Linking Classical and Quantum Key Agreement: Is There "Bound Information"?

Nicolas Gisin [1] and Stefan Wolf [2]

[1] Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland.
E-mail: Nicolas.Gisin@physics.unige.ch
[2] Department of Computer Science, ETH Zürich, CH-8092 Zürich, Switzerland.
E-mail: wolf@inf.ethz.ch

Abstract. After carrying out a protocol for quantum key agreement over a noisy quantum channel, the parties Alice and Bob must process the raw key in order to end up with identical keys about which the adversary has virtually no information. In principle, both classical and quantum protocols can be used for this processing. It is a natural question which type of protocols is more powerful. We show that the limits of tolerable noise are identical for classical and quantum protocols in many cases. More specifically, we prove that a quantum state between two parties is entangled if and only if the classical random variables resulting from optimal measurements provide some mutual classical information between the parties. In addition, we present evidence which strongly suggests that the potentials of classical and of quantum protocols are equal in every situation. An important consequence, in the purely classical regime, of such a correspondence would be the existence of a classical counterpart of so-called bound entanglement, namely "bound information" that cannot be used for generating a secret key by any protocol. This stands in sharp contrast to what was previously believed.

Keywords. Secret-key agreement, intrinsic information, secret-key rate, quantum privacy amplification, purification, entanglement.

1 Introduction

In modern cryptography there are mainly two security paradigms, namely computational and information-theoretic security. The latter is sometimes also called unconditional security. Computational security is based on the assumed hardness of certain computational problems (e.g., the integer-factoring or discrete-logarithm problems). However, since a computationally sufficiently powerful adversary can solve any computational problem, hence break any such system, and because no useful general lower bounds are known in complexity theory, computational security is always conditional and, in addition to this, in danger by progress in the theory of efficient algorithms as well as in hardware engineering (e.g., quantum computing). Information-theoretic security on the other hand is based on probability theory and on the fact that an adversary's information is limited. Such a limitation can for instance come from noise in communication channels or from the laws of quantum mechanics.

Many different settings based on noisy channels have been described and analyzed. Examples are Wyner's wire-tap channel [30], Csiszár and Körner's broadcast channel [7], or Maurer's model of key agreement from joint randomness [20], [22].

Quantum cryptography on the other hand lies in the intersection of two of the major scientific achievements of the 20th century, namely quantum physics and information theory. Various protocols for so-called quantum key agreement have been proposed (e.g., [3], [10]), and the possibility and impossibility of purification in different settings has been studied by many authors.

The goal of this paper is to derive parallels between classical and quantum key agreement and thus to show that the two paradigms are more closely related than previously recognized. These connections allow for investigating questions and solving open problems of purely classical information theory with quantum-mechanic methods. One of the possible consequences is that, in contrast to what was previously believed, there exists a classical counterpart to so-called *bound entanglement* (i.e., entanglement that cannot be purified by any quantum protocol), namely mutual information between Alice and Bob which they cannot use for generating a secret key by any classical protocol.

The outline of this paper is as follows. In Section 2 we introduce the classical (Section 2.1) and quantum (Section 2.2) models of information-theoretic key agreement and the crucial concepts and quantities, such as secret-key rate and intrinsic information on one side, and measurements, entanglement, and quantum privacy amplification on the other. In Section 3 we show the mentioned links between these two models, more precisely, between entanglement and intrinsic information (Section 3.1) as well as between quantum purification and the secret-key rate (Section 3.4). We illustrate the statements and their consequences with a number of examples (Sections 3.2 and 3.5). In Section 3.6 we define and characterize the classical counterpart of bound entanglement, called bound intrinsic information. Finally we show that not only problems in classical information theory can be addressed by quantum-mechanical methods, but that the inverse is also true: In Section 3.3 we propose a new measure for entanglement based on the intrinsic information measure.

2 Models of Information-Theoretically Secure Key Agreement

2.1 Key Agreement from Classical Information: Intrinsic Information and Secret-Key Rate

In this section we describe Maurer's general model of classical key agreement by public discussion from common information [20]. Here, two parties Alice and Bob who are willing to generate a secret key have access to repeated independent realizations of (classical) random variables X and Y, respectively, whereas an adversary Eve learns the outcomes of a random variable Z. Let P_{XYZ} be the joint distribution of the three random variables. In addition, Alice and Bob are connected by a noiseless and authentic but otherwise completely insecure channel. In this situation, the secret-key rate $S(X;Y||Z)$ has been defined as the maximal rate at which Alice and Bob can generate a secret key that is equal for Alice and Bob with overwhelming probability and about which Eve has only a negligible amount of (Shannon) information. For a detailed discussion of the general scenario and the secret-key rate as well as for various bounds on $S(X;Y||Z)$, see [20], [21], [22].

Bound (1) implies that if Bob's random variable Y provides more information about Alice's X than Eve's Z does (or vice versa), then this advantage can be exploited for generating a secret key:

$$S(X;Y||Z) \geq \max\{I(X;Y) - I(X;Z)\,,\, I(Y;X) - I(Y;Z)\}\ . \tag{1}$$

This is a consequence of a result by Csiszár and Körner [7]. It is somewhat surprising that this bound is not tight, in particular, that secret-key agreement can even be possible when the right-hand side of (1) vanishes or is negative. However, the positivity of the expression on the right-hand side of (1) is a necessary and sufficient condition for the possibility of secret-key agreement by *one-way communication*: Whenever Alice and Bob start in a disadvantageous situation with respect to Eve, *feedback* is necessary. The corresponding initial phase of the key-agreement protocol is then often called *advantage distillation* [20], [29].

The following upper bound on $S(X;Y||Z)$ is a generalization of Shannon's well-known impracticality theorem [28] and quantifies the intuitive fact that no information-theoretically secure key agreement is possible when Bob's information is independent from Alice's random variable, given Eve's information: $S(X;Y||Z) \leq I(X;Y|Z)$. However, this bound is not tight. Because it is a possible strategy of the adversary Eve to process Z, i.e., to send Z over some channel characterized by $P_{\overline{Z}|Z}$, we have for such a new random variable $\overline{Z}$ that $S(X;Y||Z) \leq I(X;Y|\overline{Z})$, and hence

$$S(X;Y||Z) \leq \min{}_{P_{\overline{Z}|Z}}\{I(X;Y|\overline{Z})\} =: I(X;Y{\downarrow}Z) \tag{2}$$

holds. The quantity $I(X;Y{\downarrow}Z)$ has been called the *intrinsic conditional information between X and Y given Z* [22]. It was conjectured, and evidence supporting this belief was given, that $S(X;Y||Z) > 0$ holds if $I(X;Y{\downarrow}Z) > 0$ does [22]. Some of the results below strongly suggest that this is true if one of the random variables X and Y is binary and the other one at most ternary, but false in general.

2.2 Quantum Key Agreement: Measurements, Entanglement, Purification

We assume that the reader is familiar with the basic quantum-theoretic concepts and notations. For an introduction, see for example [24].

