Random subspaces for encryption based on a private shared Cartesian frame

Stephen D. Bartlett,[1] Patrick Hayden,[2] and Robert W. Spekkens[3]
[1]*School of Physics, The University of Sydney, New South Wales 2006, Australia*
[2]*School of Computer Science, McGill University, Montreal, Canada*
[3]*Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
(Received 15 July 2005; published 23 November 2005)

A private shared Cartesian frame is a novel form of private shared correlation that allows for both private classical and quantum communication. Cryptography using a private shared Cartesian frame has the remarkable property that asymptotically, if perfect privacy is demanded, the private classical capacity is three times the private quantum capacity. We demonstrate that if the requirement for perfect privacy is relaxed, then it is possible to use the properties of random subspaces to nearly triple the private quantum capacity, almost closing the gap between the private classical and quantum capacities.

DOI: 10.1103/PhysRevA.72.052329 PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Pp

I. INTRODUCTION

Quantum information theory is concerned with implementing various communications tasks with a minimal use of resources [1]. In multiparty protocols, the most interesting resources are *nonlocal* ones, such as shared classical key or entanglement. Recently, it has become apparent that shared reference frames (SRFs) are another form of nonlocal resource that may be included in the accounting of any multiparty information-processing protocol. Heuristically, two parties are said to share a reference frame if there is a perfect correlation between the systems that define the bases of their respective local Hilbert spaces. For instance, if Alice and Bob each define their local Cartesian frame using classical gyroscopes in their labs, then they possess a shared reference frame if the rotation relating the frames defined by their gyroscopes is known to them.

Like entanglement, no amount of discussion between Alice and Bob will allow them to establish a shared reference frame: doing so requires a physical interaction between them that goes beyond the framework of classical information theory and, for that matter, the usual formalism of quantum information theory. For example, to establish a shared Cartesian frame between their respective labs, Alice and Bob may make use of a *pre-existing* frame such as the fixed stars or the Earth's magnetic field. However, if no such shared frame exists *a priori*, then no amount of discussion will enable them to establish one; to do so, they must exchanges physical systems that carry some directional information such as spin-$1/2$ particles. Understanding the value of a shared reference frame as a new nonlocal resource and its relation to both private and quantum communication, therefore, is an important necessary step in the ongoing effort to understand the nature of information in physics.

Substantial progress has recently been made in this direction. Most research has focused on determining the communication cost to establishing a SRF [2–8]. There have also been several investigations into the impact of SRFs (or the lack thereof) on the efficiency with which one can perform a variety of bipartite tasks, such as quantum and classical communication [9,10], key distribution [11,12], and the manipulation of entanglement [10,13–15]. Other work has studied the cryptographic consequences of the participants' lack of a SRF [13,16,17]. Here we shall be interested instead in using *private* SRFs as a resource.

A SRF is private if the systems that define Alice and Bob's local Hilbert space bases are not correlated with any other systems. In this case, the SRF can act as a new kind of key for private quantum and classical communication over a public channel. Consider a private shared Cartesian frame, as in Ref. [18]. Under the requirement that the communication have perfect fidelity and the privacy be perfect, it was found that for N transmitted qubits, the number of private qubits that can be communicated asymptotically is $\log_2 N$, and the number of private classical bits that can be communicated asymptotically is $3 \log_2 N$. This unusual factor of three relating the quantum and classical capacities is understood in terms of the details of the representation theory of SU(2) [19], but should be contrasted with the "usual" factor of two that typically relates classical and quantum schemes [20,21]. In the present paper, we ask the question of whether these capacities may be improved by allowing transmission with near-perfect rather than perfect privacy, as is usually considered in cryptography.

Note the following suggestive facts. $2N$ secret shared classical bits can be used in a one-time pad to encrypt $2N$ classical bits (cbits). However, if one asks how many private *qubits* can be transmitted using the secret key, the answer is a factor of 2 less; that same secret $2N$ cbit string can only encrypt N qubits if perfect privacy is required [21]. If only near-perfect privacy is required, on the other hand, the number of secret cbits required per encrypted qubit shrinks from 2 to 1 asymptotically [22], so that the difference between encrypting cbits and qubits disappears.

A similar effect occurs in the domain of communication using shared entanglement. The superdense coding protocol [20] uses the transmission of N qubits and the consumption of N ebits to communicate $2N$ cbits with perfect privacy. (An ebit is a pure, maximally entangled state of two qubits.) The number of qubits that can be transmitted with perfect privacy and no errors is again a factor of 2 less, as implemented in the quantum Vernam cipher [23]. If either near-perfect privacy or near-perfect transmission is permitted, however, the superdense coding protocol can be extended to allow the transmission of nearly $2N$ *qubits* [24,25], again erasing the difference between sending classical and quantum data. The fact that the methods developed in Ref. [18] for communicating private classical data using a private shared reference frame made heavy use of superdense coding suggests that it may be possible, by relaxing the security conditions, to increase the private quantum capacity by a factor of 3, from $\log_2 N$ to nearly $3 \log_2 N$. We shall show that this is indeed the case.

II. PRELIMINARIES

A. Brief comment on notation

The symbol for a state (such as φ or ρ) also denotes its density matrix. A *pure* state is always denoted as a ket (e.g., $|\varphi\rangle$) and the density matrix for a pure state $|\varphi\rangle$ is written simply as φ. We will also use the notation $x_N \sim y_N$ if $\lim_{N\to\infty} x_N / y_N = 1$. The term *irrep* denotes an irreducible representation of a group.

B. Private quantum channels using private shared correlations

Whenever Alice and Bob have some private shared correlation, that is, one to which an eavesdropper Eve does not have access, Eve's description of the systems transmitted along the channel is related to Alice's description by a decohering superoperator, denoted by $\mathcal{E}$ [18,21]. Before discussing shared reference frames specifically, we begin by formalizing the notions of the private quantum and classical capacities of this decohering superoperator.

