Physical underpinnings of privacy

Joseph M. Renes[1] and Jean-Christian Boileau[2]
[1]*Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a, 64289 Darmstadt, Germany*
[2]*Center for Quantum Information and Quantum Control, University of Toronto, Toronto, ON, Canada M5S 1A7*
(Received 20 February 2007; revised manuscript received 24 March 2008; published 29 September 2008)

One of the remarkable features of quantum mechanics is the ability to ensure secrecy. Private states embody this effect, as they are precisely those multipartite quantum states from which two parties can produce a shared secret that cannot under any circumstances be correlated with an external system. Naturally, these play an important role in quantum key distribution (QKD) and quantum information theory. However, a general distillation method has heretofore been missing. Inspired by Koashi's complementary control scenario [M. Koashi, e-print arXiv:0704.3661 (2007)], we give a new definition of private states in terms of one party's potential knowledge of two complementary measurements made on the other and use this to construct a general method of private state distillation using quantum error-correcting codes. The procedure achieves the same key rate as recent, more information-theoretic approaches while demonstrating the physical principles underlying privacy of the key. Additionally, the same approach can be used to establish the hashing inequality for entanglement distillation, as well as the direct quantum coding theorem.

DOI: 10.1103/PhysRevA.78.032335 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ud

I. INTRODUCTION

Appeal to physical concepts such as the uncertainty principle and entanglement formed the basis of the original security proofs of quantum key distribution (QKD). An uncertainty relation between complementarity observables inspired the first, Mayers's security proof of the BB84 protocol [1]. Later, building on arguments from Lo and Chau [2], Shor and Preskill [3] showed how BB84 could be understood as a virtual entanglement distillation protocol, thereby using the monogamy of entanglement to ensure the privacy of the key. This method subsequently found wide application not only to specific [4–7] and generic [8] ideal protocols, but also to protocols including a description of realistic devices [9]. Recently, Koashi combined the two methods [10] and formulated a simple security proof for BB84 with uncharacterized detectors [11].

A somewhat different, more information-theoretic approach adapts classical schemes of extracting secret bits from partially private data to the case in which the eavesdropper holds quantum information. If X, Y, and Z are classical random variables held by two honest parties Alice and Bob, along with an eavesdropping third party, Eve, then a result by Csiszár and Körner states that by one way communication from Alice to Bob the honest parties can extract a key at a rate of $I(X:Y)-I(X:Z)$ bits from asymptotically many such random variables [12]. Devetak and Winter showed how to distill secret keys from tripartite quantum states at the quantum version of this rate, obtained by replacing Bob's and Eve's classical random variables with quantum states [13]. Building on a result by Renner and König [14], Kraus, Gisin, and Renner established the security of generic QKD protocols operating at this rate using arbitrary universal hash functions [15–17].

The essential difference between the two approaches lies in the basis of privacy and the treatment of the eavesdropper. In the latter, privacy is established directly. Alice and Bob employ privacy amplification to eliminate any information Eve may have about their prospective *classical* key, even if she holds quantum information. This general approach works in any kind of cryptographic setting, classical, quantum, or otherwise, provided Alice and Bob have some estimate of Eve's information. In the quantum setting, this estimate can be obtained by assuming Eve holds the purification of the quantum state held by Alice and Bob; that this limits her information is the reason QKD is possible from this point of view.

In the former approach, the honest parties no longer concern themselves with the details of the eavesdropper, but instead concentrate on creating a *quantum* state that can produce a secret key when appropriately measured. For example, maximal entanglement will ensure privacy of a key generated in any basis by the monogamy property mentioned above. Entanglement is sufficient for this purpose, but unnecessary; the broader class of states suitable for creating keys are termed *private states* [18]. These are closely related to maximally entangled states, but may also include additional systems, collectively called the *shield*. The shield does not contribute directly to the key, but, as the name suggests, serves to block its correlations from would-be eavesdroppers. From this perspective, the success of QKD hinges on the existence of quantum correlations, which implies that the results of certain measurements are completely secret.

Each approach has its advantages. The physical picture is perhaps more intuitive, tracing the origins of privacy to physical concepts such as entanglement, complementarity, and the uncertainty principle. On the other hand, the information-theoretic approach has led to more general proofs with higher lower bounds and lower upper bounds on the secret key rate [13,15–17].

These results, specifically rates of secret key distillation, have also been used to derive some of the central results of quantum information theory, namely the hashing inequality on the asymptotic rate of entanglement distillation and the direct quantum coding theorem for the quantum channel capacity. In principle, it should be possible to arrive at the same results in the physical picture, as every key distillation pro-

tocol in principle leads to a private state distillation protocol by performing the operations coherently [19]. Put differently, the results from the information-theoretic viewpoint can be used to construct such distillation protocols, but these have not yet been fully understood from the more physical point of view.

We provide the missing piece of the puzzle in this paper by formulating a new characterization of private states based on the uncertainty principle and using this to construct a protocol using Calderbank-Shor-Steane (CSS) codes [20,21], which distills private states at the quantum Csiszár-Körner rate. The essential idea is that if and only if measurements on Alice's key system in either one of two conjugate bases can be perfectly predicted by the other systems available to the honest parties, the joint state is a private state and Eve can have no correlation with the key. In particular, Bob's key system should be perfectly correlated with Alice's, while the shield may be used to predict her conjugate observable.

Here, privacy of the key rests on quantum-mechanical complementarity, since the fact that either of the conjugate observables could be predicted by the honest parties means that Eve has no correlation with either. This echoes the recent result by Koashi showing that secret key distillation is equivalent to a protocol involving complementary measurements he termed complementary control [22], and indeed our work is inspired by these results.

By explicitly including Bob and the shield into the analysis, the means of private state distillation become clear: Alice merely needs to reveal some information about her key system such that the other systems could in principle predict both measurements. We shall demonstrate how the syndromes of a CSS code are ideally suited for this purpose, and that the resulting distillation protocol essentially amounts to applying a slightly modified Holevo-Schumacher-Westmoreland (HSW) theorem [23,24] twice. Constructing a distillation procedure in this manner, one focused on the shared quantum correlations, generalizes the quantum privacy amplification method of Deutsch *et al.* [25] ad recalls the connection between quantum privacy and quantum coherence discovered by Schumacher and Westmoreland[26].

This approach also gives a new proof of the hashing inequality, which states that the rate of one-way entanglement distillation using many copies of the state ρ_{AB} is lower bounded by the coherent information $I_c(A\rangle B)=S(B)-S(AB)$ (the same lower bound applies to the extractable one-way secure key rate). As discussed in [27], this result combined with quantum teleportation provides proof of the direct quantum coding theorem, which gives a lower bound to the quantum channel capacity in terms of the coherent information. The main difference from previous proofs is that we bound Eve's information about the key by the amount of information that Bob can obtain about Alice's conjugate basis measurement, which then leads to an explicit construction of the decoder.

The paper is organized as follows. First we give the characterization of private states in Sec. II, and show how quantitative statements of complementarity such as the entropic uncertainty principle of Maassen and Uffink [28] and a related mutual information tradeoff given by Hall [29] imply privacy of the key. We then extend this to the case of approximate private states in Sec. III, explaining the relation to Koashi's complementary control scenario. Section IV presents our main results, which we divide into two parts. We first prove a one-shot distillation theorem showing how to use the structure of CSS codes for private state distillation, in a form useful as a building block for QKD security proofs. We then give a distillation protocol based on these ideas that achieves the quantum Csiszár-Körner rate. In Sec. V, we use a coherent version of those arguments to prove the hashing inequality. In Sec. VI, we discuss relation to previous work, and we conclude in Sec. VII with a summary and open problems.

II. EXACT PRIVATE STATES

A perfect secret key shared by Alice and Bob is a uniformly distributed random variable about which the eavesdropper Eve has zero information, or more formally, $\kappa^{ABE} := (\frac{1}{d}\sum_{k=0}^{d-1} P_k^A \otimes P_k^B)\otimes \rho^E$ for some ρ^E, where $P_k := |k\rangle\langle k|$ is the projector onto "standard" basis element $|k\rangle$. Note that this choice of basis is arbitrary for each system. Although we use a quantum-mechanical description, note that Alice and Bob's systems are essentially classical; states of this form are sometimes termed *ccq* states to reflect this fact.

Private states, meanwhile, are quantum states for which standard basis measurements by Alice and Bob yield a perfect secret key. When producing a key from an alphabet of d letters, the key registers A and B are d-dimensional quantum systems. Additionally, they may possess some auxiliary "shield" systems that are not directly involved in creating the key. These systems are nevertheless important as they are not held by the eavesdropper and can shield the key correlations from her. Although the shield may have several parts distributed between Alice and Bob, here we lump them together into the system labeled S.

In contrast to the explicit reference to Eve's system in the definition of secret keys, the privacy of a state γ^{ABS} can be determined solely from the systems held by Alice and Bob. The canonical example of such an effect comes from a maximally entangled state, which by virtue of the monogamy of entanglement creates secret keys upon measurement. Though there is no shield in this example, it makes the point that the quantum correlations between Alice and Bob's systems are enough to establish secrecy of the key.

Private states are in fact closely related to maximally entangled states, as shown by [18]. To recapitulate their result, first define a *twisting operator* to be a controlled unitary of the form $U^{ABS} := \Sigma_{jk} P_j^A \otimes P_k^B \otimes V_{jk}^S$ for any arbitrary unitaries V_{jk}^S. Then Theorem 1 of [18] states that γ^{ABS} is a private state iff it is of the form

$$\gamma^{ABS} = U^{ABS}(\Phi_d^{AB} \otimes \xi^S)U^{\dagger ABS}, \tag{1}$$

where ξ^S is an arbitrary state and Φ_d^{AB} is the density operator associated with the canonical entangled state $|\Phi_d^{AB}\rangle := \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|kk\rangle^{AB}$; note that actually only the V_{kk} are relevant. Clearly, measurement of the A and B systems results in a secret key since the same key would result if the state were first untwisted, and Eve cannot distinguish the cases in which the state has been untwisted or not. Conversely, purifying a

secret key and using the fact that Eve's marginal state is fixed along with the fact that purifications of a fixed marginal are related by unitaries on the purifying system, i.e., Uhlmann's theorem [30,31], guarantees the form of Eq. (1).

With the help of the uncertainty principle, we can formulate a different characterization of private states that emphasizes the relation of privacy to complementarity and does not involve statements about Eve's system. Consider a hypothetical measurement by one party, say Alice, on her key qubit in a basis *conjugate* to the standard basis. In this context, "conjugate" refers to any basis whose elements give random outcomes when measured in the standard basis. A general conjugate basis has elements $|\tilde{x}\rangle := \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} e^{i\theta_{xk}}|k\rangle$ for some set of $\theta_{xk} \in \mathbb{R}$ such that $\frac{1}{d}\sum_k e^{i(\theta_{xk}-\theta_{yk})} = \delta_{xy}$.