In the context of quantum key agreement, the classical scenario P_{XYZ} is replaced by a quantum state vector[1] $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$, where $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_E$ are Hilbert spaces describing the systems in Alice's, Bob's, and Eve's hands, respectively. Then, measuring this quantum state by the three parties leads to a classical probability distribution. In the following, we assume that Eve is free to carry out so-called *generalized measurements* (POVMs) [24]. In other words, the set $\{|z\rangle\}$ will not be assumed to be an orthonormal basis, but any set generating the Hilbert space $\mathcal{H}_E$ and satisfying the condition $\sum_z |z\rangle\langle z| = \mathbb{1}_{\mathcal{H}_E}$. Then, if the three parties carry out measurements in certain (orthonormal) bases $\{|x\rangle\}$ and $\{|y\rangle\}$, and in the set $\{|z\rangle\}$, respectively, they end up with the classical scenario $P_{XYZ} = |\langle x, y, z|\Psi\rangle|^2$. Since this distribution depends on the chosen bases and set, a given quantum state Ψ does *not uniquely* determine a classical scenario: some measurements may lead to scenarios useful for Alice and Bob, whereas for Eve, some others may.

The analog of Alice and Bob's marginal distribution P_{XY} is the partial state ρ_{AB}, obtained by tracing over Eve's Hilbert space $\mathcal{H}_E$. More precisely, let $\Psi = \sum_{xyz} c_{xyz}|x, y, z\rangle$, where $|x, y, z\rangle$ is short for $|x\rangle \otimes |y\rangle \otimes |z\rangle$. We can write $\Psi = \sum_z \sqrt{P_Z(z)}\, \psi_z \otimes |z\rangle$, where P_Z denotes Eve's marginal distribution of P_{XYZ}. Then $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi) := \sum_z P_Z(z) P_{\psi_z}$, where P_{ψ_z} is the projector to the state vector ψ_z.

An important property is that ρ_{AB} is pure (i.e., $\rho_{AB}^2 = \rho_{AB}$) if and only if the global state Ψ factorizes, i.e., $\Psi = \psi_{AB} \otimes \psi_E$, where $\psi_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $\psi_E \in \mathcal{H}_E$. In this case Alice and Bob are independent of Eve: Eve cannot obtain any information on Alice's and Bob's states by measuring her system.

After a measurement, Alice and Bob obtain a classical distribution P_{XY}. In accordance with Landauer's principle that all information is ultimately physical, the classical scenario arises from a physical process, namely the measurements performed. Thus the quantum state Ψ, and not the distribution P_{XYZ}, is the true primitive. Note that only if also Eve performs a measurement, P_{XYZ} is at all defined. It is clear however that it might be advantageous (if technologically possible) for the adversary not to do any measurements before the public discussion. Because of this, staying in the quantum regime can simplify the analysis.

When Alice and Bob share many independent systems[2] ρ_{AB}, there are basically two possibilities for generating a secret key. Either they first measure their systems and then run a classical protocol (process classical information) secure against all measurements Eve could possibly perform (i.e., against all possible distributions P_{XYZ} that can result after Eve's measurement). Or they first run a quantum protocol (i.e., process the information in the quantum domain) and then perform their measurements. The idea of quantum protocols is to process the systems in state ρ_{AB} and to produce fewer systems in a pure state (i.e., to

[1] We consider pure states, since it is natural to assume that Eve controls all the environment outside Alice and Bob's systems.

[2] Here we do not consider the possibility that Eve coherently processes several of her systems. This corresponds to the assumption in the classical scenario that repeated realizations of X, Y, and Z are independent of each other.

purify ρ_{AB}), thus to eliminate Eve from the scenario. Moreover, the pure state Alice and Bob end up with should be maximally entangled (i.e., even for some different and incompatible measurements, Alice's and Bob's results are perfectly correlated). Finally, Alice and Bob measure their maximally entangled systems and establish a secret key. This way of obtaining a key directly from a quantum state Ψ, without any error correction nor classical privacy amplification, is called *quantum privacy amplification*[3] (QPA for short) [8], [2]. Note that the procedure described in [8] and [2] guarantees that Eve's *relative* information (relative to the key length) is arbitrarily small, but not that her *absolute* information is negligible. The analog of this problem in the classical case is discussed in [21].

The precise conditions under which a general state ρ_{AB} can be purified are not known. However, the two following conditions are necessary. First, the state must be *entangled* or, equivalently, *not separable*. A state ρ_{AB} is separable if and only if it can be written as a mixture of product states, i.e., $\rho_{AB} = \sum_j p_j \, \rho_{Aj} \otimes \rho_{Bj}$. Separable states can be generated by purely classical communication, hence it follows from bound (2) that entanglement is a necessary condition. The second condition is more subtle: The matrix ρ_{AB}^t obtained from ρ_{AB} by *partial transposition* must have at least one negative eigenvalue [17], [16]. The partial transposition of the density matrix ρ_{AB} is defined as $(\rho_{AB}^t)_{i,j;\mu,\nu} := (\rho_{AB})_{i,\nu;\mu,j}$, where the indices i and μ [j and ν] run through a basis of $\mathcal{H}_A$ [$\mathcal{H}_B$]. Note that this definition is base-dependent. However, the *eigenvalues* of ρ_{AB}^t are not [25]. The second of these conditions implies the first one: Negative partial transposition (i.e., at least one eigenvalue is negative) implies entanglement.

In the binary case ($\mathcal{H}_A$ and $\mathcal{H}_B$ both have dimension two), the above two conditions are equivalent and sufficient for the possibility of quantum key agreement: all entangled binary states can be purified. The same even holds if one Hilbert space is of dimension 2 and the other one of dimension 3. However, for larger dimensions there are examples showing that these conditions are not equivalent: There are entangled states whose partial transpose has no negative eigenvalue, hence cannot be purified [17]. Such states are called *bound entangled*, in contrast to *free entangled* states, which can be purified. Moreover, it is believed that there even exist entangled states which cannot be purified although they have negative partial transposition [9].

3 Linking Classical and Quantum Key Agreement

In this section we derive a close connection between the possibilities offered by classical and quantum protocols for key agreement. The intuition is as follows. As described in Section 2.2, there is a very natural connection between quantum states Ψ and classical distributions P_{XYZ} which can be thought of as arising

[3] The term "quantum privacy amplification" is somewhat unfortunate since it does not correspond to classical privacy amplification, but includes advantage distillation and error correction.

from Ψ by measuring in a certain basis, e.g., the standard basis[4]. (Note however that the connection is not unique even for fixed bases: For a given distribution P_{XYZ}, there are many states Ψ leading to P_{XYZ} by carrying out measurements.) When given a state Ψ between three parties Alice, Bob, and Eve, and if ρ_{AB} denotes the resulting mixed state after Eve is traced out, then the corresponding classical distribution P_{XYZ} has positive intrinsic information if and only if ρ_{AB} is entangled. However, this correspondence clearly depends on the measurement bases used by Alice, Bob, and Eve. If for instance ρ_{AB} is entangled, but Alice and Bob do very unclever measurements, then the intrinsic information may vanish. If on the other hand ρ_{AB} is separable, Eve may do such bad measurements that the intrinsic information becomes positive, despite the fact that ρ_{AB} could have been established by public discussion without any prior correlation (see Example 4). Consequently, the correspondence between intrinsic information and entanglement must involve some optimization over all possible measurements on all sides.

A similar correspondence on the protocol level is supported by many examples, but not rigorously proven: The distribution P_{XYZ} allows for classical key agreement if and only if quantum key agreement is possible starting from the state ρ_{AB}.

We show how these parallels allow for addressing problems of purely classical information-theoretic nature with the methods of quantum information theory, and vice versa.

