A survey on locking of bipartite correlations

Debbie Leung
Institute for Quantum Computing and Department of Combinatorics and Optimization,
University of Waterloo, Waterloo, Ontario, N2L3G1, Canada
E-mail: wcleung@iqc.ca

Abstract.
Unlocking of a correlation refers to the unexpected phenomenon that a small amount of
communication increases that correlation (as a function of the state of the distributed system)
by a disproportionate amount. Locking refers to the suppression of the correlation prior to
the communication. The notion was subsequently extended to abrupt changes in a correlation
due to the manipulation (in particular, the addition or removal) of a small subsystem. In this
proceeding, we review the basic ideas and summarize the results known so far.

1. Intuitive properties for correlations
Intuitively, we expect any good correlation measure to satisfy certain axiomatic properties. First,
correlation is a nonlocal property and should not increase under local processing (monotonicity).
Second, starting from an uncorrelated initial state, a certain amount of communication should
not increase the correlation in a disproportionate way. We call this property total proportionality.
In fact, we expect the above to hold for any initial state. We call this more stringent property
incremental proportionality. Other properties such as continuity or convexity are also expected.

For the most general form of communication that can involve any number of rounds of forward
or backward quantum or classical communication between Alice and Bob, the quantum mutual
information satisfies all of the above properties [1]. The quantum mutual information is defined
as $I_q(\rho) ≡ S(\rho_A) + S(\rho_B) - S(\rho)$ with $S(\eta) ≡ -Tr \log \eta$ being the von Neumann entropy and
$\rho_A = Tr_B \rho$, $\rho_B = Tr_A \rho$ being the reduced density matrices. Consequently, mutual information in
the classical setting (classical states and communication) also satisfies all the stated properties.

A natural definition of classical mutual information of a quantum state $\rho_{AB}$ is the maximum
classical mutual information that can be obtained by local measurements $M_A \otimes M_B$ [1]:

$$I_c(\rho) ≡ \max_{M_A \otimes M_B} I(A:B).$$

Here $I(A:B)$ is the classical mutual information defined as $I(A:B) ≡ H(p_A) + H(p_B) - H(p_{AB})$, $H$
is the entropy function [2], and $p_{AB}, p_A, p_B$ are the probability distributions of the joint
and individual outcomes of performing the local measurement $M_A \otimes M_B$ on $\rho$. A related measure is
the regularized quantity $I_c^\infty(\rho) ≡ \lim_{n \to \infty} \frac{1}{n} I_c(\rho^{\otimes n})$, which is known to be strictly greater than
$I_c(\rho)$ for some states. The physical relevance of $I_c$ is many-fold.

- When $\rho$ is pure, $I_c(\rho)$ is the correlation calculated in the Schmidt basis and is thus equal
to the entanglement of $\rho$ [3, 4].
• \( I_c(\rho) \) corresponds to the usual classical mutual information when \( \rho \) is “classical,” i.e. \( \rho \) is diagonal in some local product basis, corresponding to a classical distribution.

• \( I_c(\rho) \) is the maximum classical correlation, as measured by the Shannon mutual information, obtainable from one copy of \( \rho \) by arbitrary quantum but local processing.

• For a classical-quantum system (that is, the density matrix of the distributed state is block diagonal), \( I_c(\rho) \) is the accessible information of the ensemble of quantum states living in system \( B \) with classical labels in system \( A \). (See Section 2.2 Eq. (3) for the definition of the accessible information.)

• \( I_c(\rho) = 0 \) if and only if \( \rho = \rho_A \otimes \rho_B \) [5].

\( I_c \) is proved to satisfy monotonicity, total proportionality, continuity, and convexity hold [1]. Incremental proportionality was proved for pure initial states \( \rho \) for any communication [1]. \( I_c^\infty(\rho) = I_c(\rho) \) when \( \rho \) is pure or separable.

