PHYSICAL REVIEW A **85**, 052310 (2012)

Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning

Agnes Ferenczi* and Norbert Lütkenhaus

Institute for Quantum Computing & Department for Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1, Waterloo, Ontario, Canada

(Received 26 January 2012; published 16 May 2012)

We investigate the connection between the optimal collective eavesdropping attack and the optimal cloning attack where the eavesdropper employs an optimal cloner to attack the quantum key distribution (QKD) protocol. The analysis is done in the context of the security proof in Refs. [Proc. R. Soc. London A **461**, 207 (2005); Phys. Rev. Lett. **95**, 080501 (2005)] for discrete variable protocols in d-dimensional Hilbert spaces. We consider a scenario in which the protocols and cloners are equipped with symmetries. These symmetries are used to define a quantum cloning scenario. We find that, in general, it does not hold that the optimal attack is an optimal cloner. However, there are classes of protocols, where we can identify an optimal attack by an optimal cloner. We analyze protocols with 2, d and $d+1$ mutually unbiased bases where d is a prime, and show that for the protocols with 2 and $d+1$ mutually unbiased bases (MUBs) the optimal attack is an optimal cloner but, for the protocols with d MUBs, it is not. Finally, we give criteria to identify protocols which have different signal states, but the same optimal attack. Using these criteria, we present qubit protocols which have the same optimal attack as the Bennett-Brassard 1984 (BB84) protocol or the 6-state protocol.

DOI: 10.1103/PhysRevA.85.052310 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Aa

I. INTRODUCTION

The objective of quantum key distribution (QKD) is to establish a secret key between two legitimate parties (Alice and Bob), that is unknown to an eavesdropper (Eve). The secret key can be used later in cryptographic applications, for example to facilitate secure communication.

To start a QKD protocol Alice prepares quantum states (signal states) and sends them through a quantum channel to Bob, who performs measurements on them. These types of protocols are referred to as prepare-and-measure protocols and result in quantum mechanically correlated classical data being shared between Alice and Bob. They can extract a secret key from this data using classical communication protocols. For this to succeed, Alice and Bob need to be able to upper bound the amount of information Eve can gain on the correlated data. This information comes from an interaction of Eve with the signals. For any such attack, there is a tradeoff between the amount of information that leaks to Eve and the amount of disturbance that she causes to the signal states. From the observation of this disturbance, Alice and Bob can estimate Eve's information on the data and perform suitable communication protocols to distill secret keys from their data on which Eve has no information.

In this paper, we deal with the problem of finding the optimal interaction between Eve and the signals. Our approach to the security analysis is to restrict Eve to collective attacks [1,2] in which she interacts with each signal separately as the range of the validity of this attack can be shown to extend to the most general attack (see Sec. III). A collective attack is completely determined by a unitary interaction U_E between the signal states and some additional ancilla states held by Eve. The optimal attack which gives the highest amount of information to Eve (by some suitable measure) for a given amount of disturbance is denoted by U_E^{opt}.

One specific type of interaction is an optimal quantum cloner [3]. An optimal cloner is a unitary transformation U_C^{opt} that acts on the signal states and some ancilla states, with the objective of producing two copies of the signal states. The optimal cloner has the property that the copies emerge with the highest fidelity (with respect to the original signal states) allowed by quantum mechanics. An optimal cloner is called symmetric if the fidelities of the two copies are the same and asymmetric if the fidelities are different. Consider now the following eavesdropping attack: Eve uses an optimal asymmetric cloner to copy the signal states sent by Alice, forwards one copy to Bob, and keeps the other copy for herself. She chooses the optimal cloner in such a way that the fidelity of Bob's copy is in agreement with Bob's measurement outcomes. In Refs. [4–6], such cloning attacks were used to model Eve's attack, but optimality was only conjectured. Indeed, for some protocols [e.g., the Bennett-Brassard 1984 (BB84) [7] or the 6-state protocol [8]], the optimal attack is known to be an optimal cloner, but in general the relationship between optimal cloning and optimal eavesdropping is unknown.

