J Cryptol (2017) 30:1–21
DOI: 10.1007/s00145-015-9215-3

Journal of CRYPTOLOGY

Weak Locking Capacity of Quantum Channels Can be Much Larger Than Private Capacity

Andreas Winter
ICREA and Física Teòrica: Informació i Fenomens Quàntics, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain
andreas.winter@uab.cat

Communicated by Stefan Wolf.

Received 29 April 2014
Online publication 14 September 2015

Abstract. We show that it is possible for the so-called *weak locking capacity* of a quantum channel (Guha et al. in Phys Rev X 4:011016, 2014) to be much larger than its private capacity. Both reflect different ways of capturing the notion of reliable communication via a quantum system while leaking almost no information to an eavesdropper; the difference is that the latter imposes an intrinsically quantum security criterion whereas the former requires only a weaker, classical condition. The channels for which this separation is most straightforward to establish are the complementary channels of classical-quantum (cq-)channels and, hence, a subclass of Hadamard channels. We also prove that certain symmetric channels (related to photon number splitting) have positive weak locking capacity in the presence of a vanishingly small pre-shared secret, whereas their private capacity is zero. These findings are powerful illustrations of the difference between two apparently natural notions of privacy in quantum systems, relevant also to quantum key distribution: the older, naïve one based on accessible information, contrasting with the new, composable one embracing the quantum nature of the eavesdropper's information. Assuming an additivity conjecture for constrained minimum output Rényi entropies, the techniques of the first part demonstrate a single-letter formula for the weak locking capacity of complements to cq-channels, coinciding with a general upper bound of Guha et al. for these channels. Furthermore, still assuming this additivity conjecture, this upper bound is given an operational interpretation for general channels as the maximum weak locking capacity of the channel activated by a suitable noiseless channel.

Keywords. Quantum channel, Private capacity, Quantum key distribution, Accessible information, Composability, Locking capacity.

1. Introduction

Information locking [10] remains one of the most curious manifestations of the quantum nature of information, which is in contrast to our (human) exclusively classical access to it. It is based on the simple (yet nontrivial) observation that the accessible information in a nonorthogonal ensemble through a measurement can be smaller, indeed much smaller, than the Holevo information. This occurs already for two mutually unbiased bases, by the Maassen–Uffink entropic uncertainty relation [25], and the crucial realization is that availability of the basis information (one bit) before the measurement is taken can raise the accessible information by an arbitrary amount, depending on the system size.

This throws into sharp contrast two security criteria for quantum cryptography: the "naïve" one, which only asks for the eavesdropper to have small accessible information about the key, and the "correct," composable one, which demands that the quantum mutual information is small [21]. In fact, in [21], it was shown that this choice can make a big difference: A large key may appear private according to the former criterion, but not under the latter.

Quantifying this difference, Guha et al. have recently introduced the notion of locking capacity of a channel [12], following Lloyd's suggestion of "quantum enigma machines" [23], actually two capacities, one *strong* and one *weak locking capacity* of a channel. Here we will only look at the weak variant, which is the largest rate of asymptotically reliable classical communication between the "legal" users (Alice and Bob), such that the accessible information of the eavesdropper observing the channel environment (complementary channel output), about a uniformly distributed message, goes to zero.

To be precise, let Alice and Bob be connected by a quantum channel, i.e., a completely positive and trace preserving (cptp) map $\mathcal{N} : \mathcal{L}(A) \longrightarrow \mathcal{L}(B)$, with (here: finite dimensional) Hilbert spaces A and B. It has a Stinespring dilation, via an essentially unique isometry $V : A \hookrightarrow B \otimes E$, where E is the eavesdropper's system (Eve): $\mathcal{N}(\rho) = \operatorname{Tr}_E V\rho V^\dagger$. Tracing over B instead yields the *complementary channel* $\mathcal{N}^c(\rho) = \operatorname{Tr}_B V\rho V^\dagger$ from Alice to Eve. All of our discussion of privacy will be in this model, which is a quantum version of Wyner's wiretap channel [38].

To communicate via n instances of the channel, Alice and Bob employ an (n, ϵ)*-code*, which is a collection $\{(\rho_m, D_m) : m = 1, \dots, N\}$ consisting of states ρ_m on A^n and POVM elements D_m on B^n (i.e., $D_m \geq 0$, $\sum_m D_m = \mathbb{1}$), with the property that the estimate $\widehat{m}$ of m obtained by measuring (D_m) on the channel output is very likely to equal m, which is assumed to be drawn uniformly:

$$P_{\text{err}} = \Pr\{M \neq \widehat{M}\} = \frac{1}{N} \sum_{m=1}^{N} \operatorname{Tr}\big(\mathcal{N}^{\otimes n}(\rho_m)(\mathbb{1} - D_m)\big) \leq \epsilon. \tag{1}$$

Given a code, we call it δ*-private* (for the channel $\mathcal{N}$) if there exists a state ω_0 on E^n such that

$$\frac{1}{N} \sum_{m=1}^{N} \big\| (\mathcal{N}^c)^{\otimes n}(\rho_m) - \omega_0 \big\|_1 \leq \delta. \tag{2}$$

This condition captures precisely the commonly accepted notion of private communication, since it says that Eve's output is typically close to a constant, independent of the message m. Strictly speaking, the above notion is that of a *secret key generation code*, since we impose an a priori uniform distribution on the m's.

Finally, the code is called δ*-weakly locked* (always for the same channel $\mathcal{N}$), if for every POVM (Q_j) on E^n, there exists a probability distribution $\Omega = (\Omega_j)$ such that

$$\frac{1}{N}\sum_{m=1}^{N}\sum_{j}\left|\mathrm{Tr}\left[(\mathcal{N}^c)^{\otimes n}(\rho_m)Q_j\right]-\Omega_j\right|\leq\delta. \tag{3}$$

By the contractive property of the trace norm under cptp maps (in this case $\sigma \mapsto \sum_j |j\rangle\langle j| \,\mathrm{Tr}\, \sigma Q_j$), the δ-private property implies δ-weak locking. Guha et al. [12] have also defined the notion of *strong locking*, which boils down to the set of signal states ρ_m satisfying Eq. (3) for the identity channel $\mathcal{N}^c$, i.e., constant channel $\mathcal{N}$:

$$\frac{1}{N}\sum_{m=1}^{N}\sum_{j}\left|\mathrm{Tr}\,\rho_m Q_j-\Omega_j\right|\leq\delta. \tag{4}$$

However, we shall not prove any new results on strongly locked codes and include the definition only for completeness, see however recent progress in [24].

Following [12], the code in fact may depend on a sublinear secret key k (i.e., of $o(n)$ bits) pre-shared between Alice and Bob, so that in Eq. (1) the states ρ_{mk} and POVMs elements D_{mk} depend on m and k, and the error probability includes also an average over k. On the other hand, in the privacy and weak locking conditions, Eqs. (2) and (3), we have to put $\rho_m = \mathbb{E}_k \rho_{mk}$, the average over the key k, because it is unknown to Eve. An equivalent way of including the pre-shared key, which we prefer here as it allows us to keep the above definitions of wiretap channel codes, is to grant Alice and Bob the use of $o(n)$ instances of an ideal qubit channel (which automatically is perfectly private) in addition to the n instances of $\mathcal{N}$. Then all we have to do is to substitute $\mathrm{id}_2^{\otimes o(n)} \otimes \mathcal{N}^{\otimes n}$ for the main channel in Eqs. (1), (2) and (3) above.

With these notions, we can give the definitions of channel capacities as the largest asymptotic rate $R = \frac{1}{n}\log N$ attainable with arbitrarily small error:

$$\begin{aligned}
P(\mathcal{N}) &:= \sup\left\{R : \exists\ \delta\text{-private } (n,\epsilon)\text{-codes with } N \geq 2^{nR},\ \epsilon,\delta\to 0\right\},\\
L_W(\mathcal{N}) &:= \sup\left\{R : \exists\ \delta\text{-weakly locked } (n,\epsilon)\text{-codes with } N \geq 2^{nR},\ \epsilon,\delta\to 0\right\},\\
L_S(\mathcal{N}) &:= \sup\left\{R : \exists\ \delta\text{-strongly locked } (n,\epsilon)\text{-codes with } N \geq 2^{nR},\ \epsilon,\delta\to 0\right\},
\end{aligned}$$

are the private, weak locking and strong locking capacity, respectively. By definition, $L_S(\mathcal{N}) \leq L_W(\mathcal{N})$ and $P(\mathcal{N}) \leq L_W(\mathcal{N}) \leq C(\mathcal{N})$, the latter being the classical capacity of $\mathcal{N}$. It can be shown that the quantum capacity $Q(\mathcal{N})$ is a lower bound on $L_S(\mathcal{N})$, but the relation between $P(\mathcal{N})$ and $L_S(\mathcal{N})$ is unknown [12].

