Maximal Privacy without Coherence


http://dx.doi.org/10.1103/PhysRevLett.113.030502

American Physical Society

Final published version

Sun Apr 24 13:58:13 EDT 2016

http://hdl.handle.net/1721.1/88610

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.
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.

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 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 a private key, strongly suggest that \( Q(\mathcal{N}) = P(\mathcal{N}) \). Surprisingly, it was shown in [1] that not only can \( P \) and \( Q \) differ, there are channels too noisy to transmit any quantum information [that is, \( Q(\mathcal{N}) = 0 \)] but that can nevertheless be used to establish privacy [\( P(\mathcal{N}) > 0 \)]. The central idea of [1] concerns private states that by their structure embody perfectly secure classical key, much as maximally entangled pure states embody perfectly coherent correlation.

While [1] draws a qualitative distinction between the private and the quantum capacities, it remains unclear how big the difference can be. If the capacities were always close, then privacy and coherence would still be closely related concepts and the distinction would have little practical relevance. Our contribution is to present a class of channels with \( Q(\mathcal{N}_d) \leq 1 \) and \( P(\mathcal{N}_d) = \log d \), where \( d^2 \) is the input dimension and \( \log \) is taken base 2 throughout the Letter. We further establish that such a separation is tight, by proving an inequality,

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

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.

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

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

where the maximization is taken over input quantum states \( \rho_B = \tilde{\mathcal{N}}(\phi_A) \) and \( \rho_E = \tilde{\mathcal{N}}(\phi_A) \), respectively. In turn, the
quantum capacity is proved [8–10] to be the regularized coherent information: \( Q(N) = \lim_{n \to \infty} (1/n)Q^{(1)}(N^\otimes n) \). 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 \( L(\sigma) = (N \otimes I_0 + I_0 \otimes \Pi_i)(\sigma) \) and \( \Pi_i(\mu) = \langle i|\mu|i\rangle \). To see that \( M \) is degradable, note that the complementary channel of \( M \) is

\[
\hat{M}(\rho) = \frac{1}{2} [|e\rangle \langle e| \otimes |0\rangle \langle 0| + N(\rho) \otimes |1\rangle \langle 1|],
\]

where \( |e\rangle \langle e| \) is an orthogonal erase 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),

\[
P(N) \leq Q^{(1)}(M)
\]

\[
= \max_{\phi_1} [S(B_1B_2) - S(E_1E_2)]
\]

\[
= \max_{\phi_1} \left[ S(\phi_A) + S(N(\phi_A)) - S(\hat{N}(\phi_A)) \right]
\]

\[
\leq \frac{1}{2} \left[ \log d_A + Q^{(1)}(N) \right].
\]

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

\[
\begin{array}{c}
A_1 \\
\mathcal{P} \\
V \\
A_2
\end{array}
\]

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 \( P = \sum_{i=0}^{d-1} \omega^i |i\rangle \langle i| \otimes |j\rangle \langle j| \) 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 \( W_V = (I \otimes V) \), \( \hat{N}_d(\rho) = tr_B W_V \rho W_V^\dagger \), and \( \hat{N}_d = \hat{E}_d \hat{N}_d \otimes |V\rangle \langle V| \). The isometric extension is given by

\[
U_d(\psi)_{A_1A_2} = \sum_V \sqrt{\text{tr}(W_V(\psi)_{A_1A_2})} |V\rangle \langle V|_{V_d} \otimes |V\rangle \langle V|_{V_d},
\]

and the complementary channel acts as \( \hat{N}_d(\rho) = tr_B W_V \rho W_V^\dagger \otimes |V\rangle \langle V|_{V_d} \).

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 \( V \), Bob 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 \( \mathcal{E} = \{ p_i, \phi_i \} \) and channel \( N \), the private information is defined as

\[
P^{(1)}(N, \mathcal{E}) = \chi(N, \mathcal{E}) - \chi(N, \mathcal{E}),
\]

with Holevo information \( \chi(N, \mathcal{E}) = S(\rho) - \sum_i p_i S(\rho_i) \) evaluated on the induced ensemble \( N(\mathcal{E}) = \{ p_i, \rho_i = N(\phi_i) \} \) and average state \( \rho = \sum_i p_i \rho_i \) [similarly for \( \chi(N, \mathcal{E}) \)]. For any ensemble \( \mathcal{E} \), \( P^{(1)}(N, \mathcal{E}) \) 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 \( \phi_i = |i\rangle \langle i| \otimes (I/d) \), for \( i = 1, \ldots, d \) gives \( \chi(N_d, \mathcal{E}) = \log d \) and \( \chi(N_d, \mathcal{E}) = 0 \), so \( P(N_d) \leq \log d \), 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 \( R_1 \) and \( R_2 \) 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 $Q(N_d)$, we consider the asymptotic behavior of the coherent information, $Q_d^{(1)}(N_d^{\otimes n})$, 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

$$Q_d^{(1)}(N_d^{\otimes n}) = \max_{\rho_{A_1^n A_2^n}} [S(B^n|V^n_B) - S(E^n|V^n_E)].$$

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

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

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

where $x = (x_1, \ldots, x_n)$ and $|x\rangle = \bigotimes_{i=1}^n |x_i\rangle$ is a standard basis state on $A_1^n$.