A δ-private *quantum communication* scheme for $\mathcal{E}$ consists of a completely positive, trace-preserving encoding $\mathcal{C}$, mapping message states on a logical Hilbert space $\mathbb{H}_L$ to encoded states on the Hilbert space $\mathbb{H}$ of the transmitted system, such that (i) the operation $\mathcal{C}$ is invertible by Bob (who possesses the private shared correlations), allowing him to decode and recover states on $\mathbb{H}_L$ with perfect fidelity, and (ii) the encoding satisfies

$$\|\mathcal{E}(\varphi) - \rho_0\|_1 \leq \delta, \quad \forall\ |\varphi\rangle \in \mathbb{H}_L, \tag{1}$$

where ρ_0 is some fixed state on $\mathbb{H}$, $\|\rho-\sigma\|_1 \equiv \mathrm{Tr}|\rho-\sigma|$ is the trace distance between ρ and σ, and δ is a security parameter. When $\delta=0$, the scheme is said to be *perfectly private*. The *private quantum capacity* of this channel, $Q(\mathcal{E},\delta)$, is defined as $Q(\mathcal{E},\delta) = \sup_{\mathcal{C}} \log_2 \dim \mathbb{H}_L$.

A δ-private *classical communication* scheme for $\mathcal{E}$ consists of a set $\{\rho_i\}_{i=1}^m$ of density operators on $\mathbb{H}$ such that (i) the $\{\rho_i\}$ are orthogonal, so that Bob can distinguish these classical messages with certainty, and (ii) the encoding satisfies

$$\|\mathcal{E}[\rho_i] - \rho_0\|_1 \leq \delta, \quad \forall\ i, \tag{2}$$

where, again, ρ_0 is some fixed state in $\mathbb{H}$ and δ is a security parameter. The *private classical capacity* of this channel, $C(\mathcal{E},\delta)$, is defined to be $C(\mathcal{E},\delta) = \sup_{\{\rho_i\}} \log_2 |\{\rho_i\}|$, where the supremum is over sets of density operators $\{\rho_i\}$ achieving δ-privacy.

Given δ privacy, for any pair of quantum or classical messages, chosen with equal prior probabilities, the probability that Eve can distinguish these is bounded above by $(1+\delta)/2$, seen as follows. Suppose the message states are ϱ_1 and ϱ_2. These could be either an encoded pair of quantum messages, that is, $\mathcal{C}(\varrho_{L,1})$ and $\mathcal{C}(\varrho_{L,2})$ for some pair of density operators $\varrho_{L,1}$ and $\varrho_{L,2}$ on $\mathbb{H}_L$, or an encoded pair of classical messages, that is, orthogonal density operators. In either case, the optimal probability for Eve to distinguish $\mathcal{E}(\varrho_1)$ and $\mathcal{E}(\varrho_2)$ is given by $\frac{1}{2}+\frac{1}{4}\|\mathcal{E}(\varrho_1)-\mathcal{E}(\varrho_2)\|_1$ [26,27]. Making use of the triangle inequality for the trace norm $\|\cdot\|_1$, we obtain

$$\|\mathcal{E}(\varrho_1) - \mathcal{E}(\varrho_2)\|_1 \leq \|\mathcal{E}(\varrho_1) - \rho_0\|_1 + \|\mathcal{E}(\varrho_2) - \rho_0\|_1 \leq 2\delta, \tag{3}$$

where on the second line we have applied the definition of δ privacy. It follows that if the scheme is δ private, Eve's probability of distinguishing the two messages is bounded above by $(1+\delta)/2$.

C. Private quantum communication using a private shared Cartesian frame

We now determine the superoperator $\mathcal{E}$ that describes Eve's ignorance of Alice and Bob's private shared Cartesian frame for states of N spin-1/2 particles. (Our description applies equally well to any realization of a qubit that is entirely defined relative to some reference frame; another example is a single-photon polarization qubit.) The transmitted Hilbert space $\mathbb{H}$ in this case is $(\mathbb{C}^2)^{\otimes N}$. This Hilbert space carries a tensor power representation $R^{\otimes N}$ of SU(2), by which an element $\Omega \in \mathrm{SU}(2)$ acts identically on each of the N qubits. For simplicity, we restrict N to be an even integer for the remainder of this paper, but our main results apply straightforwardly to all N. Then, we can decompose

$$(\mathbb{C}^2)^{\otimes N} = \bigoplus_{j=0}^{N/2} \mathbb{H}_j, \tag{4}$$

where $\mathbb{H}_j$ is the eigenspace of total angular momentum with eigenvalue j.

Each subspace $\mathbb{H}_j$ in the direct sum can be factored into a tensor product $\mathbb{H}_j = \mathbb{H}_{jR} \otimes \mathbb{H}_{jP}$, such that SU(2) acts irreducibly on $\mathbb{H}_{jR}$ and trivially on $\mathbb{H}_{jP}$. Thus,

$$(\mathbb{C}^2)^{\otimes N} = \bigoplus_{j=0}^{N/2} \mathbb{H}_{jR} \otimes \mathbb{H}_{jP}. \tag{5}$$

The dimension of $\mathbb{H}_{jR}$ is

$$d_{jR} = 2j + 1, \tag{6}$$

and that of $\mathbb{H}_{jP}$ is

$$d_{jP} = \binom{N}{N/2 - j} \frac{2j+1}{N/2 + j + 1}. \tag{7}$$

If Alice prepares N qubits in a state ρ and sends them to Bob, an eavesdropper Eve who is uncorrelated with the private SRF will describe the state as mixed over all rotations $\Omega \in \mathrm{SU}(2)$. Thus, the superoperator $\mathcal{E}$ acting on a general density operator ρ of N qubits that describes the lack of knowledge of this private SRF is given by [9]

$$\mathcal{E}(\rho) = \int R(\Omega)^{\otimes N}\rho R^{\dagger}(\Omega)^{\otimes N}\mathrm{d}\Omega. \quad (8)$$

The effect of this superoperator is best seen through the use of the decomposition (5) of the Hilbert space. The action of the superoperator $\mathcal{E}$ can be expressed in terms of this decomposition as

$$\mathcal{E}(\rho) = \sum_{j=0}^{N/2} (\mathcal{D}_{jR} \otimes \mathcal{I}_{jP})(\Pi_j\rho\Pi_j), \quad (9)$$

where $\mathcal{D}_{jR}$ is the completely depolarizing superoperator on $\mathbb{H}_{jR}$, $\mathcal{I}_{jP}$ is the identity superoperator on $\mathbb{H}_{jP}$, and Π_j is the projector onto $\mathbb{H}_j$. The subsystems $\mathbb{H}_{jP}$ are called *decoherence-free* or *noiseless* subsystems [28] under the action of this superoperator; states encoded into these subsystems are completely protected from this decoherence. In contrast, $\mathcal{E}_N$ is completely depolarizing on each $\mathbb{H}_{jR}$ subsystem, and thus, the $\mathbb{H}_{jR}$ are called *decoherence-full* subsystems [18].