In cryptographic contexts, we would also worry about the speed of convergence of ϵ and δ, usually by introducing exponential decay rates, $\epsilon = 2^{-nE}$, $\delta = 2^{-nS}$ ($S > 0$ is called a *security parameter*), in which case we would have to study the trade-off between rate R and the error/security rates E and S. The private capacity $P(\mathcal{N})$ has been determined in [5,8], and from the proof, we know that by letting $E > 0$ and $S > 0$ sufficiently small, rates arbitrarily close to $P(\mathcal{N})$ can be achieved. A priori this is not clear for the locking capacities, although the results presented in this paper show that at least certain weak locking rates, sometimes even rates arbitrarily close to $L_W(\mathcal{N})$ can be achieved with $\epsilon,\ \delta = 2^{-\Omega(n)}$.

Remark 1. Guha et al. [12, Def. 1] give a very similar definition of locking, but demand the much stronger condition that in Eq. (3) the *conditional* distribution of m given each outcome j has to be close to uniform. This however seems too restrictive, and not in line with the usual modern definition of privacy in wiretap channels [5,8], reflected in Eq. (2); in fact, that definition would assign a private capacity of zero to the perfectly innocent and well-understood quantum erasure channel [32]. Thus we propose to use our criterion (3).

Guha et al. [12] also discuss the possibility of defining the weak locking property in terms of the Shannon mutual information between m and j in Eq. (3), the maximum of which over all measurements are the *accessible information*

$$I_{\text{acc}}(M:E^n) = I_{\text{acc}}\left(\left\{\frac{1}{M}, (\mathcal{N}^c)^{\otimes n}(\rho_m)\right\}\right)$$

of the uniform ensemble of the eavesdropper's output states. Likewise, the privacy of a code could also have been characterized in terms of the quantum mutual information $I(M:E^n)$, which equals the Holevo information of the ensemble $\left\{\frac{1}{M}, (\mathcal{N}^c)^{\otimes n}(\rho_m)\right\}$. For a generic ensemble $\mathcal{E} = \{p_x, \sigma_x\}$ of states on A, and corresponding cq-state $\sum_x p_x |x\rangle\langle x|^X \otimes \sigma_x^A$, these information quantities are defined as

$$\begin{aligned}
I(X:A) &= S(X) + S(A) - S(XA) = S(A) - S(A|X) \\
&= \chi(\mathcal{E}) = S\left(\sum_x p_x\sigma_x\right) - \sum_x p_x S(\sigma_x), \\
I_{\text{acc}}(X:A) = I_{\text{acc}}(\mathcal{E}) &= \max_{\text{POVM }(Q_y)} I(X:Y) \ \text{ with } \ \Pr\{X=x, Y=y\} = p_x \operatorname{Tr}\sigma_x Q_y.
\end{aligned}$$

By the Alicki–Fannes inequality [1], a δ-private code satisfies $I(M:E^n) \leq O(n)\delta$, and likewise a δ-weakly locking code satisfies $I_{\text{acc}}(M:E^n) \leq O(n)\delta$. Vice versa, Pinsker's inequality implies that $I(M:E^n) \leq \Delta$ and $I_{\text{acc}}(M:E^n) \leq \Delta$ imply $\sqrt{2\Delta}$-privacy and $\sqrt{2\Delta}$-weak locking, respectively (similarly for strong locking). Hence, as long as δ in our definitions above is $o(1/n)$, the resulting notions of weak and strong locking, as well as private, capacity, are equivalent to the present ones.

In the present paper, we shall take a closer look at the weak locking capacity for so-called *degradable* channels $\mathcal{N}$, which means that there is a cptp map $\mathcal{D}: \mathcal{L}(B) \longrightarrow \mathcal{L}(E)$ satisfying $\mathcal{N}^c = \mathcal{D}\circ\mathcal{N}$. We call $\mathcal{N}$ *anti-degradable* iff the complementary channel $\mathcal{N}^c$ is degradable. If a channel $\mathcal{N}$ is both degradable and anti-degradable, and specifically if the degrading map $\mathcal{D}$ is an isomorphism between B and E, we call it *symmetric*.

Remark 2. For degradable channels $\mathcal{N}$, it is well known [9,32] that

$$P(\mathcal{N}) = Q(\mathcal{N}) = \max_\rho S(\mathcal{N}(\rho)) - S(\mathcal{N}^c(\rho)),$$

where the right-hand side is the maximization of the coherent information, which is concave in ρ. By definition, any private communication code is a weak locking code for $\mathcal{N}$, hence $L_W(\mathcal{N}) \geq P(\mathcal{N})$.

For an anti-degradable channel $\mathcal{N}$, $Q(\mathcal{N}) = P(\mathcal{N}) = 0$ by the familiar "cloning argument" [4]. Below we will see that for the weak locking capacity, this does not hold.

In [12], it had been left open whether the weak locking capacity is always equal to the private capacity, or whether there can be a separation. For example, there it was shown that for channels $\mathcal{N}$ such that the complementary channel $\mathcal{N}^c$ is a qc-channel, then $L_W(\mathcal{N}) = P(\mathcal{N})$; furthermore, that if $\mathcal{N}$ is entanglement-breaking, then $L_W(\mathcal{N}) = P(\mathcal{N}) = 0$. Note that the construction in [21] (as well as [6]) may be taken as evidence for large gaps, but it is not sufficient to prove this: Namely, in those papers, it was pointed out that *if* at the end of a hypothetical key agreement protocol Alice and Bob share perfect randomness, and their correlation with Eve is described as

$$\frac{1}{N}\sum_{m=1}^{N} |m\rangle\langle m|^A \otimes |m\rangle\langle m|^B \otimes \rho_m^E,$$

with a strongly locking ensemble $\left\{\frac{1}{N}, \rho_m\right\}$, cf. Eq. (4), then the key may not be secure at all after a small portion ($\ll \log N$) of the shared secret has been leaked. Our contribution is to show that this can indeed occur naturally in the above-outlined setting of the quantum wiretap channel.

Here we show a general lower bound on $L_W(\mathcal{N})$ for channels $\mathcal{N}$ such that the complementary channel $\mathcal{N}^c$ is a cq-channel (these are automatically degradable); we establish basic properties of these channels, including an upper bound on $L_W(\mathcal{N})$, in the next Sect. 2. This bound can sometimes be much larger than P (Sect. 3). We also exhibit symmetric channels, hence with vanishing private capacity, which nonetheless have positive weak locking capacity (Sect. 4). After this, we conclude with a discussion of our results in the context of regular quantum key distribution (QKD) and several open questions, in Sect. 5.

2. Complements of cq-Channels

One subclass we will be interested in is so-called *Hadamard channels* [20], specifically those that are complementary channels of *cq-channels* [15]:

$$\mathcal{N}^c(|i\rangle\langle i'|) = \delta_{ii'}\rho_i^E, \tag{5}$$

where $\{|i\rangle\}$ is an orthonormal basis of A, and with $\rho_i^E = \mathrm{Tr}_B\, |\psi_i\rangle\langle\psi_i|^{BE}$, so that

$$\mathcal{N}(|i\rangle\langle i'|) = |i\rangle\langle i'| \otimes \mathrm{Tr}_E\, |\psi_i\rangle\langle\psi_{i'}|. \tag{6}$$

Note that in general, Hadamard channels are defined as complementary channels of entanglement-breaking channels, which results in a wider class than the ones we are looking at here [20]. The more restrictive class of channels in Eq. (6) is also known as *Schur multipliers*.

The cq-channels are called so, because they are "classical-to-quantum" [15]. The opposite concept of *qc-channel* ("quantum-to-classical") models a measurement as a cptp map; for a POVM (Q_j), it is given by

$$\mathcal{N}(\rho) = \sum_j \operatorname{Tr} \rho Q_j |j\rangle\langle j|. \tag{7}$$

We begin with an upper bound on the weak locking capacity, to have a benchmark for our lower bound later on.

Proposition 3. *Let $\mathcal{N} : \mathcal{L}(A) \longrightarrow \mathcal{L}(B)$ be a Schur multiplier, i.e., a Hadamard channel whose complementary channel $\mathcal{N}^c : \mathcal{L}(A) \longrightarrow \mathcal{L}(E)$ is a cq-channel. Then,*

$$L_W(\mathcal{N}) \leq \max_{(p_i)} S_{\text{acc}}(I|E), \text{ where}$$
$$S_{\text{acc}}(I|E) := \min_{(Q_j)} H(I|J),$$

is the eavesdropper's accessible equivocation. *Here, (p_i) is a probability distribution on the computational basis states of A, and (Q_j) is a POVM on E,* $\Pr\{I = i, J = j\} = p_i \operatorname{Tr} \rho_i Q_j$.

Proof. Basically, we evaluate the upper bound from [12, Thm. 8]: $L_W(\mathcal{N}) \leq \sup_n \frac{1}{n} L_W^{(u)}(\mathcal{N}^{\otimes n})$, where

$$L_W^{(u)}(\mathcal{N}) = \max_{\{p_x,\rho_x\}} I(X:B) - I_{\text{acc}}(X:E) \tag{8}$$

is optimized with respect to arbitrary ensembles $\{p_x, \rho_x\}$ of states on A.