Due to the conjugate nature of the $|k\rangle$ and $|\tilde{x}\rangle$ bases, complementarity places constraints on the predictability of both measurements. In particular, the entropic uncertainty relation of Maassen and Uffink [28] states that, for an arbitrary state ρ^A,

$$H(Z^A) + H(\tilde{X}^A) \geq \log_2 d, \tag{2}$$

where Z^A and $\tilde{X}^A$ are any nondegenerate observables having eigenstates $|k\rangle^A$ and $|\tilde{x}\rangle^A$, respectively, and H is the Shannon entropy of the outcome probabilities, measured in bits. Hence, if the outcome of Z is certain, then the measurement of $\tilde{X}$ must be random and vice versa.

To determine how much information is *simultaneously* available, we can include the measurement devices themselves in the description, following Hall and Cerf *et al.* [29,32]. Whatever information can be stored in separate devices is clearly simultaneously accessible, so consider a state ρ^{ACD} and POVMs $\tilde{\Lambda}^C$ and Γ^D that are restricted to systems C and D, respectively. Denoting the classical conditional entropy of Z^A given the measurement result Γ^D by $H(Z^A|\Gamma^D)$, we have:

Lemma 1 (Complementary Information Tradeoff). For a tripartite quantum state ρ^{ACD}, conjugate observables Z^A and $\tilde{X}^A$, and arbitrary measurements $\tilde{\Lambda}^C$ and Γ^D,

$$H(Z^A|\Gamma^D) + H(\tilde{X}^A|\tilde{\Lambda}^C) \geq \log_2 d \tag{3}$$

where $d = \dim(A)$.

Proof. Consider arbitrary measurements $\tilde{\Lambda}^C$ and Γ^D. Since these can be performed independently simultaneously, we can define the conditional marginal state $\rho^A_{jk} := \mathrm{Tr}_{CD}[\tilde{\Lambda}^C_j \Gamma^D_k \rho^{ACD}]/p_{jk}$, for $p_{jk} := \mathrm{Tr}[\tilde{\Lambda}^C_j \Gamma^D_k \rho^{ACD}]$. Measurements of Z^A and $\tilde{X}^A$ on each of those states must obey Eq. (2), which in the current context reads $H(Z^A|\Gamma^D=k, \tilde{\Lambda}^C=j) + H(\tilde{X}^A|\Gamma^D=k, \tilde{\Lambda}^C=j) \geq \log_2 d$. Averaging over the measurement outcomes and using the fact that conditioning reduces entropy, we obtain the desired result. ■

Note that no restriction is placed on the ability of a single system to be correlated with two complementary Alice observables, only that the correlations not be simultaneously realized. Such is the case when ρ^{AB} is maximally entangled; in the EPR state, for instance, Bob can predict either the position or momentum of Alice's system, but not both at the same time.

The information exclusion principle bears directly on the question of privacy, as conjugate information can be used to exclude the eavesdropper's information about the key. Define the key to be the outcome of Alice's observable Z^A, let Eve hold D, and suppose that system $C=BS$, i.e., the remainder of the systems under Alice and Bob's control. Then if some measurement $\tilde{\Lambda}^{BS}$ of the BS subsystem can predict the outcome of Alice's conjugate basis observable $\tilde{X}^A$, Eve can have no information about the key: $H(\tilde{X}^A|\tilde{\Lambda}^{BS})=0$ implies $H(Z^A|\Gamma^E)=\log_2 d$. Thus, complementarity assures privacy of the secret key without directly making statements about Eve's system. This line of thought leads to the new characterization of private states:

Theorem 1 (Exact Private States). γ^{ABS} is a private state with (nondegenerate) key observables Z^A and Z^B iff for some measurement $\tilde{\Lambda}^{BS}$

$$\text{(a)} \quad H(Z^A|Z^B) = 0, \tag{4}$$

$$\text{(b)} \quad H(\tilde{X}^A|\tilde{\Lambda}^{BS}) = 0. \tag{5}$$

Proof. Start with the reverse (if) implication and suppose γ^{ABS} satisfies the two conditions. By the above argument, condition (b) implies $H(Z^A|\Gamma^E)=\log_2 d$ and therefore $H(Z^A)=\log_2 d$, whence Eve's marginal states must be independent of the key. As (a) implies the key is perfectly correlated, γ^{ABS} must be a private state.

To prove the forward (only if) implication, we construct the measurement $\tilde{\Lambda}^{BS}$ from the twisting operator $U^{BS} = \sum_k P^B_k \otimes V^S_{kk}$. First, condition (a) follows immediately for γ^{ABS} a private state. The joint probability for the conjugate measurement is given by

$$\begin{aligned} p_{xy} &= \mathrm{Tr}[\gamma^{ABS} \tilde{P}^A_x \otimes \tilde{\Lambda}^{BS}_y] \\ &= \frac{1}{d^2}\sum_{jk} e^{i(\theta_{xk}-\theta_{xj})}\, \mathrm{Tr}[(|j\rangle\langle k|^B \otimes V^S_{jj}\xi^S V^{\dagger S}_{kk})\tilde{\Lambda}^{BS}_y] \\ &= \frac{1}{d^2}\sum_{jk} e^{i(\theta_{xk}-\theta_{xj})}\, \mathrm{Tr}[(|j\rangle\langle k|^B \otimes \xi^S) U^{\dagger BS}\tilde{\Lambda}^{BS}_y U^{BS}] \\ &= \frac{1}{d}\mathrm{Tr}[(\tilde{P}^{*B}_x \otimes \xi^S) U^{\dagger BS}\tilde{\Lambda}^{BS}_y U^{BS}], \end{aligned}$$

where $\tilde{P}^{*B}_y$ is the conjugate of $\tilde{P}^B_y$ in the standard basis. Condition (b) follows by setting $\tilde{\Lambda}^{BS}_y := U^{BS}(\tilde{P}^{*B}_y \otimes \mathbb{1}^S)U^{\dagger BS}$ so that $p_{xy} \propto \delta_{xy}$. ■

From this viewpoint, privacy of the key follows from the ability of one part of the honest players' systems to predict either the key or a complementary observable of the other part; here we focused on Alice's system, but clearly the same result holds for Bob's.

III. APPROXIMATE PRIVATE STATES

Of course, a realistic QKD protocol can never produce a perfect secret key or a perfect private state and instead strives

to create a good approximation. But what is a good approximation? Because the key is meant to be used in arbitrary further cryptographic applications, the definition of approximate must be *composable* so that security statements about a whole cryptographic process can be made by individually examining the constituent parts. In this framework, a sufficient notion of approximate secrecy is furnished by the probability that the actual key could be distinguished from an exact secret key. According to Helstrom's theorem [33], the probability of distinguishing between the two quantum states ρ and σ is bounded by $\frac{1}{2}+\frac{1}{4}\mathrm{Tr}|\rho-\sigma|$. Hence the trace distance $\frac{1}{2}\mathrm{Tr}|\rho-\sigma|$ is the important quantity. This motivates the definition that a shared ϵ-secret key, where ϵ is called the *security parameter*, is any ρ^{ABE} that satisfies $\mathrm{Tr}|\rho^{ABE}-\kappa^{ABE}| \leq 2\epsilon$ for some perfect secret key κ^{ABE} [14,34].

We could analogously define ϵ-private states to be states that are ϵ-close to exact private states in trace distance. These will lead to ϵ-secret keys since the measurement that creates the key is a quantum operation, and the trace distance can only decrease under quantum operations. However, the converse is not true: States not ϵ-close may nevertheless still generate ϵ-secret keys. Hence a better approach is simply to say that ψ^{ABS} is an ϵ-private state when the key measurement leads to an ϵ-secret key, with the eavesdropper system E defined as any purifying system of ψ^{ABS}.

Intuitively, the new characterization of exact private states should be extendible to the approximate case; if Alice's key and conjugate measurements are almost perfectly predictable by the *BS* systems, then the shared state ought to produce a good approximation of a secret key. Defining "almost perfect predictability" in terms of nearly zero conditional entropy, or equivalently nearly maximal mutual information, will not suffice, as this approach is not composable [35]. Instead, the following two theorems show that an alternate definition of approximate private states can be given in terms of concrete measurements having small probabilities of error. The first says that if Bob is able to distinguish Alice's state measured in either one of two conjugated bases, then they share an ϵ-private state, while the second is the converse. Only the first theorem is needed when constructing a security proof, but we provide both for completeness and to highlight the connection between our framework and Koashi's complementarity control scenario [22].

Theorem 2. A state ψ^{ABS} with nondegenerate key observables Z^A and Z^B is an $(\epsilon_z+\sqrt{\epsilon_x})$-private state if there exists a conjugate observable $\tilde{X}^A$ and corresponding measurement $\tilde{\Lambda}^{BS}$ such that

$$p_{\mathrm{e}} = \sum_{j\neq k} \mathrm{Tr}[(P_j^A \otimes P_k^B)\psi^{ABS}] \leq \epsilon_z, \tag{6}$$

$$\tilde{p}_{\mathrm{e}} = \sum_{x\neq y} \mathrm{Tr}[(\tilde{P}_x^A \otimes \tilde{\Lambda}_y^{BS})\psi^{ABS}] \leq \epsilon_x. \tag{7}$$

Theorem 3. If ψ^{ABS} is an ϵ-private state with nondegenerate key observables Z^A and Z^B, then for any conjugate observable $\tilde{X}^A$ there exists a corresponding measurement $\tilde{\Lambda}^{BS}$ such that

$$p_{\mathrm{e}} = \sum_{j\neq k} \mathrm{Tr}[(P_j^A \otimes P_k^B)\psi^{ABS}] \leq \epsilon, \tag{8}$$

$$\tilde{p}_{\mathrm{e}} = \sum_{x\neq y} \mathrm{Tr}[(\tilde{P}_x^A \otimes \tilde{\Lambda}_y^{BS})\psi^{ABS}] \leq 2\epsilon - \epsilon^2. \tag{9}$$

As the proofs are somewhat technical, we defer them to Appendix A.

IV. PRIVATE STATE DISTILLATION

With this characterization of approximate private states, it becomes simple to construct a procedure to distill private states from an arbitrary input. Alice simply needs to reveal enough information about her system so that the states of the *B* and *BS* systems can be reliably distinguished. The amount of information she must reveal depends on the details of the state, and no useful answer can be given in the general case. But when Alice and Bob share asymptotically many copies of an arbitrary state ψ^{ABS}, two applications of the HSW theorem give the distillation rate, which we show equals the quantum Csiszár-Körner rate.

