amount. In [16] it was shown that classical correlation measures of quantum states can exhibit a similar behaviour; more precisely, the accessible information can drop by an arbitrarily large amount when a single bit of information is lost. This phenomenon has been named *locking of information* or just *locking.* For tripartite states ρ_{ABE}, locking comes in two flavours: i) locking caused by removing information from Eve, ii) locking caused by removing information from Alice and/or Bob (and possibly giving it to Eve). Let us call those variants *E-locking* and *AB-locking*, respectively.

In [33] it was shown that entanglement cost as well as many other entanglement measures can be AB-locked. Further results show that squashed entanglement and entanglement of purification are also AB-lockable [34, 42]. So far the only known non-lockable entanglement measure is relative entropy of entanglement.

It was shown in [30] that distillable key is not E-lockable for classical states. In the sequel we extend this result and prove that the distillable key for quantum states ρ_{ABE} is not E-lockable, either. The proof proceeds along the lines of [30], replacing the bound of Csiszár and Körner by its quantum generalisations due to [10] (see also [11]). Let us emphasise that we leave open the question on whether distillable key is AB-lockable (even for ccc states).

Theorem 10. *Consider a state $\rho_{ABEE'}$ and let $\mathcal{P}$ be a key distillation protocol for ρ_{ABE} with rate $R_{\mathcal{P}}$. Then there exists another protocol $\mathcal{P}'$ for $\rho_{ABEE'}$ with rate $R_{\mathcal{P}'} \geq R_{\mathcal{P}} - 2S(\rho_{E'})$. If, in addition, E' is classical then $R_{\mathcal{P}'} \geq R_{\mathcal{P}} - S(\rho_{E'})$.*

Proof. For any fixed $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that the protocol $\mathcal{P}$ transforms $\rho_{ABE}^{\otimes n}$ into a ccq state σ_{ABE} which satisfies the following inequalities:

$$\|\sigma_{ABE} - \tau^{\ell}\| \leq \epsilon, \quad \frac{\ell}{n} \geq R_{\mathcal{P}} - \epsilon. \tag{8}$$

Suppose that Alice and Bob apply this map to the state $\rho_{ABEE'}^{\otimes n}$ (i.e., they try to distil key, as if the system E' was not present). The state $\rho_{ABEE'}^{\otimes n}$ is then transformed into some state $\sigma_{ABEE'}$ which traced out over E' is equal to the ccq state σ_{ABE}. Repeating this protocol m times results in $\sigma_{ABEE'}^{\otimes m}$, from which Alice and Bob can draw at least $m(I(A:B) - I(A:EE')) - o(m)$ bits of key by error correction and privacy amplification [10]. This defines a protocol $\mathcal{P}'$. To evaluate its rate, we use subadditivity of entropy which gives the estimate

$$I(A:EE')_\sigma \leq I(A:E)_\sigma + I(AE:E')_\sigma \ .$$

From (8) and Fannes' inequality we know that[11]

$$\begin{aligned} I(A:B)_\sigma &\geq \ell - 8\epsilon\ell - H(\epsilon) \\ I(A:E)_\sigma &\leq 8\epsilon\ell + H(\epsilon) \ . \end{aligned}$$

This together with (2) implies

$$K_D(\sigma_{ABEE'}) \geq I(A:B)_\sigma - I(A:EE')_\sigma \geq (1-16\epsilon)\ell - 2H(\epsilon) - I(AE:E')_\sigma \ .$$

To get the key rate of $\mathcal{P}'$, we divide the above by n and use (8),

$$R_{\mathcal{P}'} \geq \frac{1}{n}K_D(\sigma_{ABEE'}) \geq (1-16\epsilon)(R_{\mathcal{P}} - \epsilon) - \frac{1}{n}2H(\epsilon) - \frac{1}{n}I(AE:E')_\sigma \ .$$

Because this holds for any $\epsilon > 0$, the assertion follows from $I(AE:E')_\sigma \leq 2S(E')_\sigma = 2nS(E')_\rho$ and, if E' is classical, $I(AE:E')_\sigma \leq S(E')_\sigma = nS(E')_\rho$. □

Applying the above theorem to an optimal protocol leads to the statement that the key rate K_D is not E-lockable.