3.1 Entanglement and Intrinsic Information

Let us first establish the connection between intrinsic information and entanglement. Theorem 1 states that if ρ_{AB} is separable, then Eve can "force" the information between Alice's and Bob's classical random variables (given Eve's classical random variable) to be zero (whatever strategy Alice and Bob use[5]). In particular, Eve can prevent classical key agreement.

Theorem 1 *Let $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$. If ρ_{AB} is separable, then there exists a generating set $\{|z\rangle\}$ of $\mathcal{H}_\mathcal{E}$ such that for all bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, respectively, $I(X;Y|Z) = 0$ holds for $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$.*

[4] A priori, there is no privileged basis. However, physicists often write states like ρ_{AB} in a basis which seems to be more natural than others. We refer to this as the standard basis. Somewhat surprisingly, this basis is generally easy to identify, though not precisely defined. One could characterize the standard basis as the basis for which as many coefficients as possible of Ψ are real and positive. We usually represent quantum states with respect to the standard basis.

[5] The statement of Theorem 1 also holds when Alice and Bob are allowed to do generalized measurements.

Proof. If ρ_{AB} is separable, then there exist vectors $|\alpha_z\rangle$ and $|\beta_z\rangle$ such that $\rho_{AB} = \sum_{z=1}^{n_z} p_z P_{\alpha_z} \otimes P_{\beta_z}$, where P_{α_z} denotes the one-dimensional projector onto the subspace spanned by $|\alpha_z\rangle$.

Let us first assume that $n_z \leq \dim \mathcal{H}_E$. Then there exists a basis $\{|z\rangle\}$ of $\mathcal{H}_E$ such that $\Psi = \sum_z \sqrt{p_z}\, |\alpha_z, \beta_z, z\rangle$ holds [23], [12], [19].

If $n_z > \dim \mathcal{H}_E$, then Eve can add an auxiliary system $\mathcal{H}_{aux}$ to hers (usually called an *ancilla*) and we have $\Psi \otimes |\gamma_0\rangle = \sum_z \sqrt{p_z}\, |\alpha_z, \beta_z, \gamma_z\rangle$, where $|\gamma_0\rangle \in \mathcal{H}_{aux}$ is the state of Eve's auxiliary system, and $\{|\gamma_z\rangle\}$ is a basis of $\mathcal{H}_E \otimes \mathcal{H}_{aux}$. We define the (not necessarily orthonormalized) vectors $|z\rangle$ by $|z, \gamma_0\rangle = \mathbb{1}_{\mathcal{H}_E} \otimes P_{\gamma_0} |\gamma_z\rangle$. These vectors determine a generalized measurement with positive operators $O_z = |z\rangle\langle z|$. Since $\sum_z O_z \otimes P_{\gamma_0} = \sum_z |z, \gamma_0\rangle\langle z, \gamma_0| = \sum_z \mathbb{1}_{\mathcal{H}_E} \otimes P_{\gamma_0} |\gamma_z\rangle\langle\gamma_z| \mathbb{1}_{\mathcal{H}_E} \otimes P_{\gamma_0} = \mathbb{1}_{\mathcal{H}_E} \otimes P_{\gamma_0}$, the O_z satisfy $\sum_z O_z = \mathbb{1}_{\mathcal{H}_E}$, as they should in order to define a generalized measurement [24]. Note that the first case ($n_z \leq \dim \mathcal{H}_E$) is a special case of the second one, with $|\gamma_z\rangle = |z, \gamma_0\rangle$. If Eve now performs the measurement, then we have $P_{XYZ}(x, y, z) = |\langle x, y, z|\Psi\rangle|^2 = |\langle x, y, \gamma_z|\Psi, \gamma_0\rangle|^2$, and

$$P_{XY|Z}(x, y, z) = |\langle x, y|\alpha_z, \beta_z\rangle|^2 = |\langle x|\alpha_z\rangle|^2\, |\langle y|\beta_z\rangle|^2 = P_{X|Z}(x, z) P_{Y|Z}(y, z)$$

holds for all $|z\rangle$ and for all $|x, y\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Consequently, $I(X; Y|Z) = 0$. □

Theorem 2 states that if ρ_{AB} is entangled, then Eve *cannot* force the intrinsic information to be zero: Whatever she does (i.e., whatever generalized measurements she carries out), there is something Alice and Bob can do such that the intrinsic information is positive. Note that this does *not*, a priori, imply that secret-key agreement is possible in every case. Indeed, we will provide evidence for the fact that this implication does generally *not* hold.

Theorem 2 *Let $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$. If ρ_{AB} is entangled, then for all generating sets $\{|z\rangle\}$ of $\mathcal{H}_\mathcal{E}$, there are bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, respectively, such that $I(X; Y \downarrow Z) > 0$ holds for $P_{XYZ}(x, y, z) := |\langle x, y, z|\Psi\rangle|^2$.*

Proof. We prove this by contradiction. Assume that there exists a generating set $\{|z\rangle\}$ of $\mathcal{H}_E$ such that for all bases $\{|x\rangle\}$ of $\mathcal{H}_A$ and $\{|y\rangle\}$ of $\mathcal{H}_B$, we have $I(X; Y \downarrow Z) = 0$ for the resulting distribution. For such a distribution, there exists a channel, characterized by $P_{\overline{Z}|Z}$, such that $I(X; Y|\overline{Z}) = 0$ holds, i.e.,

$$P_{XY|\overline{Z}}(x, y, \overline{z}) = P_{X|\overline{Z}}(x, \overline{z}) P_{Y|\overline{Z}}(y, \overline{z}) \ . \tag{3}$$

Let $\rho_{\overline{z}} := (1/p_{\overline{z}}) \sum_z p_z P_{\overline{Z}|Z}(\overline{z}, z) P_{\psi_z}$, $p_z = P_Z(z)$, and $p_{\overline{z}} = \sum_z P_{\overline{Z}|Z}(\overline{z}, z) p_z$, where ψ_z is the state of Alice's and Bob's system conditioned on Eve's result z: $\Psi \otimes |\gamma_0\rangle = \sum_z \psi_z \otimes |\gamma_z\rangle$ (see the proof of Theorem 1).

From (3) we can conclude $\mathrm{Tr}(P_x \otimes P_y \rho_{\overline{z}}) = \mathrm{Tr}(P_x \otimes \mathbb{1} \rho_{\bar{z}})\,\mathrm{Tr}(\mathbb{1} \otimes P_y \rho_{\overline{z}})$ for all one-dimensional projectors P_x and P_y acting in $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, respectively. Consequently, the states $\rho_{\overline{z}}$ are products, i.e., $\rho_{\overline{z}} = \rho_{\alpha_{\overline{z}}} \otimes \rho_{\beta_{\overline{z}}}$, and $\rho_{AB} = \sum_{\bar{z}} p_{\bar{z}} \rho_{\bar{z}}$

is separable. □

Theorem 2 can be formulated in a more positive way. Let us first introduce the concept of a set of bases $(\{|x\rangle\}_j, \{|y\rangle\}_j)$, where the j label the different bases, as they are used in the 4-state (2 bases) and the 6-state (3 bases) protocols [3], [4], [1]. Then if ρ_{AB} is entangled there exists a set $(\{|x\rangle\}_j, \{|y\rangle\}_j)_{j=1,\ldots,N}$ of N bases such that for all generalized measurements $\{|z\rangle\}$, $I(X;Y \downarrow [Z,j]) > 0$ holds. The idea is that Alice and Bob randomly choose a basis and, after the transmission, publicly restrict to the (possibly few) cases where they happen to have chosen the same basis. Hence Eve knows j, and one has

$$I(X;Y \downarrow [Z,j]) = \frac{1}{N} \sum_{j=1}^{N} I(X^j;Y^j \downarrow Z) \ .$$

If the set of bases is large enough, then for all $\{|z\rangle\}$ there is a basis with positive intrinsic information, hence the mean is also positive. Clearly, this result is stronger if the set of bases is small. Nothing is proven about the achievable size of such sets of bases, but it is conceivable that $\max\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$ bases are always sufficient.