However, this distillation scenario contains the additional subtlety that the information Alice needs to reveal ostensibly comes from noncommuting measurements. Avoiding this problem is where CSS error-correcting codes come into play, as they enable the side information to be properly defined in terms of commuting variables and also define the form of the key system of the distilled state. CSS codes were used by Shor and Preskill [3] in their proof of the BB84 protocol for precisely the same purpose, and the following distillation scheme can be understood as an extension of this method to arbitrary private states. This section contains the main results of this paper, which for clarity are subdivided into two parts: How the CSS codes enable distillation when Alice's state has dimension d^n, and at what rate can private states be distilled from many copies of an arbitrary resource state.

A. One-shot distillation

First we recall a few facts about CSS codes. A CSS code encoding $n-m_z-m_x$ qudits into n is defined by a set of m_z+m_x (commuting) stabilizer operators, m_z operators of the form $Z^{\mathbf{s}}=Z^{s_1}\otimes Z^{s_2}\otimes\cdots\otimes Z^{s_n}$ for $0\leq s_i\leq d-1$, and m_x of the form $X^{\mathbf{t}}=X^{t_1}\otimes X^{t_2}\otimes\cdots\otimes X^{t_n}$ for $0\leq t_i\leq d-1$. We have implicitly used the definition $\mathbf{s}=(s_1,\cdots,s_1)$ and the notation that an operator raised to a string is simply the product of the operators raised to the elements of the string. To simplify notation, we adopt the following: $|\mathbf{k}\rangle=X|k_1\rangle\otimes\cdots\otimes|k_n\rangle$, $|\varphi_{\mathbf{k}}\rangle=|\varphi_{k_1}\rangle\otimes\cdots\otimes|\varphi_{k_n}\rangle$, and $P_{\mathbf{k}}$ for $P_{k_1}\otimes\cdots\otimes P_{k_n}$ and similarly for $\tilde{P}_{\mathbf{x}}$ in the conjugate basis.

The first set, the Z-type stabilizers, defines a code correcting errors in the standard basis (dit errors, or amplitude errors), while the second, the X-type stabilizers, defines a code correcting phase errors. Here, and henceforth, the operators X and Z are the generalized Pauli operators in d dimensions [36], given by $Z:=\sum_{k=0}^{d-1}\omega^k|k\rangle\langle k|$ and $X:=\sum_{k=0}^{d-1}|k+1\rangle\langle k| =\sum_{k=0}^{d-1}\omega^{-k}|\tilde{x}\rangle\langle\tilde{x}|$, where $\omega:=e^{2\pi i/d}$.

Measuring the stabilizers yields the amplitude and phase syndromes $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, to which we associate projectors $\Pi_{\boldsymbol{\alpha}}$ and $\tilde{\Pi}_{\boldsymbol{\beta}}$, respectively. Since the stabilizers are products of Z's or X's, these projectors can be expressed as $\Pi_{\boldsymbol{\alpha}}=\Sigma_{k\in[\boldsymbol{\alpha}]}P_{\mathbf{k}}$ and $\tilde{\Pi}_{\boldsymbol{\beta}}=\Sigma_{\mathbf{x}\in[\boldsymbol{\beta}]}\tilde{P}_{\mathbf{x}}$ where the $[\boldsymbol{\alpha}]$ and $[\boldsymbol{\beta}]$ are equivalence classes of standard and conjugate basis states that all share the syndromes α and β, respectively.

Commuting with the stabilizers (but not included in them) are the logical or encoded operators $\bar{Z}_{\mathbf{j}}$ and $\bar{X}_{\mathbf{j}}$, one pair for each of the $n-m_z-m_x$ encoded qudits. Crucially, these may also be chosen to be of Z and X type, respectively, an assumption we make throughout. Let $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ be the measurement outcomes of all the logical operators $\{\bar{Z}_j|1\leq j\leq n-m_x-m_z\}$ and $\{\bar{X}_j|1\leq j\leq n-m_x-m_z\}$, respectively, and $\bar{\Pi}_{\boldsymbol{\lambda}}:=\Sigma_{\mathbf{k}\in[\boldsymbol{\lambda}]}P_{\mathbf{k}}$ and $\hat{\Pi}_{\boldsymbol{\mu}}:=\Sigma_{\mathbf{x}\in[\boldsymbol{\mu}]}\tilde{P}_{\mathbf{x}}$ the associated projectors for $[\boldsymbol{\lambda}]$ and $[\boldsymbol{\mu}]$ the corresponding equivalence classes.

The idea behind one-shot distillation is for Alice to measure the syndromes $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ on her system and reveal $\boldsymbol{\alpha}$ to Bob. If the CSS code is properly chosen, this information should make it possible to distinguish the corresponding marginals of his key system and the shield, at which point Theorem 2 would apply to key observables $\bar{Z}_j$ and conjugate observables $\bar{X}_{\mathbf{j}}$. Bob only needs $\boldsymbol{\alpha}$, since the mere existence of the conjugate basis measurement implies the secrecy of the key. In QKD, measuring the encoded Z operators is equivalent to privacy amplification, and the degrees of freedom in defining the logical operators $\bar{Z}_j$ give rise to different families of privacy amplification functions. Here we present a one-shot private state distillation theorem useful for QKD security proofs [37].

Theorem 4 (One-Shot Distillation). Let Alice and Bob share an arbitrary state Ψ^{ABS} with $\dim(A)=d^n$ and purification $|\psi\rangle^{ABSE}=\Sigma_{\mathbf{k}}\sqrt{p_{\mathbf{k}}}|k\rangle^A|\varphi_{\mathbf{k}}\rangle^{BSE}$. Suppose there exists a CSS code with m_z Z-type stabilizers and m_x X-type stabilizers whose syndromes $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are associated with measurements $\Lambda^B_{\boldsymbol{\alpha},\mathbf{k}}$ and $\tilde{\Lambda}^{BS}_{\boldsymbol{\beta},\mathbf{x}}$ for which

$$p_{\mathrm{e}}=\sum_{\boldsymbol{\alpha}}\sum_{\mathbf{j}\neq\mathbf{k}}\mathrm{Tr}[(P^A_{\mathbf{j}}\otimes\Lambda^B_{\boldsymbol{\alpha},\mathbf{k}})\Pi^A_{\boldsymbol{\alpha}}\psi^{AB}]\leq\epsilon_z, \tag{10}$$

$$\tilde{p}_{\mathrm{e}}=\sum_{\boldsymbol{\beta}}\sum_{\mathbf{x}\neq\mathbf{y}}\mathrm{Tr}[(\tilde{P}^A_{\mathbf{x}}\otimes\tilde{\Lambda}^{BS}_{\boldsymbol{\beta},\mathbf{y}})\tilde{\Pi}^A_{\boldsymbol{\beta}}\psi^{ABS}]\leq\epsilon_x. \tag{11}$$

Then by one-way communication from Alice to Bob they can distill an $(\epsilon_z+\sqrt{\epsilon_x})$-private state of size $d^{n-m_z-m_x}$ whose key is the encoded value λ.

Proof. Suppose that Alice measures the syndromes α and β and makes α public. The post-measurement state is $|\Psi_1\rangle^{\lambda BSERT}:=\Sigma_{\alpha,\beta}\Pi^A_\alpha\tilde{\Pi}^A_\beta|\Psi\rangle^{ABSE}|\alpha\rangle^R|\beta\rangle^T$ where R is a new public register shared by all parties but T is held by Alice. Coherently measuring $\Lambda^B_{\alpha,k}$ with the partial isometry U^{BB_2} produces

$$|\Psi_2\rangle:=U^{BB_2}|\Psi_1\rangle=\sum_k\sqrt{\Lambda^B_{\alpha,k}}|\Psi_1\rangle^{\lambda BSERT}|k\rangle^{B_2}.$$

Bob can determine the values of $\bar{Z}^A_j$ for all j with error probability

$$\begin{aligned}p'_{\mathrm{e}}&=\sum_{\lambda\neq\lambda'}\mathrm{Tr}[(\bar{\Pi}^A_\lambda\otimes\bar{\Pi}^{B_2}_{\lambda'})\Psi^{AB_2}_2]\\&=\sum_{\lambda\neq\lambda'}\sum_{\alpha,\beta}\sum_{k\in[\lambda']}\mathrm{Tr}[(\bar{\Pi}^A_\lambda\otimes\Lambda^B_{\alpha,k})\Pi^A_\alpha\tilde{\Pi}^A_\beta\Psi^{AB}]\\&=\sum_{\lambda\neq\lambda'}\sum_{\alpha}\sum_{k\in[\lambda']}\mathrm{Tr}[(\bar{\Pi}^A_\lambda\otimes\Lambda^B_{\alpha,k})\Pi^A_\alpha\Psi^{AB}]\\&\leq\sum_\alpha\sum_{j\neq k}\mathrm{Tr}[(P^A_j\otimes\Lambda^B_{\alpha,k})\Pi^A_\alpha\Psi^{AB}]\\&\leq\epsilon_z,\end{aligned}$$

where we have used $[\bar{\Pi}^A_{\boldsymbol{\lambda}},\tilde{\Pi}^A_{\boldsymbol{\beta}}]=0$ and $\Sigma_{\boldsymbol{\beta}}\tilde{\Pi}^A_{\boldsymbol{\beta}}=\mathbb{1}^A$. Alice's conjugate basis measurement can be accurately predicted by first undoing U^{BB_2} and then measuring $\tilde{\Lambda}^{BS}_{\boldsymbol{\beta},\mathbf{y}}$. An entirely similar calculation shows that the resulting error probability is less than ϵ_x. Hence, by Theorem 2 Ψ_2 is an $(\epsilon_z+\sqrt{\epsilon_x})$-private state, whose key subsystems are the encoded subsystems $\bar{A}$ and $\bar{B}_2$. ■

As stated, the above theorem only involves one-way communication. However, it can easily be generalized to the sorts of two-way error-correction protocols presented in [35]. The idea is that, instead of making only one measurement, Alice and Bob execute successive "partial" measurements of the syndrome of the dit error correction code, each of which is followed by a round of two-way classical communication. Each measurement is still associated with a set of Z-type operators, but the Z-type operators of the ith round of measurement could depend on all their previous outcomes. One-way error correction can be interpreted as the case in which the Z-type operators are chosen independently.