Corollary 4. *For any state $\rho_{ABEE'}$, $K_D(\rho_{ABEE'}) \geq K_D(\rho_{ABE}) - 2S(\rho_{E'})$ and, if E' is classical, $K_D(\rho_{ABEE'}) \geq K_D(\rho_{ABE}) - S(\rho_E')$.*

Consider now a situation where Alice and Bob have some pre-shared key U which is not known to Eve.

A major consequence of Theorem 10 is that a pre-shared key cannot be used as a catalyst to increase the key rate. More precisely, the corollary below implies that, for any protocol $\mathcal{P}$ that uses a pre-shared key held by Alice and Bob, there is another protocol $\mathcal{P}'$ which is as efficient as $\mathcal{P}'$ (with respect to the net key rate), but does not need a pre-shared key.

[11] $H(\epsilon)$ denotes the binary entropy, i.e., the Shannon entropy of the distribution $[\epsilon, 1-\epsilon]$.

Corollary 5. *Let $\mathcal{P}$ be a key distillation protocol for $\rho_{ABE} \otimes \tau^\ell$ where τ^ℓ is some additional ℓ-bit key shared by Alice and Bob. Then there exists another protocol $\mathcal{P}'$ for ρ_{ABE} with rate $R_{\mathcal{P}'} \geq R_{\mathcal{P}} - \ell$.*

Proof. Consider the state $\rho_{A'B'EE'}$ where E' is a system containing the value U of a uniformly distributed ℓ-bit key, $A' := (A, U)$, and $B' := (B, U)$. Note that $\rho_{A'B'E}$ is equivalent to $\rho_{ABE} \otimes \tau^\ell$. The assertion then follows from the observation that any protocol which produces a secure key starting from $\rho_{A'B'EE'}$ can easily be transformed into an (equally efficient) protocol which starts from ρ_{ABE}, because Alice and Bob can always generate public shared randomness. □

The following example shows that the factor 2 in Theorem 10 and Corollary 4 is strictly necessary. Let

$$\rho_{ABEE'} = \sum_{i=1}^{4} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes |\psi_i\rangle\langle\psi_i|_{EE'}$$

where $|\psi_i\rangle$ are the four Bell states on the bipartite system EE'. Then, obviously, $K_D(\rho_{ABEE'}) = 0$, but if E' (which is only *one* qubit) is lost, then $K_D(\rho_{ABE}) = 2$, since E is then maximally mixed conditioned on i. One recognises here the effect of superdense coding.

6 Classical and quantum adversaries in QKD

Up to now, we have considered an adversary with unbounded resources. Of course, if one limits the adversary's capabilities, certain cryptographic tasks might become easier. In the following, we will examine a situation where the adversary cannot store quantum states and, hence, is forced to apply a measurement, turning them into classical data. We will exhibit an example of a $2d$-dimensional ccq state which only has key rate 1, but if Eve is forced to measure her system, the key rate raises up to roughly $\frac{1}{2}\log d$.

Note that upper bounds on the key rate which are defined in terms of an optimal measurement on Eve's system (see, e.g., [26, 19] and Section 3) are also upper bounds on the key rate in a setting where Eve has no quantum memory. Hence, our result implies that these upper bounds are generally only rough estimates for the key rate in the unbounded scenario.

Consider the state

$$\rho_{AA'BB'E} = \frac{1}{2d}\sum_{k=1}^{d} |00\rangle\langle 00|_{AB}(|kk\rangle\langle kk|_{A'B'} \otimes |k\rangle\langle k|_E) \\ + |11\rangle\langle 11|_{AB}(|kk\rangle\langle kk|_{A'B'} \otimes U|k\rangle\langle k|_E U^\dagger)$$

where U is the quantum Fourier transform on d dimensions. (Such a state has been proposed in [16] to exhibit a locking effect of the accessible information. It also corresponds to the *flower state* of [33].)