The largest decoherence-full subsystem occurs for $j_{\max}=N/2$ and has dimension $2j_{\max}+1=N+1$. As proven in Ref. [18], this decoherence-full subsystem defines the optimally efficient perfectly secure private quantum communication scheme. Thus, given a private Cartesian frame and the transmission of N qubits, Alice and Bob can with perfect privacy communicate $Q(\mathcal{E},0)=\log_2(N+1)\sim\log_2 N$ qubits asymptotically.

In contrast, in that same paper, it was shown that the private *classical* capacity using the private shared Cartesian frame was given by $C(\mathcal{E},0)\sim 3\log_2 N$. In Appendix I, we extend the result to show that $C(\mathcal{E},\delta)\leqslant 3(1+\delta)\log_2 N+3$ for $\delta\leqslant 1/2$. The δ-private classical capacity, therefore, does not change dramatically when δ is made nonzero.

D. The working space $\mathbb{H}'$

To construct a "working" Hilbert space on which to investigate large random subspaces, we use the Hilbert space on which the states in the private classical communication scheme have support. This Hilbert space is constructed as follows. Note that for all j strictly less than the maximum value $N/2$, the decoherence-free subsystem $\mathbb{H}_{jP}$ is always of *greater or equal* dimension than the decoherence-full subsystem $\mathbb{H}_{jR}$. Thus, we will employ irreps up to, but *not* including, $j=N/2$. Let $j_{\min}<N/2$ be some fixed irrep. Our working space $\mathbb{H}'$ will include elements from every irrep in the range $j_{\min}\leqslant j<N/2$, that is, for $j\in Y$, where

$$Y = \{j_{\min}, j_{\min}+1, \ldots, N/2-1\}. \quad (10)$$

For convenience, we denote the dimension of the decoherence-full subsystem of the $j_{\min}$ irrep by D, that is, $D\equiv 2j_{\min}+1$. Choose a D-dimensional subspace $\mathbb{H}'_{jR}$ of $\mathbb{H}_{jR}$ for every $j\in Y$, and a subspace $\mathbb{H}'_{jP}$ of $\mathbb{H}_{jP}$ that is of dimension $D_\alpha\equiv\lfloor(1/\alpha)D\rfloor$, for some parameter $\alpha>1$. Note that such subspaces always exist because $\dim\mathbb{H}_{jR}=2j+1\geqslant D$ and $\dim\mathbb{H}_{jP}\geqslant\dim\mathbb{H}_{jR}$ for all $j\in Y$.

The Hilbert space of interest is then

$$\mathbb{H}' = \bigoplus_{j\in Y} \mathbb{H}'_{jR} \otimes \mathbb{H}'_{jP}, \quad (11)$$

with dimensionality $K\equiv\dim\mathbb{H}'$ given by

$$K \sim \frac{1}{\alpha}\sum_{j\in Y} D^2 = \frac{1}{\alpha}(N/2-j_{\min})(2j_{\min}+1)^2. \quad (12)$$

To maximize this dimension, we choose $j_{\min}$ to be the integer nearest to $N/3$. In this case, we have asymptotically

$$K \sim \frac{2}{27}\frac{1}{\alpha}N^3. \quad (13)$$

(More precisely, $K-1$ exceeds the right-hand side for sufficiently large N, a result we will use later.)

The superoperator $\mathcal{E}$ maps a state φ on $\mathbb{H}'$ to the state

$$\mathcal{E}(\varphi) = \sum_{j\in Y} (I_{\mathbb{H}_{jR}}/d_{jR}) \otimes \mathrm{Tr}_{jR}(\Pi_j\varphi\Pi_j), \quad (14)$$

where $I_{\mathbb{H}_{jR}}$ is the identity on $\mathbb{H}_{jR}$. (Note that the state $\mathcal{E}(\varphi)$ will, in general, have support outside of $\mathbb{H}'$.) To fully exploit the working space, we will pursue an encoding such that $\mathcal{E}(\varphi)$ is close to maximally mixed on as large a subspace as possible. To this end, we define

$$\rho_0 \equiv \sum_{j\in Y} (I_{\mathbb{H}_{jR}}/d_{jR}) \otimes (I_{\mathbb{H}'_{jP}}/D_\alpha), \quad (15)$$

where $I_{\mathbb{H}'_{jP}}$ is the identity on $\mathbb{H}'_{jP}$.

III. THE MAIN RESULT

We wish to show that for fixed δ, there exists a private quantum communication scheme for $\mathcal{E}$ that scales as $3\log_2 N$. This is achieved by encoding into particular subspaces of the working space $\mathbb{H}'$. Suppose that a subspace $S\subset\mathbb{H}'$ of the appropriate dimensionality is drawn at random from some ensemble of subspaces of $\mathbb{H}'$. It is then sufficient to show that the probability that encoding in S is not δ private is strictly less than 1, because this implies that there exist subspaces in the ensemble that do yield δ-private schemes. Any such subspace can then constitute the logical Hilbert space $\mathbb{H}_L$ for such a scheme. In this case, the encoding map $\mathcal{C}$ is simply the embedding map which takes states in $S\subset(\mathbb{C}^2)^{\otimes N}$ to states in $(\mathbb{C}^2)^{\otimes N}$. Consequently, we leave the encoding map $\mathcal{C}$ implicit in the rest of the paper.