B. Achievable distillation rates

Now we turn to the achievable distillation rates. Define an (n,ϵ) distillation protocol for ψ^{ABS} to be a series of local quantum operations and classical communication such that application on $\Psi^{ABS}=(\Psi^{ABS})^{\otimes n}$ produces an ϵ-private state. If there exists an (n,ϵ_n) protocol for every n, producing a $\log_2\tau_n$-bit approximate private state, such that $\lim_{n\to\infty}\epsilon_n=0$, then the fractional yield of private outputs to raw inputs defines the achievable rate

$$R=\lim_{n\to\infty}\frac{\log_2\tau_n}{n}. \tag{12}$$

Finally, the supremum of achieveable rates is called the one-way distillable privacy $P_{\rightarrow}(\psi^{ABS})$ of the state ψ^{ABS}. In the following, we use the label ψ_a where necessary to denote that the entropy or mutual information is computed using an extended version ψ^{ACBSE}_a of the state ψ^{ABSE}. Using the previous result and a slightly modified version of the HSW theorem given in Appendix B, we quickly get the following:

Theorem 5 (One-Way Distillable Privacy). Given conjugate observables Z^A and X^A, consider an arbitrary state ψ^{ABS} and its extension ψ^{ACBS}_a obtained by copying the Z^A basis of A to C. Then

$$P_{\rightarrow}(\psi^{ABS})\geq I(Z^A{:}B)-H(Z^A)+I(X^A{:}CBS)_{\psi_a}.$$

Proof. Without loss of generality, we can assume that $d=\dim(A)$ is prime by appending additional $|k\rangle^A$ for which the corresponding weights $p_k=0$. Let C be under Alice's control so that she can perform the copy operation and consider $\psi_a^{ACBS}=(\psi_a^{ACBS})^{\otimes n}$. Pick a CSS code c from the distribution $\mathcal{C}$ given in Appendix C, so that the Z-type and X-type stabilizers give rise to universal hash functions (for a definition, see Appendix B), and let $m_z=\frac{n}{\log_2 d}[H(Z^A)-I(Z^A:B)+4\delta]$ and $m_x=\frac{n}{\log_2 d}[H(X^A)_{\psi_a}-I(X^A:CBS)_{\psi_a}+4\delta]$ for a fixed $\delta>0$. Theorem 7 implies that the measurements $\Lambda^B_{\boldsymbol{\alpha},\mathbf{k}}$ constructed from these hash functions can predict Alice's key with average error probability $\langle\epsilon_{z,c}\rangle_{\mathcal{C}}\leq 6\times 2^{-n\delta^2}$. Similarly, the average error probability of the measurements $\tilde{\Lambda}^{CBS}_{\boldsymbol{\beta},\mathbf{x}}$ in predicting the conjugate basis observable is $\langle\epsilon_{x,c}\rangle_{\mathcal{C}}\leq 6\cdot 2^{-n\delta^2}$. Now apply Theorem 4 to each CSS code, where the shield is the combined system CS, and average over the different codes. Using the concavity of the square root and the fact that $H(X^A)_{\psi_a}=\log_2 d$, it follows that Alice and Bob can create an ϵ-private state having $n[I(Z^A:B)+I(X^A:CBS)_{\psi_a}-H(Z^A)-8\delta]$ key bits, for $\epsilon\leq\langle\epsilon_{z,c}\rangle_{\mathcal{C}}+\sqrt{\langle\epsilon_{x,c}\rangle_{\mathcal{C}}}\leq 6\times 2^{-n\delta^2}+\sqrt{6\times 2^{-n\delta^2}}$. ■

By Lemma 2, $P_{\rightarrow}(\psi^{ABS})\geq I(Z^A:B)-I(Z^A:E)$, so this method achieves the same yield of secret key as the random coding method used by Devetak and Winter [13].

Lemma 2. For conjugate observables Z^A and X^A and a state of the form $|\psi_a\rangle^{ACBSE}=\sum_k\sqrt{p_k}|k\rangle^A|k\rangle^C|\varphi_k\rangle^{BSE}$, $I(X^A:CBS)=H(Z^A)-I(Z^A:E)$.

Proof. Rewrite $|\psi_a\rangle^{ACBSE}$ as $\frac{1}{\sqrt{d}}\sum_x|\tilde{x}\rangle^A|\vartheta_x\rangle^{CBSE}$ for $|\vartheta_x\rangle^{CBSE}=Z_x^C\sum_k\sqrt{p_k}|k\rangle^C|\varphi_k\rangle^{BSE}$. Hence $S(\vartheta_x^{CBS})=S(\vartheta_0^{CBS})$ for all x. From the Schmidt decomposition, $S(\vartheta_0^{CBS})=S(\vartheta_0^E)=S(E)$ and $S(CBS)=S(AE)$. Therefore,

$$I(X^A:CBS)=S(CBS)-\sum_x q_x S(\vartheta_x^{CBS})=S(AE)-S(\vartheta_0^{CBS})$$
$$=S\left(\sum_k p_k P_k^A\otimes\varphi_k^E\right)-S(E)=H(Z^A)-I(Z^A:E).$$

■

An immediate corollary is that the distillable privacy of an arbitrary state ψ^{AB} without a specified shield system must be no less than the coherent information $I_c(A\rangle B):=S(B)-S(AB)$; this can be seen as a weaker version of the hashing inequality, which we will consider in the next section.

Corollary 1. $P_{\rightarrow}(\psi^{AB})\geq I_c(A\rangle B)$.

Proof. Pick any observable Z^A and define the computational basis of A as its eigenbasis. Consider the purification $|\psi\rangle^{ABE}=\sum_k\sqrt{p_k}|k\rangle^A|\varphi_k\rangle^{BE}$ of ψ^{AB}, and note that $I_c(A\rangle B)=S(B)-S(E)=I(Z^A:B)-I(Z^A:E)$, where the last equality follows from the fact that $S(\varphi_k^B)=S(\varphi_k^E)$ for all k. From Theorem 5 and Lemma 2, $P_{\rightarrow}(\psi^{AB})\geq I(Z^A:B)-I(Z^A:E)=I_c(A\rangle B)$. ■

V. HASHING INEQUALITY

Now we turn to the related question of entanglement distillation and show how the above analysis can be modified to prove the hashing inequality on the one-way distillable entanglement $E_{\rightarrow}(\psi^{AB})$, which is defined analogously to $P_{\rightarrow}(\psi^{ABS})$. There are two main differences with the methods used in the preceding section. The first is that for Theorem 5, it does not matter how the shield is split between Alice and Bob, but of course for entanglement distillation Alice and Bob must be able to locally untwist the private state. The difficulty comes from the first step, in which Alice copies her key to system C, which was then considered part of the shield. Here, we avoid this problem by showing that after Bob makes the $\Lambda^B_{\boldsymbol{\alpha}}$ measurement, he effectively has system C. Thus, he has the entire shield, and can perform the untwisting operator himself.

The second difference stems from the definition of approximate private states as states that yield approximate secret keys when measured. Because we must now perform all measurements coherently, these results are not directly applicable. Modifying them is possible, but we prefer to give a more direct argument, which has the side benefit of yielding a better approximation parameter.

Theorem 6 (Hashing Inequality). $E_{\rightarrow}(\psi^{AB})\geq I_c(A\rangle B)$.

Proof. The proof proceeds by successively performing the $\Lambda^B_{\boldsymbol{\alpha}}$ and $\tilde{\Lambda}^B_{\boldsymbol{\beta}}$ measurements coherently and showing how the result is close to an entangled state. Purify ψ^{AB} to $|\psi\rangle^{ABE}=\sum_{k=0}^{d-1}\sqrt{p_k}|k\rangle^A|\varphi_k\rangle^{BE}$. Without loss of generality, we can assume that $d=\dim(A)$ is prime by appending additional states $|k\rangle$ for which $p_k=0$. Now define $|\Psi\rangle^{ABE}:=(|\psi\rangle^{ABE})^{\otimes n}=\sum_{\mathbf{k}}\sqrt{p_{\mathbf{k}}}|\mathbf{k}\rangle^A|\varphi_{\mathbf{k}}\rangle^{BE}$, where $p_{\mathbf{k}}=p_{k_1}p_{k_2},\ldots,p_{k_n}$, $|\mathbf{k}\rangle=|k_1\rangle|k_2\rangle,\ldots,|k_n\rangle$, and $|\varphi_{\mathbf{k}}\rangle=|\varphi_{k_1}\rangle|\varphi_{k_2}\rangle,\ldots,|\varphi_{k_n}\rangle$.

Now suppose Alice picks a CSS code c from the distribution $\mathcal{C}$ described in Appendix C with m_z Z-type and m_x X-type stabilizers, measures the dit and phase error syndromes α and β, and declares them publicly. This transforms the state into

$$|\Psi_1\rangle:=\sum_{\boldsymbol{\alpha},\boldsymbol{\beta}}\Pi^A_{\boldsymbol{\alpha}}\tilde{\Pi}^A_{\boldsymbol{\beta}}|\Psi\rangle^{ABE}|\alpha,\beta\rangle^R, \tag{13}$$

where R is a publicly-held register.

Let $m_z=\frac{n}{\log_2 d}[H(Z^A)_{\psi}-I(Z^A:B)_{\psi}+4\delta]$ for some arbitrary $\delta>0$. By Theorem 7, there exists a measurement $\Lambda^B_{\boldsymbol{\alpha}}$ that predicts Alice's key with error probability $\epsilon_{z,c}$ such that $\langle\epsilon_{z,c}\rangle_{\mathcal{C}}\leq 6\times 2^{-n\delta^2}$. Performing this measurement coherently yields

$$|\Psi_2\rangle:=\sum_{\mathbf{k},\boldsymbol{\alpha},\boldsymbol{\beta}}\Pi^A_{\boldsymbol{\alpha}}\tilde{\Pi}^A_{\boldsymbol{\beta}}\sqrt{\Lambda^B_{\alpha,\mathbf{k}}}|\Psi\rangle^{ABE}|\mathbf{k}\rangle^C|\alpha,\beta\rangle^R,$$

where the output is stored in system C. This state is essentially identical to the one in which Bob simply has a copy of Alice's key,

$$|\Psi_2'\rangle:=\sum_{\boldsymbol{\alpha},\boldsymbol{\beta}}\Pi^A_{\boldsymbol{\alpha}}\tilde{\Pi}^A_{\boldsymbol{\beta}}|\Psi_a\rangle^{ABCE}|\alpha,\beta\rangle^R, \tag{14}$$

where $|\Psi_a\rangle=|\psi_a\rangle^{\otimes n}$, as defined in Theorem 5, except that Bob holds C. Computing the fidelity, we obtain

$$\langle\Psi_2|\Psi_2'\rangle=\sum_{\boldsymbol{\alpha},\mathbf{k}\in[\boldsymbol{\alpha}]}p_{\mathbf{k}}\langle\varphi_{\mathbf{k}}|\sqrt{\Lambda^B_{\boldsymbol{\alpha},\mathbf{k}}}|\varphi_{\mathbf{k}}\rangle^{BE}$$
$$\geq\sum_{\boldsymbol{\alpha},\mathbf{k}\in[\boldsymbol{\alpha}]}p_{\mathbf{k}}\langle\varphi_{\mathbf{k}}|\Lambda^B_{\boldsymbol{\alpha},\mathbf{k}}|\varphi_{\mathbf{k}}\rangle^{BE}\geq 1-\epsilon_{z,c},$$

using the fact that $\sqrt{\Lambda}\geq\Lambda$ for $0\leq\Lambda\leq\mathbb{1}$. Since the fidelity

bounds the trace distance via $\mathrm{Tr}|\rho-\sigma| \leq 2\sqrt{1-F(\rho,\sigma)^2}$ [38], we have $\mathrm{Tr}|\Psi_2-\Psi_2'| \leq 2\sqrt{2\epsilon_{z,c}}$.