The goal of the present work is to establish the connection between optimal eavesdropping on QKD protocols and optimal cloning in the context of the security definition in Refs. [1,2] for protocols with direct, one-way reconciliation. We consider protocols with symmetries so that, without loss of generality, the optimal attack is found in a set with a corresponding symmetry. In this scenario, it turns out that a necessary condition for an optimal cloner to be a candidate for an optimal attack is the strong covariance condition [9]. This condition ensures that the optimal cloner and the optimal attack are drawn from the same set, and that the optimal cloner uses the same number of ancilla states as the optimal eavesdropping attack. If strong covariance does not hold for the optimal cloner

*aferenczi@iqc.ca

 ©2012 American Physical Society

defined by the signal states of the QKD protocol, we can already conclude that the optimal attack on the QKD protocol is not an optimal cloner.

In this paper, we calculate the optimal attack for qubit-based protocols (e.g., the BB84 and the 6-state protocol) and for protocols in d-dimensional Hilbert spaces using mutually unbiased bases (MUBs) (e.g., protocols with 2 MUBs, $d+1$ MUBs [4] or d MUBs) and compare the results to the optimal cloner. The security of these protocols has been studied previously in Refs. [4,6,8,10–12]. In Ref. [13], in particular, the security was proven for protocols with 2 and $d+1$ MUBs using the security proof methods of Refs. [1,2].

Additionally, we observe that some groups of QKD protocols that share some common symmetry features can be proven to have the same optimal attack, despite having different sets of signal states. As an example, we present qubit protocols which have the same optimal attack as the BB84 protocol or the 6-state protocol, and we give criteria to identify protocols with the same optimal attack.

This paper is organized as follows: In Sec. II we describe prepare-and-measure protocols using a thought setup that includes entangled states and is referred to as the source-replacement scheme. In Sec. III we summarize the security proofs given in Refs. [1,2]. In Sec. IV, we provide two theorems about the convexity and concavity properties, as well as a lemma about the invariance property of the classical mutual information and the Holevo quantity. In Sec. V we describe protocols with a symmetry in the signal states. Under the assumption that Alice and Bob use only averaged measurement quantities and that the classical postprocessing respects certain symmetry properties, we show that the symmetries of the signal states can be transferred to Eve's interaction. This holds true in particular for the class of protocols where the signal states are composed of complete sets of basis states, and where Alice and Bob discard data where they disagree on the basis after the measurement. The formalism of quantum cloners is summarized in Sec. VI along the lines of Ref. [9]. The main statement of Sec. VII is that the optimal cloner must be strongly covariant in order to be an optimal attack. However, strong covariance alone does not yet uniquely determine if the optimal attack is an optimal cloner. We summarize the features of the class of protocols where the signal states are invariant under the generalized Pauli group, for which the corresponding cloning attack is known to be strong covariant. In Sec. VIII we give examples of protocols which use the mutually unbiased eigenbases of the generalized Pauli operators and analyze the relation between the optimal attack and the optimal cloner. In Sec. IX we provide a theorem for the class of protocols with complete sets of basis states and basis sifting, which allows us to determine when the optimal attacks of different protocols in this class are the same. Finally, we draw conclusions in Sec. X.

II. SOURCE-REPLACEMENT SCHEME

A typical QKD protocol consists of a quantum and a classical phase. In the quantum phase, Alice chooses signal states $|\varphi_x\rangle$ from a set $\mathbf{S}$ with probability $p(x)$ defined on a d-dimensional Hilbert space. She sends the signal states through a quantum channel to Bob, who performs measurements on them by means of a positive operator valued measures (POVM) $\mathbf{M}_B = \{B_y\}$, resulting in a joint probability distribution $p(x,y)$. This signal preparation scheme is typically called a prepare-and-measure scheme. In the classical phase, Alice and Bob perform error correction and privacy amplification in order extract a secret key from their measurement data.