We shall consider the ensemble of subspaces that is generated by drawing uniformly at random from among all subspaces of $\mathbb{H}'$ of a given dimension. More precisely, we shall take $S=US_0$, where S_0 is a fixed subspace of $\mathbb{H}'$ and U is a unitary on $\mathbb{H}'$ chosen according to the Haar measure dU. The condition that we require S to satisfy in order to yield a δ-private scheme is that for all $|\varphi\rangle\in S$, $\|\mathcal{E}(\varphi)-\rho_0\|_1\leqslant\delta$ for ρ_0 given by Eq. (15), so that from Eve's perspective all the encoded states φ are nearly indistinguishable. This condition is equivalent to demanding that

$$\max_{|\varphi\rangle\in S}\|\mathcal{E}(\varphi)-\rho_0\|_1 \leqslant \delta, \quad (16)$$

where the maximization is over all pure states in S. The probability that S fails to be δ private is, therefore,

$$\Pr_S\left(\max_{|\varphi\rangle\in S}\|\mathcal{E}(\varphi)-\rho_0\|_1>\delta\right), \tag{17}$$

where we define the probability $\Pr_S(g(S)>\delta)$ that a randomly chosen S satisfies some inequality $g(S)>\delta$ by

$$\Pr_S(g(S)>\delta)\equiv\int_{\{U:g(US_0)>\delta\}}dU. \tag{18}$$

For at least one of the S to be δ private, we require that

$$\Pr_S\left(\max_{|\varphi\rangle\in S}\|\mathcal{E}(\varphi)-\rho_0\|_1>\delta\right)<1, \tag{19}$$

for some ρ_0. The following theorem implies that such subspaces S, with dimension scaling in the desired fashion, do exist.

Theorem 1. For the decoherence map $\mathcal{E}$ associated with lacking a reference frame for SU(2), the condition

$$\Pr_S\left(\max_{|\varphi\rangle\in S}\|\mathcal{E}(\varphi)-\rho_0\|_1>\delta\right)<1, \tag{20}$$

holds for sufficiently large N, where the probability is with respect to the unitarily invariant measure on subspaces S of $\mathbb{H}'$, provided

$$\log_2\dim S<3\log_2 N+7/2\log_2\delta+C', \tag{21}$$

where C' is a constant.

Consider, for example, $1/\delta=\mathrm{polylog}(N)$, i.e., a polynomial in $\log(N)$. Then we can find $S\subset\mathbb{H}'$ with $\|\mathcal{E}(\varphi)-\rho_0\|_1\leqslant\delta$ for $|\varphi\rangle\in S$ such that

$$\log_2\dim S\sim 3\log_2 N, \tag{22}$$

recovering the same asymptotic rate as the classical private capacity. In this case, $Q(\mathcal{E},\delta)\sim C(\mathcal{E},0)$.

We prove Theorem 1 via a sequence of lemmas. Our starting point is the following result, known as Levy's Lemma [29]:

Lemma 2 (Levy). Let $f:S^k\to\mathbb{R}$ be a continuous real-valued function on the k sphere with Lipschitz constant η with respect to the Euclidean metric. Then, if x is selected at random from S^k according to the uniform measure,

$$\Pr_x\big(|f(x)-M|>\gamma\big)<\exp_2\big(-C(k-1)\gamma^2/\eta^2\big), \tag{23}$$

where $C>0$ is a constant and M is a median for f.

The function of interest is

$$f(\varphi)\equiv\|\mathcal{E}(\varphi)-\rho_0\|_1. \tag{24}$$

Note that the Hilbert space norm on $\mathbb{H}'$ is precisely the Euclidean norm if the Hilbert space is considered as the real vector space $\mathbb{R}^{2K}$. The following lemma bounds the Lipschitz constant of this function.

Lemma 3 (Lipschitz constant). The Lipschitz constant of $f(\varphi)$ is bounded above by 2.

Proof. Using the triangle inequality gives

$$|f(\varphi)-f(\tilde{\varphi})|=\big|\|\mathcal{E}(\varphi)-\rho_0\|_1-\|\mathcal{E}(\tilde{\varphi})-\rho_0\|_1\big|\leqslant\|\mathcal{E}(\varphi)-\mathcal{E}(\tilde{\varphi})\|_1. \tag{25}$$

Because $\mathcal{E}$ is a completely positive trace-preserving map, and the trace distance is nonincreasing under such maps,

$$\|\mathcal{E}(\varphi)-\mathcal{E}(\tilde{\varphi})\|_1\leqslant\|\varphi-\tilde{\varphi}\|_1. \tag{26}$$

Combining these inequalities with the fact that

$$\||\varphi\rangle-|\tilde{\varphi}\rangle\|_2^2=2-2\,\mathrm{Re}\langle\varphi|\tilde{\varphi}\rangle \tag{27}$$

$$\geqslant 1-|\langle\varphi|\tilde{\varphi}\rangle^2 \tag{28}$$

$$=\left(\frac{1}{2}\|\varphi-\tilde{\varphi}\|_1\right)^2, \tag{29}$$

we obtain

$$|f(\varphi)-f(\tilde{\varphi})|\leqslant 2\||\varphi\rangle-|\tilde{\varphi}\rangle\|_2, \tag{30}$$

which is the desired bound on the Lipschitz constant. ■

The next corollary, an immediate consequence of Levy's Lemma, bounds the probability that Eve can distinguish a random state on $\mathbb{H}'$ from ρ_0 substantially better than she can distinguish states on average.

Corollary 4 (Concentration of f). Let $|\varphi\rangle$ be chosen at random from the uniform measure on the unit sphere in $\mathbb{H}'$ and M a median for f. Then

$$\Pr_\varphi(|f(\varphi)-M|>\gamma)\leqslant\exp_2\left(\frac{-C(K-1)\gamma^2}{2}\right). \tag{31}$$

Proof. Apply Levy to the function $f(\varphi)$ of Eq. (24). In this case, $k=2K-1$ and $\eta\leqslant 2$. ■

Next, we relate the median of f to its mean, which is easier to estimate. Write

$$\mathbb{E}_\varphi f\equiv\int f(\varphi)d\nu(\varphi) \tag{32}$$

for the expectation of f with respect to the unitarily invariant measure $d\nu(\varphi)$ on pure states in $\mathbb{H}'$. Let $A_{\geqslant}\subset\mathbb{H}'$ be the set of points $|\varphi\rangle$ on the unit sphere for which $f(\varphi)\geqslant M$. By the definition of the median,

$$\int_{A_{\geqslant}}f(\varphi)d\nu(\varphi)\geqslant M\int_{A_{\geqslant}}d\nu(\varphi)=M\times\frac{1}{2}. \tag{33}$$

Letting $A_<$ be defined analogously, we get

$$\mathbb{E}_\varphi f=\int_{A_<}f(\varphi)d\nu(\varphi)+\int_{A_{\geqslant}}f(\varphi)d\nu(\varphi)\geqslant\frac{M}{2}, \tag{34}$$

because $f(\varphi)\geqslant 0$.