Now rewrite $|\Psi_2'\rangle$ as $|\Psi_2'\rangle = \Sigma_{\mathbf{x}} \sqrt{q_{\mathbf{x}}} |\tilde{\mathbf{x}}\rangle^A |\vartheta_{\mathbf{x}}\rangle^{BCE}$ and let $m_x = \frac{n}{\log_2 d}[H(X^A)_{\psi_a} - I(X^A:BC)_{\psi_a} + 4\delta]$. By Theorem 7, there exists a measurement $\tilde{\Lambda}_{\boldsymbol{\beta}}^{BC}$ that can predict the outcome of a conjugate measurement on A with error probability $\epsilon_{x,c}$ such that $\langle \epsilon_{x,c} \rangle_{\mathcal{C}} \leq 6 \times 2^{-n\delta^2}$. Starting from $|\Psi_2'\rangle$, suppose Bob coherently measures $\tilde{\Lambda}_{\boldsymbol{\beta}}$ and store the result in D. This gives

$$|\Psi_3'\rangle := \sum_{\mathbf{y},\boldsymbol{\alpha},\boldsymbol{\beta}} \Pi_{\boldsymbol{\alpha}}^A \tilde{\Pi}_{\boldsymbol{\beta}}^A \sqrt{\tilde{\Lambda}_{\boldsymbol{\beta},\mathbf{y}}^{BC}} |\Psi_a\rangle^{ABCE} |\tilde{\mathbf{y}}\rangle^D |\alpha,\beta\rangle^R.$$

As before, this is essentially the same as the state $|\Psi_3''\rangle$ in which Bob has a copy of Alice's string $\mathbf{x}$ in system D,

$$|\Psi_3''\rangle = \sum_{\mathbf{x},\boldsymbol{\alpha},\boldsymbol{\beta}} \sqrt{q_{\mathbf{x}}} \Pi_{\boldsymbol{\alpha}}^A \tilde{\Pi}_{\boldsymbol{\beta}}^A |\tilde{\mathbf{x}}\rangle^A |\tilde{\mathbf{x}}\rangle^D |\vartheta_{\mathbf{x}}\rangle^{BCE} |\alpha,\beta\rangle^R, \tag{15}$$

and a similar calculation to the one above shows that $\mathrm{Tr}|\Psi_3' - \Psi_3''| \leq 2\sqrt{2\epsilon_{x,c}}$.

Implicit in rewriting $|\Psi_2'\rangle$ using Alice's conjugate basis is the fact that $\sqrt{q_{\mathbf{x}}}|\vartheta_{\mathbf{x}}\rangle^{BCE} = \Sigma_{\mathbf{k}} \sqrt{p_{\mathbf{k}}} \langle \tilde{\mathbf{x}}|\mathbf{k}\rangle |\mathbf{k}\rangle^C |\varphi_{\mathbf{k}}\rangle^{BE}$. Substituting this in Eq. (15) gives

$$|\Psi_3''\rangle = \frac{1}{\sqrt{d^n}} \sum_{\mathbf{x},\alpha,\beta} \Pi_\alpha^A \tilde{\Pi}_\beta^A |\tilde{\mathbf{x}}\rangle^A |\tilde{\mathbf{x}}\rangle^D |\alpha,\beta\rangle^R \otimes \sum_{\mathbf{k}} \sqrt{p_{\mathbf{k}}} \omega^{\mathbf{x}\cdot\mathbf{k}} |\mathbf{k}\rangle^C |\varphi_{\mathbf{k}}\rangle^{BE}.$$

Bob can now decouple subsystem BCE by using the operator $U^{BD} := \Sigma_{\mathbf{k},\mathbf{x}} \omega^{-\mathbf{x}\cdot\mathbf{k}} \tilde{P}_{\mathbf{x}}^D \otimes P_{\mathbf{k}}^B$, and the result is an entangled state in the encoded subsystem $\bar{A}\bar{D}$,

$$|\Psi_4''\rangle := U^{BD} |\Psi_3''\rangle = \frac{1}{\sqrt{d^n}} \sum_{\alpha,\beta} \Pi_\alpha^A \tilde{\Pi}_\beta^A |\Phi_{d^n}\rangle^{AD} |\alpha,\beta\rangle^R \otimes \sum_{\mathbf{k}} \sqrt{p_{\mathbf{k}}} |\mathbf{k}\rangle^C |\varphi_{\mathbf{k}}\rangle^{BE}. \tag{16}$$

Since they never hold exactly $|\Psi_2'\rangle$ or $|\Psi_3''\rangle$, Alice and Bob only end up with a good approximation to an entangled state. To determine how good, we can use properties of the trace distance. Call the unitaries implementing the coherent measurements U_z^{BC} and U_x^{BCD}, respectively, and define $W^{BCD} := U^{BD} U_x^{BCD} U_z^{BC}$. Applying W to Ψ_1 generates Ψ_4, and by the triangle inequality and unitary invariance of the trace distance, we have

$$\mathrm{Tr}|\Psi_4 - \Psi_4''| \leq 2(\sqrt{2\epsilon_{z,c}} + \sqrt{2\epsilon_{x,c}}). \tag{17}$$

The next step is to average over all CSS codes. Using the concavity of the square root and the fact that the trace distance cannot increase under the partial trace, we obtain

$$\mathrm{Tr}|\Psi_4^{\bar{A}\bar{D}} - \Phi^{\bar{A}\bar{D}}| \leq 8\sqrt{3 \times 2^{-n\delta^2}}. \tag{18}$$

Finally, we must show that the resulting rate is given by the coherent information. Since $H(X^A)_{\psi_a} = \log_2 d$, $(n - m_x - m_z)\log_2 d = n[I(Z^A:B)_\psi + I(X^A:BC)_{\psi_a} - H(Z^A)_\psi - 8\delta]$. By Lemma 2, $I(X^A:BC)_{\psi_a} = H(Z^A)_{\psi_a} - I(Z^A:E)_{\psi_a}$. Clearly $H(Z^A)_\psi = H(Z^A)_{\psi_a}$ and similarly for the quantum mutual information of Z^A with B or E. Since $I(A\rangle B)_{\psi_a} = I(Z^A:B)_\psi - I(Z^A:E)_\psi$, as in Corollary 1, $(n - m_x - m_z)\log_2 d = n I_c(A\rangle B)_\psi - 8n\delta$, which concludes the proof. ■

VI. RELATION TO PREVIOUS WORK

The present work is an outgrowth of earlier work on private states by one of us [39] and draws much inspiration from the work of Koashi [10,22]. In particular, Theorems 2 and 3 are closely related to the first two theorems of [22], in which Koashi defines the two protocols of the complementary control scenario. It is easy to see that our condition on the predictability of the key is equivalent to his condition on the primary protocol, and that our condition on the measurement $\tilde{\Lambda}^{BS}$ implies his condition on the secondary protocol. Therefore, Theorem 2 is a corollary of the first theorem of [22]. Although we were not able to show that the condition on the secondary protocol implies our condition on the measurement $\tilde{\Lambda}^{BS}$, Theorem 3 can be proven using arguments very similar to those found in [22].

Meanwhile, Theorem 4 corresponds conceptually to the inclusion of the complementary control scenario in the security analysis of [10], with several important differences in the details. First, we do not consider parameter estimation at all, while [10] presents a full security analysis for BB84. To complete a security proof using our results, one would need to determine what quantum states ψ^{ABS} are compatible with the output of the parameter estimation phase of the protocol in order to apply Theorems 4 and 5. This can be done with an estimate of the quantum channel noise obtained indirectly from the experimental measurements. The advantage of Theorem 4 is that it could be used to prove the security of a more general set of QKD protocols, even those including preprocessing. Second, [10] assumes that Bob's conjugate measurement is independent of $\boldsymbol{\beta}$, with the supplemental information supplied only after the measurement is made. In our method, Bob uses the syndrome $\boldsymbol{\beta}$ to construct the measurement $\tilde{\Lambda}_{\boldsymbol{\beta}}^{BS}$. Generally, the latter is no less powerful than the former, and avoids the pitfalls of *locking* of accessible information [40]. In Appendix D we provide a concrete example in which allowing $\tilde{\Lambda}_{\boldsymbol{\beta}}^{BS}$ to depend on $\boldsymbol{\beta}$ yields a better security parameter than if it were independent.

The smaller difference concerns the step in [10] of having Alice encrypt the amplitude error syndromes using a preshared secret key. This removes the need to use a CSS code [41], but requires a key of size $O(n \log d)$ bits [in addition to the authentication key, of size $O(\log n \cdot \log d)$] and makes a small but practically significant difference for QKD. Theorem 4 can be modified to encrypt the syndrome $\boldsymbol{\alpha}$ of an arbitrary (not necessarily linear) code as follows. Supposing Alice and Bob already share a perfect secret key ℓ of the same size as the amplitude error syndrome $\boldsymbol{\alpha}$. Alice publicly transmits $\boldsymbol{\alpha} + \ell$ to Bob. He recovers $\boldsymbol{\alpha}$ using ℓ and can then make the $\Lambda_{\boldsymbol{\alpha}}^B$ measurement. The system R storing the value of $\boldsymbol{\alpha}$ is unknown to Eve and can be decoupled with the operator $\Sigma_{\boldsymbol{\alpha}} \Pi_{\boldsymbol{\alpha}}^B \otimes (X^R)^{-\alpha}$ since this does not affect the key measurements. We can now apply Theorem 4 directly on the resulting correlated state. Using these ideas, one can easily

show that the final security parameter would have a similar form with or without encrypting of the dit error syndrome.

By adapting Koashi's complementarity scenario, we are able to construct a means for distilling private states from arbitrary resource states at a rate given by the quantum Csiszár-Körner bound. This complements the result of Devetak and Winter [27], showing more directly how physical (quantum-mechanical) phenomena are responsible for the privacy of the key. As mentioned before, it must be possible to view their result as private state distillation by performing the operations coherently, and indeed a twisting operator plays an important role in their derivation of the hashing inequality, specifically the operator U defined on p. 8 of [13]. Mathematically speaking, the difference in the two approaches can be traced to the origins of this operator: here from the measurement used in the HSW theorem to determine the outcome of Alice's conjugate measurement, there from the quantum Chernoff bound via Uhlmann's theorem.

