Maximal Privacy without Coherence

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th><strong>Citation</strong></th>
<th>Leung, Debbie, Ke Li, Graeme Smith, and John A. Smolin. &quot;Maximal Privacy without Coherence,&quot; Phys. Rev. Lett. 113, 030502 (July 2014). © 2014 American Physical Society</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>As Published</strong></td>
<td><a href="http://dx.doi.org/10.1103/PhysRevLett.113.030502">http://dx.doi.org/10.1103/PhysRevLett.113.030502</a></td>
</tr>
<tr>
<td><strong>Publisher</strong></td>
<td>American Physical Society</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Final published version</td>
</tr>
<tr>
<td><strong>Accessed</strong></td>
<td>Sat Feb 16 00:15:14 EST 2019</td>
</tr>
<tr>
<td><strong>Citable Link</strong></td>
<td><a href="http://hdl.handle.net/1721.1/88610">http://hdl.handle.net/1721.1/88610</a></td>
</tr>
<tr>
<td><strong>Terms of Use</strong></td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.</td>
</tr>
<tr>
<td><strong>Detailed Terms</strong></td>
<td></td>
</tr>
</tbody>
</table>
Maximal Privacy without Coherence

Debbie Leung,1 Ke Li,2,3 Graeme Smith,2 and John A. Smolin2

1Institute for Quantum Computing, University of Waterloo, Waterloo N2L 3G1, Ontario, Canada
2IBM T. J. Watson Research Center, Yorktown Heights, New York 10598, USA
3Center for Theoretic Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

(Received 7 February 2014; published 16 July 2014)

Privacy is a fundamental feature of quantum mechanics. A coherently transmitted quantum state is inherently private. Remarkably, coherent quantum communication is not a prerequisite for privacy: there are quantum channels that are too noisy to transmit any quantum information reliably that can nevertheless send private classical information. Here, we ask how much private classical information a channel can transmit if it has little quantum capacity. We present a class of channels \(\mathcal{N}_d\) with input dimension \(d^2\), quantum capacity \(Q(\mathcal{N}_d) \leq 1\), and private capacity \(P(\mathcal{N}_d) = \log d\). These channels asymptotically saturate an interesting inequality \(P(\mathcal{N}) \leq (1/2)[\log d_A + Q(\mathcal{N})]\) for any channel \(\mathcal{N}\) with input dimension \(d_A\) and capture the essence of privacy stripped of the confounding influence of coherence.

Any communication link can be modeled as a (noisy) quantum channel. Given a sender, Alice, and a receiver, Bob, a quantum channel from Alice to Bob is a completely positive trace preserving map from an input space \(A\) to an output space \(B\). The capability of a quantum channel for communication is measured by various capacities, one for each type of information to be transmitted. The classical capacity \(C(\mathcal{N})\) quantifies the capability of a quantum channel \(\mathcal{N}\) for transmitting classical information, in bits per channel use. The private capacity \(P(\mathcal{N})\) gives the maximum rate of private classical communication and quantifies the optimal performance for key exchange. Finally, the quantum capacity \(Q(\mathcal{N})\), measured in qubits per channel use, establishes the ultimate limit for transmitting quantum information and the performance of quantum error correction.

The three capacities mentioned above clearly satisfy \(Q(\mathcal{N}) \leq P(\mathcal{N}) \leq C(\mathcal{N})\). The analogies between coherent transmission and privacy, and between entanglement and quantum error correction. As an aside, our channels combine features of private states from [1] and retrocorrectable or random-phase-coupling channels of [4–7] (these channels have large assisted capacities but small \(C, P,\) and \(Q\)). In addition to finding a very tight bound on \(Q(\mathcal{N}_d)\), we can also compute both \(P(\mathcal{N}_d)\) and \(C(\mathcal{N}_d)\), a relative rarity in quantum information, especially for a highly nontrivial channel.