Lemma 5 (Expectation of f). The expectation value of $f(\varphi)$ satisfies

$$\mathbb{E}_\varphi f\leqslant\frac{1}{\sqrt{\alpha}}. \tag{35}$$

The proof is supplied in Appendix II, but can be understood intuitively in terms of the action of $\mathcal{E}$ on $\mathbb{H}'$. If the subspaces $\mathbb{H}'_{jP}$ were one-dimensional, then by virtue of the fact that the $\mathbb{H}_{jR}$ are decoherence full, we would have complete decoherence on $\mathbb{H}_{jR}\otimes\mathbb{H}'_{jP}$. Because $1/\alpha\sim\dim\mathbb{H}'_{jP}/\dim\mathbb{H}'_{jR}$, the larger the value of α, the smaller the dimension of $\mathbb{H}'_{jR}$ relative to $\mathbb{H}'_{jR}$, and the less distinguishable on average are states on $\mathbb{H}_{jR}\otimes\mathbb{H}'_{jR}$ subsequent to the action of $\mathcal{E}$. One might expect that states could be distinguished by their relative supports on the different irreps $j\in Y$, because these supports are invariant under the action of $\mathcal{E}$. However, the proof demonstrates that because we use only sufficiently large irreps, all encoded states will have similar supports on all irreps and, thus, not be significantly more distinguishable than if a single irrep had been used.

We note that the proof of the lemma requires that, within each irrep $j\in Y$, the dimension D_α of $\mathbb{H}'_{jP}$ be much smaller than the dimension D of the decoherence-full subsystem $\mathbb{H}_{jR}$. For this reason, our result does not apply directly to cryptography using a U(1) phase reference, for which the decoherence-full subsystems are all one-dimensional. However, for any other reference frame that satisfies this condition, our results should be directly applicable.

We conclude that the median M is upper bounded by $2/\sqrt{\alpha}$ which, using Corollary 1, leads to the result

$$\Pr_{\varphi}\left(\|\mathcal{E}(\varphi)-\rho_0\|_1>\gamma+\frac{2}{\sqrt{\alpha}}\right)\leqslant \exp_2\left(-\frac{C}{2}(K-1)\gamma^2\right). \tag{36}$$

This inequality is sufficiently strong that we will be able to use it to conclude that large subspaces of $\mathbb{H}'$ have the property that the distinguishability of *all* states in the subspace are bounded.

Lemma 6 (Existence of good subspaces). Let $S_0\subset\mathbb{H}'$ be a fixed subspace and $|\varphi_0\rangle$ a fixed state on S_0. Let $S=US_0$ be a random subspace obtained from S_0 using a Haar-distributed unitary U on $\mathbb{H}'$. Then, for any $\delta>0$ and $0<\varepsilon<1/2$,

$$\Pr_S(\max_{|\varphi\rangle\in S} f(\varphi)>\delta)\leqslant\left(\frac{5}{\varepsilon}\right)^{2\dim S}\Pr_U(f(U|\varphi_0\rangle)>\delta-\varepsilon). \tag{37}$$

Proof. Fix an $\epsilon/2$-net $\mathcal{N}_0$ for the unit sphere of a fixed subspace S_0 of $\mathbb{H}'$ with the Hilbert space norm. The net can be chosen such that the number of elements in the net satisfies $|\mathcal{N}_0|\leqslant(5/\epsilon)^{2\dim S_0}$. (See Ref. [25] for a proof of this fact.) By definition, given any $|\varphi\rangle\in S_0$, there exists a state $|\tilde{\varphi}\rangle\in\mathcal{N}_0$ such that $\||\varphi\rangle-|\tilde{\varphi}\rangle\|_2\leqslant\epsilon/2$. By Lemma 2, this implies that $|f(\varphi)-f(\tilde{\varphi})|\leqslant\epsilon$.

Now choose a random subspace $S=US_0$ using a Haar-distributed unitary. This unitary U maps the net $\mathcal{N}_0$ for S_0 into a net $\mathcal{N}$ for S. Let $|\varphi^*\rangle$ be defined by

$$f(\varphi^*)=\max_{|\varphi\rangle\in S} f(\varphi). \tag{38}$$

By definition, there exists a state $|\tilde{\varphi}^*\rangle\in\mathcal{N}$ such that $\||\varphi^*\rangle-|\tilde{\varphi}^*\rangle\|_2\leqslant\epsilon/2$ and, consequently, $|f(\varphi^*)-f(\tilde{\varphi}^*)|\leqslant\epsilon$. It follows that if $f(\varphi^*)>\delta$, then $f(\tilde{\varphi}^*)>\delta-\epsilon$. Therefore, if

$$\max_{|\varphi\rangle\in S} f(\varphi)>\delta,\quad \text{then}\ \max_{|\tilde{\varphi}\rangle\in\mathcal{N}} f(\tilde{\varphi})>\delta-\epsilon. \tag{39}$$

Finally, if x implies y, then $\Pr(x)\leqslant\Pr(y)$, so we conclude that

$$\Pr_S\left(\max_{|\varphi\rangle\in S} f(\varphi)>\delta\right)\leqslant\Pr_U\left(\max_{|\tilde{\varphi}\rangle\in\mathcal{N}_0} f(U|\tilde{\varphi}\rangle)>\delta-\epsilon\right), \tag{40}$$

where $\Pr_U$ reminds the reader that we are varying over unitaries. We then have

$$\begin{aligned}\Pr_U\left(\max_{|\tilde{\varphi}\rangle\in\mathcal{N}_0} f(U|\tilde{\varphi}\rangle)>\delta-\epsilon\right)&\leqslant\sum_{|\tilde{\varphi}\rangle\in\mathcal{N}_0}\Pr_U\left(f(U|\tilde{\varphi}\rangle)>\delta-\epsilon\right)\\&=|\mathcal{N}_0|\Pr_U\left(f(U|\tilde{\varphi}_0\rangle)>\delta-\epsilon\right),\end{aligned} \tag{41}$$

where the first inequality is the union bound for probabilities and the second line follows from the fact that the expression inside the sum over $|\tilde{\varphi}\rangle$ is independent of $|\tilde{\varphi}\rangle$ ($|\tilde{\varphi}_0\rangle$ is an arbitrary state in $\mathbb{H}'$). Recalling that $|\mathcal{N}_0|\leqslant(5/\epsilon)^{2\dim S_0}$ establishes what we set out to prove. ■