The security proof of a protocol is more conveniently described in the source-replacement scheme, which is equivalent to the prepare-and-measure scheme. The source-replacement scheme is a thought setup in which Alice creates the bipartite entangled state (source state)

$$|\Phi\rangle = \sum_x \sqrt{p(x)}|x\rangle_X|\varphi_x\rangle_S \tag{1}$$

in her laboratory, keeps the first half for herself and sends the other half to Bob. The states $|x\rangle$ form an orthonormal basis $\mathcal{X} = \{|x\rangle;\ x = 0,\ldots,|\mathbf{S}|-1\}$ of an $|\mathbf{S}|$-dimensional Hilbert space $\mathcal{H}_X$. In order to prepare the state $|\varphi_x\rangle$ at Bob's side, Alice performs a projective measurement in the basis $\mathcal{X}$, which triggers the source state to collapse onto the conditional state $|\varphi_x\rangle$ with probability $p(x)$.

If the signal states are linearly dependent, we can rewrite the source state in a more compact form using the Schmidt decomposition of pure states. For this purpose, we define a d-dimensional subsystem $\mathcal{H}_A$ of $\mathcal{H}_X$ and express the source state on the "compressed" space $\mathcal{H}_A \otimes \mathcal{H}_S$:

$$|\Phi\rangle_{AS} = \sum_{i=0}^{d-1} \sqrt{\kappa_i}|\bar{i}\rangle_A|i\rangle_S. \tag{2}$$

In this expression the Schmidt basis $\mathcal{B} = \{|i\rangle_S;\ i = 0,\ldots,d-1\}$ of system S and the Schmidt coefficients $\sqrt{\kappa_i}$ are defined as the eigenbasis and the square roots of the eigenvalues of the reduced operator $\phi_S = \mathrm{tr}_X\{|\Phi\rangle_{XS}\langle\Phi|\}$. The Schmidt basis $\mathcal{A} = \{|\bar{i}\rangle_A;\ i = 0,\ldots,d-1\}$ of system A can be explicitly given by the orthonormal vectors $|\bar{i}\rangle = \sum_x \sqrt{p(x)}\alpha_i^{(x)}|x\rangle/\sqrt{\kappa_i}$, where the $\alpha_i^{(x)} = \langle i|\varphi_x\rangle$ are the coefficients of the signal states in the Schmidt basis $\mathcal{B}$. In the following, we omit the bar in $|\bar{i}\rangle$ for simplicity.

Furthermore, Alice's von Neumann measurement in the basis $\mathcal{X}$ on the larger space $\mathcal{H}_X$ is the Naimark extension of a measurement $\mathbf{M}_A = \{A_x\}$ with respect to rank-one POVM elements A_x on the smaller space $\mathcal{H}_A$ given by

$$A_x = p(x)\sqrt{\rho_A}^{-1}|\varphi_x^*\rangle\langle\varphi_x^*|\sqrt{\rho_A}^{-1}. \tag{3}$$

Here we define the density matrix of Alice's reduced state as

$$\rho_A = \mathrm{tr}_S\{|\Phi\rangle_{AS}\langle\Phi|\}, \tag{4}$$

and the states

$$|\varphi_x^*\rangle = \sum_i |i\rangle\langle\varphi_x|i\rangle = \sum_i |i\rangle\big(\alpha_i^{(x)}\big)^*, \tag{5}$$

where the symbol $*$ denotes the complex conjugate with respect to the Schmidt basis $\mathcal{A}$. The operators A_x are positive, sum up to the identity, and satisfy the property $\mathrm{tr}_A\{A_x \otimes \mathbb{1}|\Phi\rangle\langle\Phi|\} = p(x)|\varphi_x\rangle\langle\varphi_x|$.

