Linking Classical and Quantum Key Agreement: Is There a Classical Analog to Bound Entanglement? *

Nicolas Gisin † Renato Renner ‡ Stefan Wolf §

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 contrast to what was previously believed.

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

*Some of the results of this paper already appeared in [18], [17], and [16].

†Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland. E-mail: Nicolas.Gisin@physics.unige.ch

‡Computer Science Department, Swiss Federal Institute of Technology (ETH Zürich), CH-8092 Zurich, Switzerland. E-mail: renner@inf.ethz.ch

§Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: wolf@iro.umontreal.ca

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 cryptographic settings based on noisy channels have been described and analyzed. Examples are Wyner's wire-tap channel [37], Csiszár and Körner's broadcast channel [7], or Maurer's model of key agreement from joint randomness [26], [28].

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], [11]), and the possibility and impossibility of such key agreement 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 2.2) and quantum (Section 2.3) 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 purification 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 4 we define and characterize the classical counterpart of bound entanglement, called bound intrinsic information. 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.

The results of Section 3 already appeared in [18] and [17]. Proposition 4 in Section 4 was proved in [16], whereas the other results in Section 4 have not been published previously.

2 Unconditionally Secure Key Agreement

Shannon [34] has defined an encryption scheme to be *perfectly secret* if the ciphertext does not reveal any information about the encrypted message. Such a system is unconditionally secure with respect to a ciphertext-only attack; in particular, an exhaustive search over the key space is of no help for finding the cleartext. Shannon proved in the same paper that, unfortunately, such a high level of secrecy has its price: it is, roughly spoken, only possible between parties who share an information-theoretically secure key that is at least as long as the message to be encrypted. The so-called *one-time pad* [35], a computationally very simple encryption that just bit-wisely XORs the key to the message, on the other hand shows that perfectly secure encryption is possible between parties who do share a key of that length. Since we assume that insecure channels are always available, the one-time pad reduces the problem of information-theoretically secure encryption to information-theoretically secure *key agreement*, which we will consider in the following.

2.1 Information-Theoretic Key Agreement from Classical and Quantum Information

We assume that two parties Alice and Bob, who are connected by an authentic but otherwise completely insecure channel, are willing to generate a secret key. More precisely, Alice and Bob want to compute, after some rounds of communication (where the random variable C summarizes the communication carried out over the public channel), strings S_A and S_B, respectively, with the property that they are most likely both equal to a uniformly distributed string S about which the adversary Eve has virtually no information. More precisely,

$$\mathrm{Prob}\,[S_A = S_B = S] \geq 1 - \varepsilon\ , \quad H(S) = \log_2 |\mathcal{S}|\ , \quad \text{and} \quad I(S;C) < \varepsilon \qquad (1)$$

(where $\mathcal{S}$ is the range of S and $|\mathcal{S}|$ is its cardinality) should hold for some small ε. Note that the security condition in (1) is information-theoretic (sometimes also called unconditional): Even an adversary with unlimited computer power must be unable to obtain useful information. In contrast to this, the Diffie-Hellman protocol [9] for instance achieves the goal of key agreement by insecure communication only with respect to computationally bounded adversaries.

It is a straight-forward generalization of Shannon's mentioned impossibility result that information-theoretic secrecy cannot be generated in this setting, i.e., from authenticity only: Public-key systems are never unconditionally secure. Hence we have to assume some additional structure in the initial setting, for instance some pieces of information given to Alice and Bob (and also Eve), respectively.

2.2 Classical Information

The general case where this information given to the three parties initially consists of the outcomes of some random experiment has been studied intensively [26], [28], [36]. Here, it is assumed that Alice, Bob, and Eve have access to realizations of random variables X, Y, and Z, respectively, jointly distributed according to P_{XYZ}. A special case is when all the parties receive noisy versions of a (binary) signal broadcast by some information source.

It was shown that if the setting is modified this way (where the secrecy condition in (1) must be replaced by $I(S;CZ) < \varepsilon$), then secret-key agreement is often possible. Shannon's pessimistic result now generalizes to the statement that the size of the resulting secret key S cannot exceed the quantity

$$I(X;Y \downarrow Z) := \min_{XY \to Z \to \overline{Z}} I(X;Y|\overline{Z})$$

(where the minimum is taken over all Markov chains $XY \to Z \to \overline{Z}$) which was defined in [28] as the *intrinsic conditional information between X and Y, given Z*.