Corollary 3 *Let $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$. Then the following statements are equivalent:*

(i) ρ_{AB} is entangled,

(ii) for all generating sets $\{|z\rangle\}$ of $\mathcal{H}_E$, there exist bases $\{|x\rangle\}$ of $\mathcal{H}_A$ and $\{|y\rangle\}$ of $\mathcal{H}_B$ such that the distribution $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$ satisfies $I(X;Y{\downarrow}Z) > 0$,

(iii) for all generating sets $\{|z\rangle\}$ of $\mathcal{H}_E$, there exist bases $\{|x\rangle\}$ of $\mathcal{H}_A$ and $\{|y\rangle\}$ of $\mathcal{H}_B$ such that the distribution $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$ satisfies $I(X;Y|Z) > 0$.

A first consequence of the fact that Corollary 3 often holds with respect to the standard bases (see below) is that it yields, at least in the binary case, a criterion for $I(X;Y{\downarrow}Z) > 0$ that is efficiently verifiable since it is based on the positivity of the eigenvalues of a 4×4 matrix. Previously, the quantity $I(X;Y{\downarrow}Z)$ has been considered hard to handle.

3.2 Examples I

The following examples illustrate the correspondence established in Section 3.1. They show in particular that very often (Examples 1, 2, and 3), but not always (Example 4), the direct connection between entanglement and positive intrinsic information holds with respect to the standard bases (i.e., the bases physicists use by commodity and intuition). Example 1 was already analyzed in [15]. The examples of this section will be discussed further in Section 3.5 under the aspect of the existence of key-agreement protocols in the classical and quantum regimes.

Example 1. Let us consider the so-called 4-state protocol of [3]. The analysis of the 6-state protocol [1] is analogous and leads to similar results. We compare the possibility of quantum and classical key agreement given the quantum state and the corresponding classical distribution, respectively, arising from this protocol. The conclusion is, under the assumption of incoherent eavesdropping, that key agreement in one setting is possible if and only if this is true also for the other.

After carrying out the 4-state protocol, and under the assumption of optimal eavesdropping (in terms of Shannon information), the resulting quantum state is [11]

$$\Psi = \sqrt{F/2}\,|0,0\rangle \otimes \xi_{00} + \sqrt{D/2}\,|0,1\rangle \otimes \xi_{01} + \sqrt{D/2}\,|1,0\rangle \otimes \xi_{10} + \sqrt{F/2}\,|1,1\rangle \otimes \xi_{11}\ ,$$

where D (the *disturbance*) is the probability that $X \neq Y$ holds if X and Y are the classical random variables of Alice and Bob, respectively, where $F = 1 - D$ (the *fidelity*), and where the ξ_{ij} satisfy $\langle \xi_{00}|\xi_{11}\rangle = \langle \xi_{01}|\xi_{10}\rangle = 1-2D$ and $\langle \xi_{ii}|\xi_{ij}\rangle = 0$ for all $i \neq j$. Then the state ρ_{AB} is (in the basis $\{|\,00\,\rangle,\ |\,01\,\rangle,\ |\,10\,\rangle,\ |\,11\,\rangle\}$)

$$\rho_{AB} = \frac{1}{2}\begin{pmatrix} D & 0 & 0 & -D(1-2D) \\ 0 & 1-D & -(1-D)(1-2D) & 0 \\ 0 & -(1-D)(1-2D) & 1-D & 0 \\ -D(1-2D) & 0 & 0 & D \end{pmatrix}\ ,$$

and its partial transpose

$$\rho_{AB}^{t} = \frac{1}{2}\begin{pmatrix} D & 0 & 0 & -(1-D)(1-2D) \\ 0 & 1-D & -D(1-2D) & 0 \\ 0 & -D(1-2D) & 1-D & 0 \\ -(1-D)(1-2D) & 0 & 0 & D \end{pmatrix}$$

has the eigenvalues $(1/2)(D \pm (1-D)(1-2D))$ and $(1/2)((1-D) \pm D(1-2D))$, which are all non-negative (i.e., ρ_{AB} is separable) if

$$D \geq 1 - \frac{1}{\sqrt{2}}\ . \tag{4}$$

From the classical viewpoint, the corresponding distributions (arising from measuring the above quantum system in the standard bases) are as follows. First, X and Y are both symmetric bits with $\text{Prob}\,[X \neq Y] = D$. Eve's random variable $Z = [Z_1, Z_2]$ is composed of 2 bits Z_1 and Z_2, where $Z_1 = X \oplus Y$, i.e., Z_1 tells Eve whether Bob received the qubit disturbed ($Z_1 = 1$) or not ($Z_1 = 0$) (this is a consequence of the fact that the ξ_{ii} and ξ_{ij} ($i \neq j$) states generate orthogonal subspaces), and where the probability that Eve's second bit indicates the correct value of Bob's bit is $\text{Prob}[Z_2 = Y] = \delta = (1 + \sqrt{1 - \langle \xi_{00}|\xi_{11}\rangle^2})/2 = 1/2 + \sqrt{D(1-D)}$. We now prove that for this distribution, the intrinsic information is zero if and only if

$$\frac{D}{1-D} \geq 2\sqrt{(1-\delta)\delta} = 1 - 2D \tag{5}$$

holds. We show that if the condition (5) is satisfied, then $I(X;Y{\downarrow}Z)=0$ holds. The inverse implication follows from the existence of a key-agreement protocol in all other cases (see Example 1 (cont'd) in Section 3.5). If (5) holds, we can construct a random variable $\overline{Z}$, that is generated by sending Z over a channel characterized by $P_{\overline{Z}|Z}$, for which $I(X;Y|\overline{Z})=0$ holds. We can restrict ourselves to the case of equality in (5) because Eve can always increase δ by adding noise.

Consider now the channel characterized by the following conditional distribution $P_{\overline{Z}|Z}$ (where $\overline{\mathcal{Z}}=\{u,v\}$):

$$P_{\overline{Z}|Z}(u,[0,0]) = P_{\overline{Z}|Z}(v,[0,1]) = 1 \ ,$$
$$P_{\overline{Z}|Z}(l,[1,0]) = P_{\overline{Z}|Z}(l,[1,1]) = 1/2$$

for $l\in\{u,v\}$. We show $I(X;Y|\overline{Z}) = \mathrm{E}_{\overline{Z}}[I(X;Y|\overline{Z}=\overline{z})] = 0$, i.e., that $I(X;Y|\overline{Z}=u)=0$ and $I(X;Y|\overline{Z}=v)=0$ hold. By symmetry it is sufficient to show the first equality. For $a_{ij} := P_{XY\overline{Z}}(i,j,u)$, we get

$$a_{00} = (1-D)(1-\delta)/2\,,\ a_{11} = (1-D)\delta/2\,,\ a_{01} = a_{10} = (D(1-\delta)/2+D\delta/2)/2 = D/4\,.$$

From equality in (5) we conclude $a_{00}a_{11} = a_{01}a_{10}$, which is equivalent to the fact that X and Y are independent, given $\overline{Z}=u$.