A different approach to private state distillation is taken in [42], whose ultimate goal is to show that key distribution is still possible over channels whose quantum capacity is zero, rather than give rates on private state distillation. The distillation portion of the protocol accepts only certain inputs, namely twisted versions of noisy entangled states, and thus the distillation procedure works by untwisting the state and then applying entanglement distillation. The difficulty in this scheme then lies in determining the optimal combination of twisting operator and noise such that the given input can be expressed in this form. As such, no closed-form distillation rate expressions can be given, and happily this is not relevant to their goal.

Our method of private state distillation gives a new proof of the hashing inequality, which then also implies a new proof of the direct quantum coding theorem. This version differs from previous work [13,43–48] in several ways, mainly by the explicit use of CSS codes from the beginning and the fact that the decoder is constructed from the measurement used in the HSW theorem, rather than by decoupling Eve and appealing to Uhlmann's theorem. This construction resolves the open question raised in the conclusion of [48] as here the decoder is directly linked to the bit and phase syndromes of the CSS code.

Finally, we would like to point out the connections to recent work on complementary channels. In [49–51], it has been shown that a correctable channel implies that the complementary channel is private, and vice versa. Theorems 2 and 3 are essentially a static version of this (dynamic) result, applied to bipartite states instead of channels and starting from different assumptions.

VII. CONCLUSION

We provide a characterization of private states in terms of an information exclusion principle for complementary observables, and we generalize the security proof methods based on entanglement distillation and the uncertainty principle. This generalization is formulated as a one-shot distillation theorem (Theorem 4). Exploiting this framework, we give alternative proofs of the quantum Csiszár-Körner bound on distillable secret key (Theorem 5 and Lemma 2) and the hashing inequality on distillable entanglement (Theorem 6).

One of the main applications of this work is of course to QKD, particularly proofs for realistic protocols. These involve more physical systems than just those describing the keys and the eavesdropper, and one challenge has been determining how to use information the honest parties have about such systems. Including the shield system into the security analysis and picturing the QKD process as private state distillation gives a general method for doing so, a point also emphasized by Koashi [10]. The importance of these extra systems is how they contribute to knowledge of hypothetical conjugate basis measurements made on the key system of either party.

This is dramatically exemplified by Koashi's security proof of the BB84 protocol with uncharacterized detectors, which proceeds by noting that this protocol directly furnishes Bob with an estimate of Alice's conjugate basis result, regardless of the detector details. Our results provide a more detailed and complete picture of how shield systems contribute to privacy, which should expand the range of protocol and device imperfections that can be treated. For instance, it would be interesting to investigate the unconditional security of QKD protocols that are not permutation invariant [52,53]. This possibility is particularly appealing since Theorem 4 does not require a permutation of the input state nor does it depend on a particular method of parameter estimation. We plan to examine these issues and other implications for realistic protocols in an upcoming publication.

As a final remark, we note that our approach to the hashing inequality is closely related to [48], which also makes use of an information-uncertainty relation. In fact, that relation is simply the "quantum" version of Hall's the complementary information tradeoff, Lemma 1, replacing the classical conditional entropy H with the classical-quantum conditional entropy S to obtain

$$S(Z^A|E) + S(\tilde{X}^A|B) \geq \log_2 d \tag{19}$$

for any state ρ^{ABE}, conjugate observables Z^A and $\tilde{X}^A$, and $d = \dim(A)$. As the "classical" version can easily be generalized to nonconjugate observables simply by using the general form of the entropic uncertainty relation, it becomes reasonable to ask if the "quantum" version of the same holds as it does for strictly conjugate observables. Numerical evidence supports this claim, and we explore this subject in more detail in Ref. [54].

ACKNOWLEDGMENTS

We thank Gernot Alber, Aram Harrow, Hoi-Kwong Lo, Norbert Lütkenhaus, and Graeme Smith for helpful discussions. J.M.R. received support from the Alexander von Humboldt Foundation and the European IST project SECOQC, and J.C.B. from the Natural Sciences and Engineering Research Council of Canada and Quantumworks.

APPENDIX A: APPROXIMATE PRIVATE STATE PROOFS

Here we present the proofs of Theorems 2 and 3.

Proof of Theorem 2. Write the purification of ψ^{ABS} as

$|\psi\rangle^{ABSE}=\Sigma_{jk}\sqrt{p_{jk}}|jk\rangle^{AB}|\varphi_{jk}\rangle^{SE}$ for some (normalized) states $|\varphi_{jk}\rangle^{SE}$. Copying the standard basis of Bob's state to a blank register $|0\rangle^{B'}$ with the unitary $C^{BB'}$ yields $|\psi_1\rangle^{ABSEB'}=\Sigma_{jk}\sqrt{p_{jk}}|jk\rangle^{AB}|k\rangle^{B'}|\varphi_{jk}\rangle^{SE}$. Let $\bar{\psi}_1^{ABB'SE}$ be the state after measuring Z^A and Z^B and consider the related state $|\psi_1'\rangle^{ABB'SE}=\Sigma_k\sqrt{p_{jk}}|jj\rangle^{AB}|k\rangle^{B'}|\varphi_{jk}\rangle^{SE}$. Performing the same measurement on ψ' and computing the trace distance between the states, we find

$$\mathrm{Tr}|\bar{\psi}_1^{ABE}-\bar{\psi}_1'^{ABE}|=2\sum_{j\neq k}p_{jk}=2p_{\mathrm{e}}\leq 2\epsilon_z. \tag{A1}$$

Observe that $|\psi_1'\rangle^{ABB'SE}=C^{AB}|\psi\rangle^{AB'SE}|0\rangle^B$. Rewrite the original state as $|\psi\rangle^{AB'SE}=\Sigma_x\sqrt{q_x}|\tilde{x}\rangle^A|\vartheta_x\rangle^{B'SE}$ for some probability distribution q_x and normalized states $|\vartheta_x\rangle^{B'SE}$. Coherently performing the $\tilde{\Lambda}_y^{B'S}$ measurement with unitary $U^{B'ST}$, where the extra system T stores the result, we find

$$|\psi_2\rangle=C^{AB}U^{B'ST}|\psi\rangle^{AB'SE}|0\rangle^B|0\rangle^T \tag{A2}$$

$$=\sum_{xy}\sqrt{q_x}C^{AB}|\tilde{x}\rangle^A|0\rangle^B\sqrt{\tilde{\Lambda}_y^{B'S}}|\vartheta_x\rangle^{B'SE}|y\rangle^T. \tag{A3}$$

Define $|\psi_2'\rangle=\Sigma_x\frac{\sqrt{q_x}}{\sqrt{1-\tilde{p}_{\mathrm{e}}}}C^{AB}|\tilde{x}\rangle^A|0\rangle^B\sqrt{\tilde{\Lambda}_x^{B'S}}|\vartheta_x\rangle^{B'SE}|x\rangle^T$; its fidelity with $|\psi_2\rangle^{AB'SET}$ is

$$\langle\psi_2|\psi_2'\rangle=\sqrt{1-\tilde{p}_{\mathrm{e}}}\geq\sqrt{1-\epsilon_x}. \tag{A4}$$

In general, the fidelity between two quantum states is defined as $F(\rho,\sigma):=\mathrm{Tr}|\sqrt{\rho}\sqrt{\sigma}|$. Note that $|\psi_2'\rangle^{ABB'SET}$ is a private state with key systems AB and shield $B'ST$. One way to see this is to rewrite $|\tilde{x}\rangle$ in terms of $|k\rangle$,

$$|\psi_2'\rangle=\frac{1}{\sqrt{d}}\sum_{kx}\frac{\sqrt{q_x}}{\sqrt{1-\tilde{p}_{\mathrm{e}}}}e^{i\theta_{kx}}|kk\rangle^{AB}\sqrt{\Lambda_x^{B'S}}|\vartheta_x\rangle^{B'SE}|x\rangle^T.$$

Applying the unitary operator $W^{BT}=\Sigma_{kx}e^{-i\theta_{kx}}P_k^B\otimes P_x^T$ results in a maximally entangled state $|\Phi\rangle^{AB}$ in the AB subsystem. Since W^{BT} is a twisting operator, $|\psi_2'\rangle$ is a private state.

If we now define $|\psi_3\rangle^{ABB'SET}:=U^{\dagger B'ST}|\psi_2'\rangle^{ABB'SET}$, also a private state since $U^{\dagger B'ST}$ acts only on the shield, it follows from unitary invariance of the inner product that

$$F(|\psi_3\rangle^{ABB'SET},|\psi_1'\rangle^{ABB'SE}|0\rangle^T)\geq\sqrt{1-\epsilon_x}. \tag{A5}$$

Finally, bound the trace distance with the fidelity, using the relation $\mathrm{Tr}|\rho-\sigma|\leq\sqrt{1-F(\rho,\sigma)^2}$. This implies $\mathrm{Tr}|\bar{\psi}_3^{ABE}-\bar{\psi}_1'^{ABE}|\leq 2\sqrt{\epsilon_x}$, and using the triangle inequality we obtain $\mathrm{Tr}|\bar{\psi}^{ABE}-\bar{\psi}_3^{ABE}|\leq 2(\epsilon_z+\sqrt{\epsilon_x})$. ■

Proof of Theorem 3. Assume Eve holds the purification of ψ^{ABS} and measure AB to create the key. This yields $\bar{\psi}^{ABE}=\Sigma_{jk}(P_j^A\otimes P_k^B)\psi^{ABE}(P_j^A\otimes P_k^B)$. A simple and direct calculation using the triangle inequality gives $2p_{\mathrm{e}}\leq\mathrm{Tr}|\bar{\psi}^{AB}-\kappa^{AB}|$. Since ψ^{ABS} is an ϵ-approximate private state, $\mathrm{Tr}|\bar{\psi}^{ABE}-\kappa^{ABE}|\leq 2\epsilon$. Tracing out E does increase this distance, therefore $p_{\mathrm{e}}\leq\epsilon$.

To prove the analog statement for the conjugate basis, we must define a suitable $\tilde{\Lambda}^{BS}$. For this we adapt the corresponding measurement from the purification of κ^{ABE}, which is a private state. First bound the fidelity with the trace distance, using the fact that $1-\frac{1}{2}\mathrm{Tr}|\rho-\sigma|\leq F(\rho,\sigma)$ [38]. Thus $F(\bar{\psi}^{ABE},\kappa^{ABE})\geq 1-\epsilon$. Uhlmann's theorem asserts that for any purification $|\psi\rangle^{ABER}$ of $\bar{\psi}^{ABE}$, there exists a purification $|\kappa\rangle^{ABER}$ of κ^{ABE} such that $F(\bar{\psi}^{ABE},\kappa^{ABE})=F(|\psi\rangle^{ABER},|\kappa\rangle^{ABER})$. We can set $R=SA'B'$ and take the former purification to be $|\psi\rangle^{ABER}:=C^{AA'}C^{BB'}|\psi\rangle^{ABSE}|0\rangle^{A'}|0\rangle^{B'}$ for $C^{AA'}$ and $C^{BB'}$ unitary operations such that $C^{AA'}|k\rangle^A|0\rangle^{A'}=|k\rangle^A|k\rangle^{A'}$.