In the special case where the parties' initial information consists of the outcomes of many independent repetitions of the same random experiment given by P_{XYZ} (i.e., Alice knows $X^N := [X_1, X_2, \ldots, X_N]$, and similarly for Bob and Eve), the *secret-key rate* $S(X;Y||Z)$ was defined as the maximal key-generation rate (measured with respect to the number of required realizations of P_{XYZ}) that is asymptotically achievable (for $N \to \infty$). The above-mentioned result then implies

$$S(X;Y||Z) \leq I(X;Y{\downarrow}Z) \ ,$$

and it was conjectured that intrinsic information can always be distilled into a secret key, i.e., that $I(X;Y \downarrow Z) > 0$ implies $S(X;Y||Z) > 0$ [28], [36]. This conjecture was supported by some evidence given in [28]; however, it is the objective of this paper to give much stronger evidence for the opposite, i.e., that there exist types of intrinsic information *not* allowing for secret-key agreement. The motivation for the corresponding considerations comes from quantum mechanics or, more precisely, from the concept of *bound entanglement* in quantum information theory.

2.3 Quantum Information

When considering the model where certain pieces of information are given initially to the involved parties, it is a natural question where this information comes from. According to Landauer, information is always physical and hence ultimately quantum mechanical [24], [25]. Thus the random variables could come from measuring a certain quantum state $|\Psi\rangle$. In this case, however, it seems to be overly restrictive to force Alice and Bob to measure their quantum systems right at the beginning of the key-agreement process. It is possibly advantageous for them to carry out a protocol first (using classical communication and local quantum operations on their systems) after which they end up with a "quantum key," i.e., a number of quantum bits in a maximally entangled state. Measuring them finally leads to a (classical) secret key. The first phase of this protocol is called *quantum (entanglement) purification*.

In order to understand what happens in a purification protocol and for which initial states such a protocol is at all possible, we recall some basic facts about quantum (information) theory. In contrast to a classical bit (*Cbit* for short) which can take either of the values 0 or 1, a quantum bit (*Qbit*) can exist in a superposition of these two extremal states (with complex *probability amplitudes* a and b satisfying $|a|^2 + |b|^2 = 1$):

$$|\psi\rangle = a|0\rangle + b|1\rangle \ .$$

When measuring this state with respect to the basis $\{|0\rangle, |1\rangle\}$, we obtain $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ otherwise. All (pure) states of one Qbit can be represented as unit vectors in the Hilbert space $\mathbf{C}^2$.

A possible state of a system of two Qbits can be

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =: |\psi_1\psi_2\rangle \ ,$$

which is simply the tensor product of the states $|\psi_1\rangle$ and $|\psi_2\rangle$ of the first and second Qbit, respectively. Such a state is called a *product state*. However, (normalized) linear combinations of quantum states lead to additional states; for instance,

$$|\psi^-\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$$

is also a possible state of the two-Qbit system. This state is called *singlet state* and has the property that whenever the Qbits are measured with respect to the same basis, the outcomes are opposite bits. There is no classical explanation for this behavior which is called *(maximal) entanglement*. We conclude that two Qbits are not the same as "two times one Qbit."

As described above, the objective of Alice and Bob doing quantum purification is to generate two-Qbit systems in the state $|\psi^-\rangle$ (or in states very close to it) by classical communication and local quantum operations. The states they start with can for instance be their view of a pure state $|\Psi\rangle$ living in Alice's, Bob's, and a possible adversary Eve's (who is assumed to have total control over the entire environment) Hilbert spaces:

$$|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E \ .$$

In analogy to Alice and Bob's marginal distribution P_{XY} in the classical setting, one can define Alice and Bob's view of the state $|\Psi\rangle$, the so-called *trace over the environment* $\mathcal{H}_E$,

$$\rho_{AB} := \mathrm{Tr}_{\mathcal{H}_E}(P_\Psi) \ .$$

The state ρ_{AB} is generally a *mixed state*. In contrast to a pure state, which can be represented by a vector in a Hilbert space, a mixed state is described by a probability distribution over such a space. A mixed state, such as ρ_{AB}, can be represented by a $(\dim \mathcal{H}_A) \cdot (\dim \mathcal{H}_B) \times (\dim \mathcal{H}_A) \cdot (\dim \mathcal{H}_B)$ matrix, namely the weighted sum (with respect to the probability distribution) of the projectors to the subspaces generated by the corresponding pure states. This matrix is called *density matrix*.

It is important to note that "purification," which transforms the mixed state ρ_{AB} into pure (singlet) states, actually means key agreement: Alice and Bob's final state is pure and hence not entangled with anything else, in particular not with anything under Eve's control. The adversary is out of the picture, whatever operations and measurements she performs.