Upper bound on privacy.—Recall that any quantum channel can be expressed as an isometry followed by a partial trace, \(\mathcal{N}(\rho) = \text{tr}_E U \rho U^\dagger\), where \(U : A \rightarrow BE\) with \(U^\dagger U = I\). The complementary channel acts as \(\mathcal{N}^*(\rho) = \text{tr}_B U \rho U^\dagger\), and allows us to define the coherent information of a channel as

\[
Q^{(1)}(\mathcal{N}) = \max_{\phi_A} I_{\text{coh}}(\mathcal{N}, \phi_A) = \max_{\phi_A} \left[ S(B) - S(E) \right],
\]

where the maximization is taken over input quantum states \(\phi_A\), and \(S(B), S(E)\) are the von Neumann entropies of \(\rho_B = \mathcal{N}(\phi_A)\) and \(\rho_E = \mathcal{N}^*(\phi_A)\), respectively. In turn, the

\[
P(\mathcal{N}) \leq \frac{1}{2} \left[ \log d_A + Q(\mathcal{N}) \right],
\]

for any channel \(\mathcal{N}\) with input dimension \(d_A\), quantifying the effect of incoherence in the channel transmission on privacy: inasmuch as a channel cannot simply transmit quantum information, it must devote half of its input space to acting as a “shield” system (as defined in [1]). While Eq. (1) can be inferred from properties of squashed entanglement of quantum states [2,3], this particular form appears to be new. Our relatively simple proof involves very different techniques.

As an aside, our channels combine features of private states from [1] and retrocorrectable or random-phase-coupling channels of [4–7] (these channels have large assisted capacities but small \(C, P,\) and \(Q\)). In addition to finding a very tight bound on \(Q(\mathcal{N}_d)\), we can also compute both \(P(\mathcal{N}_d)\) and \(C(\mathcal{N}_d)\), a relative rarity in quantum information, especially for a highly nontrivial channel.
quantum capacity is proved [8–10] to be the regularized coherent information:  
\[ Q(N) = \lim_{n \to \infty} (1/n)Q^{(1)}(N^n). \]
We say that a quantum channel \( N \) is degradable if \( \hat{N} = D \circ N \) for some channel \( D \) [11] (\( N \) can be degraded to generate \( \hat{N} \)). For degradable channels, \( P(N) = Q(N) = Q^{(1)}(N) \) [12]. Degradable channels also provide a powerful tool for upper bounding the capacities of general channels [13]. If a channel \( N = L \circ M \) is a composition of two channels \( L \) and \( M \) with \( M \) degradable, we have
\[
Q(N) \leq P(N) = P(L \circ M) \leq P(M) = Q^{(1)}(M).
\]

We now have all the tools for proving Eq. (1). For any channel \( N \), define \( M \) as
\[
M(\rho) = \frac{1}{2} [\rho \otimes |0\rangle\langle 0| + N(\rho) \otimes |1\rangle\langle 1|].
\]
Then, \( \hat{N} = L \circ M \), where \( L(\sigma) = (N \otimes \Pi_0 + I \otimes \Pi_1)(\sigma) \) and \( \Pi_i(\mu) = \langle i|\mu|i\rangle \). To see that \( M \) is degradable, note that the complementary channel of \( M \) is
\[
\hat{M}(\rho) = \frac{1}{2} [|e\rangle\langle e| \otimes |0\rangle\langle 0| + \hat{N}(\rho) \otimes |1\rangle\langle 1|],
\]
where \( |e\rangle \langle e| \) is an orthogonal erasure flag. Choose a degrading map \( D \) that first flips the flag qubit (the second register), and then conditioned on the flag being \( |1\rangle \) or \( |0\rangle \), applies \( \hat{N} \) to the first register or resets it to \( |e\rangle \langle e| \). So, \( \hat{M} = D \circ M \). Now, applying Eq. (2),
\[
P(N) \leq Q^{(1)}(M)
\]
\[
= \max_{\phi_A} [S(B_1B_2) - S(E_1E_2)]
\]
\[
= \max_{\phi_A} [S(\phi_A) + S(N(\phi_A)) - S(\hat{N}(\phi_A))]
\]
\[
\leq \frac{1}{2} [\log d_A + Q^{(1)}(N)].
\]
This bound is, in fact, stronger than Eq. (1), since \( Q^{(1)}(N) \leq Q(N) \).