2. Violation of intuition – Locking of \( I_c \)

2.1. Earliest example

While working on [1], the authors were initially trying to prove incremental proportionality for \( I_c \), only to find states that violate it [5]. These states, \( \rho_{ACB} \), are supported on \( \mathbb{C}^d \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \) such that \( I_c(\rho_{ACB}) = \frac{1}{4} \log d \) and \( I_c(\rho_{AC|B}) = \log d + 1 \) (we use “\("”) to indicate the bipartite cut that defines the correlation). Furthermore, systems \( AC \) are classical. Thus an alternative statement of the result is that, providing Bob with one extra bit of classical information \( C \) increases his accessible information by \( \frac{1}{4} \log d \) where \( d \) is his system dimension. Naturally, we think of system \( C \) as the “key” that “locks” his accessible information.

Many of the subsequent developments in the subject are based on this specific example provided in [5]. In detail,

\[
\rho_{ACB} = \frac{1}{2d} \sum_{x=0}^{d-1} \sum_{k=0}^{1} (|x\rangle \langle x| \otimes |k\rangle \langle k|)_A \otimes |k\rangle \langle k|_C \otimes (U_k|x\rangle \langle x|U_k^\dagger)_B .
\]  

(2)

Here \( U_0 = I \) and \( U_1 \) is any unitary that changes the computational basis to a conjugate basis \( \langle \eta_{i,x} | (|U_1|x\rangle) = \frac{1}{\sqrt{d}} \). In this example, Bob is given a message \( |x\rangle \) uniformly distributed over \( d \) possibilities in two possible random bases (depending on whether \( k = 0 \) or \( 1 \)), while Alice holds the classical label of his state (both the message and the key). The 1-bit communication that unlocks the message is the basis information. Clearly, \( I_c(\rho_{AC|B}) = \log d + 1 \). The challenge is to prove that \( I_c(\rho_{AC|B}) = \frac{1}{2} \log d \). This has to be done for all possible POVM measurements that Bob can apply.

2.2. Connection to entropic uncertainty

Now we prove that \( I_c(\rho_{AC|B}) = \frac{1}{2} \log d \). This takes several steps and a connection to a subject concerning “entropic uncertainty relations.”

First, the complete measurement \( M_A \) along \( \{|x\rangle \otimes |k\rangle\} \) is provably optimal for Alice: Since the outcome tells her precisely which pure state from the ensemble she has, she can apply classical, local post-processing to obtain the output distribution for any other measurement she could have performed. For Alice’s choice of optimal measurement, \( I_c(\rho_{AC|B}) \) is simply Bob’s accessible information \( I_{acc}[3] \) about the uniform ensemble of states \( \{|x\rangle, U_1|x\rangle\}_{x=0,...,d-1} \).

In general, let \( I \) be a random variable such that outcome \( i \) occurs with probability \( p_i \geq 0 \). A draw from the ensemble of states \( \mathcal{E} = \{p_i, \eta_i\} \) is a specimen of the corresponding random state \( \eta_I \). The accessible information \( I_{acc} \) is the maximum mutual information between the random variable \( I \) and the outcome of a measurement performed on \( \eta_I \). \( I_{acc}(\mathcal{E}) \) can be
maximized by a POVM that has only rank-1 elements [3]. Let \( M = \{ \alpha_j | \phi_j \rangle \langle \phi_j | \} \) stand for a POVM with rank-1 elements where each \( | \phi_j \rangle \) is normalized and \( \alpha_j > 0 \). Then \( I_{acc}(E) \) can be expressed as

\[
I_{acc}(E) = \max_M \left[ -\sum_i p_i \log p_i + \sum_i \sum_j p_i \alpha_j \langle \phi_j | \eta_i \rangle \langle \phi_j | \rangle \log \frac{p_i \langle \phi_j | \eta_i \rangle \langle \phi_j | \rangle}{\langle \phi_j | \mu \rangle \langle \phi_j | \rangle} \right],
\]

(3)

where \( \mu = \sum_j p_i \eta_i \).