Using this lemma together with Eq. (36), we obtain

$$\begin{aligned}&\Pr_S\left(\max_{|\varphi\rangle\in S}\|\mathcal{E}(\varphi)-\rho_0\|_1>\delta\right)\\&\quad\leqslant\left(\frac{5}{\varepsilon}\right)^{2\dim S}\exp_2\left[-\frac{C}{2}(K-1)\left(\delta-\varepsilon-\frac{2}{\sqrt{\alpha}}\right)^2\right].\end{aligned} \tag{42}$$

If $\dim S$ is chosen such that the right-hand side is bounded away from 1, then the left-hand side will also be bounded away from 1, and there will exist a δ-private encoding into a subspace S. We will, therefore, seek the largest value of $\dim S$ that satisfies the inequality

$$\left(\frac{5}{\varepsilon}\right)^{2\dim S}<\exp_2\left[\frac{C}{2}(K-1)\left(\delta-\varepsilon-\frac{2}{\sqrt{\alpha}}\right)^2\right], \tag{43}$$

or equivalently

$$\dim S<\frac{\ln 2}{\ln\left(\frac{5}{\varepsilon}\right)}\frac{C}{4}(K-1)\left(\delta-\varepsilon-\frac{2}{\sqrt{\alpha}}\right)^2. \tag{44}$$

Given that $\ln x\leqslant\sqrt{x}$, we have $1/\ln(\frac{5}{\varepsilon})\geqslant 1/\sqrt{\frac{5}{\varepsilon}}$ and any S satisfying

$$\dim S<\sqrt{\frac{\varepsilon}{5}}\frac{C\ln 2}{4}(K-1)\left(\delta-\varepsilon-\frac{2}{\sqrt{\alpha}}\right)^2, \tag{45}$$

will also satisfy Eq. (44). Using the expression for K in Eq. (13), it is sufficient to require that

$$\dim S<\frac{C\ln 2}{54\sqrt{5}}\frac{1}{\alpha}N^3\left(\delta-\varepsilon-\frac{2}{\sqrt{\alpha}}\right)^2\sqrt{\varepsilon} \tag{46}$$

for sufficiently large N. If we choose $\varepsilon=\delta/3$ and $\alpha=36/\delta^2$, then this expression reduces to

$$\dim S<\frac{C\ln 2}{5832\sqrt{15}}N^3\delta^{7/2}. \tag{47}$$

It is, therefore, possible to choose S such that $f(\varphi)\leqslant\delta$ for all $|\varphi\rangle\in S$, whenever

$$\log_2 \dim S < 3 \log_2 N + 7/2 \log_2 \delta + C', \tag{48}$$

where $C' = \log_2[(C \ln 2)/(5832\sqrt{15})]$, completing the proof of Theorem 1.

IV. DISCUSSION

We have seen that for fixed $\delta > 0$, the δ-private quantum capacity of a secret SU(2) reference frame is at least three times as large as its perfectly private quantum capacity. Indeed, the relaxation of the security requirement to $\delta > 0$ causes the private quantum capacity to jump almost to the value of the perfectly private classical capacity, which is approximately $3 \log_2 N$, and within a factor of $1+\delta$ of the δ-private classical capacity. In earlier work, a similar relaxation of the security condition in the quantum one time pad led to a doubling of the private quantum capacity of a shared secret key string [22] as well as a similar doubling of the capacity of a maximally entangled state [24,25]. The tripling of the capacity seen here, however, is unusual and reflects the particular structure of the tensor power representation of SU(2).

Because the private capacity of a shared reference frame is proportional to $\log_2 N$ rather than N, however, the values of δ that provide an improvement over the perfectly private schemes are quite restricted. From Theorem 1, we see that for sufficiently large N,

$$Q(\mathcal{E}, \delta) \geq 3 \log_2 N + \frac{7}{2} \log_2 \delta + C' \tag{49}$$

for some constant C'. In order to improve upon the perfectly private scheme, we require that $Q(\mathcal{E}, \delta) > \log_2 N$, which implies that $1/\delta \in O(N^{4/7})$. In particular, our construction does not allow δ to be an exponentially decreasing function of N, which would obviously be more desirable for cryptographic applications.

Some questions remain about the optimality of the private quantum communication schemes we have presented here. In particular, our upper bounds on the private quantum capacity do not exclude the possibility that δ could be made to shrink exponentially with N while maintaining a number of qubits sent scaling as $3 \log_2 N$. Also, we have not attempted to construct δ-private classical communication schemes meeting the upper bound of Theorem 7 in Appendix I.

Finally, we note that a shared Cartesian frame is not the only possible form of a shared reference [18], and it is useful to consider other practical examples such as a shared phase reference, shared direction, or reference ordering. These examples have different Hilbert space structures arising from their group representation theory, and in general will result in different relations between their private classical and quantum capacities. We note that our technique should apply directly to cryptography using a reference frame for $U(K)$, with $K \geq 2$, because the Hilbert space structures for these groups satisfy the conditions required for our proof. Whether similar differences between perfectly private and δ-private capacities can be found for other reference frames is an open question.

ACKNOWLEDGMENTS

The authors gratefully acknowledge J. Emerson, D. Gottesman, and T. Rudolph for helpful discussions. S.D.B. acknowledges support from the Australian Research Council, P.H. appreciates the support of the Canadian Institute for Advanced Research, and both P.H. and R.W.S. are grateful for support from the Natural Science and Engineering Research Council of Canada.

APPENDIX A: δ-PRIVATE CLASSICAL CAPACITY

Theorem 2. For $\delta \leq 1/2$, the δ-private classical capacity satisfies $C(\mathcal{E}, \delta) \leq 3(1+\delta) \log_2 N + 3$.

Proof. Suppose we have a δ-private classical communication scheme for $\mathcal{E}$ consisting of m states on $\mathbb{H}$. If such a scheme exists, then there is also a m-state scheme using pure states, which we will label $\{|\psi_i\rangle\}_{i=1}^m$. We will use the privacy condition to find a small subspace of $\mathbb{H}$ such that these states are almost entirely contained within the subspace. Combining the Holevo bound with the fact that the original states were all distinguishable will then lead to an upper bound on m, the number of states in the scheme.