**Channel construction.**—The family of channels \( N_d \) asymptotically saturating Eq. (1) is given by
\[
\text{A}_1 \quad \text{P} \quad \text{B}, \text{“V”}
\]
\[
\text{A}_2 \quad \text{V} \quad \text{E}, \text{“V”}
\]

The isometric extension of the channel \( N_d \) is given by the operations in the dashed box. \( N_d \) has two input registers \( A_1 \) and \( A_2 \), each of dimension \( d \). A random unitary \( V \) is applied to \( A_2 \), followed by a controlled phase gate \( P = \sum_{j=0}^{d-1} \omega^{(j)} |i\rangle \otimes |j\rangle \langle j| \) acting on \( A_1A_2 \), where \( \omega \) is a primitive \( d \)th root of unity. Bob receives only \( A_1 \) (now relabeled \( B \)) and “V,” which denotes a classical register with a description of \( V \). The \( A_2 \) register is discarded. The complementary channel has outputs \( A_2 \) and “V.” More formally, let \( W_V = (I \otimes V) \), \( N^V(\rho) = \text{tr}_B W_V \rho W_V^\dagger \), and \( N_d = E_V N^V \otimes |V\rangle\langle V|_{V_B} \), where the register \( V_B \) holds “V.” The isometric extension is given by
\[
U_d|\psi\rangle_{A_1A_2} = \sum_{V} \text{tr}[V](W_V|\psi\rangle_{A_2}) \otimes |V\rangle_{V_B} \otimes |V\rangle_{V_B'},
\]
and the complementary channel acts as \( \hat{N}_d(\rho) = \text{tr}_{B_{V_B}} U_d \rho U_d^\dagger = E_{V_B} \text{tr}_B W_V \rho W_V^\dagger \otimes |V\rangle\langle V|_{V_B'} \).

Here is the intuition behind the construction: The classical capacity of this channel is at least \( \log d \), since the \( d \) computation basis states of \( A_1 \) are transmitted without error. Furthermore, we will see that inserting a maximally mixed state into \( A_2 \) keeps the environment ignorant of the transmitted message so \( P(N_d) \geq \log d \). However, as the classical capacity is no greater than the output entropy, and “V” is independent of the input, \( C(N_d) \leq \log d \), so, \( C(N_d) = P(N_d) = \log d \). However, the channel is constructed to suppress the quantum capacity, since without knowing \( V \), Alice cannot avoid the \( P \) gate from entangling \( A_1 \) with \( A_2 \), thereby dephasing \( A_1 \). We will prove \( Q(N_d) \leq 1 \).

Our proofs of the above statements hold for any \( V \) drawn from a so-called exact unitary 2-design, and thus, \( V \) can be a random Clifford gate [14]. In our work to lower bound \( Q(N) \), a Haar distributed \( V \) is analyzed as a first attempt. We expect a similar conclusion for random Clifford gate \( V \).

**Private capacity.**—For an ensemble \( E = \{p_i, \phi_i\} \) and channel \( N \), the private information is defined as
\[
P^{(1)}(N, E) = \chi(N, E) - \chi(\hat{N}, E),
\]
with Holevo information \( \chi(N, E) = S(\rho) - \sum_i p_i S(\rho_i) \) evaluated on the induced ensemble \( N(E) = \{p_i, \rho_i = N(\phi_i)\} \) and average state \( \rho = \sum_i p_i \rho_i \) [similarly for \( \chi(N, E) \)]. For any ensemble \( E \), \( P^{(1)}(N, E) \) is an achievable rate for private communication and thus a lower bound on \( P(N) \) [10].