After Eve's interaction with the signal states, but prior to Alice and Bob's measurements, the state held by Alice and Bob is described by an unknown (mixed) state ρ_{AB} instead of a perfect copy of the source state. Nevertheless, Alice and Bob have some information about ρ_{AB} due to their measurements.

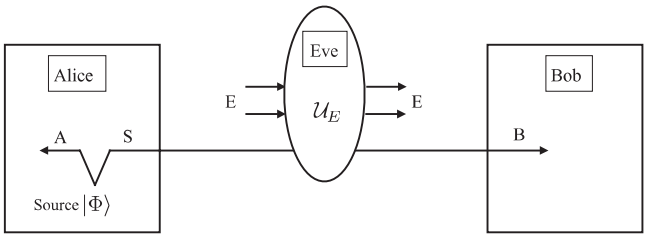

FIG. 1. In the source-replacement scheme, Alice prepares the entangled state $|\Phi\rangle$. The system A is kept by Alice, while the system S is sent through the quantum channel to Bob. Eve attaches ancillae to the signal states and performs a unitary transformation on the joint system SE, transforming it to BE. She resends the system B to Bob. After Eve's interaction, Alice and Bob no longer share a perfect copy of $|\Phi\rangle$, but a bipartite state ρ_{AB}, which is only partially characterized by their observations.

They can constrain the form of ρ_{AB} from the probability distribution of their measurement outcomes

$$p(x,y) = \mathrm{tr}\{A_x \otimes B_y\ \rho_{AB}\} \tag{6}$$

in a process called parameter estimation. In addition, Alice and Bob know that Alice's reduced density matrix of ρ_{AB} remains unchanged, as already anticipated in Eq. (4), because the system A never leaves Alice's laboratory (see Fig. 1). However, unless Alice and Bob's measurements are sufficient to obtain a tomographically complete parametrization of ρ_{AB}, there could be many states ρ_{AB} that are compatible with $p(x,y)$ and ρ_A. For what follows, it is useful to make the following definition:

Definition 1. The set $\mathbf{\Gamma}$ contains all bipartite states ρ_{AB} that are compatible with the measurement outcomes $p(x,y)$ and that have a given reduced state ρ_A.

In the source-replacement scheme Eve attaches ancillae (defined on the system E) to the second half of the source state $|\Phi\rangle_{AS}$ followed by a unitary transformation U_E which takes the composite system SE to BE. She then keeps the transformed ancillae for herself, and resends the remaining system B to Bob (see Fig. 1). The mixed state ρ_{AB} is the result of Eve's interaction with the signal states. Eve's unitary transformation U_E is equivalently characterized by the purification $|\Psi\rangle_{ABE}$ of ρ_{AB} on the dilated space $\mathcal{H}_{ABE}$, where the dimension of the purifying system E is the same as the dimension of AB. In order to guarantee unconditional security of the protocol, we must assume that Eve can exploit everything allowed by quantum mechanics for her attack, which is realized by giving her full control over $|\Psi\rangle_{ABE}$.

Note that, to each ρ_{AB}, an entire class of purifications $|\Psi\rangle^W_{ABE} = \mathbb{1}_{AB} \otimes W_E|\Psi\rangle_{ABE}$ can be constructed, where W is local unitary transformation on Eve's system. In what follows such local transformations on Eve's system are irrelevant.

III. KEY RATE

The security proof presented in Refs. [1,2,14] provides a bound on the rate at which Alice and Bob can extract a secret key. The proof is valid for collective attacks and for one-way classical communication. In many cases the proof can also be extended to hold for coherent attacks and two-way communication [15,16].

Assume that Alice, Bob, and Eve share the purification $|\Psi\rangle$ of the state ρ_{AB}. After Alice and Bob measure their systems with respect to A_x and B_y, they share the tripartite classical-classical-quantum (ccq) state [1]

$$\rho_{XYE} = \sum_{x,y} p(x,y)|x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho_E^{xy}, \tag{7}$$

where $|x\rangle$ and $|y\rangle$ are two sets of orthonormal bases, and $\rho_E^{xy} = \mathrm{tr}_{AB}\{A_x \otimes B_y \otimes \mathbb{1}_E|\Psi\rangle\langle\Psi|\}/p(x,y)$ are Eve's quantum states conditioned on the event that Alice and Bob's outcomes were x and y.