Let us consider some properties of mixed states. A state ρ_{AB} which is *separable*, i.e., a mixture of product states, can be prepared remotely by purely classical communication. States that are not separable are called *entangled* and cannot be prepared this way. It is a natural question which states ρ_{AB} *can be purified* and which cannot. Separable states cannot be purified because of the property just described and because of the generalization of Shannon's theorem mentioned at he beginning of this paper: No information-theoretic key agreement is possible from authentic but public (classical) communication. On the other hand, if Alice's and Bob's subsystems are two-dimensional[1] (i.e., Qbits) and entangled, then purification is always possible [20]. However, the surprising fact was recently discovered that the same is not true for higher-dimensional systems: There exist entangled states which cannot be purified [21]. This follows from the fact that the eigenvalues of the so-called partial transposition of certain entangled density matrices ρ_{AB} are non-negative [31]. This type of entanglement is called *bound* (in contrast to *free* entanglement, which *can* be purified). From the perspective of classical information theory, the interesting point is that bound entanglement seems to have a classical counterpart with unexpected properties.

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. First of all, there is a very natural connection between quantum states Ψ and classical distributions P_{XYZ} which can be thought of as arising from Ψ by measuring in a certain basis, e.g., the standard basis[2]. Such a measurement leads

[1] The same is even true if one of the spaces has dimension two and the other one has dimension three.

[2] A priori, there is no privileged basis. However, physicists often write states 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 are real

to classical information with some probability distribution depending on the quantum state. In the following, we assume that Eve is free to carry out so-called *generalized measurements* (POVMs) [30]. 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 bases $\{|x\rangle\}$ and $\{|y\rangle\}$, and in the set $\{|z\rangle\}$, respectively, they end up with the classical scenario $P_{XYZ} = |\langle x,y,z|\Psi\rangle|^2$.

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} will have 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[3]). 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 $\mathcal{H}_E$ such that for all bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, $I(X;Y|Z) = 0$ holds for $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$.*

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 $|\alpha_z\rangle$.

and positive. We usually represent quantum states with respect to the standard basis.

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

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 [29], [13], [23].

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 [30]. 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 $|x, y\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. 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 $\mathcal{H}_E$, there are bases $\{|x\rangle\}$ and $\{|y\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, 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.,

$$P_{XY|\overline{Z}}(x, y, \overline{z}) = P_{X|\overline{Z}}(x, \overline{z}) P_{Y|\overline{Z}}(y, \overline{z}) \ . \tag{2}$$

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

It is important to note in this context that when the measurements are actually carried out by the parties, then Alice and Bob can obtain positive intrinsic information only if Eve cannot choose her measurement basis adaptively (i.e., *after* learning what bases Alice and Bob have used).

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 the statement of 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 the partial transpose of the density matrix, i.e., 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 [18]. 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 [12]

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

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 $\{|\,01\,\rangle,\ |\,00\,\rangle,\ |\,11\,\rangle,\ |\,10\,\rangle\}$)

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

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

$$D \geq 1 - \frac{1}{\sqrt{2}} \ . \tag{3}$$

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 Qbit 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 sub-spaces), 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

$$\frac{D}{1-D} \geq 2\sqrt{(1-\delta)\delta} = 1 - 2D \tag{4}$$

holds. We show that if the condition (4) 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 (4) 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 (4) because Eve can always increase δ by adding noise.

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

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

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

$$\begin{array}{rcl} a_{00} & = & (1-D)\delta/2\,, \\ a_{11} & = & (1-D)(1-\delta)/2\,, \\ a_{01} & = & a_{10} \;\; = \;\; (D(1-\delta)/2 + D\delta/2)/2 \;\; = \;\; D/4\,. \end{array}$$

From equality in (4) 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 (3) and (4) 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 [21]. 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

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

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 [21] 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 $z \not\in \{0,1\}$.

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 $I(X;Y\!\downarrow\! Z) = 0$. Since $I(X;Y\!\downarrow\! Z)$ is the minimum, taken over all discrete channels $P_{\overline{Z}|Z}$, of $I(X;Y|\overline{Z})$, there must exist 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

$$1 \geq \sum_i \frac{a_i(a_i + x_i/2)}{s_i} \ . \tag{5}$$

We prove that (5) 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 (5) 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 [28]. 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 [22]) is discussed. The example is particularly instructive 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 $0 \leq \alpha \leq 3$.

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

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

is separable if and only if $\alpha \in [2,3]$, bound entangled for $\alpha \in [1,2)$, and free entangled if $\alpha \in [0,1)$ [22] (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 $\alpha < 2$. $\diamondsuit$

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

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

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

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

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 [32]. Corollary 3 above suggests the following measure, which is based on classical information theory.