Choosing any probability distribution (p_i) on the computational basis states $\rho_i = |i\rangle\langle i|$, we get $I(I:B) = H(I)$ and hence $L_W^{(u)}(\mathcal{N}) \geq S_{\text{acc}}(I|E)$. Furthermore, for the tensor product $\mathcal{N}_1 \otimes \mathcal{N}_2$ of two complements of cq-channels,

$$\max_{(p_{i_1 i_2})} S_{\text{acc}}(I_1 I_2|E_1 E_2) = \max_{(p_{i_1})} S_{\text{acc}}(I_1|E_1) + \max_{(p_{i_2})} S_{\text{acc}}(I_2|E_2),$$

by Lemma 4 below. This shows in fact that for any integer n, $\frac{1}{n} L_W^{(u)}\left(\mathcal{N}^{\otimes n}\right) \geq \max_{(p_i)} S_{\text{acc}}(I|E)$.

Thus, it remains to show $L_W^{(u)}(\mathcal{N}) \leq \max_{(p_i)} S_{\text{acc}}(I|E)$. To do so, we shall first show that for degradable channels, an optimal ensemble for Eq. (8) consists w.l.o.g. of pure states $\rho_x = |\varphi_x\rangle\langle\varphi_x|$, and then in a second step that we can choose these pure states as computational basis states, modifying the ensemble accordingly.

1. For the degradable channel $\mathcal{N}$, choose a Stinespring isometry $V_0 : A \hookrightarrow B \otimes E$, and for the degrading map an isometry $V_1 : B \hookrightarrow E' \otimes F$. The accessible information requires a measurement (Q_j)—w.l.o.g. consisting of rank-one operators—for whose associated qc-channel we choose an isometry (acting on E' but of course equally on E) $V_2 : E' \hookrightarrow J \otimes J'$. Now, given an ensemble $\mathcal{E} = \{p_x, \rho_x\}$,

$$\begin{aligned} I(X:B) - I_{\text{acc}}(X:E) &= I(X:FJJ') - I(X:J) \\ &= I(X:FJ'|J) \\ &= H(FJ'|J) - H(FJ'|JX), \end{aligned} \tag{9}$$

where all expressions except the l.h.s. are with respect to the state

$$\omega^{XFJJ'} = \sum_x p_x |x\rangle\langle x|^X \otimes \left(V_2 V_1 \mathcal{N}(\rho_x) V_1^\dagger V_2^\dagger\right)^{FJJ'}.$$

On the r.h.s. of Eq. (9), $H(FJ'|J)$ depends only on $\omega^{FJJ'}$ and so is unchanged if we replace each ρ_x in $\mathcal{E}$ by any of its pure-state decompositions. On the other hand,

$$H(FJ'|JX)_\omega = \sum_x p_x H(FJ'|J)_{V_2 V_1 \mathcal{N}(\rho_x) V_1^\dagger V_2^\dagger},$$

and since the conditional entropy is concave in the state [22], this replacement can make the latter quantity only smaller.

2. Now that we know that we may assume a pure-state ensemble $\mathcal{E} = \{p_x, \rho_x = |\varphi_x\rangle\langle\varphi_x|\}$, we specialize to the complements of cq-channels. Looking at Eqs. (5) and (6), we see that $\mathcal{N}^c$ is invariant, and $\mathcal{N}$ covariant, under conjugation by phase (diagonal) unitaries. By twirling the ensemble by phase unitaries (i.e., replacing each $|\varphi_x\rangle$ by a uniform distribution over $U^{\text{diag}}|\varphi_x\rangle$), we thus can only increase the r.h.s. of Eq. (9) by leaving $H(FJ'|JX)$ alone, while $H(FJ'|J)$ can only increase, since $\omega^{FJJ'}$ is now invariant under conjugation by phase unitaries.

The proof will be concluded by showing that

$$H(FJ'|JX) = \sum_x p_x H(FJ'|J)_{V_2 V_1 \mathcal{N}(|\varphi_x\rangle\langle\varphi_x|) V_1^\dagger V_2^\dagger}$$

can only decrease if we replace each $|\varphi_x\rangle = \sum_i \alpha_{i|x}|i\rangle$ by the ensemble $\{p_{i|x} = |\alpha_{i|x}|^2, |i\rangle\langle i|\}$, hence the original ensemble $\mathcal{E}$ by $\widetilde{\mathcal{E}} = \{p_{xi} = p_x p_{i|x}, |i\rangle\langle i|\}$, which in turn has the same value of the expression (9) as $\{p_i = \sum_x p_{xi}, |i\rangle\langle i|\}$. Indeed, the corresponding $\widetilde{\omega}$ has the same reduction on FJJ', $\omega^{FJJ'} = \widetilde{\omega}^{FJJ'}$, and for every x, we have

$$H(FJ'|J)_{V_2 V_1 \mathcal{N}(|\varphi_x\rangle\langle\varphi_x|) V_1^\dagger V_2^\dagger} \geq \sum_i p_{i|x} H(FJ'|J)_{V_2 V_1 \mathcal{N}(|i\rangle\langle i|) V_1^\dagger V_2^\dagger}. \tag{10}$$

To see this, we expand the l.h.s. as

$$\begin{aligned} H(FJ'|J)_{V_2 V_1 \mathcal{N}(|\varphi_x\rangle\langle\varphi_x|) V_1^\dagger V_2^\dagger} &= H(FJJ')_{V_2 V_1 \mathcal{N}(|\varphi_x\rangle\langle\varphi_x|) V_1^\dagger V_2^\dagger} - H(J)_{V_2 V_1 \mathcal{N}(|\varphi_x\rangle\langle\varphi_x|) V_1^\dagger V_2^\dagger} \\ &= S\big(\mathcal{N}(|\varphi_x\rangle\langle\varphi_x|)\big) - H\big(\{\operatorname{Tr} \mathcal{N}^c(|\varphi_x\rangle\langle\varphi_x|) Q_j\}_j\big) \\ &= S\big(\mathcal{N}^c(|\varphi_x\rangle\langle\varphi_x|)\big) - H\big(\{\operatorname{Tr} \mathcal{N}^c(|\varphi_x\rangle\langle\varphi_x|) Q_j\}_j\big), \end{aligned}$$

and observe $\mathcal{N}^c(|\varphi_x\rangle\langle\varphi_x|) = \sum_i p_{i|x}\mathcal{N}^c(|i\rangle\langle i|) = \sum_i p_{i|x}\rho_i =: \overline{\rho}$. While on the r.h.s., for each i,

$$\begin{aligned} H(FJ'|J)_{V_2V_1\mathcal{N}(|i\rangle\langle i|)V_1^\dagger V_2^\dagger} &= H(FJJ')_{V_2V_1\mathcal{N}(|i\rangle\langle i|)V_1^\dagger V_2^\dagger} - H(J)_{V_2V_1\mathcal{N}(|i\rangle\langle i|)V_1^\dagger V_2^\dagger} \\ &= S\big(\mathcal{N}(|i\rangle\langle i|)\big) - H\big(\{\operatorname{Tr}\mathcal{N}^c(|i\rangle\langle i|)Q_j\}_j\big) \\ &= S\big(\mathcal{N}^c(|i\rangle\langle i|)\big) - H\big(\{\operatorname{Tr}\mathcal{N}^c(|i\rangle\langle i|)Q_j\}_j\big) \\ &= S\big(\rho_i\big) - H\big(\{\operatorname{Tr}\rho_i Q_j\}_j\big). \end{aligned}$$

Hence, the difference between l.h.s. and r.h.s. of Eq. (10) is

$$\begin{aligned} &H(FJ'|J)_{V_2V_1\mathcal{N}(|\varphi_x\rangle\langle\varphi_x|)V_1^\dagger V_2^\dagger} - \sum_i p_{i|x} H(FJ'|J)_{V_2V_1\mathcal{N}(|i\rangle\langle i|)V_1^\dagger V_2^\dagger} \\ &= S(\overline{\rho}) - \sum_i p_{i|x} S(\rho_i) - H\big(\{\operatorname{Tr}\overline{\rho}Q_j\}_j\big) + \sum_i p_{i|x} H\big(\{\operatorname{Tr}|i\rangle\langle i|Q_j\}_j\big) \\ &= I(I:E) - I(I:J) \geq 0, \end{aligned}$$

the last inequality by the famous Holevo bound [14], and we are done. □

Lemma 4. *For the tensor product of channels $\mathcal{N}_1$ and $\mathcal{N}_2$, each of which is the complement of a cq-channel,*

$$\max_{(p_{i_1i_2})} S_{\text{acc}}(I_1I_2|E_1E_2) = \max_{(p_{i_1})} S_{\text{acc}}(I_1|E_1) + \max_{(p_{i_2})} S_{\text{acc}}(I_2|E_2).$$