Finally, note that the conditions (4) and (5) are equivalent for $D\in[0,1/2]$. This shows that the bounds of tolerable noise are indeed the same for the quantum and classical scenarios. $\diamondsuit$

Example 2. We consider the bound entangled state presented in [17]. This example received quite a lot of attention by the quantum-information community because it was the first known example of bound entanglement (i.e., entanglement without the possibility of quantum key agreement). We show that its classical counterpart seems to have similarly surprising properties. Let $0<a<1$ and

$$\Psi = \sqrt{\frac{3a}{8a+1}}\,\psi\otimes|0\rangle+\sqrt{\frac{1}{8a+1}}\,\phi_a\otimes|1\rangle+\sqrt{\frac{a}{8a+1}}\,(|122\rangle+|133\rangle+|214\rangle+|235\rangle+|326\rangle)\ ,$$

where $\psi = (|11\rangle+|22\rangle+|33\rangle)/\sqrt{3}$ and $\phi_a = \sqrt{(1+a)/2}\,|31\rangle+\sqrt{(1-a)/2}\,|33\rangle$. It has been shown in [17] that the resulting state ρ_{AB} is entangled.

The corresponding classical distribution is as follows. The ranges are $\mathcal{X} = \mathcal{Y} = \{1,2,3\}$ and $\mathcal{Z} = \{0,1,2,3,4,5,6\}$. We write $(ijk) = P_{XYZ}(i,j,k)$. Then we have $(110) = (220) = (330) = (122) = (133) = (214) = (235) = (326) = 2a/(16a+2)$, $(311) = (1+a)/(16a+2)$, and $(331) = (1-a)/(16a+2)$. We study the special case $a=1/2$. Consider the following representation of the resulting distribution (to be normalized). For instance, the entry "(0) 1 , (1) 1/2" for $X=Y=3$ means $P_{XYZ}(3,3,0) = 1/10$ (normalized), $P_{XYZ}(3,3,1) = 1/20$, and $P_{XYZ}(3,3,z) = 0$ for all $z\notin\{0,1\}$.

X / Y (Z)	1	2	3
1	(0) 1	(4) 1	(1) 3/2
2	(2) 1	(0) 1	(6) 1
3	(3) 1	(5) 1	(0) 1 (1) 1/2

As we would expect, the intrinsic information is positive in this scenario. This can be seen by contradiction as follows. Assume $I(X;Y{\downarrow}Z) = 0$. Hence there exists a discrete channel, characterized by the conditional distribution $P_{\overline{Z}|Z}$, such that $I(X;Y|\overline{Z}) = 0$ holds. Let $\overline{\mathcal{Z}} \subseteq \mathbf{N}$ be the range of $\overline{Z}$, and let $P_{\overline{Z}|Z}(i,0) =: a_i$, $P_{\overline{Z}|Z}(i,1) =: x_i$, $P_{\overline{Z}|Z}(i,6) =: s_i$. Then we must have $a_i, x_i, s_i \in [0,1]$ and $\sum_i a_i = \sum_i x_i = \sum_i s_i = 1$. Using $I(X;Y|\overline{Z}) = 0$, we obtain the following distributions $P_{XY|\overline{Z}=i}$ (to be normalized):

X / Y	1	2	3
1	a_i	$\frac{3a_ix_i}{2s_i}$	$\frac{3x_i}{2}$
2	$\frac{2a_is_i}{3x_i}$	a_i	s_i
3	$\frac{2a_i(a_i+x_i/2)}{3x_i}$	$\frac{a_i(a_i+x_i/2)}{s_i}$	$a_i + \frac{x_i}{2}$

By comparing the $(2,3)$-entries of the two tables above, we obtain

$$1 \geq \sum_i \frac{a_i(a_i + x_i/2)}{s_i} \ . \tag{6}$$

We prove that (6) implies $s_i \equiv a_i$ (i.e., $s_i = a_i$ for all i) and $x_i \equiv 0$. Clearly, this does not lead to a solution and is hence a contradiction. For instance, $P_{XY|\overline{Z}=i}(1,2) = 2a_is_i/3x_i$ is not even defined in this case if $a_i > 0$.

It remains to show that (6) implies $a_i \equiv s_i$ and $x_i \equiv 0$. We show that whenever $\sum_i a_i = \sum_i s_i = 1$ and $a_i \not\equiv s_i$, then $\sum_i a_i^2/s_i > 1$. First, note that $\sum_i a_i^2/s_i = \sum_i a_i = 1$ for $a_i \equiv s_i$. Let now $s_{i_1} \leq a_{i_1}$ and $s_{i_2} \geq a_{i_2}$. We show that $a_{i_1}^2/s_{i_1} + a_{i_2}^2/s_{i_2} < a_{i_1}^2/(s_{i_1} - \varepsilon) + a_{i_2}^2/(s_{i_2} + \varepsilon)$ holds for every $\varepsilon > 0$, which obviously implies the above statement. It is straightforward to see that this is equivalent to $a_{i_1}^2 s_{i_2}(s_{i_2} + \varepsilon) > a_{i_2}^2 s_{i_1}(s_{i_1} - \varepsilon)$, and holds because of $a_{i_1}^2 s_{i_2}(s_{i_2} + \varepsilon) > a_{i_1}^2 a_{i_2}^2$ and $a_{i_2}^2 s_{i_1}(s_{i_1} - \varepsilon) < a_{i_1}^2 a_{i_2}^2$. This concludes the proof of $I(X;Y{\downarrow}Z) > 0$. $\diamondsuit$

As mentioned, the interesting point about Example 2 is that the quantum state is bound entangled, and that also classical key agreement seems impossible despite the fact that $I(X;Y{\downarrow}Z) > 0$ holds. This is a contradiction to a conjecture stated in [22]. The classical translation of the bound entangled state leads to a classical distribution with very strange properties as well! (See Example 2 (cont'd) in Section 3.5).

In Example 3, another bound entangled state (first proposed in [18]) is discussed. The example is particularly nice because, depending on the choice of a parameter α, the quantum state can be made separable, bound entangled, and free entangled.

Example 3. We consider the following distribution (to be normalized). Let $2 \leq \alpha \leq 5$.

X / Y (Z)	1	2	3
1	(0) 2	(4) $5-\alpha$	(3) α
2	(1) α	(0) 2	(5) $5-\alpha$
3	(6) $5-\alpha$	(2) α	(0) 2

This distribution arises when measuring the following quantum state. Let $\psi := (1/\sqrt{3})\,(|11\rangle + |22\rangle + |33\rangle)$. Then

$$\begin{aligned} \Psi &= \sqrt{\frac{2}{7}}\,\psi \otimes |0\rangle + \sqrt{\frac{a}{21}}\,(|12\rangle \otimes |1\rangle + |23\rangle \otimes |2\rangle + |31\rangle \otimes |3\rangle) \\ &\quad + \sqrt{\frac{5-a}{21}}\,(|21\rangle \otimes |4\rangle + |32\rangle \otimes |5\rangle + |13\rangle \otimes |6\rangle), \qquad \text{and} \\ \rho_{AB} &= \frac{2}{7}\,P_\psi + \frac{a}{21}\,(P_{12} + P_{23} + P_{31}) + \frac{5-a}{21}\,(P_{21} + P_{32} + P_{13}) \end{aligned}$$

is separable if and only if $\alpha \in [2,3]$, bound entangled for $\alpha \in (3,4]$, and free entangled if $\alpha \in (4,5]$ [18] (see Figure 1).