Definition 1. Let for a quantum state ρ_{AB}

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

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 [30]) $\psi_{AB} = \sum_j c_j|x_j,y_j\rangle$, and $\mu(\rho_{AB}) = -\mathrm{Tr}(\rho_A \log \rho_A)$ (where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$) as it should [32]. 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 $\rho_{AB} = \lambda P_{\psi^{(-)}} + ((1-\lambda)/4)\mathbb{1}$. 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 $q = 2\lambda/(1+\lambda)$. ◊

3.4 Classical Protocols and Quantum Purification

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 [28] 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 purification 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 purification 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 [26] or [36]). $\diamondsuit$

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 [26], [28] 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, $1 \leq \alpha < 2$ corresponds to bound entanglement, whereas for $\alpha < 1$, QPA is possible and allows for generating a secret key [22]. 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 $\alpha < 1$. However, this does not imply (although it appears very plausible) that no classical protocol exists at all for the case $\alpha \geq 1$.

Let $\alpha < 1$. We consider the following protocol for classical key agreement. First of all, Alice and Bob both restrict their ranges to $\{1,3\}$ (i.e., publicly reject a realization unless $X \in \{1,3\}$ and $Y \in \{1,3\}$). We will later call this a *binarization* of the corresponding random variables and show that this concept is of great importance in the context of possibility and impossibility of secret-key agreement, both classical and quantum.

The resulting distribution is as follows (to be normalized):

X Y (Z)	1	3
1	(0) 2	(3) α
3	(6) $5-\alpha$	(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 $X = 1$ $[Y = 3]$ to $\overline{X} = 3$ $[\overline{Y} = 1]$ with probability $(5 - 2\alpha)/(14 - 2\alpha)$, and leaves X $[Y]$ unchanged otherwise. The distribution $P_{\overline{XY}Z}$ is then

$\overline{X}$ $\overline{Y}$ (Z)	1	3
1	(0) $2 \cdot \frac{9}{14-2\alpha}$ (6) $(5-\alpha) \cdot \frac{9}{14-2\alpha} \cdot \frac{5-2\alpha}{14-2\alpha}$	(3) α (6) $(5-\alpha)\left(\frac{5-2\alpha}{14-2\alpha}\right)^2$ (0) $2 \cdot 2 \cdot \frac{5-2\alpha}{14-2\alpha}$
3	(6) $(5-\alpha)\left(\frac{9}{14-2\alpha}\right)^2$	(0) $2 \cdot \frac{9}{14-2\alpha}$ (6) $(5-\alpha) \cdot \frac{9}{14-2\alpha} \cdot \frac{5-2\alpha}{14-2\alpha}$

It is not difficult to see that for $\alpha < 1$, we have 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 [26], [36]. For $\alpha \geq 1$, classical key agreement, like quantum key agreement, seems impossible however. We will discuss this further in Section 4. The results of Example 3 are illustrated in Figure 1. $\diamondsuit$

4 Bound Intrinsic Information and Binarizations

Conjecture 1 suggests that, in contrast to previous beliefs in classical information theory, bound entanglement has a classical counterpart, which we call *bound information*.

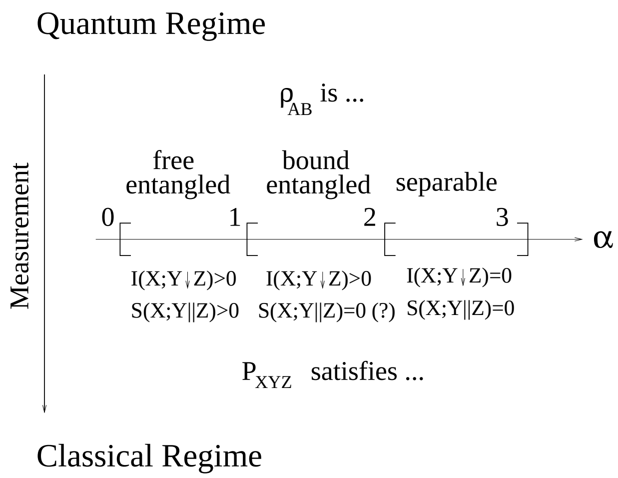

Figure 1: The Results of Example 3

Definition 2. Let P_{XYZ} be a distribution with $I(X;Y{\downarrow}Z) > 0$. Then 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*. ○

We are now interested in a proof of the existence of such bound information. In view of the fact that Conjecture 1 might be hard to prove in general, it is worth to look at a classical "translation" of a bound entangled quantum state directly and analyze it with the tools of classical information theory.

This analysis shows that an important concept in the context of key agreement from classical information are so-called *binarizations*. We give evidence for the fact that classical information can be used for key agreement only if the random variables X and Y can be made binary by local operations (i.e., by sending them over some binary-output channel) in such a way that the resulting *binary* random variables still share some information. The quantum counterpart of this insight may result in an easy characterization and better understanding of the strange phenomenon of bound entanglement.