Let $\mathbb{H}_{jQ}$ be the subspace of $\mathbb{H}_{jP}$ corresponding to the nonzero eigenvalues of $\mathrm{Tr}_{jR}[\Pi_j \psi_1 \Pi_j]$ and let Π_{jQ} be the projector onto $\mathbb{H}_{jQ}$. It follows from the Schmidt decomposition for $\Pi_j|\psi_1\rangle$ that $\dim \mathbb{H}_{jQ} \leq \min(d_{jR}, d_{jP})$. Also let $\Pi' = \Sigma_j \Pi_{jR} \otimes \Pi_{jQ}$, where Π_{jR} is the projector onto $\mathbb{H}_{jR}$. Observe that for any ψ_i,

$$\mathrm{Tr}[\Pi' \psi_i \Pi'] = \mathrm{Tr}[\mathcal{E}(\Pi' \psi_i \Pi')] = \mathrm{Tr}[\Pi' \mathcal{E}(\psi_i) \Pi'], \tag{A1}$$

because $\mathcal{E}$ is trace preserving and because projection by Π' commutes with $\mathcal{E}$. By the privacy condition, however,

$$\delta \geq \|\mathcal{E}(\psi_1) - \mathcal{E}(\psi_i)\|_1 \tag{A2}$$

$$\geq 2\{\mathrm{Tr}[\Pi' \mathcal{E}(\psi_1) \Pi'] - \mathrm{Tr}[\Pi' \mathcal{E}(\psi_i) \Pi']\} \tag{A3}$$

$$= 2\{1 - \mathrm{Tr}[\Pi' \mathcal{E}(\psi_i) \Pi']\}. \tag{A4}$$

The second inequality holds because $\|X\|_1 = 2 \max_P \mathrm{Tr}[PX]$ for traceless, Hermitian X, where the optimization is over projectors of all ranks. (See, for example, Ref. [1].) Combining (A4) with (A1) shows that $\mathrm{Tr}[\Pi' \psi_i \Pi'] \geq 1 - \delta/2$. Thus the states $\{|\psi_i\rangle\}_{i=1}^m$ are essentially contained within the subspace defined by Π'.

Now consider the set of states $\{|\psi_i'\rangle\}_{i=1}^m$, where

$$|\psi_i'\rangle = \frac{\Pi'|\psi_i\rangle}{\sqrt{\mathrm{Tr}[\Pi' \psi_i \Pi']}}. \tag{A5}$$

Because $|\langle\psi_i|\psi_i'\rangle|^2=\mathrm{Tr}[\Pi'\psi_i\Pi']$, performing the measurement $\{|\psi_j\rangle\langle\psi_j|\}_{j=1}^m$ on the set of states $\{|\psi_i'\rangle\}_{i=1}^m$ will correctly identify the state with probability at least $1-\delta/2$. Assume a state $|\psi_i'\rangle$ is chosen from the uniform distribution. By Fano's inequality [30],

$$H(i|j) \leqslant 1 + \frac{\delta}{2}\log_2 m, \tag{A6}$$

where H is the Shannon conditional entropy function, which in turn implies that

$$I(i;j) \geqslant (1-\delta/2)\log_2 m - 1, \tag{A7}$$

where I is the mutual information function. Because all the states $|\psi_i'\rangle$ are contained in the support of Π', however, the Holevo bound [31] implies that $I(i;j)$ is no more than the logarithm of rank Π', which satisfies

$$\mathrm{rank}\,\Pi' \leqslant \sum_j d_{jR}\min(d_{jR},d_{jP}). \tag{A8}$$

In the case of a private shared SU(2) reference frame, for which $d_{jR}=2j+1$,

$$\mathrm{rank}\,\Pi' \leqslant (N/2+1)(N+1)^2 \leqslant 2N^3, \tag{A9}$$

where the second inequality holds for all $N\geqslant 2$. This implies that

$$\log_2 m \leqslant \frac{3\log_2 N + 2}{1-\delta/2} \tag{A10}$$

$$\leqslant 3(1+\delta)\log_2 N + 3, \tag{A11}$$

provided $\delta\leqslant 1/2$.

APPENDIX B: PROOF OF LEMMA 3

The map $\mathcal{E}$ depolarizes each of the systems $\mathbb{H}_{jR}$ but for the purposes of calculation, it is easier to simply discard them. In the proof, therefore, we will work with the space $\mathbb{H}'_P=\oplus_{j\in Y}\mathbb{H}'_{jP}$, which has dimension $d_P\equiv\dim\mathbb{H}'_P$. Observe that if we introduce

$$\mathcal{F}(\rho) = \sum_{j\in Y}\mathrm{Tr}_{jR}(\Pi_j\rho\Pi_j), \tag{B1}$$

which gives a normalized state on $\mathbb{H}'_P$, then

$$\|\mathcal{E}(\varphi)-\rho_0\|_1 = \|\mathcal{F}(\varphi)-\varrho_0\|_1, \tag{B2}$$

where $\varrho_0=I_P/d_P$ is the normalized identity operator on $\mathbb{H}'_P$.

Using $\|X\|_1\leqslant\sqrt{\mathrm{rank}\,X}\|X\|_2$ gives

$$\|\mathcal{F}(\varphi)-\varrho_0\|_1 \leqslant \sqrt{d_P}\|\mathcal{F}(\varphi)-\varrho_0\|_2. \tag{B3}$$

Therefore, we have

$$\begin{aligned}\mathbb{E}_\varphi f &\leqslant \sqrt{d_P}\int \|\mathcal{F}(\varphi)-\varrho_0\|_2 d\nu(\varphi)\\ &= \sqrt{d_P}\int \sqrt{\mathrm{Tr}[\mathcal{F}(\varphi)^2-\mathcal{F}(\varphi)/d_P+I_P/d_P^2]}d\nu(\varphi).\end{aligned} \tag{B4}$$

Using the normalization $\mathrm{Tr}\,\mathcal{F}(\varphi)=1$ and the concavity of the square root function, this expression reduces to

$$\mathbb{E}_\varphi f \leqslant \sqrt{\int d_P\,\mathrm{Tr}[\mathcal{F}(\varphi)^2]d\nu(\varphi) - 1}. \tag{B5}$$