We now apply Eq. (3) to the present problem. Our ensemble is \( \{ \frac{1}{2d} U_k | x \rangle \} \) with \( i = x, k \) a double index, \( p_{x,k} = \frac{1}{2d}, \mu = \frac{d}{2} \), and \( \langle \phi_j | \mu \rangle \langle \phi_j | \rangle = \frac{1}{2} \) for all \( j \). Putting all these in Eq. (3),

\[
I_c(\rho_{AC|B}) = \max_M \left[ \log 2d + \sum_{jxk} \frac{\alpha_j}{2d} |\langle \phi_j | U_k | x \rangle|^2 \log \frac{|\langle \phi_j | U_k | x \rangle|^2}{2} \right]
\]

\[
= \max_M \left[ \log d + \sum_j \frac{\alpha_j}{d} \left( \frac{1}{2} \sum_{xk} |\langle \phi_j | U_k | x \rangle|^2 \log |\langle \phi_j | U_k | x \rangle|^2 \right) \right]
\]

where we have used \( \sum_j \alpha_j = d \) and \( \forall j, \sum_k |\langle \phi_j | U_k | x \rangle|^2 = 1 \) to obtain the last line. Since \( \sum_j \alpha_j = d \), the second term is a convex combination, and can be upper bounded by maximization over just one term:

\[
I_c(\rho_{AC|B}) \leq \log d + \max_{\langle \phi |} \frac{1}{2} \sum_{xk} |\langle \phi | U_k | x \rangle|^2 \log |\langle \phi | U_k | x \rangle|^2 .
\]

(4)

Note that \(-\sum_{xk} |\langle \phi | U_k | x \rangle|^2 \log |\langle \phi | U_k | x \rangle|^2 \) is the sum of the entropies of measuring \( | \phi \rangle \) in the computational basis and the conjugate basis. Reference [6] proves that such a sum of entropies is at least \( \log d \), no matter how \( | \phi \rangle \) is chosen. Lower bounds of this type are called entropic uncertainty inequalities, which quantify how much a vector \( | \phi \rangle \) cannot be simultaneously aligned with states from a set of bases. It follows that \( I_c(\rho_{AC|B}) \leq \frac{1}{2} \log d \). Equality can in fact be attained when Bob measures in the computational basis, so that \( I_c(\rho_{AC|B}) = \frac{1}{2} \log d \) and \( I_c(\rho_{A|BC}) - I_c(\rho_{AC|B}) = 1 + \frac{1}{2} \log d \).

We remark that incremental proportionality remains violated for multiple copies of \( \rho \). Wootters proved that [7] the accessible information from \( m \) independent draws of an ensemble \( E \) of separable states is additive, \( I_{acc}(E^{\otimes m}) = m I_{acc}(E) \). It follows \( I_c(\rho^{\otimes m}) = m I_c(\rho) \) in our example.

2.3. Direct generalizations – locking by encoding in an unknown basis

The result in Section 2.1 is suggestive – when encoding the classical message in a number of possible bases, Bob’s best measurement is to guess the basis and measure accordingly.

Consider direct generalizations of the locking scheme above – in which multiple bases are used to lock accessible information for Bob. It is highly desirable to be able to lock all but a negligible amount of accessible information, using a key with size negligible compared to the change in \( I_{acc} \). Furthermore, beyond information theoretical considerations, it will also be nice to have schemes that can be efficiently implemented. A variety of interesting results are obtained in the past 5 years, but there are no definitive solution. We now explain these results briefly.

2.3.1. Full set of mutually unbiased bases

The earliest example uses 2 conjugate bases to lock the message. There is a natural generalization of 2 conjugate bases to a set of \textit{mutual unbiased bases} (MUBs) [8, 9], with the defining property that the inner product between any two states from two different bases has magnitude \( \frac{1}{\sqrt{d}} \) in a \( d \)-dimensional system.
Thus, it is natural to suspect that the same effect holds for $t \geq 2$ mutual unbiased bases (MUBs) [9] — that Bob’s accessible information is upper bounded by $\frac{1}{t} \log d$ before the communication. Indeed, for the case when the dimension $d$ is a prime power and a full set of MUBs are used ($t = d + 1$)

$$I_c(\rho_{AC}|B) \leq \log d - \log(d + 1) + 1 = 1 - \log \left(1 + \frac{1}{d}\right)$$

and

$$I_c(\rho_{AB|C}) - I_c(\rho_{A|BC}) \geq 2\log(d + 1) - 1$$

This follows from an entropic uncertainty inequality for the full set of MUBs due to Sanchez [10].