Let us look at the states Ψ_α of Example 3 again. First, we prove that whenever the random variable Y is "binarized," i.e., sent through a binary-output channel $P_{\overline{Y}|Y}$ (or a ternary-output channel but where only two symbols are actually considered in the computation of the mutual information), then the intrinsic information vanishes (Proposition 4).

Proposition 5 on the other hand suggests that intrinsic information which does not resist any binarization must be bound: Whenever secret-key agreement is possible with X and Y and with respect to Z, there exist binarizations of a certain number of repetitions of X and Y such that the intrinsic information remains positive.

Proposition 4. *Let P_{XYZ} be the distribution of Example 3 with $\alpha \in [1,2)$. Let $P_{\overline{Y}|Y}$ be an arbitrary conditional distribution with $\overline{\mathcal{Y}} = \{0,1,\Delta\}$, and let E be the event that $\overline{Y} \in \{0,1\}$. Then $I(X;\overline{Y} \downarrow Z \,|\, E) = 0$.*

Proof. We only have to consider the case $\alpha = 1$. This implies the statement for all $\alpha \in [1,2)$. Let the following channel $P_{\overline{Y}|Y}$ be given (where $\overline{\mathcal{Y}} = \{0,1,\Delta\}$):

$$
\begin{array}{lllll}
P_{\overline{Y}|Y}(0,1) = x\ , & P_{\overline{Y}|Y}(0,2) = y\ , & P_{\overline{Y}|Y}(0,3) = z\ , \\
P_{\overline{Y}|Y}(1,1) = u\ , & P_{\overline{Y}|Y}(1,2) = v\ , & P_{\overline{Y}|Y}(1,3) = w\ .
\end{array}
$$

Here, we have $x,y,z,u,v,w,x+u,y+v,z+w \in [0,1]$. We get the following distribution $P_{X\overline{Y}Z|E}$ (to be normalized).

X / $\overline{Y}$ (Z)	1	2	3
0	(0) $2x$ (1) y (6) $4z$	(0) $2y$ (4) $4x$ (2) z	(0) $2z$ (3) x (5) $4y$
1	(0) $2u$ (1) v (6) $4w$	(0) $2v$ (4) $4u$ (2) w	(0) $2w$ (3) u (5) $4v$

The only symbol z of Z for which $I(X;\overline{Y}|Z=z,E) > 0$ holds is $z=0$. Let us now consider a channel $P_{\overline{Z}|Z}$ with $\overline{\mathcal{Z}} = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$ and $P_{\overline{Z}|Z}(\overline{0},0) = 1$. Furthermore, $P_{\overline{Z}|Z}(\overline{0},1) = a$ and $P_{\overline{Z}|Z}(\overline{1},1) = 1-a$, and analogously for $Z = 2,3,4,5,$ and 6 with transition probabilities $d,e,c,f,$ and b, respectively. Then we get for the column vectors of the $P_{X\overline{Y}|\overline{Z}=\overline{0}}$ matrix:

$$
\left[2\binom{x}{u} + a\binom{y}{v} + 4b\binom{z}{w}\,,\, 4c\binom{x}{u} + 2\binom{y}{v} + d\binom{z}{w}\,,\, e\binom{x}{u} + 4f\binom{y}{v} + 2\binom{z}{w}\right].
$$

Clearly, the three vectors are linearly dependent. We can assume that

$$
\binom{x}{u} = \lambda_1\binom{y}{v} + \lambda_2\binom{z}{w}
$$

holds for some $\lambda_1, \lambda_2 \in [0,\infty)$. (The other cases are analogous.)

Let $\vec{s} := \binom{y}{v}$ and $\vec{t} := \binom{z}{w}$. We then get for the above matrix

$$
\left[(a+2\lambda_1)\vec{s} + (4b+2\lambda_2)\vec{t}, (2+4c\lambda_1)\vec{s} + (d+4c\lambda_2)\vec{t}, (4f+e\lambda_1)\vec{s} + (2+e\lambda_2)\vec{t}\right].
$$

The corresponding distribution satisfies $I(X;\overline{Y}|\overline{Z}=\overline{0},E) = 0$ if

$$
\frac{a+2\lambda_1}{4b+2\lambda_2} = \frac{2+4c\lambda_1}{d+4c\lambda_2} = \frac{4f+e\lambda_1}{2+e\lambda_2}
$$

holds. This is equivalent to

$$\begin{aligned}\lambda_1(2d-16bc)+\lambda_2(4ac-4) &= 8b-ad\ ,\\ \lambda_1(4-4be)+\lambda_2(ae-8f) &= 16bf-2a\ .\end{aligned}$$

We show that this system is solvable, with $(a,b,c,d,e,f)\in[0,1]^6$, for all $\lambda_1,\lambda_2\in[0,\infty)$. For this, we prove that for all sufficiently large numbers $R>0$, the equations are solvable for all pairs (λ_1,λ_2) on the path $(0,0)$-$(R,0)$-(R,R)-$(0,R)$-$(0,0)$, and that the corresponding path in $[0,1]^6$ is homeomorphic to S^1. Then the claim follows by a simple topological argument.