Proof. First, for any distribution $(p_{i_1i_2})$, and any measurement POVM (Q_j), we have, by subadditivity of the entropy, $H(I_1I_2|J) \leq H(I_1|J) + H(I_2|J)$, hence, choosing the POVM to be a tensor product of local POVMs, $Q_{j_1j_2} = Q_{j_1} \otimes Q_{j_2}$, we get

$$S_{\text{acc}}(I_1I_2|E_1E_2) \leq S_{\text{acc}}(I_1|E_1) + S_{\text{acc}}(I_2|E_2).$$

On the other hand, consider a product distribution $p_{i_1i_2} = p_{i_1}p_{i_2}$, the output of $(\mathcal{N}_1 \otimes \mathcal{N}_2)^c$ is a product ensemble $\{p_{i_1}, \rho_{i_1}\} \otimes \{p_{i_2}, \rho_{i_2}\}$. For a generic POVM (Q_j) on E_1E_2, we can switch around the roles of the ensemble and of the POVM, observing that with $\overline{\rho}^{(b)} = \sum_{i_b} p_{i_b}\rho_{i_b}$ and the POVMs(!) composed of the operators $M_{i_b} = \left(\overline{\rho}^{(b)}\right)^{-\frac{1}{2}} p_{i_b}\rho_{i_b} \left(\overline{\rho}^{(b)}\right)^{-\frac{1}{2}}$ $(b = 0, 1)$,

$$\begin{aligned} \Pr\{I_1 = i_1, I_2 = i_2, J = j\} &= p_{i_1}p_{i_2} \operatorname{Tr}(\rho_{i_1} \otimes \rho_{i_2})Q_j \\ &= \operatorname{Tr}\left(\sqrt{\overline{\rho}^{(1)} \otimes \overline{\rho}^{(2)}}\, Q_j \sqrt{\overline{\rho}^{(1)} \otimes \overline{\rho}^{(2)}}\right)(M_{i_1} \otimes M_{i_2}) \\ &=: q_j \operatorname{Tr}\sigma_j(M_{i_1} \otimes M_{i_2}). \end{aligned}$$

Thus,

$$H(I_1 I_2|J) = \sum_j q_j S\big((\mathcal{M}_1 \otimes \mathcal{M}_2)\sigma_j\big),$$

where $\mathcal{M}_b$ is the qc-channel representing the POVM (M_{i_b}) $(b = 0, 1)$. This means

$$S_{\text{acc}}(I_1 I_2|E_1 E_2) = \widehat{H}\big(\mathcal{M}_1 \otimes \mathcal{M}_2|\overline{\rho}^{(1)} \otimes \overline{\rho}^{(2)}\big),$$

and likewise

$$S_{\text{acc}}(I_1|E_1) = \widehat{H}\big(\mathcal{M}_1|\overline{\rho}^{(1)}\big), \quad S_{\text{acc}}(I_2|E_2) = \widehat{H}\big(\mathcal{M}_2|\overline{\rho}^{(2)}\big),$$

where

$$\widehat{H}(\mathcal{M}|\sigma) := \min_{\{q_j, \psi_j\}} \sum_j q_j H\big(\mathcal{M}(\psi_j)\big) \quad \text{s.t.} \quad \sum_j q_j \psi_j = \sigma$$

is the *constrained minimum output entropy*. But now we can invoke [19, Lemma 3], by which

$$\widehat{H}\big(\mathcal{M}_1 \otimes \mathcal{M}_2|\overline{\rho}^{(1)} \otimes \overline{\rho}^{(2)}\big) = \widehat{H}\big(\mathcal{M}_1|\overline{\rho}^{(1)}\big) + \widehat{H}\big(\mathcal{M}_2|\overline{\rho}^{(2)}\big),$$

concluding the proof. □

Even though we do not make use of it here, we cannot pass without noting the following fundamental property of the optimization of $H(I|J)$:

Lemma 5. *For an ensemble $\mathcal{E} = \{p_i, \rho_i\}$ and a POVM $Q = (Q_j)$, the function $\eta(\mathcal{E}; Q) = H(I|J)$ is concave in $\mathcal{E}$ and convex (actually affine) in Q, in the following sense: For ensembles $\mathcal{E}^{(0)} = \{p_i^{(0)}, \rho_i\}$ and $\mathcal{E}^{(1)} = \{p_i^{(1)}, \rho_i\}$ (without loss of generality sharing the same set of states), $\mathcal{E} = \lambda\mathcal{E}^{(0)} + (1-\lambda)\mathcal{E}^{(1)} = \{\lambda p_i^{(0)} + (1-\lambda)p_i^{(1)}, \rho_i\}$ satisfies*

$$\eta(\lambda\mathcal{E}^{(0)} + (1-\lambda)\mathcal{E}^{(1)}, Q) \geq \lambda\eta(\mathcal{E}^{(0)}, Q) + (1-\lambda)\eta(\mathcal{E}^{(1)}, Q).$$

Instead, for POVMs $(Q_j^{(0)})$ and $(Q_k^{(1)})$ on disjoint *index sets $\{j\}$ and $\{k\}$, $Q = \lambda Q^{(0)} \oplus (1-\lambda)Q^{(1)} = \big(\lambda Q_j^{(0)}, (1-\lambda)Q_k^{(1)}\big)$ satisfies*

$$\eta(\mathcal{E}, \lambda Q^{(0)} \oplus (1-\lambda)Q^{(1)}) = \lambda\eta(\mathcal{E}, Q^{(0)}) + (1-\lambda)\eta(\mathcal{E}, Q^{(1)}).$$

Consequently,

$$\max_{(p_i)} S_{\text{acc}}(I|E) = \max_{(p_i)} \min_{(Q_j)} H(I|J) = \min_{(Q_j)} \max_{(p_i)} H(I|J).$$

Proof. The concavity property boils down to the concavity of the Shannon entropy. The affine linearity is evident from the definition. Finally, the minimax statement is an application of the concavity in the first and convexity in the second argument, invoking von Neumann's minimax theorem [31,36]. □

3. Lower Bound on L_W for Complements of cq-Channels

We shall need the following auxiliary lemma, which was proved by Damgaard et al. [7] in a very similar form. In "Appendix," we give a simple proof of it, based on the additivity of the minimum output Rényi entropy for entanglement-breaking channels [19].

Proposition 6. *Consider a POVM $M = (M_i)$ and its associated qc-channel $\mathcal{M}$, with minimum output entropy $\widehat{H}(\mathcal{M}) := \min_{\psi \text{ state}} H(\mathcal{M}(\psi))$, where $H(\mathcal{M}(\psi)) = H\big(\{q_i = \operatorname{Tr}\psi M_i\}\big)$. Then, for any $0 < \epsilon,\ \delta < 1$, and any state ψ on n input systems,*

$$H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq n\big(\widehat{H}(\mathcal{M}) - \delta\big) - 16(\log d)^2\frac{1}{\delta}\log\frac{1}{\epsilon}.$$

For a suitable choice of δ (depending on ϵ), we get (for sufficiently large n, ensuring that $\delta < 1$):

$$H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq n\widehat{H}(\mathcal{M}) - 8(\log d)\sqrt{n\log\frac{1}{\epsilon}}.$$

Here, $H_{\min}^{\epsilon}$ is the *smooth min-entropy* [28]:

Definition 7. For a state ρ, the *min-entropy* is $H_{\min}(\rho) := -\log\|\rho\|$, and the *smooth min-entropy*

$$H_{\min}^{\epsilon}(\rho) = \max H_{\min}(\rho') \quad \text{s.t.} \quad \frac{1}{2}\|\rho - \rho'\|_1 \leq \epsilon.$$

More generally, for a bipartite state ρ^{AB},

$$\begin{aligned} H_{\min}(A|B)_\rho &:= -\log\min\lambda \quad \text{s.t.} \quad \rho^{AB} \leq \lambda(\mathbb{1}^A \otimes \sigma^B),\ \sigma \text{ state} \\ &\geq -\log\left\|(\mathbb{1}\otimes\rho^B)^{-1/2}\rho(\mathbb{1}\otimes\rho^B)^{-1/2}\right\| =: H_\infty(A|B)_\rho, \end{aligned}$$

and

$$H_{\min}^{\epsilon}(A|B)_\rho := \max H_{\min}(A|B)_{\rho'} \quad \text{s.t.} \quad \frac{1}{2}\|\rho - \rho'\|_1 \leq \epsilon.$$

Remark 8. Unlike the nowadays standard definition of smooth (conditional) min-entropy, which uses the so-called *purified distance* [34], we employ the trace distance. This is essentially equivalent, since the two metrics are dominating each other (in fact, trace distance is upper bounded by the purified distance). However, it makes for more direct application of classical randomness extraction results later.

Note that for a qc-state $\rho^{AB} = \sum_j q_j \rho_j^A \otimes |j\rangle\langle j|^B$,

$$H_{\min}(A|B)_\rho \geq \min_j H_{\min}(\rho_j),$$
$$H_{\min}^{\epsilon+\delta}(A|B)_\rho \geq \min_{j\in\mathcal{T}} H_{\min}^{\epsilon}(\rho_j),$$

for any set $\mathcal{T}$ of indices with $\Pr\{j \notin \mathcal{T}\} \leq \delta$.