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

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

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

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

since $P$ commutes with $N_d$, and $P$ is unitary 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 $\phi_x^{A_2^n}$ in Eq. (8) can be taken to be pure. Fix an arbitrary $x$. Let $\bar{\phi}_x^{A_2^n} = \sum_m q(m|x) |\mu_m\rangle \langle \mu_m|$, and for each $w$,

$$\eta_{A_1^n A_2^n}^{w} = p_x |x\rangle \langle x| \otimes |\mu_x\rangle \langle \mu_x| + \sum_{y \neq x} p_y |y\rangle \langle y| \otimes \phi_x^{A_2^n}.$$ 

We now show that

$$\exists w \text{ s.t. } I_{coh}(N_d^{\otimes n}, \eta_{A_1^n A_2^n}^{w}) \geq I_{coh}(N_d^{\otimes n}, \sigma_{A_1^n A_2^n}).$$

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

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

so $\tilde{\sigma}_{A_2^n}^{w}(\sigma_{A_1^n A_2^n}) = \sum_w q(w|x) \tilde{\sigma}_{A_1^n A_2^n}^{w}$, and by concavity of entropy,

$$S(E^n V^n_E, \tilde{\sigma}_{A_1^n A_2^n}^{w}) \geq \sum_w q(w|x) S(E^n V^n_E, \tilde{\sigma}_{A_1^n A_2^n}).$$

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 $P = \sum_{i=1}^d |i\rangle \langle i| \otimes Z_i$, 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

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

where

$$\rho_x^{E^n V^n_E} = Z^x V |\phi_x\rangle \langle \phi_x| V^\dagger Z^{-x}.$$ (11)

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

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

$$\mathbb{E}_V \text{tr} \rho_x^{E^n} \rho_x^{E^n} \leq \frac{1}{(d-1)^2 d_H(x, y)}$$

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 $\rho_x^{E^n}$ using Lemma 2.

**Lemma 3:** For an input given by Eq. (7), conditioned on $V$, the output state on the environment $\rho_x^{E^n} = \sum_{x \in [d^n]} p_x \rho_x^{E^n}$ satisfies
We can almost do so on intuition and a proof sketch. By the convexity of $S$, the left-hand side of the above equation is approximatively upper bounded by $mE_V S(\rho_{E}^V)$. On the right-hand side, $S_2(X_m) \approx mS(X)$ because the typical set contains roughly equiprobable elements, so the two entropies are similar. Finally, dividing by $m$ gives Eq. (13).

We provide an airtight proof in the Supplemental Material (Lemma I.3) [16]. There, we have a version of Eq. (13) that includes all the correction terms incurred by the two approximations taken in the last paragraph. Then, we show that when $m$ is large and $\epsilon$ is small, the correction terms vanish, thereby proving Eq. (13).

Together, $Q^{(1)}(N_d^{0m}) \leq n$, so $Q(N_d) \leq 1$.

When proving the upper bound on $Q$, we cannot assume \textit{a priori} that the entropy of $B^nV^n_B$ is maximal for the optimal input, ruling out the simpler path to show that the entropy of $E^nV^n_E$ is maximal. Instead, we have to show that $S(B^nV^n_B) - S(E^nV^n_E)$ is small for all distributions. Perhaps our technique has other applications. Also, Lemma 3 effectively converts a statement concerning the Rényi-2 entropy into an analogue for the entropy for a large family of states, which may be of interest elsewhere.

\section{Achievable quantum rate}

We have shown that $Q(N_d) \leq 1$, but could it actually be 0? It turns out that it cannot. In the Supplemental Material [16], we consider a specific input state $\phi_{A_1A_2} = (I/d)A_1 \otimes |0\rangle\langle 0|A_2$ for one use of the channel, and prove an explicit lower bound $Q(N_d) \geq Q^{(1)}(N_d^{0m}) \geq (1-\gamma) log e \approx 0.61$ as $d \to \infty$, where $\gamma = \lim_{n \to \infty} (\sum_{k=1}^{m} k \frac{1}{k} - \ln n)$ is the Euler-Mascheroni constant.

Here, we provide some intuition behind the choice of the input and the lower bound. First, note that the input (given for one use of the channel) still has the form given by Eq. (7) (with $p_x = 1/d$ for all $x$), so the subsequent analysis holds. We revisit the discussion after Eq. (11), but now with the converse in mind, and with $n = 1$ (omitted): If for some $V$, $\rho_{E}^V$ and $\rho_{E}^{VN}$ are not orthogonal, then $S(E|V_E) < S(p_X)$ and $Q^{(1)}(N_d) > 0$. For the specific input state, $\phi_{A_1A_2} = (I/d)A_1 \otimes |0\rangle\langle 0|A_2$, $|\phi^V\rangle = |0\rangle$ for
all \( x \). So, for any \( x \neq y \), \( \rho_x^{V_E} \) and \( \rho_y^{V_E} \) 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.