We only sketch the remainder of the proof. For $(\lambda_1,\lambda_2)=(0,0)$, the equations are solvable by setting

$$d=f=1 \ \text{ and } \ 8b=d\ . \tag{6}$$

For $(\lambda_1,\lambda_2)=(R,0)$, where we assume R to be sufficiently large, a solution is given by

$$b\approx e\approx 1 \ \text{ and } \ d\approx 8c$$

(where additionally both equations of (6) should *not* be satisfied nor approximately satisfied). For $(\lambda_1,\lambda_2)=(R,R)$, the equalities are

$$\begin{aligned}R(2d-16bc+4ac-4) &= 8b-ad\\ R(4-4be+ae-8f) &= 16bf-2a\end{aligned}$$

with a possible approximate solution

$$b\approx e\approx 0\ ,\quad c\approx d\approx 1\ ,\quad a\approx f\approx 1/2\ .$$

Finally, the case $(\lambda_1,\lambda_2)=(0,R)$ can be solved by

$$a\approx c\approx 1 \ \text{ and } \ e\approx 8f\ .$$

When combining the solutions for the different cases, it is not difficult to see that there exists a path γ in $[0,1]^6$ that, mapped to the (λ_1,λ_2) plane, exactly corresponds to the square $(0,0)$-$(R,0)$-(R,R)-$(0,R)$-$(0,0)$. This is true for all sufficiently large R, and thus the argument is finished. □

Proposition 5. *Let X, Y, and Z be random variables with $S(X;Y\|Z)>0$. Then for each $\varepsilon>0$ there exist a number N and ternary-output channels $P_{\overline{X}|X^N}$ and $P_{\overline{Y}|Y^N}$ with ranges $\overline{\mathcal{X}}=\overline{\mathcal{Y}}=\{0,1,\Delta\}$ such that*

$$\begin{aligned}\mathrm{Prob}[E] &> 0 &(7)\\ P[\overline{X}=\overline{Y}|E] &> 1-\varepsilon &(8)\\ P[\overline{X}=0|E']=P[\overline{X}=1|E'] &= 1/2 &(9)\\ H(\overline{X}|Z^N,E) &> 1-\varepsilon &(10)\end{aligned}$$

where E and E' are the events defined by $\overline{X}\neq\Delta\neq\overline{Y}$ and $\overline{X}=\overline{Y}\neq\Delta$, respectively (note that $E'=E\cap[\overline{X}=\overline{Y}]$). In particular, we have $I(\overline{X};\overline{Y}\downarrow Z^N,E)>0$.

Proof. According to the definition of the secret-key rate, for each ε' there exist a number N and a protocol that allows Alice and Bob for computing keys $S_A, S_B \in \{0,1\}^K$ out of N realizations of the random variables X and Y such that

$$\begin{aligned} P[S_A \neq S_B] &< \varepsilon' && (11) \\ H(S_A|Z^N C) &> K - \varepsilon' && (12) \end{aligned}$$

where C is the communication exchanged over the public channel. Let S'_A and S'_B to be the first bit of S_A and S_B, respectively. It is clear from (11) that

$$P[S'_A \neq S'_B] < \varepsilon' \tag{13}$$

and from (12)

$$H(S'_A|Z^N C) = H(S_A|Z^N C) - H(S_A|S'_A Z^N C) > K - \varepsilon' - (K-1) = 1 - \varepsilon'. \tag{14}$$

Define the functions

$$e : c \mapsto P[S'_A \neq S'_B | C = c] \tag{15}$$

and

$$k : c \mapsto 1 - H(S'_A|Z^N, C = c). \tag{16}$$

From conditions (13) and (14) we have that $E_C[e(C)] < \varepsilon'$ and $E_C[k(C)] < \varepsilon'$ (where E_C is the expectation value over all possible communications $c \in \mathcal{C}$). Since both e and k only take on positive values, it follows immediately that $P[e(C) < 2\varepsilon'] \geq 1/2$ and $P[k(C) < 2\varepsilon'] \geq 1/2$, which implies that there exists a particular communication string $c \in \mathcal{C}$ such that $e(c) < 2\varepsilon'$ and $k(c) < 2\varepsilon'$, or

$$\begin{aligned} P[S'_A \neq S'_B | C = c] &< 2\varepsilon' && (17) \\ H(S'_A|Z^N, C = c) &> 1 - 2\varepsilon'. && (18) \end{aligned}$$