Corollary 9. *Let $\{p_i, \rho_i\}$ be an ensemble on a Hilbert space E with associated average state $\overline{\rho}$ and POVM $(M_i = \overline{\rho}^{-\frac{1}{2}} p_i \rho_i \overline{\rho}^{-\frac{1}{2}})$. Then, for any POVM $Q = (Q_j)$ on E^n, i.i.d. $I_1, \ldots, I_n \sim (p_i)$ and $0 < \delta < 1$,*

$$H_{\min}^{\epsilon}(I^n|J) \geq n\big(\widehat{H}(\mathcal{M}) - \delta\big) - 16(\log d)^2 \frac{1}{\delta} \log \frac{1}{\epsilon},$$

and for sufficiently large n,

$$H_{\min}^{\epsilon}(I^n|J) \geq n\widehat{H}(\mathcal{M}) - 8(\log d)\sqrt{n \log \frac{1}{\epsilon}}.$$

Proof. Simply use the trick to switch between ensembles and POVMs, to write

$$\begin{aligned}
\Pr\{I^n = i^n, J = j\} &= p_{i_1} \ldots p_{i_n} \operatorname{Tr}(\rho_{i_1} \otimes \cdots \otimes \rho_{i_n}) Q_j \\
&= \operatorname{Tr}\big(\sqrt{\overline{\rho}}^{\otimes n} Q_j \sqrt{\overline{\rho}}^{\otimes n}\big)(M_{i_1} \otimes \cdots \otimes M_{i_n}) \\
&= q_j \operatorname{Tr} \sigma_j (M_{i_1} \otimes \cdots \otimes M_{i_n}).
\end{aligned}$$

Thus (cf. Remark 8),

$$\begin{aligned}
H_{\min}^{\epsilon}(I^n|J) &\geq \min_j H_{\min}^{\epsilon}(I^n|J = j) \\
&= \min_j H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\sigma_j)\big) \\
&\geq \min_\psi H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big),
\end{aligned}$$

and the claim follows from the lower bound of Proposition 6. □

Theorem 10. *For any Schur multiplier, i.e., a Hadamard channel $\mathcal{N} : \mathcal{L}(A) \longrightarrow \mathcal{L}(B)$ whose complementary channel $\mathcal{N}^c : \mathcal{L}(A) \longrightarrow \mathcal{L}(E)$ is a cq-channel, $\mathcal{N}^c(|i\rangle\langle j|) = \delta_{ij}\rho_i$, consider a distribution (p_i) on the input computational basis states. Let $(M_i = \overline{\rho}^{-\frac{1}{2}} p_i \rho_i \overline{\rho}^{-\frac{1}{2}})$ be the POVM associated with the ensemble $\{p_i, \rho_i\}$ and denote the corresponding qc-channel $\mathcal{M} : \mathcal{L}(E) \longrightarrow \mathcal{L}(A)$. Then,*

$$L_W(\mathcal{N}) \geq \widehat{H}(\mathcal{M}) = \min_{\psi \text{ state}} H(\mathcal{M}(\psi)).$$

Proof. We first describe a secret key generation protocol in the sense of weak locking: Alice generates i.i.d. $I_1, \ldots, I_n \sim (p_i)$ and sends the basis states $|I_1\rangle \cdots |I_n\rangle$ down the channel; Bob, by the nature of the channel, receives these basis states without noise, and so the string $I^n = I_1 \ldots I_n$ serves as a raw key shared between them.

Eve on the other hand, after measuring a POVM Q on her output states and obtaining outcomes J, has a certain min-entropy of I^n given J, which by Corollary 9 satisfies

$$H_{\min}^{\epsilon}(I^n|J) \geq n\big(\widehat{H}(\mathcal{M}) - \delta\big) - 16(\log d)^2 \frac{1}{\delta} \log \frac{1}{\epsilon}.$$

Thus, using a min-entropy extractor with $O(\log n)$ bits of "seed" randomness (which Alice and Bob are allowed as part of the sublinear amount of key they may pre-share), they can convert almost all of the smooth min-entropy into almost-uniform key K that is almost independent of J; cf. [35, Section 6.2] and references therein. Mathematically, the extractor (more precisely: *strong extractor*) is given by a function $e : \mathcal{I}^n \times \mathcal{S} \longrightarrow \mathcal{K} = \{0, 1\}^{nR}$, $R = \widehat{H}(\mathcal{M}) - 2\delta$ and $|\mathcal{S}| = \text{poly}(n)$. It has the property that for every random variable $I^{(n)} \sim P^{(n)}$ on $\mathcal{I}^n$ with min-entropy $\geq n(\widehat{H}(\mathcal{M}) - \delta) - 16(\log d)^2 \frac{1}{\delta} \log \frac{1}{\epsilon}$ and uniformly distributed $S \in \mathcal{S}$, $K = e(I^{(n)}, S)$ is almost uniformly distributed:

$$\|\mathbb{P}(K, S) - \mathbb{U}_{\mathcal{K}} \otimes \mathbb{U}_{\mathcal{S}}\|_1 \leq \frac{1}{\text{poly}(n)}, \tag{11}$$

where $\mathbb{U}_{\mathcal{K}} \otimes \mathbb{U}_{\mathcal{S}}$ is the uniform distribution on $\mathcal{K} \times \mathcal{S}$. This implies by triangle inequality, for Eve's measurement result J,

$$\|\mathbb{P}(J, K, S) - \mathbb{P}(J) \otimes \mathbb{U}_{\mathcal{K}} \otimes \mathbb{U}_{\mathcal{S}}\|_1 \leq \eta := \epsilon + \frac{1}{\text{poly}(n)}. \tag{12}$$

Observe that the bound $\frac{1}{\text{poly}(n)}$ comes from adding the error terms $\frac{1}{\text{poly}(|\mathcal{S}|)}$ and $2^{-n\Omega(\delta)}$ of the extractor [35]. Thus, making the seed space $\mathcal{S}$ larger we can suppress η more, up to any quantity decaying to zero slower than exponentially.

Now, to obtain a scheme to securely send uniformly distributed messages from $\mathcal{K}$, we "run the extractor backwards": From the joint distribution of I^n [i.i.d. according to (p_i)], S (uniform) and $K = e(I^n, S)$ we can construct a conditional distribution $\mathbb{P}(I^n|K, S) =: E(i^n|k, s)$, which describes a stochastic encoding mapping $E : \mathcal{K} \times \mathcal{S} \longrightarrow \mathcal{I}^n$. Note that we may assume $I^n = E(K, S)$ as random variables.

To send the uniformly distributed message $\widehat{K} \in \mathcal{K}$, Alice and Bob share a uniformly distributed private $\widehat{S} \in \mathcal{S}$, and Alice puts $\widehat{I}^{(n)} = E(\widehat{K}, \widehat{S}) \in \mathcal{I}^n$. We claim that this is a good code. Indeed, since he gets $\widehat{I}^{(n)}$ from the channel output, using $\widehat{S}$, Bob can decode $\widehat{K} = e(\widehat{I}^{(n)}, \widehat{S})$ with certainty.

On the other hand, Eve can obtain almost no information about $\widehat{K}$, because Eq. (11) means

$$\big\|\mathbb{P}(K, S) - \mathbb{P}(\widehat{K}, \widehat{S})\big\|_1 \leq \eta,$$

hence, applying the encoding map E,

$$\left\| \mathbb{P}(I^n, K, S) - \mathbb{P}(\widehat{I}^{(n)}, \widehat{K}, \widehat{S}) \right\|_1 \leq \eta.$$

Applying the complementary channel as well as Eve's POVM Q, we find

$$\left\| \mathbb{P}(J, K, S) - \mathbb{P}(\widehat{J}, \widehat{K}, \widehat{S}) \right\|_1 \leq \eta.$$

Putting this together with Eq. (12), and tracing out the seed, we finally obtain

$$\left\| \mathbb{P}(\widehat{J}, \widehat{K}) - \mathbb{P}(J) \otimes \mathbb{U}_{\mathcal{K}} \right\|_1 \leq 2\eta,$$

and letting ϵ and δ go to zero (slow enough) as $n \to \infty$, we are done. □

Remark 11. By using a seed of $o(n)$ bits in Eq. (11), and choosing $\epsilon = 2^{-o(n)}$ in Eq. (12), we get η-weak locking codes, with asymptotically the same rate and $\eta = 2^{-o(n)}$.

Example 12. Consider $|E| = d$, $|A| = |B| = 2d$ and the cq-channel $\mathcal{N}^c$ with pure output states $|v_{0i}\rangle = |i\rangle$ and $|v_{1i}\rangle = |\varphi_i\rangle$ ($i = 1, \ldots, d$), which are the eigenstates of the generalized Z and X operators, respectively.