The scheme removes nearly all the accessible information from Bob, but the key size is now comparable to the change in $I_c$ and thus the scheme cannot be properly considered as “locking.”

2.3.2. Small number of MUBs Since a set of MUBs conceals accessible information well (for $t = 2$ or $t = d + 1$), researchers naturally turn to the possibility of locking with a small number of MUBs, with the hope that choosing one out of $t$ MUBs at random to encode a message can lock the accessible information down to $\frac{1}{t} \log d$. (We will see in Section 2.4 that one cannot lock better.)

The problem of bounding Bob’s accessible information appears to be mathematically complicated. The community only has some partial results.

(i) A simple investigation is a numerical optimization of Bob’s measurements for small primes $d$. During the investigation leading to [5], an optimization for $|\phi\rangle$ in Eq.(4) was performed to provide a numerical upper bound of the accessible information that varies as $\approx \frac{1}{t} \log d + c$ where $c \approx 1$ is independent of $t$.

It becomes clear in this investigation that different $t$-subsets of the full set of MUBs are generally inequivalent, and the numerical bound depends on the particular choice. Since the observed dependence is small, this simulation uses a particular order of the MUBs and simply takes the first $t$ MUBs. This study focusing on prime values of $d$ misses an important phenomenon to be discussed next.

(ii) For a while, mutual unbiasedness was believed to be a central ingredient for locking. Such intuition turns out questionable. Reference [11] presents special choices of $t = \sqrt{d}$ MUBs that do not lock better than $t = 2$ MUBs.

One simple example holds when $t$ is a prime-power. Let $X$ and $Z$ be the generalized Pauli matrices acting on $t$ dimensions, and $\omega$ be a primitive $t^{th}$ root of unity. (In other words, $X|a\rangle = |(a+1) \mod t\rangle$ and $Z|a\rangle = \omega^a|a\rangle$.)

Consider the eigenbases of $Z$ and $XZ^k$ for $k = 0, \ldots, t-1$. It was shown in [12] that they form a maximal set of MUBs on $t$ dimensions. The encoded message can be taken as the label for the eigenvalue of the eigenvector used.

Let $B_1, B_2$ be a pair of MUBs for a Hilbert space $H_1$, and $B_3, B_4$ be another pair of MUBs for another Hilbert space $H_2$. Consider the tensor product basis formed from $B_1$ and $B_3$, and that formed from $B_2$ and $B_4$. They are mutually unbiased on $H_1 \otimes H_2$.

The above method can be used to define $t+1 = \sqrt{d+1}$ MUBs for a $d$-dimensional Hilbert space as follows. The first one is the tensor product basis defined by $Z$ and $Z^{-1}$. The log $d$-bit message has two parts — the label of the eigenvalue of $Z \otimes I$ and that of $I \otimes Z^{-1}$. Each of the other $t$ bases is the tensor product basis defined by $XZ^k$ and $XZ^{-k}$ for $k = 0, \ldots, t-1$. The message consists of the labels of the eigenvalues of $XZ^k \otimes I$ and $I \otimes XZ^{-k}$.
Now, Bob’s optimal measurement is that of $X \otimes X$ and $Z \otimes Z^{-1}$ (this is the measurement along the generalized Bell basis). To see optimality, note that Bob can multiply the appropriate powers of his two measurement outcomes to obtain the product of the pair of messages for each possible choice of the basis, thus his accessible information is at least $\frac{1}{2} \log d$. Following earlier work for $t = 2$, it cannot be higher.

(iii) Note that locking is defined information theoretically, without reference to limitations of computation power. In practical applications, for states with dimension $d$ or size $n = \log d$, it makes sense to consider a weaker notion of locking in which Bob’s optimal measurement is limited to those implementable with poly($n$)-sized circuits. This was proposed and analyzed in [13]. It states that, if Bob’s circuit has size at most $n^k$, then, choosing $(k + 2) \log n + 3$ bases randomly from the full set of $d + 1$ MUBs can lock Bob’s accessible information down to less than 2 bits.