In general, a secret-key agreement protocol consists of $2M$ steps (where M is itself a random variable) such that in each step Alice sends the information C_i to Bob (for i odd) or Bob sends C_i to Alice (for i even). After this communication phase, Alice and Bob compute their secret-key bits S'_A and S'_B, respectively. We thus have

$$\begin{aligned} P_{S'_A S'_B C|X^N Y^N} = \; & P_{S'_A|X^N C} \cdot P_{S'_B|Y^N C} \cdot P_{C_{2M}|C^{2M-1} Y^N} \cdot P_{C_{2M-1}|C^{2M-2} X^N} \cdot \\ & \ldots \cdot P_{C_2|C_1 Y^N} \cdot P_{C_1|X^N} \end{aligned}$$

(the arguments are omitted in this expression), where $C^i := C_1 \cdots C_i$ and $C := C^{2M}$. When the terms are rearranged, this expression can be written as

$$P_{S'_A S'_B C|X^N Y^N}(s_A, s_B, c, x, y) = p_A(s_A, c, x) \cdot p_B(s_B, c, y) \tag{19}$$

for appropriate functions p_A and p_B. For a communication string $c \in \mathcal{C}$ satisfying (17) and (18), we define

$$
\begin{aligned}
P_{\overline{X}'|X^N}(\overline{x}', x) &:= p_A(\overline{x}', c, x) && (20)\\
P_{\overline{X}'|X^N}(\overline{\Delta}, x) &:= 1 - p_A(0, c, x) - p_A(1, c, x) && (21)\\
P_{\overline{Y}'|Y^N}(\overline{y}', y) &:= p_B(\overline{y}', c, y) && (22)\\
P_{\overline{Y}'|Y^N}(\overline{\Delta}, y) &:= 1 - p_B(0, c, y) - p_B(1, c, y)\ . && (23)
\end{aligned}
$$

for all $\overline{x}', \overline{y}' \in \{0,1\}$, $x \in \mathcal{X}^N$, $y \in \mathcal{Y}^N$. (Note that this completely determines the channels $P_{\overline{X}'|X^N}$ and $P_{\overline{Y}'|Y^N}$.) Then we get from (17) and (18)

$$
\begin{aligned}
P[\overline{X}' \neq \overline{Y}' | \overline{X}' \neq \Delta \neq \overline{Y}'] &< 2\varepsilon' && (24)\\
H(\overline{X}' | Z^N, \overline{X}' \neq \Delta \neq \overline{Y}') &> 1 - 2\varepsilon'\ . && (25)
\end{aligned}
$$

It remains to show that equality (9) holds. Let therefore

$$\delta := 1/2 - P[\overline{X}' = 0 | \overline{X}' = \overline{Y}' \neq \Delta] \tag{26}$$

and assume without loss of generality that $\delta \geq 0$. Define

$$P_{\overline{X}|\overline{X}'}(\overline{x}, \overline{x}') = \begin{cases} 1 & \text{if } \overline{x} = \overline{x}' = \Delta \text{ or } \overline{x} = \overline{x}' = 0 \\ \frac{1/2-\delta}{1/2+\delta} & \text{if } \overline{x} = \overline{x}' = 1 \\ 1 - \frac{1/2-\delta}{1/2+\delta} & \text{if } \overline{x} = \Delta \text{ and } \overline{x}' = 1 \\ 0 & \text{otherwise} \end{cases} \tag{27}$$

and $\overline{Y} := \overline{Y}'$. Then

$$P[\overline{X} = 0 | E'] = P[\overline{X} = 1 | E'] = 1/2. \tag{28}$$

It can easily be verified from (25) that δ is of order ε' and thus the assertion follows from (24) and (25). □

Propositions 4 and 5 do not imply that Alice and Bob share bound information in the considered distribution. More precisely, the following statement, which we give as a conjecture, is the missing gap in the way towards proving the existence of bound information.

Conjecture 3. *Let P_{XYZ} be a distribution. Then there exist binary-output channels $P_{\overline{X}|X}$ and $P_{\overline{Y}|Y}$ with $I(\overline{X};\overline{Y} \downarrow Z) > 0$ if and only if there exist, for some N, binary-output channels $P_{\overline{X}|X^N}$ and $P_{\overline{Y}|Y^N}$ such that $I(\overline{X};\overline{Y} \downarrow Z^N) > 0$ holds.*

Proposition 5 states that classical information which allows for generating a secret key can be binarized by the two parties in the sense that they can send their pieces of information over certain noisy binary-output channels such that the two resulting bits are equal with probability almost 1 and such that the adversary has virtually no information about them.