Using the concavity of the coherent information and the covariance of the channel under the action of the discrete Weyl group, it is easy to see that the coherent information is maximized for the uniform input, and so

$$P(\mathcal{N}) = 1. \tag{13}$$

On the other hand, for uniform input distribution over the $2d$ basis states, the POVM $\left(\frac{1}{2}M_{0i}\right) \cup \left(\frac{1}{2}M_{1i}\right)$, where $M_{bi} = |v_{bi}\rangle\langle v_{bi}|$, is the random choice of one of the observables X or Z, and measurement of its eigenbasis. By the Maassen–Uffink entropic uncertainty relation [25], $\widehat{H}(\mathcal{M}) = 1 + \frac{1}{2}\log d$, which by Theorem 10 is a lower bound on $L_W(\mathcal{N})$. By Proposition 3, it is also an upper bound, since regardless of the input distribution over the computational basis states $i0, i1$, Eve can randomly choose and measure either X or Z, and get an accessible equivocation of at most $1 + \frac{1}{2}\log d$. Hence,

$$L_W(\mathcal{N}) = 1 + \frac{1}{2}\log d; \tag{14}$$

and thus the gap between the private and (weak) locking capacities of a d-dimensional channel can be as large as a constant versus $\Omega(\log d)$.

The Choi-Jamiołkowski state obtained from using the above channel with maximally entangled input was previously considered by Christandl et al. [6, Sec. 6], finding the same numbers for the secret key rate as Eqs. (13) and (14) as secret key rate against quantum and classical eavesdropper, respectively. Note however that for the latter conclusion, they have to assume that Eve applies the same measurement to each copy of the shared state. The proof of Theorem 10 shows that the conclusion of [6] holds for arbitrary measurements of the n systems in Eve's possession. □

In the next section, we shall exhibit an example of an even more striking effect: A channel whose private capacity, and indeed key generation capacity, is zero, because Bob and Eve see the exact same quantum information, but whose locking capacity is arbitrarily large.

4. Symmetric Channels with $\mathbf{L_W > 0 = P}$

Compared to Sect. 3, are there even channels with vanishing private capacity, i.e., $P(\mathcal{N}) = 0$, but positive locking capacity, $L_W(\mathcal{N}) > 0$? Note that the construction in the previous section, to yield nonzero locking capacity, requires a degradable Hadamard channel, and so its private capacity is also nonzero. In this case, note also that the sublinear pre-shared key between Alice and Bob is unnecessary, since they can use a sublinear number of channel uses and a private code to create the key from scratch.

In this section, we consider symmetric channels, which trivially have $P = 0$; on the other hand, the pre-shared key, even if only sublinear, can be enough of an advantage to get a locking capacity. For concreteness, let us look a little closer at the channel

$$\mathcal{S} : \mathcal{L}\big(\mathrm{Sym}^2(B)\big) \longrightarrow \mathcal{L}(B), \tag{15}$$

with $B \simeq E \simeq \mathbb{C}^d$, which has as its Stinespring dilation the isometric embedding of the $d \times d$ symmetric subspace $A = \mathrm{Sym}^2(B) \simeq \mathbb{C}^{d(d+1)/2}$ into $B \otimes E$.

One "reasonable" strategy to encode information is this: Use the product states $|\psi\rangle|\psi\rangle \in A$, which yield the same pure output state $|\psi\rangle$ for both Bob and Eve, or rather sequences of such state on n channel uses. Now, similar to the protocol in Sect. 3, use input states which result in either Z-basis or X-basis eigenstates output (equally for Bob and Eve, obviously), on small blocks of size k in n transmissions, so that only $\frac{n}{k}$ bits of key are required for both Alice and Bob to know the basis and to have a perfect communication channel. On the other hand, Eve, without this bit of basis information, faces uniformly random states in one of two mutually unbiased bases in dimension d^k, namely the Z eigenstates $|i^k\rangle$ and the X eigenstates $|\varphi_{i^k}\rangle$. Hence, for any POVM $Q = (Q_j)$ on E^k,

$$H(I|J) \geq \min_{\psi} S\big(\mathcal{M}(\psi)\big) = 1 + \frac{1}{2} k \log d,$$

and so we can invoke Proposition 6 and Corollary 9: For $\ell = \frac{n}{k}$ uses of this scheme, we obtain, for the measurement outcomes J of an arbitrary POVM (Q_j),

$$\begin{aligned} H_{\min}^{\epsilon}(I^{\ell}|J) &\geq n\left(\frac{1}{2} - \frac{\delta}{k}\right)\log d + \frac{n}{k} - \frac{16k^2(\log d)^2}{\delta}\log\frac{1}{\epsilon} \\ &\geq n\left(\frac{1}{2} - \frac{\delta}{k}\right)\log d, \end{aligned}$$

where for the last line, we have made the choice

$$k = \sqrt[3]{n \frac{\delta}{16(\log d)^2 \log \frac{1}{\epsilon}}}.$$

Now the argument progresses as in Sect. 3: On the top of the $\frac{n}{k}$ bits of key, we use another $o(n)$ bits for the randomness extractor. The key rate goes to zero as long as $k \longrightarrow \infty$. We see that we can achieve the locking rate $\frac{1}{2}\log d$, and even let $\frac{\delta}{k}$ and ϵ go to 0 sufficiently slowly: for instance, constant δ and $\epsilon = 2^{-n^\gamma}$, with any $\gamma < 1$. Thus we have proved the following theorem.

Theorem 13. *The symmetric subspace channel $\mathcal{S} : \mathcal{L}(Sym^2(\mathbb{C}^d)) \longrightarrow \mathcal{L}(\mathbb{C}^d)$ has zero private capacity, $P(\mathcal{S}) = 0$ (since it gives a copy of every output state of Bob to Eve), but $L_W(\mathcal{S}) \geq \frac{1}{2}\log d$.* □

This result dramatically improves the argument in [21] and [6]: Here we have a regular quantum cryptographic system, which could be BB84 sending a copy of each of the four states not only to Bob but also to Eve, very much like in the "photon number splitting attack" [17]—hence there can be no private communication capacity in the present setting of only a sublinear pre-shared key. But it can be perfectly good key as judged by the accessible information of Eve.

Remark 14. It may even be possible to show that for large enough d, the locking capacity $L_W(\mathcal{S})$ can be arbitrarily close to $C(\mathcal{N}) = \log d$, by using encodings into $m > 2$ many bases. What we would need is that repeating the basis a small number of times would still result in a "strong" uncertainty relation (cf. [37]), as it was shown for $k = 1$ in [13] and [11].

To be precise, denote the bases $(U_t|i\rangle)_{i=1}^d$, with unitaries U_t $(t = 0, \dots, m)$, so that we get m "repeated" bases $U_t^{\otimes k}$, each of which defines an orthogonal measurement $\left(M_{i_k}^{(t)} = U_t^{\otimes k}|i^k\rangle\langle i^k|U_t^{\otimes k\dagger}\right)$. The question then is, whether it is possible to find U_t such that for all states ψ on $(\mathbb{C}^d)^{\otimes k}$,

$$\frac{1}{m}\sum_{t=1}^{m} H\left(\{\operatorname{Tr}\psi M_{i^k}^{(t)}\}_{i^k}\right) \geq c(k,m)\log d^k,$$

with $c(k,m) \to 1$ as $k \to \infty$ and $m \leq 2^{k^c}$ for some $0 < c < 1$. With such an uncertainty relation in hand, we could go through the proof of Theorem 13, letting $n = \text{poly}(k)$ as before and thus using $\sim \frac{n}{k}k^c = o(n)$ bits of key, while attaining a locking rate of $c(k,m)\log d$.

5. Conclusion and Possible Further Developments

Our results on separations between $P(\mathcal{N})$ and $L_W(\mathcal{N})$, Theorems 10 and 13, and Example 12, have an interpretation in terms of quantum key distribution (QKD): $\mathcal{N}$ may be the effective channel between Alice and Bob if Eve applies a so-called *collective attack*, the same and known isometry V to all transmissions. In fact, the security definition of the weak locking capacity is the old-style notion put forward in the very first complete analyses of BB84 and related protocols [26], cf. the historical account in the nice review [30] (footnote 20). Indeed, in these older texts, it was assumed that it is enough to bound the "knowledge of Eve about the key," understood as the (Shannon) information she can obtain by making a suitable measurement after collecting all sorts of quantum and classical systems during the protocol. The definition of $L_W(\mathcal{N})$ is essentially based on taking this notion of cryptographic security of the key literally. It was only with the discovery of quantum information locking [10] and its subsequent development [11,13] that it was eventually understood that this is a very badly behaved security criterion, in particular not composable, and subject to chosen plaintext attacks (where the eavesdropper has side information about the message to be transmitted) [6,21]. The timing problem of *when* the measurement should take place, and hence whether side information becomes available before or after it, is at the heart of this issue, and has been investigated in its own right [3]. The new, modern, information theoretic security definition [28] is at the basis of the notion of private capacity $P(\mathcal{N})$.

Furthermore, Theorem 13 shows that it is possible for the locking capacity to be positive where "evidently," due to the symmetry of the channel between legal and eavesdropping users, there can be no secrecy. The coding scheme may even be interpreted in the context of the famous *photon number splitting attack* on coherent state-based QKD protocols [17]: The protocol of Theorem 13 is as if Alice *always* prepares a state of two photons, in fact two identical copies of her chosen polarization—and naturally Bob and Eve each get one.