It is easy to see that the bit in the system AB is uncorrelated to Eve's information and, hence, completely secret, i.e., $K_D(\rho_{AA'BB'E}) = K_D(\rho_{AB}) \geq 1$. On the other hand, if this bit is known to Eve then she has full knowledge on the state in $A'B'$, i.e., $K_D(\rho_{AA'BB'EE'}) \leq I(AA' : BB' \downarrow EE')_\rho = 0$, where E' is a classical system carrying the value of the bit in AB (see Theorem 2). From this and Corollary 4 (or, alternatively, Theorem 4), we conclude that the key rate (relative to an unbounded adversary) is given by

$$K_D(\rho_{AA'BB'E}) = K_D(\rho_{AB}) = 1 \ .$$

Let us now assume that Eve applies a measurement on her system E, transforming the state defined above into a ccc state $\sigma_{AA'BB'E}$. Because the values of Alice and Bob are maximally correlated, it is easy to see that the key rate of this state satisfies $K_D(\sigma_{AA'BB'E}) = S(A|E)_\sigma = S(A)_\sigma - I(A : E)_\sigma$. Note that $S(A)_\sigma = 1 + \log d$. Moreover, the mutual information $I(A : E)_\sigma$ for an optimal measurement on E corresponds to the so-called accessible information, which equals $\frac{1}{2} \log d$, as shown in [16]. We thus conclude that

$$K_D(\sigma_{AA'BB'E}) = 1 + \frac{1}{2} \log d \ .$$

Note that the accessible information is additive, so even if the measurements are applied to blocks of states, the amount of key that can be generated is given by this expression.

The above result gives some insights into the strength of attacks considered in the context of quantum key distribution (QKD). A so-called *individual attack* corresponds to a situation where the adversary transforms his information into classical values. In contrast, a *collective attack* is more general and allows the storage of quantum states.

As shown in [18], for most QKD protocols, security against collective attacks implies security against any attack allowed by the laws of quantum physics. The above result implies that the same is not true for individual attacks, i.e., these might be arbitrarily weaker than collective (and, hence, also general) attacks.

Acknowledgment

We are grateful to Karol Horodecki and Norbert Lütkenhaus for their valuable input and many enlightening discussions. We would also like to thank the anonymous reviewers for their helpful comments and suggestions. This work was supported by the European Commission through the FP6-FET Integrated Projects SCALA CT-015714 and QAP, and through SECOQC. MC acknowledges the support of an EPSRC Postdoctoral Fellowship and a Nevile Research Fellowship, which he holds at Magdalene College Cambridge. RR is supported by HP Labs Bristol.

References

1. Shannon, C.E.: Communication theory of secrecy systems. Bell Systems Technical Journal **28** (1949) 656–715
2. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory **39**(3) (1993) 733–742
3. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24** (1978) 339–348
4. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. IEEE Transactions on Information Theory **39**(4) (1993) 1121–1132
5. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, IEEE Computer Society Press, New York (1984) 175–179
6. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett **67** (1991) 661–663
7. Renner, R., Wolf, S.: New bounds in secret-key agreement: the gap between formation and secrecy extraction. In: Proceedings of EUROCRYPT 2003. Lecture Notes in Computer Science, Springer (2003) 562–577
8. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal **54**(8) (1975) 1355–1387
9. Gisin, N., Wolf, S.: Linking classical and quantum key agreement: is there 'bound information'. In: Advances in Cryptology — CRYPTO 2000. Lecture Notes in Computer Science, Springer (2000) 482–500
10. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. Roy. Soc. Lond. Ser. A **461** (2004) 207–235
11. Renner, R., König, R.: Universally composable privacy amplification against quantum adversaries. In: Second Theory of Cryptography Conference, TCC 2005. Volume 3378 of Lecture Notes in Computer Science., Springer (February 2005) 407–425
12. Cerf, N.J., Massar, S., Schneider, S.: Multipartite classical and quantum secrecy monotones. Phys. Rev. A **66** (2002) 042309
13. Maurer, U., Wolf, S.: The intrinsic conditional mutual information and perfect secrecy. In: Proceedings of the 1997 IEEE Symposium on Information Theory. (1997) 88
14. Horodecki, M.: Entanglement measures. Quantum Inf. Comp. **1** (2001) 3–26
15. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Secure key from bound entanglement. Phys. Rev. Lett **94** (2005) 160502
16. DiVincenzo, D., Horodecki, M., Leung, D., Smolin, J., Terhal, B.: Locking classical correlation in quantum states. Phys. Rev. Lett **92** (2004) 067902
17. Maurer, U., Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free. In: Advances in Cryptology — EUROCRYPT 2000. Volume 1807 of Lecture Notes in Computer Science., Springer (2000) 351–368
18. Renner, R.: Security of Quantum Key Distribution. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich (2005) quant-ph/0512258.
19. Christandl, M., Renner, R.: On intrinsic information. In: Proceedings of the 2004 IEEE International Symposion on Information Theory. (2004) 135
20. Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. In: Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Computer Science (2005) 386–406