The idea is simple. The bound by Sanchez [10] states that the MUBs locks well on average, thus a random choice of a small subset also locks quite well (according to the Chernoff bound) and the probability that the random choice fails is small. (Such argument can be made rigorous since the effectiveness of locking can be quantified by the entropic uncertainty inequalities.) Now, the computational bound states that there are at most $2^{n^k}$ possible measurements for some constant $c$. The union bound over all such measurements can then be applied to obtain the stated result. Note that the argument is an existential proof of an efficient scheme.

A main advantage of MUBs is that, the encoding and decoding schemes are easy to implement. However, locking with MUBs occurs to be extremely difficult to analyze. It is still an open question to find an efficiently implementable locking scheme which takes a negligible key and provably locks all but a negligible amount of accessible information.

However, if the concern is primarily information theoretic – focusing on the limit to which accessible information can be locked rather than practicality, then locking schemes such as those using random bases are much easier to analyze.

2.3.3. Locking with random bases One expects random bases to lock at least as well as MUBs because two random bases are approximately mutually unbiased in large dimensions. The advantage of using random bases is that they are much easier to analyse.

More precise, the new locking scheme can be obtained from Eq. (2) by replacing the $t = 2$ conjugate bases with an arbitrary number $t$ of independently drawn random bases. In other words, the $U_0, \cdots, U_{t-1}$ are independently drawn from the Haar measure.

The analysis in Section 2.2 stays the same, but now it is possible to prove an entropic uncertainty inequality for these random bases [14]. It was proved that there is a positive constant $C''$ such that

$$\Pr \left( \inf_{\phi} \frac{1}{t} \sum_{j=1}^{t} H_j \leq (1-\epsilon) \log d - 3 \right) \leq (\frac{10}{\epsilon})^{2d} \exp \left[ - t \left( \frac{e^{C''d}}{2(\log d)^2} - 1 \right) \right],$$

(7)

where $p_j(i) = |\langle i | U_j^\dagger | \phi \rangle|^2$, and $H_j$ is the entropy for the distribution $p_j$. Choosing $t = (\log d)^3$ ensure the vanishing of the RHS of Eq. (7) – in particular it is smaller than 1 and there exist instances (of the random $U_k$’s) with $\inf_{\phi} \frac{1}{t} \sum_{j=1}^{t} H_j > (1-\epsilon) \log d - 3$. Then both $I_{\epsilon}(\rho_{ACB}) \leq \epsilon \log d + 3$ and the key size $\log t = 3 \log \log d$ are negligible compared to $\log d$.

In [13] it is noted that choosing $\epsilon = \frac{1}{\log d}$ and $t = (\log d)^4$ in the above can lock the accessible information to $\leq 4$ bits (a constant) while increasing the key size only to $\log t = 4 \log \log d$. 


2.4. Limitations of locking with bases
We have seen various results on the locking scheme based on Eq. (2). Each of these schemes consists of a set of bases known to both Alice and Bob, and Alice encodes the message $|x\rangle$ in one of these bases at random. Each can be specified by the dimension $d$, the number of bases $t$, and the set of bases.

2.4.1. Lower bound on accessible information
By using a full set of MUBs, the accessible information is upper bounded by 1, and by using poly$(\log \log d)$ random bases, the accessible information is upper bounded by 4 or so.

This begs the question – are there better choices of the unitaries that removes the small residual accessible information? This question was studied at the very early days of “modern quantum information” (1994). Reference [15] presents a lower bound of $\approx 0.577$ (Euler’s constant) on the accessible information of any ensemble of pure states. It means that even for very big dimension and key size, the accessible information is a constant far from being “small.”

In contrast, consider encryption of a quantum or classical message using a classical key (the classical or quantum one-time-pad [16, 17, 18]) which is similar to locking in encoding the message in a basis unknown to the eavesdropper who has possession of the encrypted/encoded state. The key size is at least as big as the message in this case, but the accessible information on the encoded message is exactly 0.

The reason for the difference is the following. In locking, we consider the accessible information of the ensemble of all possible (pure) states sent to Bob, each with a label on the message $x$ and one on the basis $k$. In encryption, the key is not part of the classical label in the ensemble. In particular, the ensemble consists of mixed states $\rho_x = \frac{1}{t} \sum_{k=1}^{t} U_k |x\rangle \langle x| U_k^\dagger$. In Section 2.5, we will discuss locking schemes involving mixed states.