The main open question about the Hadamard channels considered in Sect. 3 is, whether $S_{\text{acc}}(I|E)$, or in other words, the constrained minimum output entropy of the associated POVM for a given distribution (p_i) of the inputs,

$$\widehat{H}(\mathcal{M}|\sigma) = \min_{\{q_j,\psi_j\}} \sum_j q_j H\big(\mathcal{M}(\psi_j)\big) \quad \text{s.t.} \quad \sum_j q_j \psi_j = \sigma,$$

is an achievable locking rate.

The obvious first step to try would be to consider the Rényi entropic version of this,

$$\widehat{H}_\alpha(\mathcal{M}|\sigma) = \min H_\alpha(I|J) \quad \text{s.t.} \quad \sum_j q_j \psi_j = \sigma,$$

where

$$H_\alpha(I|J) = -\frac{\alpha}{\alpha-1} \log\left(\sum_j q_j \left(\sum_i (\operatorname{Tr} \psi_j M_i)^\alpha \right)^{1/\alpha} \right)$$

is the conditional α-entropy (cf. [27, Def. 4], where the classical case is attributed to Arimoto [2]). Note that it relates to the smooth conditional min-entropy and the conditional von Neumann entropy in analogous ways as the nonconditional versions [34], here stated as Lemmas 16 and 18 in "Appendix."

What is missing is an additivity proof. So this is the question: For two POVMs $M^{(1)}$ and $M^{(2)}$, and states σ_1 and σ_2, does it hold that

$$\widehat{H}_\alpha(\mathcal{M}^{(1)} \otimes \mathcal{M}^{(2)}|\sigma_1 \otimes \sigma_2) = \widehat{H}_\alpha(\mathcal{M}^{(1)}|\sigma_1) + \widehat{H}_\alpha(\mathcal{M}^{(2)}|\sigma_2)\,? \tag{16}$$

[Note that "$\leq$" is trivially true.] If that is the case, we are done, by substituting $\widehat{H}_\alpha(\mathcal{M}|\sigma)$ for the simpler, and smaller, $\widehat{H}_\alpha(\mathcal{M})$, in the proof of Theorem 10. In the limit $\alpha \to 1$, this is true by [19, Lemma 3]; see also the proof of our Lemma 4.

This would give the weak locking capacity for those channels, since the achievable rate, optimized over all input distributions, i.e., $L_W(\mathcal{N}) \geq \max_{(p_i)} S_{\mathrm{acc}}(I|E)$, would then match the multi-letter converse from [12] for these channels, which by Proposition 3 for the present channels simplifies to $L_W(\mathcal{N}) \leq \max_{(p_i)} S_{\mathrm{acc}}(I|E)$.

It should be noted that what we really need is a lower bound on the smooth min-entropy of the i.i.d. I^n conditioned on the measurement outcomes J from the POVM on E^n, of the form

$$H^{\epsilon}_{\min}(I^n|J) \overset{?}{\gtrsim} n\big(S_{\mathrm{acc}}(I|E) - \delta\big), \tag{17}$$

analogous to [7]. This would be implied by Eq. (16) being true, along the lines of the proof in "Appendix." But even if the additivity fails, there might be a direct proof of Eq. (17).

Going on to more general channels, we could then approach the problem of how tight is the upper bound on $L_W(\mathcal{N})$ in terms of the regularization of

$$L^{(u)}_W(\mathcal{N}) = \max_{\{p_x,\rho_x\}} I(X:B) - I_{\mathrm{acc}}(X:E).$$

This seems a difficult question, as it has to be noted that there is no obvious way how to attain it as a rate for a locking code. The problem lies in the term $I(X:B)$, which suggests that we should select a code for the channel on blocks of length n, rather than i.i.d. copies X^n, cf. [5,8]. But when the i.i.d. ensemble structure of the inputs X^n is disrupted, the accessible information $I_{\mathrm{acc}}(X^n:E^n)$ can possibly change dramatically, because of the very locking effect [10].

A possible way forward would be to allow the use of another, private, channel, let us say for concreteness a noiseless channel of sufficiently large dimension k. Then, Alice can use an ensemble decomposition of the i.i.d. X^n into good codes for the channel $\mathcal{N}^{\otimes n}$ to Bob, choose one of them at random and inform him about the choice over the auxiliary channel; any $\log k \gtrsim H(X|B)$ will do. Via the code she can send $I(X:B)$ bits per channel use to Bob. For Eve, on the other hand, the noiseless channel id_k does not yield any information, and $\mathcal{N}$ appears to be used with i.i.d. X^n from her point of view. Then, assuming the additivity hypothesis (16), or rather the min-entropy uncertainty relation (17) above, this "raw key" can be hashed down to $S_{\mathrm{acc}}(X|E)$ locked bits per channel use. By the same argument of "running the extractor backwards" as in the proof of Theorem 10, we thus would get $L_W(\mathcal{N} \otimes \mathrm{id}_k) \geq L^{(u)}_W(\mathcal{N}) + \log k = L^{(u)}_W(\mathcal{N} \otimes \mathrm{id}_k)$.

This sketch of a proof should suffice to show the following:

Theorem 15. *If the additivity hypothesis (16), or more specifically, the min-entropy uncertainty relation (17) is true, then for $\mathcal{N}$ the complement of a cq-channel,*

$$L_W(\mathcal{N}) = \max_{(p_i)} S_{acc}(I|E) = L_W^{(u)}(\mathcal{N}).$$

Furthermore, for an arbitrary channel $\mathcal{N}$, the activated *(or* amortized*)* weak locking capacity $\overline{L}_W(\mathcal{N}) := \sup_k L_W(\mathcal{N} \otimes \mathrm{id}_k) - \log k \geq L_W(\mathcal{N})$ *is given by*

$$\overline{L}_W(\mathcal{N}) = \sup_n \frac{1}{n} L_W^{(u)}(\mathcal{N}^{\otimes n}).$$

□

Of course, we do not know at this point whether $L_W(\mathcal{N}) = \overline{L}_W(\mathcal{N})$ for all channels. Note however that strict inequality would imply that L_W is nonadditive even when combining a noisy channel with a noiseless one. On the other hand, maybe $\overline{L}_W$ is a more natural definition of locking capacity, since the (amortized) use of the noiseless channel really amounts to allowing a linear secret key rate, rather than a sublinear amount, but letting the users pay for it.

Regarding the original locking capacity papers [12,23], a very interesting problem would be to find a nontrivial lower bound on the weak locking capacity of Gaussian channels, such as the pure-loss bosonic channel. Indeed, maybe the 50 % lossy channel, which has private capacity 0, can be analyzed along the lines of Sect. 4? Note however, that from [12] we have a *constant* upper bound on its weak locking capacity, irrespective of the input power, at least for coherent state encodings. It may be observed here that indeed [12, Thms. 26 and 27] hold also for more general encodings into statistical mixtures of coherent states, which would be the kind of code that our main constructions would yield, even starting from pure coherent state ensembles.

Finally, to close this long list of open questions, let us turn to the strong locking capacity [12], which we have not touched upon at all in this paper. In fact, there might be link between weak and strong locking, suggested by a simple generalization of the symmetric channel (15):

$$\mathcal{S}_k : \mathcal{L}\big(\mathrm{Sym}^k(B)\big) \longrightarrow \mathcal{L}(B),$$

with $B \simeq \mathbb{C}^d$ and $E \simeq \mathrm{Sym}^{k-1}(B) \subset (\mathbb{C}^d)^{\otimes k-1}$, which has as its Stinespring dilation the isometric embedding of the k-fold symmetric subspace $A = \mathrm{Sym}^k(B)$ into $B \otimes E$. The generalization of the scheme in Sect. 4 would be to encode information into $|\psi\rangle^{\otimes k} \in A$, so that Bob gets one, Eve instead $k-1$ copies of $|\psi\rangle$, chosen from one of several bases determined by the pre-shared key. It seems quite reasonable to expect that all of these (anti-degradable) channels have positive weak locking capacity. But weak locking for $\mathcal{S}_k$ implies strong locking for $\mathcal{S}_{k-1}$, and so we expect that $L_S(\mathcal{S}_k) \geq L_W(\mathcal{S}_{k+1}) > 0$ for all $k \geq 2$.

Acknowledgements

I thank Mark Wilde for enlightening discussions on information locking, for introducing me to locking capacities and for first raising the problem of separating the private capacity from the weak locking capacity. The keen interest he and Saikat Guha took in this project helped immensely to develop the ideas of the present paper. This research was supported by the European Commission (STREP "RAQUEL"), the European Research Council (Advanced Grant "IRQUAT") and the Spanish MINECO (project FIS2008-01236) with FEDER funds. Part of this work was done during the program "Mathematical Challenges in Quantum Information" (MQI), 27/8-20/12/2013, at the Isaac Newton Institute in Cambridge, whose hospitality during the semester is gratefully acknowledged.