For our channel \( N_d \), choosing probabilities \( p_i = 1/d \) and states \( \phi_i = |i\rangle|\langle i|_{A_1} \otimes (I/d)_{A_2} \) for \( i = 1, \ldots, d \) gives \( \chi(N_d, E) = \log d \) and \( \chi(\hat{N}_d, E) = 0 \), so \( P(N_d) \geq \log d \), as claimed.

Bipartite states carrying a key (called private states) are defined and characterized in [1]. We note that the Choi state of \( N_d \) with Alice holding \( R_1 \), \( R_2 \) is an exact private state of key systems \( R_1 \) and \( B \) and a single shield system \( R_2 \). We refer interested readers to Ref. [1] for further details.
Upper bound on quantum capacity.—To get an upper bound on $Q(N_d^n)$, we consider the asymptotic behavior of the coherent information, $Q^{(1)}(N_d^n)$, for arbitrarily large $n$. We first define suitable notations. We group together the first input $A_1$ from all $n$ channel uses, call it $A_1^n$, and we similarly define $A_2^n, B^n, V^n_B$, and $V^n_E$. We use $x$ to denote an $n$-tuple of integers $(x_1, x_2, \ldots, x_n)$, where each $x_i$ has range $\{0, 1, \ldots, d - 1\}$, and similarly for $y$. Finally, a random $V$ is drawn from each channel use, and we denote the tensor product of $n$ such independent and identically drawn unitaries by $V$.

We consider the $n$-shot coherent information $Q^{(1)}(N_d^n) = \max_{\phi_{A_1^n A_2^n}} [S(B^n|V^n_B) - S(E^n V^n_E)]$. Since Bob and the environment receive the same classical description “$V$,” $Q^{(1)}(N_d^n) = \max_{\phi_{A_1^n A_2^n}} [S(B^n|V^n_B) - S(E^n|V^n_E)]$. First, we show that the optimal input state has a special form.

**Lemma 1:** For the channel $N_d^n$ of Eq (5), the coherent information $I_{coh}(N_d^n, \phi_{A_1 A_2})$ is maximized on states of the form

$$\phi_{A_1 A_2} = \sum_x p_x |x\rangle \langle x|_{A_1^n} \otimes |\phi^x\rangle \langle \phi^x|_{A_2^n},$$

where $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ is a standard basis state on $A_1^n$.

**Proof:** First, we show that the optimal state has the form

$$\sigma_{A_1 A_2} = \sum_x p_x |x\rangle \langle x|_{A_1^n} \otimes |\phi^x\rangle \langle \phi^x|_{A_2^n},$$

where $|\phi^x\rangle$ is potentially mixed. To see this, let $\psi_{A_1 A_2}^x$ be an arbitrary input state, and $\sigma_{A_1 A_2} = (P^{\otimes n} \otimes I_{A_2^n}) |\psi_{A_1 A_2}^x\rangle \langle \psi_{A_1 A_2}^x|$, where $P = (1/d) \sum_{i=1}^d Z_i \rho Z_i^\dagger$ is the completely depolarizing map. So, $\sigma_{A_1 A_2}$ indeed has the form given by Eq. (8). Now,

$$I_{coh}(N_d^n, \sigma_{A_1 A_2}) = I_{coh}(N_d^n \circ (P^{\otimes n} \otimes I_{A_2^n}), |\psi_{A_1 A_2}^x\rangle \langle \psi_{A_1 A_2}^x|) = I_{coh}(P^{\otimes n} \circ N_d^n, |\psi_{A_1 A_2}^x\rangle \langle \psi_{A_1 A_2}^x|) \geq I_{coh}(N_d^n, |\psi_{A_1 A_2}^x\rangle \langle \psi_{A_1 A_2}^x|),$$

since $P$ commutes with $N_d^n$, and $P$ is unital so the entropy cannot decrease. Meanwhile, the reduced state on $E^n V^n_E$ remains the same, so the coherent information cannot decrease.