Let us consider the quantity $I(X;Y\!\downarrow\! Z)$. First of all, it is clear that $I(X;Y\!\downarrow\! Z) = 0$ holds for $\alpha \in [2,3]$. The reason is that $\alpha \geq 2$ and $5-\alpha \geq 2$ together imply that Eve can "mix" her symbol $Z = 0$ with the remaining symbols in such a way that when given that $\overline{Z}$ takes the "mixed value," then XY is uniformly distributed; in particular, X and Y are independent. Moreover, it can be shown in analogy to Example 2 that $I(X;Y\!\downarrow\! Z) > 0$ holds for $\alpha > 3$. $\diamondsuit$

Examples 1, 2, and 3 suggest that the correspondence between separability and entanglement on one side and vanishing and non-vanishing intrinsic information on the other always holds with respect to the standard bases or even arbitrary bases. This is however not true in general: Alice and Bob as well as Eve can perform bad measurements and give away an initial advantage. The following is a simple example where measuring in the standard basis is a bad choice for Eve.

Example 4. Let us consider the quantum states

$$\Psi = \frac{1}{\sqrt{5}}\,(|00+01+10\rangle \otimes |0\rangle + |00+11\rangle \otimes |1\rangle)\,, \quad \rho_{AB} = \frac{3}{5}\,P_{|00+01+10\rangle} + \frac{2}{5}\,P_{|00+11\rangle}\,.$$

If Alice, Bob, and Eve measure in the standard bases, we get the classical distribution (to be normalized)

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

For this distribution, $I(X;Y{\downarrow}Z) > 0$ holds. Indeed, even $S(X;Y||Z) > 0$ holds. This is not surprising since both X and Y are binary, and since the described parallels suggest that in this case, positive intrinsic information implies that a secret-key agreement protocol exists.

The proof of $S(X;Y||Z) > 0$ in this situation is analogous to the proof of this fact in Example 3. The protocol consists of Alice and Bob independently making their bits symmetric. Then the repeat-code protocol can be applied.

However, the partial-transpose condition shows that ρ_{AB} is separable. This means that measuring in the standard basis is bad for Eve. Indeed, let us rewrite Ψ and ρ_{AB} as

$$\Psi = \sqrt{\Lambda}\,|m,m\rangle \otimes |\tilde{0}\rangle + \sqrt{1-\Lambda}\,|-m,-m\rangle \otimes |\tilde{1}\rangle \ ,$$
$$\rho_{AB} = \frac{5+\sqrt{5}}{10}\,P_{|m,m\rangle} + \frac{5-\sqrt{5}}{10}\,P_{|-m,-m\rangle} \ ,$$

where $\Lambda = (5+\sqrt{5})/10$, $|m,m\rangle = |m\rangle \otimes |m\rangle$, $|\pm m\rangle = \sqrt{(1\pm\eta)/2}\,|0\rangle \pm \sqrt{(1\mp\eta)/2}\,|1\rangle$, and $\eta = 1/\sqrt{5}$.

In this representation, ρ_{AB} is obviously separable. It also means that Eve's optimal measurement basis is

$$|\tilde{0}\rangle = \sqrt{\Lambda}\,|0\rangle - \frac{1}{\sqrt{5\Lambda}}\,|1\rangle \ , \quad |\tilde{1}\rangle = -\sqrt{1-\Lambda}\,|0\rangle - \frac{1}{\sqrt{5(1-\Lambda)}}\,|1\rangle \ .$$

Then, $I(X;Y{\downarrow}Z) = 0$ holds for the resulting classical distribution. ◊

3.3 A Classical Measure for Quantum Entanglement

It is a challenging problem of theoretical quantum physics to find good measures for entanglement [26]. Corollary 3 above suggests the following measure, which is based on classical information theory.

Definition 1 Let for a quantum state ρ_{AB}

$$\mu(\rho_{AB}) := \min_{\{|z\rangle\}} \big(\max_{\{|x\rangle\},\{|y\rangle\}} (I(X;Y{\downarrow}Z)) \big) \ ,$$

where the minimum is taken over all $\Psi = \sum_z \sqrt{p_z}\psi_z \otimes |z\rangle$ such that $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$ holds and over all generating sets $\{|z\rangle\}$ of $\mathcal{H}_E$, the maximum is over all bases $\{|x\rangle\}$ of $\mathcal{H}_A$ and $\{|y\rangle\}$ of $\mathcal{H}_B$, and where $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$. ○

The function μ has all the properties required from such a measure. If ρ_{AB} is pure, i.e., $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, then we have in the Schmidt basis (see for example [24]) $\psi_{AB} = \sum_j c_j|x_j, y_j\rangle$, and $\mu(\rho_{AB}) = -\mathrm{Tr}(\rho_A \log \rho_A)$ (where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$) as it should [26]. It is obvious that μ is convex, i.e., $\mu(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda\mu(\rho_1) + (1-\lambda)\mu(\rho_2)$.

Example 5. This example is based on Werner's states. Let $\Psi = \sqrt{\lambda}\,\psi^{(-)} \otimes |0\rangle + \sqrt{(1-\lambda)/4}\,|001 + 012 + 103 + 114\rangle$, where $\psi^{(-)} = |10 - 01\rangle/\sqrt{2}$, and $\rho_{AB} = \lambda P_{\psi^{(-)}} + ((1-\lambda)/4)\mathbf{1}$. It is well-known that ρ_{AB} is separable if and only if $\lambda \leq 1/3$. Then the classical distribution is $P(010) = P(100) = \lambda/2$ and $P(001) = P(012) = P(103) = P(114) = (1-\lambda)/4$.

If $\lambda \leq 1/3$, then consider the channel $P_{\overline{Z}|Z}(0,0) = P_{\overline{Z}|Z}(2,2) = P_{\overline{Z}|Z}(3,3) = 1\,,\ P_{\overline{Z}|Z}(0,1) = P_{\overline{Z}|Z}(0,4) = \xi\,,\ P_{\overline{Z}|Z}(1,1) = P_{\overline{Z}|Z}(4,4) = 1-\xi\,,$ where $\xi = 2\lambda/(1-\lambda) \leq 1$. Then $\mu(\rho_{AB}) = I(X;Y{\downarrow}Z) = I(X;Y|\overline{Z}) = 0$ holds, as it should.