Appendix: High-Order Min-Entropy Uncertainty Relation via Additivity of Output Rényi Entropies

Here we give a simple direct proof of Proposition 6. In [7], it was first shown using Azuma's inequality for tails of martingales and a nontrivial truncation trick. The following proof rests on lower bounding the smooth min-entropy in terms of Rényi entropies, and lower bounding the latter in terms of von Neumann entropies. This idea can be traced back to [33]. The relevant lemmas are stated here for completeness, and they are direct corollaries of the citations given.

Lemma 16. (Renner/Wolf [29]) *For any state ρ and $\alpha > 1$,*

$$H_{\min}^{\epsilon}(\rho) \geq H_\alpha(\rho) - \frac{1}{\alpha - 1} \log \frac{1}{\epsilon}.$$

□

Remark 17. Under smoothing with respect to the purified distance, the above relation would read

$$H_{\min}^{\epsilon}(\rho) \geq H_\alpha(\rho) - \frac{1}{\alpha - 1} \log \frac{2}{\epsilon^2}.$$

(Cf. Tomamichel [34, Prop. 6.2].) As pointed out already, in the present paper, we are using instead the smoothing w.r.t. the trace norm.

Lemma 18. (Tomamichel [34, Lemma 6.3]) *For any state ρ on a d-dimensional Hilbert space, and $1 < \alpha < 1 + \frac{\log 3}{4 \log \nu}$, with $\nu = 2 + \sqrt{d}$,*

$$H_\alpha(\rho) \geq H(\rho) - 4(\alpha - 1)(\log \nu)^2.$$

A simplified version reads thus: For $1 < \alpha < 1 + \frac{\log 3}{16 \log d}$ and $d \geq 2$,

$$H_\alpha(\rho) \geq H(\rho) - 16(\alpha-1)(\log d)^2.$$

□

Proof (of Proposition 6). By Lemma 16, for arbitrary n and state ψ,

$$H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq H_\alpha\big(\mathcal{M}^{\otimes n}(\psi)\big) - \frac{1}{\alpha-1}\log\frac{1}{\epsilon}.$$

On the other hand, by the additivity of the minimum output α-Rényi entropy of qc-channels, and more generally entanglement-breaking channels [18,19], cf. also [16],

$$H_\alpha\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq n\widehat{H}_\alpha(\mathcal{M}),$$

with $\widehat{H}_\alpha(\mathcal{M}) := \min_{\psi \text{ state}} H_\alpha\big(M(\psi)\big)$. Hence, using now Lemma 18,

$$H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq n\big(\widehat{H}(\mathcal{M}) - 16(\alpha-1)(\log d)^2\big) - \frac{1}{\alpha-1}\log\frac{1}{\epsilon},$$

as along as α is close enough to 1. Letting $\alpha = 1 + \frac{\delta}{16(\log d)^2}$, we conclude

$$H_{\min}^{\epsilon}\big(\mathcal{M}^{\otimes n}(\psi)\big) \geq n\big(\widehat{H}(\mathcal{M}) - \delta\big) - 16(\log d)^2\frac{1}{\delta}\log\frac{1}{\epsilon}.$$

□

References

[1] R. Alicki, M. Fannes, Continuity of quantum conditional information. J. Phys. A: Math. Gen. **37**, L55–L57 (2004)

[2] S. Arimoto, Information measures and capacity of order α for discrete memoryless channels, in: *Topics in Information Theory—2nd Colloquium*, *Colloq. Math. Soc. J. Bolyai* **16**, pp. 41–52, I. Csiszár and P. Elias (eds.), North Holland, Amsterdam, 1977

[3] M.A. Ballester, S. Wehner, A. Winter, State Discrimination With Post-Measurement Information. IEEE Trans. Inf. Theory **54**(9), 4183–4198 (2008)

[4] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**(5), 3824–3851 (1996)

[5] N. Cai, A. Winter, R.W. Yeung, Quantum Privacy and Quantum Wiretap Channels. Probl. Inf. Transm. **40**(4), 318–336 (2004)

[6] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, R. Renner, Unifying Classical and Quantum Key Distillation, in: *Proc. TCC 2007*, LNCS 4392, pp. 456–478, Springer Verlag, Berlin, 2007; arXiv:quant-ph/0608199

[7] I. Damgaard, S. Fehr, R. Renner, L. Salvail, C. Schaffner, A Tight High-Order Entropic Quantum Uncertainty Relation with Applications, in: *Proc. CRYPTO 2007*, LNCS 4622, pp. 360–378, Springer Verlag, Berlin, 2007; arXiv:quant-ph/0612014

[8] I. Devetak, The Private Classical Capacity and Quantum Capacity of a Quantum Channel. IEEE Trans. Inf. Theory **51**(1), 44–55 (2005)

[9] I. Devetak, P.W. Shor, The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information. Commun. Math. Phys. **256**(2), 287–303 (2005)

[10] D.P. DiVincenzo, M. Horodecki, D.W. Leung, J.A. Smolin, B.M. Terhal, Locking classical correlations in quantum states. Phys. Rev. Lett. **92**, 067902 (2004)
[11] O. Fawzi, P. Hayden, P. Sen, From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking, *J. ACM* **60**(6), article no. 44, 2013
[12] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J.H. Shapiro, M. Takeoka, M.M. Wilde, Quantum enigma machines and the locking capacity of a quantum channel. Phys. Rev. X **4**, 011016 (2014)
[13] P. Hayden, D. Leung, P.W. Shor, A. Winter, Randomizing Quantum States: Constructions and Applications. Commun. Math. Phys. **250**, 371–391 (2004)
[14] A.S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel. Probl. Inf. Transm. **9**(3), 177–183 (1973)
[15] A.S. Holevo, Problems in the mathematical theory of quantum communication channels. Rep. Math. Phys. **12**(2), 273–278 (1977)
[16] A.S. Holevo, Multiplicativity of p-norms of completely positive maps and the additivity problem in quantum information theory. Russian Math. Surveys **61**(2), 301–339 (2006)
[17] B. Huttner, N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent states. Phys. Rev. A **51**(3), 1863–1869 (1995)
[18] C. King, Maximization of capacity and ℓ_p norms for some product channels. J. Math. Phys. **43**(3), 1247–1260 (2002)
[19] C. King, Maximal p-norms of entanglement breaking channels. Quantum. Inf. Comput. **3**(2), 186–190 (2003)
[20] C. King, K. Matsumoto, M. Nathanson, M.-B. Ruskai, Properties of conjugate channels with applications to additivity and multiplicativity. Markov Proc. Rel. Fields **13**(2), 391–423 (2007)
[21] R. Koenig, R. Renner, A. Bariska, U. Maurer, Small Accessible Quantum Information Does Not Imply Security. Phys. Rev. Lett. **98**, 140502 (2007)
[22] E.H. Lieb, M.B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy. J. Math. Phys. **14**(12), 1938–1941 (1973)
[23] S. Lloyd, Quantum enigma machines, arXiv:1307.0380 [quant-ph], 2013
[24] C. Lupo, S. Lloyd, Quantum data locking for high-rate private communication. New J. Phys. **17**, 033022 (2015)
[25] H. Maassen, J.B.M. Uffink, Generalized Entropic Uncertainty Relations. Phys. Rev. Lett. **60**(12), 1103–1106 (1988)
[26] D. Mayers, Unconditional Security in Quantum Cryptography. J. ACM **48**(3), 351–406 (2001)
[27] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel, On quantum Rényi entropies: A new generalization and some properties. J. Math. Phys. **54**, 122203 (2013)
[28] R. Renner, *Security of Quantum Key Distribution*, PhD thesis, ETH Zürich, 2005. arXiv:quant-ph/0512258
[29] R. Renner and S. Wolf, Smooth Rényi entropy and applications, in: *Proc. ISIT 2004*, p. 232, 2004
[30] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution. Rev. Mod. Phys. **81**(3), 1301–1350 (2009)
[31] M. Sion, On General Minimax Theorems. Pacific J. Math. **8**(1), 171–176 (1957)
[32] G. Smith, Private classical capacity with a symmetric side channel and its application to quantum cryptography. Phys. Rev. A **78**, 022306 (2008)
[33] M. Tomamichel, R. Colbeck, R. Renner, A Fully Quantum Asymptotic Equipartition Property. IEEE Trans. Inf. Theory **55**(12), 5840–5847 (2009)
[34] M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, PhD thesis, ETH Zürich, 2012. arXiv:1203.2142 [quant-ph]
[35] S. P. Vadhan, *Pseudorandomness*, draft, 2013. http://people.seas.harvard.edu/~salil/pseudorandomness/
[36] J. von Neumann, Zur Theorie der Gesellschaftsspiele. Math. Ann. **100**, 295–320 (1928)
[37] S. Wehner, A. Winter, Entropic uncertainty relations–a survey. New J. Phys. **12**(2), 025009 (2010)
[38] A.D. Wyner, The Wire-Tap Channel. Bell Syst. Tech. J. **54**(6), 1355–1387 (1975)