By definition, $|\kappa\rangle^{ABER}$ is an exact private state, and so is $|\kappa'\rangle^{ABER}:=C^{\dagger AA'}C^{\dagger BB'}|\kappa_p\rangle^{ABER}$. Since fidelity is invariant under a unitary transformation, $F(|\psi\rangle^{ABSE}|0\rangle^{A'}|0\rangle^{B'},|\kappa'\rangle^{ABER})=F(|\psi\rangle^{ABER},|\kappa\rangle^{ABER})$. Hence there exists $\Lambda_y'^{BR}$ such that measuring $\tilde{P}_x^A\otimes\Lambda_y'^{BR}$ on $|\kappa'\rangle^{ABER}$ produces the uniform distribution $\frac{1}{d}\delta_{xy}$. Making the same measurement on $|\psi\rangle^{ABSE}|0\rangle^{A'}|0\rangle^{B'}$ results in some probability distribution $\tilde{q}_{xy}$. Observe that measuring $\Lambda_y'^{BR}$ on $|\psi\rangle^{ABSE}|0\rangle^{A'}|0\rangle^{B'}$ is the same as measuring $\Lambda_y^{BS}:=\langle 00|^{A'B'}\Lambda_y'^{BR}|00\rangle^{A'B'}$ on $|\psi\rangle^{ABSE}$.

Since a quantum operation cannot decrease the fidelity, we immediately have $F(|\psi\rangle^{ABSE}|0\rangle^{A'}|0\rangle^{B'},|\kappa'\rangle^{ABER})\leq F(\tilde{q}_{xy},\frac{1}{d}\delta_{xy})$. But

$$F\left(\tilde{q}_{xy},\frac{1}{d}\delta_{xy}\right)=\frac{1}{\sqrt{d}}\sum_x\sqrt{\tilde{q}_{xx}}\leq\sqrt{\sum_{x\neq y}\tilde{q}_{xy}}=\sqrt{1-\tilde{p}_{\mathrm{e}}} \tag{A6}$$

by the concavity of the square root function. Collecting the inequalities, we find $\tilde{p}_{\mathrm{e}}\leq 2\epsilon-\epsilon^2$. ■

APPENDIX B: STATIC HSW THEOREM

Suppose a source described by the ensemble $\mathcal{E}=\{p_k,\varphi_k\}$ distributes classical letters $k\in\{0,1,\ldots,d-1\}$ to Alice and quantum states φ_k to Bob. Alice would like to communicate the value of k to Bob, using as few resources as possible. Bob already possesses some information about k in the form of φ_k, but in general cannot reliably distinguish between all these states. But Bob can learn k if Alice reveals some information about k, a "hint" that narrows the set of φ_k to some that he can reliably distinguish.

This is the "static" version, first studied in [55,56], of the standard HSW scenario in which Alice actively encodes the information s she wants to send to Bob using the signal ensemble $\mathcal{E}$ [23,24]. Typically this problem is considered in the asymptotic setting of many identical and independent samples from $\mathcal{E}$. Alice then encodes her information into a block of such samples and Bob performs a collective measurement, a version of the so-called pretty good measurement (PGM) [57], to decode the message. Properties of typical sequences and subspaces are used to prove that the PGM has a low probability of error.

Although in the main text we are concerned with using linear functions to generate the side information, in this appendix we shall consider the more general method of *universal hashing* [58] (also called 2-universal hashing), since it is not any more difficult and random linear functions are universal. In universal hashing, the hint is generated by choos-

ing a random $f:\{0,\ldots,d^n-1\}\to\{0,\ldots,m-1\}$ from a family $\mathcal{F}$ of hash functions and computing $t=f(x)$. Each function defines the subset $\mathcal{S}_t$ of possible inputs having the same output value; hopefully Bob will be able to distinguish between the elements of this set. The family is called universal when the probability of collision, $f(x)=f(y)$ for $x\neq y$, is the same as for random functions: $\Pr_f[f(x)=f(y)]\leq 1/m$. Put differently, the probability of any two elements being included in some $\mathcal{S}_t$ is also the same as if Alice chose the subsets completely at random, which is random enough for the procedure to work.

In the i.i.d. scenario, Alice and Bob share n copies of the state $\psi^{AB}=\Sigma_{k=0}^{d-1}p_k P_k^A\otimes\varphi_k^B$, which we write as $\Psi^{AB}=\Sigma_{\mathbf{k}}p_{\mathbf{k}}P_{\mathbf{k}}^A\otimes\varphi_{\mathbf{k}}^B$ for By the following static HSW theorem, a hint roughly of size $\log_2 m=n[H(p_k)-\chi(p_k,\varphi_k)]=n[H(Z^A)-I(Z^A:B)]$ suffices for Bob to learn k with exponentially small average probability of error.

Theorem 7 (Static HSW Theorem for Universal Hash Functions). *For n copies of an arbitrary state of the form $\psi^{AB}=\Sigma_{k=0}^{d-1}p_k P_k^A\otimes\varphi_k^B$, fix $\delta>0$. Then for a universal family of hash functions $f:\{0,\ldots,d^n-1\}\to\{0,\ldots,m-1\}$ where $\log_2 m=n[H(Z^A)-I(Z^A:B)+4\delta]$, there exist measurements $\Lambda_{f(\mathbf{k}),\ell}$ such that*

$$p_{\mathrm{e}}=\left\langle\sum_{\ell\neq\mathbf{k}}\mathrm{Tr}[\Lambda_{f(\mathbf{k}),\ell}\varphi_{\mathbf{k}}]\right\rangle_{f,\mathbf{k}}\leq 6\times 2^{-n\delta^2}. \tag{B1}$$

Proof. Fix a $\delta>0$ and start by Alice measuring her share of the state in the computational basis. With probability greater than $1-\epsilon$ for $\epsilon=e^{-n\delta^2/2}$, the resulting string $\mathbf{k}$ is typical, meaning $\mathbf{k}\in\mathcal{T}_\delta^n=\{\ell\cdot 2^{-nH(p_k)-n\delta}\leq p_{\hat{\ell}}\leq 2^{-nH(p_k)+n\delta})\}$ [59]. If $\mathbf{k}$ is not typical, the protocol aborts.

If it does not abort, Alice randomly picks f from a universal family $\mathcal{F}$ and sends $f(\mathbf{k})$ to Bob via the public channel. This narrows the set of possible $\mathbf{k}$ to the subset $\mathcal{C}_{f(\mathbf{k})}$ of typical elements of $\mathcal{S}_{f(\mathbf{k})}$. Bob will try to determine $\mathbf{k}$ by making a measurement to distinguish the φ_ℓ for $\ell\in\mathcal{C}_{f(\mathbf{k})}$. For this he uses the PGM defined by Eq. (11) in [23], which is represented by the POVM elements

$$\Lambda_{f(\mathbf{k}),\ell}^B=\left(\sum_{\ell\in\mathcal{C}_{f(\mathbf{k})}}QQ_\ell Q\right)^{-1/2}QQ_{\mathbf{k}}Q\left(\sum_{\ell\in\mathcal{C}_{f(\mathbf{k})}}QQ_\ell Q\right)^{-1/2}, \tag{B2}$$

where Q and $Q_{\mathbf{k}}$ are the projections into the typical subspaces (subspaces spanned by eigenstates with typical eigenvalues) of $\bar{\varphi}^{\otimes n}$ and $\varphi_{\mathbf{k}}$, respectively For a specific f and $\mathbf{k}$, a bound for the average error probability of this measurement is given by Eq. (17) of [23], except that we do not yet need to average over all codewords,

$$p_{\mathrm{e}}(\mathbf{k})\leq 3\ \mathrm{Tr}[\varphi_{\mathbf{k}}(\mathbb{1}-Q)]+\mathrm{Tr}[\varphi_{\mathbf{k}}(\mathbb{1}-Q_{\mathbf{k}})]+\sum_{\ell\in\mathcal{C}_{f(\mathbf{k})}}\mathrm{Tr}[Q\varphi_{\mathbf{k}}QQ_\ell]+\eta_{\mathbf{k}},$$

where $\eta_{\mathbf{k}}$ is 1 if $\mathbf{k}$ is typical and 0 otherwise. In our case, we are interested in the probability of error averaged over all f and $\mathbf{k}$, i.e., $\langle P_{\mathrm{e}}(\mathbf{k})\rangle_{f,\mathbf{k}}$. To compute it, we need the following relations (see [23] for details):

$$\mathrm{Tr}[\bar{\varphi}^{\otimes n}(\mathbb{1}-Q)]\leq\epsilon, \tag{B3}$$

$$\left\langle\mathrm{Tr}[\varphi_{\mathbf{k}}(\mathbb{1}-Q_{\mathbf{k}})]\right\rangle_{\mathbf{k}}\leq\epsilon, \tag{B4}$$

$$Q_{\mathbf{k}}\leq 2^{n\Sigma_i p_i S(\varphi_i)+n\delta}\varphi_{\mathbf{k}}, \tag{B5}$$

$$\sum_{\mathbf{k}\in\mathcal{T}_\delta^n}\varphi_{\mathbf{k}}\leq 2^{nH(p_i)+n\delta}\bar{\varphi}^{\otimes n}, \tag{B6}$$

$$\|Q\bar{\varphi}^{\otimes n}Q\|_\infty\leq 2^{-nS(\bar{\varphi})+n\delta}, \tag{B7}$$

where $\|M\|_\infty$ is the maximal eigenvalue of M. Since $\langle\varphi_{\mathbf{k}}\rangle_{\mathbf{k}}=\bar{\varphi}^{\otimes n}$, we have

$$\langle P_{\mathrm{e}}(\mathbf{k})\rangle_{\mathbf{k},f}\leq 5\epsilon+\left\langle\sum_{\boldsymbol{\mu}\in\mathcal{C}_{f(\mathbf{k})}}\mathrm{Tr}[Q\varphi_{\mathbf{k}}QQ_{\boldsymbol{\mu}}]\right\rangle_{\mathbf{k},f}\leq 5\epsilon+\left\langle\sum_{\boldsymbol{\mu}\in\mathcal{T}_\delta^n}\Pr_f[f(\boldsymbol{\mu})=f(\mathbf{k})]\mathrm{Tr}[Q\varphi_{\mathbf{k}}QQ_{\boldsymbol{\mu}}]\right\rangle_{\mathbf{k}}.$$

Straightforward calculations give

$$\langle P_{\mathrm{e}}(\mathbf{k})\rangle_{\mathbf{k},f}\leq 5\epsilon+\frac{1}{m}2^{nH(p_i)+n\Sigma_i p_i S(\varphi_i)+2n\delta}\mathrm{Tr}[Q\bar{\varphi}^{\otimes n}Q\bar{\varphi}^{\otimes n}]\leq 5\epsilon+\frac{1}{m}2^{nH(p_i)-nS(\bar{\varphi})+n\Sigma_i p_i S(\varphi_i)+3n\delta},$$

where for the last step we use the relation $\mathrm{Tr}[Q\bar{\varphi}^{\otimes n}Q\bar{\varphi}^{\otimes n}]\leq\|Q\bar{\varphi}^{\otimes n}Q\|_\infty\mathrm{Tr}[\bar{\varphi}^{\otimes n}]=\|Q\bar{\varphi}^{\otimes n}Q\|_\infty$. Choosing $\log_2 m\geq n[H(p_i)-S(\bar{\varphi})+\Sigma_i p_i S(\varphi_i)+4\delta]$ completes the proof. ■

APPENDIX C: UNIVERSAL DISTRIBUTION FOR STABILIZERS OF CSS CODES

The question we explore in this appendix is how to pick a family of CSS codes such that both the Z- and X-type stabilizers are universal hash functions. The problem is that the two stabilizers are not independent; they must commute with each other. The Z and X stabilizers can be represented by an m_z by n matrix M_z and the m_x by n matrix M_x, respectively, where each entry is an integer modulo d. We have the following:

Lemma 3. Consider the set of all m_x+m_z by n matrices R such that each row is orthogonal to the others and where each entry is an integer modulo a prime number d. Let M_z be the first m_z rows of R, and M_x be the last m_x rows of R. Then the linear functions associated with M_z and M_x are both universal.