Using error correction and privacy amplification, Alice and Bob extract a secret key from the ccq state ρ_{XYE}. A typical choice for the error correction is one-way reconciliation, in which the data of one party is set as a reference for the key, and the other party must correct her or his noisy data to match the reference. For our purposes, we will consider protocols with direct reconciliation; that is, Alice's data serves as the reference key and Bob corrects his data accordingly. The rate, established in Refs. [1,2,14], at which an unconditionally secure key against collective attacks can be extracted is given by

$$r(\rho_{XYE}) = I(X:Y) - \chi(X:E), \tag{8}$$

where $I(X:Y) = H(X) + H(Y) - H(X,Y)$ is the classical mutual information of Alice and Bob's data, and $\chi(X:E) = H(X) + S(E) - S(X,E)$ is the Holevo quantity or quantum mutual information between Alice and Eve. H and S denote the Shannon entropy and the von Neumann entropy, respectively. The Holevo quantity is explicitly given by

$$\chi(X:E) = S(\rho_E) - \sum_x p(x) S\left(\rho_E^x\right), \tag{9}$$

where ρ_E^x is Eve's state conditioned on Alice's value x and $\rho_E = \sum_x p(x)\rho_E^x$ is Eve's reduced state. For the practical calculation of the Holevo quantity, an explicit reference to the system E can be eliminated, because the entropies $S(\rho_E)$ and $S(\rho_E^x)$ can be expressed in terms of quantities on the systems AB: If the state $|\Psi\rangle$ is pure, then $S(\rho_{AB}) = S(\rho_E)$. If, furthermore, Alice uses rank-one POVM elements, then the conditional states $\rho_{BE}^x = \mathrm{tr}_A\{A_x \otimes \mathbb{1}_{BE}|\Psi\rangle\langle\Psi|\}/p(x)$ are pure, and therefore $S(\rho_E^x) = S(\rho_B^x)$. In this situation, the Holevo quantity simplifies to

$$\chi(X:E) = S(\rho_{AB}) - \sum_x p(x) S\left(\rho_B^x\right). \tag{10}$$

Usually, the key is not directly extracted from the state ρ_{XYE}, because the data $p(x,y)$ might be only weakly correlated. Alice and Bob typically postselect on highly correlated data before proceeding with the protocol. For example, Alice and Bob might ignore events which they measured in different bases—so-called basis sifting—or they might discard data, where Bob did not record a detection event. Effectively, the key is extracted from a postselected state $\mathcal{E}(\rho_{AB})$, which has again two classical registers XY on Alice and Bob's side and a quantum register E on Eve's side, but also additional classical registers carrying the information about the communication (announcements) between Alice and Bob that arise during the postselection.

Here we give a short description of the postselection that leads to $\mathcal{E}(\rho_{AB})$. For a more detailed formalism see Appendix A: Alice and Bob announce some information about each signal to the public, that typically does not reveal any direct knowledge about the secret key. In the case of the sifting process, for example, they announce their basis choices. Depending on the announcement, the signal is either kept or discarded. Let us denote the announcements of the kept signals by u. On the level of the quantum state ρ_{AB}, the measurement with respect to $\mathbf{M}_A$ and $\mathbf{M}_B$ followed by the announcement and the discarding is equivalently described by first a filtering operation on ρ_{AB} followed by new measurements. The filtering yields transformed states ρ^u_{AB} depending on the announcement u. The state held by Alice and Bob before the new measurement is then a convex combination of states ρ^u_{AB} over the classical subsets u with probability $p(u)$