21. König, R., Renner, R., Bariska, A., Maurer, U.: Locking of accessible information and implications for the security of quantum cryptography. quant-ph/0512021
22. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: General paradigm for distilling classical key from quantum states. quant-ph/0506189 (2005)
23. Horodecki, M., Horodecki, P., Horodecki, R.: Limits for entanglement measures. Phys. Rev. Lett **84** (2000) 2014
24. Donald, M., Horodecki, M., Rudolph, O.: The uniqueness theorem for entanglement measures. J. Math. Phys. **43** (2002) 4252–4272
25. Vidal, G., Werner, R.: A computable measure of entanglement. Phys. Rev. A **65** (2002) 032314
26. Moroder, T., Curty, M., Lütkenhaus, N.: Upper bound on the secret key rate distillable from effective quantum correlations with imperfect detectors. Phys. Rev. A **73** (2006) 012311
27. Christandl, M., Winter, A.: Squashed entanglement — an additive entanglement measure. J. Math. Phys. **45**(3) (2004) 829–840
28. Alicki, R., Fannes, M.: Continuity of conditional quantum mutual information. J. Phys. A **37** (2003)
29. Christandl, M.: The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography. PhD thesis, University of Cambridge (2006)
30. Renner, R., Wolf, S.: New bounds in secret-key agreement: The gap between formation and secrecy extraction. In: Advances in Cryptology - EUROCRYPT 2003, Lecture Notes in Computer Science, Springer (2003)
31. Vedral, V., Plenio, M.B., Rippin, M.A., Knight, P.L.: Quantifying entanglement. Phys. Rev. Lett **78** (1997) 2275–2279
32. Vedral, V., Plenio, M.B.: Entanglement measures and purification procedures. Phys. Rev. A **57** (1998) 1619–1633
33. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Locking entanglement with a single qubit. Phys. Rev. Lett **94** (2005) 200501
34. Christandl, M., Winter, A.: Uncertainty, monogamy and locking of quantum correlations. IEEE Transactions on Information Theory **51**(9) (2005) 3159–3165 quant-ph/0501090.
35. Bennett, C.H., DiVincenzo, D.P., Fuchs, C.A., Mor, T., Rains, E., Shor, P.W., Smolin, J., Wootters, W.K.: Quantum nonlocality without entanglement. Phys. Rev. A **59** (1999) 1070
36. Badziąg, P., Horodecki, M., Sen(De), A., Sen, U.: Universal Holevo-like bound for locally accesible information. Phys. Rev. Lett **91** (2003) 117901
37. Acin, A., Cirac, I., Massanes, L.: Multipartite bound information exists and can be activated. Phys. Rev. Lett. **92** (2004) 107903
38. Bennett, C.H., DiVincenzo, D.P., Smolin, J., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54** (1997) 3824–3851
39. Christandl, M.: The quantum analog to intrinsic information. Diploma Thesis, Institute for Theoretical Computer Science, ETH Zurich (2002)
40. Renner, R.: Linking information theoretic secret-key agreement and quantum purification. Diploma Thesis, Institute for Theoretical Computer Science, ETH Zurich (2000)
41. Horodecki, P., Lewenstein, M.: Bound entanglement and continuous variables. Phys. Rev. Lett **85** (2000) 2657
42. Winter, A.: Secret, public and quantum correlation cost of triples of random variables. In: Proceedings of the 2005 IEEE International Symposium on Information Theory. (2005) 2270–2274