Next, we show that $|\phi^x\rangle$ in Eq. (8) can be taken to be pure. Fix an arbitrary $x$. Let $\phi^x_{A_2^n} = \sum_w q(w|x) |\mu^w\rangle \langle \mu^w|$, and for each $w$, let

$$\eta^w_{A_1 A_2^n} = p_x |x\rangle \langle x|_{A_1^n} \otimes |\mu^w\rangle \langle \mu^w| + \sum_{y \neq x} p_y |y\rangle \langle y|_{A_1^n} \otimes |\phi^y_{A_2^n}|.$$

We now show that

$$\exists w \text{ s.t. } I_{coh}(N_d^n, \eta^w_{A_1 A_2^n}) \geq I_{coh}(N_d^n, \phi_{A_1 A_2^n}).$$

To see this, note that for each $x$ and $w$, $N_d^n(\sigma_{A_1 A_2}) = N_d^n(\eta^w_{A_1 A_2^n})$, so those states have the same entropy. For the complementary channel, observe that by construction,

$$\sigma_{A_1 A_2} = \sum_w q(w|x) \eta^w_{A_1 A_2^n},$$

so $N_d^n(\sigma_{A_1 A_2}) = \sum_w q(w|x) \hat{N}_d^n(\eta^w_{A_1 A_2^n})$, and by concavity of entropy,

$$S(E^n V^n_E|\hat{N}_d^n(\eta^w_{A_1 A_2^n})) \geq \sum_w q(w|x) S(E^n V^n_E|\hat{N}_d^n(\eta^w_{A_1 A_2^n})).$$

so Eq. (9) holds. Iterating this process gives an optimal state of the form given by Eq. (7).

The optimal input in Eq. (7) gives a conditional output entropy of $S(B^n|V^n_B) = S(p_x) = -\sum_x p_x \log p_x$. (Taking classical distributions as diagonal density matrices, we use $S$ to denote both the von Neumann and the Shannon entropies.) We need to compare $S(B^n|V^n_B)$ to the conditional output entropy of the environment, $S(E^n|V^n_E)$. To do so, note that the controlled-phase gate for one channel can be expressed as $P = \sum_i Z_i |i\rangle \otimes Z_i$, where $Z_i |j\rangle = \omega^{ij} |j\rangle$. For the $n$-tuple $x$, we define $Z^x = Z_{x_1} \otimes \cdots \otimes Z_{x_n}$. The output state on the environment is

$$\rho_{E^n V^n_E} = \mathbb{E}_V \sum_x p_x \rho^n_{E^n} \otimes |V\rangle \langle V|_{V^n_E},$$

where

$$\rho^n_{E^n} = Z^n V^n |\phi^x\rangle \langle \phi^x| V^n^\dagger Z^{-x}.$$

If, for each $V$ and $x \neq y$, $\rho^n_{E^n}$ and $\rho^n_{E^n}$ were orthogonal, we would have $S(E^n|V^n_E) = S(p_x)$ and $Q^{(1)}(N_d^n) = 0$. Instead, we prove in the Supplemental Material (Lemma L.2) [16] that the Hilbert-Schmidt inner product $\mathbb{E}_V \text{tr} \rho^n_{E^n} \rho^n_{E^n}$ is low on average (over the choice of $V$).

**Lemma 2:** The states $\rho^n_{E^n}$ given by Eq. (11) satisfy

$$\mathbb{E}_V \text{tr} \rho^n_{E^n} \rho^n_{E^n} \leq \frac{1}{(d-1)^2 d_{H(x,y)}},$$

where $d_{H}(x,y) = \{|i| x_i \neq y_i\}$ is the Hamming distance between $x$ and $y$.

Next, we derive a lower bound on the output entropy of the environment, by considering the Rényi-2 entropy of many copies of $\rho^n_{E^n}$ using Lemma 2.