Therefore, it suffices to evaluate

$$\int \mathrm{Tr}[\mathcal{F}(\varphi)^2]d\nu(\varphi) = \int \mathrm{Tr}\Big[\Big(\sum_{j\in Y}\mathrm{Tr}_{jR}(\Pi_j\varphi\Pi_j)\Big)^2\Big]d\nu(\varphi). \tag{B6}$$

Because Π_j has the form $\Pi_j=\Pi_{jR}\otimes\Pi_{jP}$, where Π_{jR} and Π_{jP} are the projectors onto $\mathbb{H}_{jR}$ and $\mathbb{H}_{jP}$, respectively, $\mathrm{Tr}_{jR}(\Pi_j\varphi\Pi_j)$ and $\mathrm{Tr}_{kR}(\Pi_k\varphi\Pi_k)$ have orthogonal supports, implying that

$$\mathrm{Tr}\left[\left(\sum_{j\in Y}\mathrm{Tr}_{jR}(\Pi_j\varphi\Pi_j)\right)^2\right] = \mathrm{Tr}\left[\sum_{j\in Y}(\mathrm{Tr}_{jR}(\Pi_j\varphi\Pi_j))^2\right]. \tag{B7}$$

To evaluate the resulting integral, fix bases $\{|m\rangle\}_{m=1}^D$ and $\{|l\rangle\}_{l=1}^{D_\alpha}$ for the spaces $\mathbb{H}'_{jR}$ and $\mathbb{H}'_{jP}$, respectively. (Note that we identify bases labeled by different values of j.) Also let $|\varphi_0\rangle=|j_0m_0l_0\rangle$ for some fixed values of j_0,m_0, and l_0. Using Eq. (B7) and making use of the invariance of the measure, we can expand the integral of Eq. (B6) as

$$\begin{aligned}&\int_{\mathrm{U}(K)}\mathrm{Tr}[\mathcal{F}(U\varphi_0U^\dagger)^2]dU\\ &\quad=\sum_{j\in Y}\sum_{m,m'=1}^{D}\sum_{l,l'=1}^{D_\alpha}\int_{\mathrm{U}(K)}U_{jml,j_0m_0l_0}U^*_{jml',j_0m_0l_0}\\ &\qquad\times U_{jm'l',j_0m_0l_0}U^*_{jm'l,j_0m_0l_0}dU,\end{aligned} \tag{B8}$$

which can be evaluated using the identity (see, for example, Ref. [32])

$$\begin{aligned}\int_{\mathrm{U}(K)}U_{ij}U^*_{kl}U_{mn}U^*_{pq}dU = \frac{1}{K^2-1}\Big\{&\delta_{ij,kl}\delta_{mn,pq}+\delta_{ij,pq}\delta_{kl,mn}\\ &-\frac{1}{K}\delta_{ik}\delta_{jq}\delta_{ln}\delta_{mp}-\frac{1}{K}\delta_{ip}\delta_{jl}\delta_{km}\delta_{nq}\Big\}.\end{aligned} \tag{B9}$$

We obtain

$$\begin{aligned}&\int_{\mathrm{U}(K)}\mathrm{Tr}[\mathcal{F}(U\varphi_0U^\dagger)^2]dU\\ &\quad=\sum_{j\in Y}\sum_{m,m'=1}^{D}\sum_{l,l'=1}^{D_\alpha}\frac{1}{K(K+1)}\{\delta_{l,l'}+\delta_{m,m'}\}\end{aligned} \tag{B10}$$

$$=\frac{\sum_{j\in Y}(D^2D_\alpha+D_\alpha^2D)}{K(K+1)}. \tag{B11}$$

Substituting this back into the expression for $\mathbb{E}_\varphi f$ yields

$$\mathbb{E}_\varphi f \leqslant \sqrt{\frac{d_P}{K(K+1)}\left(\sum_{j \in Y} (D^2 D_\alpha + D_\alpha^2 D)\right) - 1}. \quad \text{(B12)}$$

Recalling that $d_P = \Sigma_{j \in Y} D_\alpha$ and $K = \Sigma_{j \in Y} D_\alpha D$, we get $\mathbb{E}_\varphi f \leqslant \sqrt{D_\alpha / D}$. Because $D_\alpha \leqslant \frac{1}{\alpha} D$, we have the desired inequality

$$\mathbb{E}_\varphi f \leqslant \sqrt{\frac{1}{\alpha}}. \quad \text{(B13)}$$

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).
[3] A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001).
[4] E. Bagan, M. Baig, A. Brey, R. Muñoz-Tapia, and R. Tarrach, Phys. Rev. A **63**, 052309 (2001).
[5] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001).
[6] E. Bagan, M. Baig, and R. Muñoz-Tapia, Phys. Rev. Lett. **87**, 257903 (2001).
[7] N. H. Lindner, A. Peres, and D. R. Terno, Phys. Rev. A **68**, 042308 (2003).
[8] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. Lett. **93**, 180503 (2004).
[9] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).
[10] S. J. van Enk, Phys. Rev. A **71**, 032339 (2005).
[11] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
[12] J-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[13] F. Verstraete and J. I. Cirac, Phys. Rev. Lett. **91**, 010404 (2003).
[14] S. D. Bartlett and H. M. Wiseman, Phys. Rev. Lett. **91**, 097903 (2003).
[15] S. D. Bartlett, A. C. Doherty, R. W. Spekkens, and H. M. Wiseman, quant-ph/0412158 (unpublished).
[16] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).
[17] A. Harrow, R. Oliveira, and B. Terhal, quant-ph/0506133 (unpublished).
[18] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. A **70**, 032307 (2004).
[19] W. Fulton and J. Harris, *Representation Theory: A First Course* (Springer-Verlag, Berlin, 1991).
[20] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[21] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proc. 41st Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 2000), p. 547.
[22] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**(2), 371 (2004).
[23] D. Leung, Quantum Inf. Comput. **2**(1), 14 (2002).
[24] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).
[25] P. Hayden, D. W. Leung, and A. Winter, quant-ph/0407049 (unpublished).
[26] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[27] C. A. Fuchs, Fortschr. Phys. **46**(4,5), 535 (1998).
[28] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[29] V. D. Milman and G. Schechtman, *Asymptotic Theory of Finite Dimensional Normed Spaces* (Springer-Verlag, Berlin, 1986).
[30] T. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[31] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).
[32] S. Aubert and C. S. Lam, J. Math. Phys. **44**, 6112 (2003).