2.4.2. Necessity of a uniform prior message distribution
Note that in the proof of the locking effect, uniformity of the distribution of $x, k$ is not just a mathematical convenience, but is crucial for the result. It is still open what type of nearly uniform distribution for $x, k$ will retain the locking feature.

2.4.3. The guessing bound [5]
When locking with an unknown basis, and more generally, when the message system $C$ is classical, one possible measurement for Bob to perform on $\rho_{AC|B}$ (the locked state) is to guess the message $C$ and then apply the corresponding optimal measurement. This provides an upper bound (called the guessing bound) on the jump of the classical mutual information in terms of the size of $C$. Let there be $t$ possible messages, i.e., the size of $C$ is $\log t$ bits. Then, the above argument says

$$\frac{1}{t} \left( I_c(\rho_{A|CB}) - \log t \right) \leq I_c(\rho_{AC|B})$$

and thus the jump is upper bounded as

$$I_c(\rho_{A|CB}) - I_c(\rho_{AC|B}) \leq \log t + (t - 1) I_c(\rho_{AC|B}).$$

2.4.4. The continuity bound [5]
Finally, the amount of initial correlation also limits the extent of the locking effect. In particular, an initially uncorrelated state does not exhibit locking. A continuity argument can be used to bound the extent of locking as a function of the initial (locked) mutual information. This holds for the most general communication structure...
Choose an arbitrary unitary $U$ of concern. In this case, we can consider a locking scheme given by

$$\rho_{ACB} = \frac{1}{dt} \sum_{x,k} |x⟩⟨x|_A \otimes |k⟩⟨k|_C \otimes (U_k|x⟩⟨x|U_k^†)_B.$$  \hspace{1cm} (11)

$I_c(\rho_{AC|B})$ is simply the accessible information on the uniform ensemble of states $\eta_x = \frac{1}{t} \sum_k U_k|x⟩⟨x|U_k^†.$

The analysis is similar to (and easier than) that in Section 2.2 and Eq. (4) is replaced by

$$I_c(\rho_{AC|B}) \leq \log d - \min_{|φ⟩} H(\{q_x\}) \hspace{1cm} (12)$$

where $q_x = 〈φ|\frac{1}{t} \sum_k U_k|x⟩⟨x|U_k^†|φ⟩$. The Lipschitz constant of $H(\{q_x\})$ is upper bounded by $rac{1}{t} \left( 4 + 8 \log d \right)^2$ and the expectation is $\log d$. A standard randomized argument then shows that $I_c(\rho_{AC|B}) \to 0$ for $t \approx \text{polylog}(d)$.

An interesting fact to note is the following. We can denote the three random variables: the (a) message, (b) Bob’s measurement outcome, and (c) the basis by $X$, $Y$, and $K$ respectively. Somewhat surprisingly, $I(X:Y|K) = I(XK:Y)$, because they are both equal to $I(X:Y|K)$ – this can be proved by using the chain rule and noting that $I(X:K) = I(Y:K) = 0$. Thus, the lower bound of Euler’s constant on $I(X:Y|K)$ also applies to $I(X:Y|K) = I(XY) + I(XK|Y)$. But the mixed state locking scheme makes the locked mutual information $I(X:Y)$ vanish and thus the $I(X:K|Y)$ term is responsible for the lower bound, and it is the correlation created between $X$ and $K$ (initially uncorrelated) due to knowing $Y$. This is what Bob learns in the pure state locking scheme!

2.5.2. Symmetric locking [20] Consider a computation basis $|xk⟩$ in $\mathbb{C}^d \otimes \mathbb{C}^t$. Consider the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^t \otimes \mathbb{C}^d \otimes \mathbb{C}^t$, and call the 4 systems 1, 2, 3, 4. Consider the state

$$\frac{1}{dt} \sum_{x=1}^d \sum_{k=1}^t |xk⟩⟨xk| \otimes |xk⟩⟨xk| \hspace{1cm} (13)$$

Choose an arbitrary unitary $U \in \mathcal{U}(\mathbb{C}^d \otimes \mathbb{C}^t)$ according to the Haar measure, and fix it for the rest of the discussion.