$$\rho = \sum_u p(u)\rho^u_{AB} \otimes |u\rangle\langle u|. \tag{11}$$

The new measurement is then performed on each ρ^u_{AB} independently. In order to preserve the probability distributions of the measurement outcomes, we identify new pairs of POVMs $\mathbf{M}^u_A$ and $\mathbf{M}^u_B$ conditioned on the announcement u. By giving to Eve the purification of each ρ^u_{AB}, we obtain new ccq states ρ^u_{XYE} for each announcement u after the measurement with respect to $\mathbf{M}^u_A$ and $\mathbf{M}^u_B$. The effective state $\mathcal{E}(\rho_{AB})$ after the postselection is then described by the convex combination

$$\mathcal{E}(\rho_{AB}) = \sum_u p(u)\rho^u_{XYE} \otimes |u\rangle\langle u|. \tag{12}$$

If we choose to extract the key from each ρ^u_{XYE} independently, the effective key rate is given by

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \sum_u p(u) r\left(\rho^u_{XYE}\right), \tag{13}$$

where r is the key rate given in Eq. (8). Other choices of key extraction may combine different outcomes into one stream, but here we choose to analyze the simpler case of separate processing.

By defining the total Holevo quantity and the total mutual information by

$$\bar{\chi}\left(\mathcal{E}(\rho_{AB})\right) := \sum_u p(u)\chi_u(X:E), \tag{14}$$

$$\bar{I}\left(\mathcal{E}(\rho_{AB})\right) := \sum_u p(u) I_u(X:Y), \tag{15}$$

where $\chi_u(X:E)$ and $I_u(X:Y)$ are the Holevo quantity and the mutual information of the state ρ^u_{XYE}, we can rewrite the effective key rate as

$$\bar{r}\left(\mathcal{E}(\rho_{AB})\right) = \bar{I}\left(\mathcal{E}(\rho_{AB})\right) - \bar{\chi}\left(\mathcal{E}(\rho_{AB})\right). \tag{16}$$

If Alice and Bob knew Eve's attack strategy, the calculation of the key rate would be straightforward. However, all Alice and Bob know is that they share a state ρ_{AB} from the set $\mathbf{\Gamma}$ in Def. 1. Therefore, Eve has the freedom to chose any attack, as long as it creates a state ρ_{AB} that is compatible with $\mathbf{\Gamma}$. Among all these possible attacks, the one that generates the lowest key rate

$$r_{\min} = \inf_{\rho_{AB}\in\mathbf{\Gamma}} \bar{r}(\mathcal{E}(\rho_{AB})) \tag{17}$$

is defined as the optimal attack. We call the pure state corresponding to the optimal attack $|\Psi\rangle^{\text{opt}}$ with the reduced state ρ^{opt}_{AB}. If Alice and Bob want to guarantee that their protocol is secure, they must assume that Eve performed the optimal attack. Hence, they cannot generate a secret key at a rate higher than $r_{\min}$ for the given protocol.

IV. PROPERTIES OF MUTUAL INFORMATION AND HOLEVO QUANTITY

In this section we give three properties of the classical mutual information and the Holevo quantity.

At first, we introduce a new notation for the mutual information and the Holevo quantity that is more convenient for our purposes throughout the rest of this paper. Let Alice and Bob share a quantum state ρ_{AB}, which they measure with respect to the POVM $\mathbf{M}_{AB} = \{A_x \otimes B_y : A_x \in \mathbf{M}_A, B_y \in \mathbf{M}_B\}$. We always assume that Eve holds the purification $|\Psi\rangle$ of ρ_{AB}. Instead of denoting $I(X:Y)$ with the dependence on the registers XY, we denote the mutual information by

$$I(\rho_{AB}, \mathbf{M}_{AB}) := I(X:Y). \tag{18}$$

By specifying the quantum state ρ_{AB} and the POVM $\mathbf{M}_{AB}$, the measured state on the registers XY is entirely defined. On the other hand, the Holevo quantity can be directly calculated from the classical-quantum (cq) state ρ_{XE} that emerges after Alice's measurement of $|\Psi\rangle$ and after tracing over Bob's system. We write

$$\chi(\rho_{AB}, \mathbf{M}_A) := \chi(X:E) \tag{19}$$

for the Holevo quantity, implying that there is a step from ρ_{AB} to $|\Psi\rangle$.