Proof. Let $\mathbf{r}_i$ be the ith row of R. All possible strings have the same probability to be $\mathbf{r}_1$. Therefore, for any distinct n dit-strings $\mathbf{k}$ and $\mathbf{k}'$, $\Pr_R[\mathbf{r}_1\cdot\mathbf{k}=\mathbf{r}_1\cdot\mathbf{k}']=\frac{1}{d}$. This is not generally true if d is not prime. Now we proceed by induction. Assume that we have a set R_ℓ of strings $\mathbf{r}_1$, $\mathbf{r}_2$, … and $\mathbf{r}_\ell$ such that $\Pr_R[\mathbf{r}_i\cdot\mathbf{k}=\mathbf{r}_i\cdot\mathbf{k}'\,|\,1\leq i\leq\ell]\leq\frac{1}{d^\ell}$. Conditional on R_ℓ, the next row $\mathbf{r}_{\ell+1}$ is uniformly distributed over the space of strings orthogonal to the set R_ℓ. If $\mathbf{r}_j\cdot\mathbf{k}\neq\mathbf{r}_j\cdot\mathbf{k}'$ for some $1\leq j\leq\ell$, then $\Pr[\mathbf{r}_i\cdot\mathbf{k}=\mathbf{r}_i\cdot\mathbf{r}'\,|\,1\leq i\leq\ell+1]=0$. So we can consider only the case in which $\mathbf{r}_i\cdot\mathbf{k}=\mathbf{r}_i\cdot\mathbf{k}'$ for all $1\leq i\leq\ell$. In that situation, $\mathbf{k}-\mathbf{k}'$ can be expended in any basis of the space orthogonal to R_ℓ (the coefficients being integers from 0 to $d-1$). Pick one such basis. $\mathbf{r}_{\ell+1}$ is uniformly distributed

over all strings that are spanned by this basis, therefore $\Pr_{R\cdot R_\ell}[\mathbf{r}_{\ell+1}\cdot\mathbf{k}=\mathbf{r}_{\ell+1}\cdot\mathbf{k}']=\frac{1}{d}$, where we assumed $\mathbf{r}_i\cdot\mathbf{k}=\mathbf{r}_i\cdot\mathbf{k}'$ for all $1\leq i\leq\ell$. Including all possible cases, we deduce that $\Pr_R[\mathbf{r}_i\cdot\mathbf{k}=\mathbf{r}_i\cdot\mathbf{k}'\cdot 1\leq i\leq\ell+1]<\frac{1}{d^{\ell+1}}$.

Since there is no distinction between the order of the rows of R, we conclude that any function associated with a matrix composed of a subset of rows of R is universal. ■

APPENDIX D: ON THE ONE-SHOT DISTILLATION THEOREM

Parameter estimation aside, Theorem 4 is stronger than the security proof of [10]. Constructing an example where this is the case is not too difficult and we will simply give an example in which the optimal $\tilde{\Lambda}_\beta^{BS}$ for guessing Alice's conjugate basis measurement is not independent of β. Consider two copies (i.e., $n=2$) of the state

$$|\psi\rangle^{ABSE}=\frac{1}{2}(|0\rangle^A|0\rangle^B+|1\rangle^A|1\rangle^B)|\phi_0\rangle^S|0\rangle^E + \frac{1}{2}(|0\rangle^A|0\rangle^B-|1\rangle^A|1\rangle^B)|\phi_1\rangle^S|1\rangle^E,$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are two different nonorthogonal states. Bob can guess Alice's key without an error by measuring his state in the computational basis. His ability to predict the conjugate basis will depend on the overlap of $|\phi_0\rangle$ and $|\phi_1\rangle$. Assuming this is not nearly maximal, Alice will have to provide Bob with some additional information, which in this case would be the result of measuring some set of stabilizers. Measuring two stabilizers defeats their purpose, since then no secret key can be distilled. Hence Alice measures either $X\otimes X$, $X\otimes\mathbf{1}$, or $\mathbf{1}\otimes X$. The case where $X\otimes\mathbf{1}$ or $\mathbf{1}\otimes X$ is used simply reduces to the case in which Alice and Bob only share one state $|\psi\rangle^{ABSE}$. In that case, Bob's minimum error probability of guessing Alice's measurement in the conjugated basis is given by $\frac{1}{2}-\frac{1}{2}\sqrt{1-|\langle\phi_0|\phi_1\rangle|^2}$ (which follows from Helstrom's result [33] for pure states) and the measurement used is independent of β. However, if $X\otimes X$ is used instead, then the minimum error probability of the optimal measurement given any β is $\frac{1}{2}-\frac{1}{2}\sqrt{1-|\langle\phi_0|\phi_1\rangle|^4}$, which is smaller than $\frac{1}{2}-\frac{1}{2}\sqrt{1-|\langle\phi_0|\phi_1\rangle|^2}$. For each value of β, the optimal measurement is, for $\beta=0$, the two projections $\hat{P}_\pm^{\beta=0}$ on the range of the positive and negative parts of $(\phi_0^S)^{\otimes 2}-(\phi_1^S)^{\otimes 2}$ and the extra projection so that the sum of them is $\mathbf{1}$. For $\beta=1$, the optimal measurement is the two projections $\hat{P}_\pm^{\beta=1}$ on the range of the positive and negative parts of $\phi_0^S\otimes\phi_1^S-\phi_1^S\otimes\phi_0^S$ added with an extra projection so that the sum of them is $\mathbf{1}$. Since the projection $\hat{P}_+^{\beta=0}$ overlaps with both $\hat{P}_\pm^{\beta=1}$, the optimal measurement $\tilde{\Lambda}_\beta^{BS}$ cannot be independent of β.

Despite this example, we have not shown that the asymptotic rates of some protocols (for $n\to\infty$) could not be achieved using a measurement $\tilde{\Lambda}^{BS}$ that is independent of β, but it seems reasonable to conjuncture that this is the case. Even if it were unnecessary, allowing $\tilde{\Lambda}^{BS}$ to depend on β does help to prove Theorems 5 and 6.

[1] D. Mayers, in *Advances in Cryptology—CRYPTO '96*, Vol. 1109/1996 of Lecture Notes in Computer Science (Springer, Berlin, 1996), pp. 343–357.
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[5] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[6] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[7] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
[8] J. M. Renes and M. Grassl, Phys. Rev. A **74**, 022317 (2006).
[9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[10] M. Koashi, J. Phys.: Conf. Ser. **36**, 98 (2006).
[11] M. Koashi, e-print arXiv:quant-ph/0609180 (2006).
[12] I. Csiszar and J. Korner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[13] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[14] R. Renner and R. König, in *Second Theory of Cryptography Conference* (Springer, Cambridge, MA, 2005), Vol. 3378, pp. 407–425.
[15] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[16] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[17] R. Renner, Ph.D. thesis, ETH Zürich (2006).
[18] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, e-print arXiv:quant-ph/0506189v2 (2008).
[20] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[21] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[22] M. Koashi, e-print arXiv:0704.3661 (2007).
[23] A. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[24] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[25] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[26] B. Schumacher and M. D. WestmorelandPhys. Rev. Lett. **80**, 5695 (1998).
[27] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).
[28] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[29] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).
[30] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[31] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[32] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys.

Rev. Lett. **88**, 127902 (2002);
[33] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Vol. 123 of Mathematics in Science and Engineering (Academic, London, 1976).
[34] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Second Theory of Cryptography Conference* (Springer, Cambridge, MA, 2005), Vol. 3378, pp. 386–406.
[35] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[36] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[37] The other major step in a complete proof is a parameter estimation scheme to determine what state Alice and Bob share, given their measurement results.
[38] C. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).
[39] J. M. Renes and G. Smith, Phys. Rev. Lett. **98**, 020502 (2007).
[40] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[41] H.-K. Lo, New J. Phys. **5**, 36 (2003).
[42] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, IEEE Trans. Inf. Theory **54**, 2604 (2008)
[43] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[44] P. W. Shor, The Quantum Channel Capacity and Coherent Information, MSRI Seminar (2002); http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1
[45] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[46] M. Horodecki, S. Lloyd, and A. Winter, Open Syst. Inf. Dyn. **15**, 47 (2008).
[47] P. Hayden, M. Horodecki, J. Yard, and A. Winter, Open Syst. Inf. Dyn. **15**, 7 (2008).
[48] P. Hayden, P. W. Shor, and A. Winter, Open Syst. Inf. Dyn. **15**, 71 (2008).
[49] D. Kretschmann, D. Schlingemann, and R. F. Werner, IEEE Trans. Inf. Theory **54**, 1708 (2008).
[50] D. Kretschmann, D. Schlingemann, and R. F. Werner, e-print arXiv:0710.2495 (2007).
[51] D. Kretschmann, D. W. Kribs, and R. W. Spekkens, e-print arXiv:0711.3438 (2007).
[52] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[53] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[54] J. M. Renes and J.-C. Boileau, e-print arXiv:0806.3984v1 (unpublished).
[55] A. Winter, Ph.D. thesis, Universität Bielefeld (1999).
[56] I. Devetak and A. Winter, Phys. Rev. A **68**, 042301 (2003).
[57] P. Hausladen and W. K. Wootters, J. Mod. Opt. **41**, 2385 (1994).
[58] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
[59] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, New York, 1991).