Apply the unitary $I_{12} \otimes U_{34}$ to the state, trace out system 4, and the remaining state has negligible accessible information across systems 12 vs 3, when $t \approx \text{polylog}(d)$. 

(quantum, two-way). More precisely, let $ρ$ be a bipartite state on $C^d \otimes C^d$ and $ρ’$ be obtained from $ρ$ by $l$ qubits of two-way communication. If $I_c(ρ) \leq \frac{1}{6 \ln^2 (d+1)}$, then,

$$I_c(ρ’) - I_c(ρ) \leq 2l - (2d)^2 \sqrt{2 \ln 2} I_c(ρ) \log \sqrt{2 \ln 2} I_c(ρ). \hspace{1cm} (10)$$

Note that the bound grows weak rapidly with the dimension $d$.

2.5. Mixed state locking schemes

We have seen in Section 2.4.1 that pure state schemes cannot lock accessible information to below Euler’s constant. However, if we use mixed states for encoding the message, the accessible information can be made vanishing while the key remains negligibly-sized compared to the amount of mutual information it can unlock.

2.5.1. Locking only the message but not the key [19] In some applications, the secrecy of the key is not of concern. In this case, we can consider a locking scheme given by

$$I_c(ρ_{AC|B}) \leq \min \{ H(\{q_x\}) \}$$  \hspace{1cm} (12)
2.6. Implications on security measures and blackhole information paradox

The fact accessible information can increase abruptly with a little extra classical information has implications on various other subjects.

First, in quantum key distribution (QKD), security of the protocol has been measured in terms of the expected accessible information available to the most powerful eavesdropper on the key generated. However, implicit in such security definition is the assumption that the eavesdropper applies the best measurement in the end of the QKD protocol. But in practice, the eavesdropper can delay the measurement until more quantum or classical information concerning the key becomes available, in particular when the key is being used in other cryptographic protocols. The possibility of a disproportionate increase in accessible information means that it is not a suitable security measure [21, 22]. The locking effect has motivated research in better security measure of QKD (universally composable security definition [21, 23]).

Second, [24] pointed out that possible locking effect should be considered in the study of evaporating blackholes. For the simplest example, a message can be dropped into a blackhole which subsequently evaporates. Even when the evaporation is nearly (and not totally) complete, the emission can have little accessible information on the message, if a small random subsystem is left inside the blackhole, due to the symmetric locking effect. On the other hand, conclusion based on locking is difficult to make, because a message that is not uniformly distributed or encoded in an error correcting code may not be locked.

3. Locking other quantities

The schemes for locking accessible information (with unknown basis) can be applied to locking accessible information of Eve (the environment) which makes the entanglement of formation $E_F$ nearly maximal (by using the construction in [25] but the random basis locking scheme). Giving the environment the key (by discarding) changes $E_F$ to nearly zero. The same holds for the entanglement costs $E_C$ which is just $E_F$ in that example. A very different method but similar result for $E_F$ is given in [26] (but whether $E_F = E_C$ is unknown in this case).

Acknowledgments

My deepest thanks to friends and colleagues whose research and discussion in this area have been a source of profound excitement and inspiration to me. Risking some careless omissions, this list includes Andris Ambainis, Manuel Ballester, Harry Buhrman, Matthias Christandl, David DiVincenzo, Frederic Dupuis, Aram Harrow, Patrick Hayden, Karol, Michal, and Pawel Horodecki, Robert Koenig, Hoi-Kwong Lo, Jonathan Oppenheim, Renato Renner, Graeme Smith, John Smolin, Barbara Terhal, Steph Wehner, Andreas Winter, and Jan whose last name I still have to learn.