If $\lambda > 1/3$, then consider the (obviously optimal) channel $P_{\overline{Z}|Z}(0,0) = P_{\overline{Z}|Z}(2,2) = P_{\overline{Z}|Z}(3,3) = P_{\overline{Z}|Z}(0,1) = P_{\overline{Z}|Z}(0,4) = 1$. Then

$$\begin{aligned}\mu(\rho_{AB}) = I(X;Y{\downarrow}Z) = I(X;Y|\overline{Z}) &= P_{\overline{Z}}(0) \cdot I(X;Y|\overline{Z}=0) \\ &= \frac{1+\lambda}{2} \cdot (1 - q\log_2 q - (1-q)\log_2(1-q))\ ,\end{aligned}$$

where $q = 2\lambda/(1+\lambda)$. $\diamondsuit$

3.4 Classical Protocols and Quantum Privacy Amplification

It is a natural question whether the analogy between entanglement and intrinsic information (see Section 3.1) carries over to the protocol level. The examples given in Section 3.5 support this belief. A quite interesting and surprising consequence would be that there exists a classical counterpart to bound entanglement, namely intrinsic information that cannot be distilled into a secret key by any classical protocol, if $|\mathcal{X}| + |\mathcal{Y}| > 5$, where $\mathcal{X}$ and $\mathcal{Y}$ are the ranges of X and Y, respectively. In other words, the conjecture in [22] that such information can always be distilled would be *proved* for $|\mathcal{X}| + |\mathcal{Y}| \leq 5$, but *disproved* otherwise.

Conjecture 1 *Let $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$. Assume that for all generating sets $\{|z\rangle\}$ of $\mathcal{H}_E$ there are bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, such that $S(X;Y||Z) > 0$ holds for the distribution $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$. Then quantum privacy amplification is possible with the state ρ_{AB}, i.e., ρ_{AB} is free entangled.*

Conjecture 2 *Let $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and $\rho_{AB} = \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi)$. Assume that there exists a generating set $\{|z\rangle\}$ of $\mathcal{H}_E$ such that for all bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, $S(X;Y||Z) = 0$ holds for the distribution $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$. Then quantum privacy amplification is impossible with the state ρ_{AB}, i.e., ρ_{AB} is bound entangled or separable.*

3.5 Examples II

The following examples support Conjectures 1 and 2 and illustrate their consequences. We consider mainly the same distributions as in Section 3.2, but this time under the aspect of the existence of classical and quantum key-agreement protocols.

Example 1 (cont'd). We have shown in Section 3.2 that the resulting quantum state is entangled if and only if the intrinsic information of the corresponding classical situation (with respect to the standard bases) is non-zero. Such a correspondence also holds on the protocol level. First of all, it is clear for the quantum state that QPA is possible whenever the state is entangled because both $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension two. On the other hand, the same is also true for the corresponding classical situation, i.e., secret-key agreement is possible whenever $D/(1-D) < 2\sqrt{(1-\delta)\delta}$ holds, i.e., if the intrinsic information is positive. The necessary protocol includes an interactive phase, called *advantage distillation*, based on a repeat code or on parity checks (see [20] or [29]). $\diamondsuit$

Example 2 (cont'd). The quantum state ρ_{AB} in this example is bound entangled, meaning that the entanglement cannot be used for QPA. Interestingly, but not surprisingly given the discussion above, the corresponding classical distribution has the property that $I(X;Y{\downarrow}Z) > 0$, but nevertheless, all the known classical advantage-distillation protocols [20], [22] fail for this distribution! It seems that $S(X;Y||Z) = 0$ holds (although it is not clear how this fact could be rigorously proven). $\diamondsuit$

Example 3 (cont'd). We have seen already that for $2 \leq \alpha \leq 3$, the quantum state is separable and the corresponding classical distribution (with respect to the standard bases) has vanishing intrinsic information. Moreover, it has been shown that for the quantum situation, $3 < \alpha \leq 4$ corresponds to bound entanglement, whereas for $\alpha > 4$, QPA is possible and allows for generating a secret key [18]. We describe a classical protocol here which suggests that the situation for the classical translation of the scenario is totally analogous: The protocol allows classical key agreement exactly for $\alpha > 4$. However, this does not imply (although it appears very plausible) that no classical protocol exists at all for the case $\alpha \leq 4$.

Let $\alpha > 4$. We consider the following protocol for classical key agreement. First of all, Alice and Bob both restrict their ranges to $\{1, 2\}$ (i.e., publicly reject a realization unless $X \in \{1, 2\}$ and $Y \in \{1, 2\}$). The resulting distribution is as follows (to be normalized):

X / Y (Z)	1	2
1	(0) 2	(4) $5-\alpha$
2	(2) α	(0) 2

Then, Alice and Bob both send their bits locally over channels $P_{\overline{X}|X}$ and $P_{\overline{Y}|Y}$, respectively, such that the resulting bits $\overline{X}$ and $\overline{Y}$ are symmetric. The channel $P_{\overline{X}|X}$ $[P_{\overline{Y}|Y}]$ sends $X = 0$ $[Y = 1]$ to $\overline{X} = 1$ $[\overline{Y} = 0]$ with probability $(2\alpha - 5)/(2\alpha + 4)$, and leaves X $[Y]$ unchanged otherwise. The distribution $P_{\overline{X}\overline{Y}Z}$ is then

$\overline{Y}$ (Z) \ $\overline{X}$	1	2
1	(0) $2 \cdot \frac{9}{2\alpha+4}$ (2) $\alpha \cdot \frac{9}{2\alpha+4} \cdot \frac{2\alpha-5}{2\alpha+4}$	(1) $5 - \alpha$ (2) $\alpha \left(\frac{2\alpha-5}{2\alpha+4}\right)^2$ (0) $2 \cdot 2 \cdot \frac{2\alpha-5}{2\alpha+4}$
2	(2) $\alpha \left(\frac{9}{2\alpha+4}\right)^2$	(0) $2 \cdot \frac{9}{2\alpha+4}$ (2) $\alpha \cdot \frac{9}{2\alpha+4} \cdot \frac{2\alpha-5}{2\alpha+4}$

It is not difficult to see that for $\alpha > 4$, we have $\text{Prob}[\overline{X} = \overline{Y}] > 1/2$ and that, given that $\overline{X} = \overline{Y}$ holds, Eve has no information at all about what this bit is. This means that the repeat-code protocol mentioned in Example 1 allows for classical key agreement in this situation [20], [29]. For $\alpha \leq 4$, classical key agreement, like quantum key agreement, seems impossible however. The results of Example 3 are illustrated in Figure 1. $\diamondsuit$

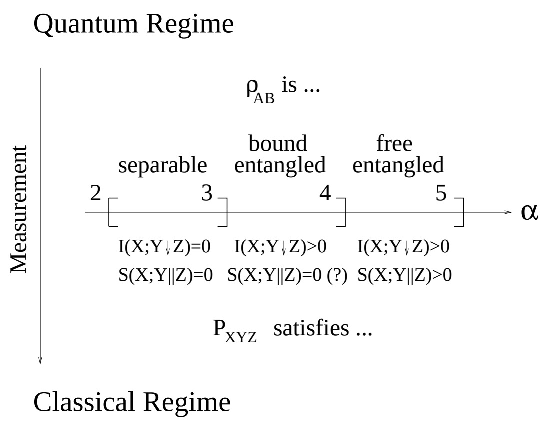

Fig. 1. The Results of Example 3

3.6 Bound Intrinsic Information

Examples 2 and 3 suggest that, in analogy to bound entanglement of a quantum state, *bound classical information* exists, i.e., conditional intrinsic information which cannot be used to generate a secret key in the classical scenario. We give a formal definition of bound intrinsic information.