A similar result on the quantum side has been shown in [19]: If a density matrix ρ_{AB} can be purified, then Alice and Bob can, by simple local projections to two-dimensional systems of n copies of the state (for some n), generate a Qbit pair that is arbitrarily close to a fully entangled pair.

Motivated by the classical scenario, we finally state as an open question whether free entanglement is characterized by the possibility of *single-copy* "entanglement binarization."

Open Question. Let ρ_{AB} be a mixed state over $\mathcal{H}_A \otimes \mathcal{H}_B$. Is it true that ρ_{AB} is free entangled if and only if there are two-dimensional projectors P_A and P_B such that $(P_A \otimes P_B)\rho_{AB}(P_A \otimes P_B)$ is an entangled two-Qbit state?

Note that it is clear that if Alice and Bob can produce entangled Qbits, then they can always purify the original state because these Qbits are free entangled. The question is whether the reverse implication is also true. An affirmative answer would mean that ρ_{AB} is free entangled if and only if Alice and Bob can produce entangled Qbits using *a single copy* of ρ_{AB}.

5 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.

Furthermore, examples have been presented that provide 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-purification protocols immediately carry over to the classical scenario, where it is often unclear how to show that no protocol exists. Many examples coming from measuring bound entangled states, and for which none of the known classical secret-key agreement protocols is successful, as well as some general facts on binarizing classical information, 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. This is one of the rare examples for which a concept of information processing is first discovered on the quantum domain and then leads to new insight in the classical regime.

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 Gilles Brassard, Nicolas Cerf, Claude Crépeau, Serge Massar, Ueli Maurer, Michele Mosca, Sandu Popescu, and Alain Tapp for interesting discussions, and two anonymous referees for their helpful comments. The first and the third author were partially supported by Switzerland's SNF, and the third author was partially supported by Canada's NSERC.

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

[10] 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.

[11] 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.

[12] 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.

[13] N. Gisin, Stochastic quantum dynamics and relativity, *Helv. Phys. Acta*, Vol. 62, pp. 363–371, 1989.

[14] N. Gisin and B. Huttner, Quantum cloning, eavesdropping, and Bell inequality, *Phys. Lett. A*, Vol. 228, pp. 13–21, 1997.

[15] N. Gisin and S. Massar, Optimal quantum cloning machines, *Phys. Rev. Lett.*, Vol. 79, pp. 2153–2156, 1997.

[16] N. Gisin, R. Renner, and S. Wolf, Bound information: the classical analog to bound entanglement, in *Proceedings of 3ecm*, Birkhäuser Verlag, 2000.

[17] N. Gisin and S. Wolf, Linking classical and quantum key agreement: is there "bound information"?, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science, vol. 1880, pp. 482–500, Springer-Verlag, 2000.

[18] 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.

[19] 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.

[20] M. Horodecki, P. Horodecki, and R. Horodecki, Inseparable 2 spin 1/2 density matrices can be distilled to a singlet form, *Phys. Rev. Lett.*, Vol. 78, p. 574, 1997.

[21] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, Vol. 232, p. 333, 1997.

[22] P. Horodecki, M. Horodecki, and R. Horodecki, Bound entanglement can be activated, *Phys. Rev. Lett.*, Vol. 82, pp. 1056–1059, 1999. quant-ph/9806058.

[23] 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.

[24] R. Landauer, Information is inevitably physical, *Feynman and Computation 2*, Addison Wesley, Reading, 1998.

[25] R. Landauer, The physical nature of information, *Phys. Lett. A*, Vol. 217, p. 188, 1996.

[26] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[27] 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.

[28] 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.

[29] N. D. Mermin, The Ithaca interpretation of quantum mechanics, *Pramana*, Vol. 51, pp. 549–565, 1998.

[30] A. Peres, *Quantum theory: concepts and methods*, Kluwer Academic Publishers, 1993.

[31] A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.*, Vol. 77, pp. 1413–1415, 1996.

[32] S. Popescu and D. Rohrlich, Thermodynamics and the measure of entanglement, quant-ph/9610044, 1996.

[33] 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.

[34] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.

[35] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, *Journal of the American Institute for Electrical Engineers*, Vol. 55, pp. 109–115, 1926.

[36] S. Wolf, *Information-theoretically and computationally secure key agreement in cryptography*, ETH dissertation No. 13138, Swiss Federal Institute of Technology (ETH Zurich), May 1999.

[37] A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.

[38] H. Zbinden, H. Bechmann, G. Ribordy, and N. Gisin, Quantum cryptography, *Applied Physics B*, Vol. 67, pp. 743–748, 1998.