References

[1] Terhal B M, Horodecki M, Leung D W and DiVincenzo D P 2002 The entanglement of purification J. Math. Phys. 43 4286 (Preprint quant-ph/0202044)
[2] Cover T and Thomas J 1991 Elements of Information Theory. (New York: Wiley)
[3] Peres A 1993 Quantum Theory: Concepts and Methods (Dordrecht: Kluwer Academic)
[4] When $\rho$ is classical (pure), the measurement along the local product basis (Schmidt basis) is optimal by the data processing inequality [2] and the fact other measurement outcomes are obtainable by local processing of the optimal one.
[5] DiVincenzo D, Horodecki M, Leung D, Smolin J and Terhal B 2004 Locking classical correlation in quantum states Phys. Rev. Lett. 92 067902
[6] Maassen H and Uffink J 1988 Generalized entropic uncertainty relations Phys. Rev. Lett. 60 1103
[7] DiVincenzo D, Leung D and Terhal B 2001 Quantum data hiding IEEE Trans. Info. Theory 48 580 (Preprint quant-ph/0103098)
[8] Schwinger J 1960 Unitary operator bases Proc. Nat. Acad. Sci. USA 46 570
[9] Wootters W and Fields B 1989 Geometrical description of quantum state determination *Annals of Physics* **191** 368
[10] Sanchez J 1993 Entropy uncertainty and certainty relations for complementary observables *Phys. Lett.* A **173** 233
[11] Ballester M and Wehner S 2006 Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases *Phys. Rev.* A **73** 022110
[12] Bhattacharya S, Boykin P, Roychowdhury V and Vatan F 2001 A new proof for the existence of mutually unbiased bases *Preprint* quant-ph/0103162
[13] Buhrman H, Christandl M, Hayden P, Lo H-K and Wehner S 2005 Possibility, impossibility and cheatsensitivity of quantum bit string commitment *Preprint* quant-ph/0504078v1, Section 5.3 and Appendix
[14] Hayden P, Leung D W, Shor P W and Winter A 2004 Randomizing quantum states: Constructions and applications *Commun. Math. Phys.* **205** 371 (*Preprint* quant-ph/0307104)
[15] Jozsa R, Robb D and Wootters W 1994 A lower bound for accessible information in quantum mechanics *Phys. Rev.* A **49** 668
[16] Shannon C E 1949 Communication theory of secrecy systems *Bell Sys. Tech. J.* **28** 656
[17] Ambainis A, Mosca M, Tapp A and de Wolf R 2000 Private quantum channels in *IEEE Symposium on Foundations of Computer Science (FOCS)* 547 (*Preprint* quant-ph/0003101)
[18] Boykin P O and Roychowdhury V 2000 Optimal encryption of quantum bits *Preprint* quant-ph/0003059
[19] “Locking only the message but not the key,” the possibility to bring the accessible information on x (but not on k) to a vanishing amount was brought up during a Bellairs Workshop on Randomization Techniques in March 2005, between P. Hayden, D. Leung, G. Smith, and A. Winter. A photograph of the blackboard on which an upper bound of the Lipschitz constant was derived remains the only write-up.
[20] Dupuis F, Hayden P, Leung D and Jan, Symmetric locking in preparation
[21] Ben-Or M, Horodecki M, Leung D, Mayers D and Oppenheim J 2005 The universal composably security of quantum key distribution in *The 2nd Theory of Cryptography Conference (TCC 2005) LNCS* ed Kilian J (Berline Heidelberg: Springer-Verlag) p 385 (*Preprint* quant-ph/0409078)
[22] Koenig R, Renner R, Bariska A and Maurer U 2007 Locking of accessible information and implications for the security of quantum cryptography *Phys. Rev. Lett.* **98** 140502 (*Preprint* quant-ph/0512021)
[23] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries in *The 2nd Theory of Cryptography Conference (TCC 2005) LNCS* ed Kilian J (Berline Heidelberg: Springer-Verlag) p 407 (*Preprint* quant-ph/0403133)
[24] Smolin J and Oppenheim J 2006 Locking information in black holes *Phys. Rev. Lett.* **96** 081302 (*Preprint* quant-ph/0507287)
[25] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Locking entanglement measures with a single qubit *Phys. Rev. Lett.* **94** 200501 (*Preprint* quant-ph/0404096)
[26] Hayden P, Leung D W and Winter A 2006 Aspects of generic entanglement *Commun. Math. Phys.* **265** 95 (*Preprint* quant-ph/0407049)