Definition 2 Let P_{XYZ} be a distribution with $I(X;Y{\downarrow}Z) > 0$. If $S(X;Y||Z) > 0$ holds for this distribution, the intrinsic information between X and Y, given Z, is called *free*. Otherwise, if $S(X;Y||Z) = 0$, the intrinsic information is called *bound*. ○

Note that the existence of bound intrinsic information could not be proven so far. However, all known examples of bound entanglement, combined with all known advantage-distillation protocols, do not lead to a contradiction to Conjecture 1! Clearly, it would be very interesting to rigorously prove this conjecture because then, all pessimistic results known for the quantum scenario would immediately carry over to the classical setting (where such results appear to be much harder to prove).

Examples 2 and 3 also illustrate nicely what the nature of bound information is. Of course, $I(X;Y{\downarrow}Z) > 0$ implies both $I(X;Y) > 0$ and $I(X;Y|Z) > 0$. However, if $|\mathcal{X}|+|\mathcal{Y}| > 5$, it is possible that the dependence between X and Y and the dependence between X and Y, given $\overline{Z}$, are "orthogonal." By the latter we mean that for all fixed (deterministic or probabilistic) functions $f : \mathcal{X} \to \{0,1\}$ and $g : \mathcal{Y} \to \{0,1\}$ for which the correlation of $f(X)$ and $g(Y)$ is positive, i.e.,

$$P_{f(X)g(Y)}(0,0) \cdot P_{f(X)g(Y)}(1,1) > P_{f(X)g(Y)}(0,1) \cdot P_{f(X)g(Y)}(1,0) \ ,$$

the correlation between the same binary random variables, given $\overline{Z} = \overline{z}$, is negative (or "zero") for all $\overline{z} \in \overline{\mathcal{Z}}$, where $\overline{Z}$ is the random variable generated by sending Z over Eve's optimal channel $P_{\overline{Z}|Z}$.

A complete understanding of bound intrinsic information is of interest also because it automatically leads to a better understanding of bound entanglement in quantum information theory.

4 Concluding Remarks

We have considered the model of information-theoretic key agreement by public discussion from correlated information. More precisely, we have compared scenarios where the joint information is given by classical random variables and by quantum states (e.g., after execution of a quantum protocol). We proved a close connection between such classical and quantum information, namely between intrinsic information and entanglement. As an application, the derived parallels lead to an efficiently verifiable criterion for the fact that the intrinsic information vanishes. Previously, this quantity was considered to be quite hard to handle.

Furthermore, we have presented examples providing evidence for the fact that the close connections between classical and quantum information extend to the level of the protocols. A consequence would be that the powerful tools and statements on the existence or rather non-existence of quantum-privacy-amplification protocols immediately carry over to the classical scenario, where it is often unclear how to show that no protocol exists. Many examples (only some of which are presented above due to space limitations) coming from measuring bound entangled states, and for which none of the known classical secret-key agreement protocols is successful, strongly suggest that bound entanglement has a classical counterpart: intrinsic information which cannot be distilled to a secret key. This stands in sharp contrast to what was previously believed about classical key agreement. We state as an open problem to rigorously prove Conjectures 1 and 2.

Finally, we have proposed a measure for entanglement, based on classical information theory, with all the properties required for such a measure.

Acknowledgments

The authors thank Claude Crépeau, Artur Ekert, Bruno Huttner, Itoshi Inamori, Ueli Maurer, and Sandu Popescu for interesting discussions, and the referees for their helpful comments. This work was partially supported by the Swiss National Science Foundation (SNF).

References

1. H. Bechmann-Pasquinucci and N. Gisin, Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography, *Phys. Rev. A*, Vol. 59, No. 6, pp. 4238–4248, 1999.
2. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wooters, Purification of noisy entanglement and faithful teleportation via noisy channels, *Phys. Rev. Lett.*, Vol. 76, pp. 722–725, 1996.
3. C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing*, IEEE, pp. 175–179, 1984.
4. D. Bruss, Optimal eavesdropping in quantum cryptography with six states, *Phys. Rev. Lett.*, Vol. 81, No. 14, pp. 3018–3021, 1998.
5. V. Bužek and M. Hillery, Quantum copying: beyond the no-cloning theorem, *Phys. Rev. A*, Vol. 54, pp. 1844–1852, 1996.
6. J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.*, Vol. 23, pp. 880–884, 1969.
7. I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. IT-24, pp. 339–348, 1978.
8. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Phys. Rev. Lett.*, Vol. 77, pp. 2818–2821, 1996.
9. D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, Evidence for bound entangled states with negative partial transpose, quant-ph/9910026, 1999.
10. A. E. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, Vol. 67, pp. 661–663, 1991. See also *Physics World*, March 1998.
11. C. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Optimal eavesdropping in quantum cryptography – I: information bound and optimal strategy, *Phys. Rev. A*, Vol. 56, pp. 1163–1172, 1997.
12. N. Gisin, Stochastic quantum dynamics and relativity, *Helv. Phys. Acta*, Vol. 62, pp. 363–371, 1989.

13. N. Gisin and B. Huttner, Quantum cloning, eavesdropping, and Bell inequality, *Phys. Lett. A*, Vol. 228, pp. 13–21, 1997.
14. N. Gisin and S. Massar, Optimal quantum cloning machines, *Phys. Rev. Lett.*, Vol. 79, pp. 2153–2156, 1997.
15. N. Gisin and S. Wolf, Quantum cryptography on noisy channels: quantum versus classical key agreement protocols, *Phys. Rev. Lett.*, Vol. 83, pp. 4200–4203, 1999.
16. M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?, *Phys. Rev. Lett.*, Vol. 80, pp. 5239–5242, 1998.
17. P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, Vol. 232, p. 333, 1997.
18. P. Horodecki, M. Horodecki, and R. Horodecki, Bound entanglement can be activated, *Phys. Rev. Lett.*, Vol. 82, pp. 1056–1059, 1999. quant-ph/9806058.
19. L. P. Hughston, R. Jozsa, and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, *Phys. Lett. A*, Vol. 183, pp. 14–18, 1993.
20. U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.
21. U. Maurer and S. Wolf, Information-theoretic key agreement: from weak to strong secrecy for free, *Proceedings of EUROCRYPT 2000*, Lecture Notes in Computer Science, Vol. 1807, pp. 352–368, Springer-Verlag, 2000.
22. U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.
23. N. D. Mermin, The Ithaca interpretation of quantum mechanics, *Pramana*, Vol. 51, pp. 549–565, 1998.
24. A. Peres, *Quantum theory: concepts and methods*, Kluwer Academic Publishers, 1993.
25. A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.*, Vol. 77, pp. 1413–1415, 1996.
26. S. Popescu and D. Rohrlich, Thermodynamics and the measure of entanglement, quant-ph/9610044, 1996.
27. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Automated plug and play quantum key distribution, *Electron. Lett.*, Vol. 34, pp. 2116–2117, 1998.
28. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.
29. S. Wolf, *Information-theoretically and computationally secure key agreement in cryptography*, ETH dissertation No. 13138, Swiss Federal Institute of Technology (ETH Zurich), May 1999.
30. A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.
31. H. Zbinden, H. Bechmann, G. Ribordy, and N. Gisin, Quantum cryptography, *Applied Physics B*, Vol. 67, pp. 743–748, 1998.