**Lemma 3:** For an input given by Eq. (7), conditioned on $V$, the output state on the environment $\rho^n_{E^n}$ satisfies

$$\sum_{x \in [d]^n} p_x \rho^n_{E^n}$$
We thus have can almost do so on results in an output state. Conditioning on the random unitaries of the channels, this state. The state ρ_E^N involves a mixture over (X)^m, which is m i.i.d. copies of X. Let X_m be the restriction of (X)^m to its typical set \{x^m : -(1/m)log p_{x^m} - S(X) \leq e\}. The typical set contains only x^m with almost equal probabilities. The asymptotic equipartition theorem (cf. Ref. [15], for example) says that, for any ε > 0, ∃m such that with probability at least 1 − ε, x^m is in the typical set. Consequently, the state ρ_E^N can be well approximated by ρ_E^{mN}, where the mixture is only taken over X_m.

Note that Eq. (12) applies to ρ_E^{N}, so

$$\mathbb{E}_V \text{tr}(\rho_E^V)^2 = \mathbb{E}_V \sum_{x,y} p_x p_y \text{tr}(\rho_E^{xV} \rho_E^{yV})$$

$$\leq \sum_{x,y} p_x p_y \frac{1}{(d-1)^{d_{(x,y)}}}$$

$$= \sum_{w=0}^n \frac{1}{(d-1)^w} \sum_x y_{d_{(x,y)} = w} p_x p_y$$

$$= \sum_{w=0}^n \frac{1}{(d-1)^w} \sum_x \sum_w p_x \rho_{x+w}$$

where the first inequality follows from Lemma 2. By the Cauchy-Schwartz inequality,

$$\sum_x p_x \rho_{x+w} \leq \sqrt{\sum_x p_x^2} \sqrt{\sum_x \rho_{x+w}^2} = \sum_x p_x^2.$$

We thus have

$$\mathbb{E}_V \text{tr}(\rho_E^V)^2 \leq \sum_{w=0}^n \frac{1}{(d-1)^w} \sum_x \sum_w p_x^2$$

$$= \sum_{w=0}^n \frac{1}{(d-1)^w} \left( \frac{n}{w} \right) (d-1)^w \sum_x p_x^2$$

$$= 2^n \sum_x p_x^2.$$

For the second statement Eq. (13), we first provide some intuition and a proof sketch. By the convexity of −log, Eq. (12) translates to

$$\mathbb{E}_V S_2(\rho_E^V) \geq S_2(X) - n,$$

where the Rényi-2 entropy S_2 is defined as S_2(\rho) := −log tr\rho^2. If we can turn S_2 into S, we would have Eq. (13). We cannot do so on one copy of ρ_E^V, but we can almost do so on m copies of ρ_E^V, if we restrict to the “typical” approximation of ρ_E^V, explained below.

Consider the case that we input m copies of the state given by Eq. (7) into mn copies of the channel N_d. Conditioning on the random unitaries of the channels, this results in an output state ρ_E^{mN} = ⊗_i=1^m ρ_E^V on the environment. The state ρ_E^{mN} involves a mixture over (X)^m, which is

$$\mathbb{E}_V \text{tr}(\rho_E^{mN})^2 \leq 2^n \sum_x p_x^2,$$

and

$$S(E^n|V_E^N) = \mathbb{E}_V S(\rho_E^{mN}) \geq S(X) - n.$$
all \( x \). So, for any \( x \neq y \), \( \rho_E^{xV} \) and \( \rho_E^{yV} \) are orthogonal only for a vanishing fraction of all possible \( V \), contributing to a significantly large \( Q^{(1)}(N_d) \).

Discussion.—In [1] it was shown that privacy and distillable entanglement can be different, indeed privacy can be nonzero even for bound-entangled states. What we have shown is similar, but somewhat incomparable. Our result is stronger in that the separation is maximal, saturating Eq. (1), but it only applies to the channel case, implicitly not allowing classical communication. The two-way assisted quantum capacity \( Q_2(N_d) \) is maximal (not zero!) and equal to the private capacity \( \log d \). An open question is how big the separation can be in the two-way setting?

D.L. was supported by NSERC, DAS, CRC, and CIFAR, K.L. by NSF Grants No. CCF-1110961 and No. CCF-1111382, and G.S. and J.A.S. by DARPA QUEST.