In the first theorem of this section we show that the classical mutual information $I(\rho_{AB},\mathbf{M}_{AB})$ is convex over ρ_{AB} with fixed probability distribution $p(x) = \text{tr}\{A_x\ \rho_A\}$. We call this feature "weak convexity" to indicate that convexity only holds with the restriction on $p(x)$.

Theorem 1 (weak convexity). Given the states ρ_{AB}, σ_{AB} and the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$ for $\lambda \in [0,1]$ with probability distributions $p(x,y) = \text{tr}\{A_x \otimes B_y\ \rho_{AB}\}$, $q(x,y) = \text{tr}\{A_x \otimes B_y\ \sigma_{AB}\}$ and $\bar{p}(x,y) = \lambda p(x,y) + (1-\lambda)q(x,y)$. If the probability distributions satisfy $p(x) = q(x)$ for all x, then the mutual information is convex in the sense that

$$I(\bar{\rho}_{AB},\mathbf{M}_{AB}) \leqslant \lambda I(\rho_{AB},\mathbf{M}_{AB}) + (1-\lambda) I(\sigma_{AB},\mathbf{M}_{AB}). \tag{20}$$

The proof of this theorem is given in Appendix B.

Second, we show that the Holevo quantity $\chi(\rho_{AB},\mathbf{M}_A)$ is concave as a function of ρ_{AB}.

Theorem 2 (concavity). Given the states ρ_{AB}, σ_{AB} and the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$ for $\lambda \in [0,1]$. Then, the Holevo quantity is concave, meaning that it satisfies the property

$$\chi(\bar{\rho}_{AB}, \mathbf{M}_A) \geqslant \lambda\chi(\rho_{AB}, \mathbf{M}_A) + (1-\lambda)\chi(\sigma_{AB}, \mathbf{M}_A). \tag{21}$$

The proof of this theorem is in Appendix C.

Since we use postselection in our protocols, we need to extend these theorems to hold for the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ in the following sense:

$$\bar{r}(\mathcal{E}(\bar{\rho}_{AB})) \leqslant \lambda \bar{r}(\mathcal{E}(\rho_{AB})) + (1-\lambda)\bar{r}(\mathcal{E}(\sigma_{AB})). \tag{22}$$

This property (22) does not hold in general. For example, under certain postselection strategies, the restriction $p(x) = q(x)$ in Theorem 1 may be violated. We will show later that, for sifting on orthogonal basis states, the convexity property (22) holds.

Third, we show how $I(\rho_{AB}, \mathbf{M}_{AB})$ and $\chi(\rho_{AB}, \mathbf{M}_A)$ change under unitary transformations of the input state ρ_{AB}.

Lemma 1. Given the states ρ_{AB} and $\sigma_{AB} = U \otimes V \rho_{AB} U^\dagger \otimes V^\dagger$. The mutual information and the Holevo quantity transform as follows:

$$I(\sigma_{AB}, \mathbf{M}_{AB}) = I(\rho_{AB}, U^\dagger \otimes V^\dagger \mathbf{M}_{AB} U \otimes V), \tag{23}$$

$$\chi(\sigma_{AB}, \mathbf{M}_A) = \chi(\rho_{AB}, U^\dagger \mathbf{M}_A U), \tag{24}$$

where we define the sets

$$U^\dagger \mathbf{M}_A U := \{U^\dagger A_x U\}, \tag{25}$$

$$V^\dagger \mathbf{M}_B V := \{V^\dagger B_y V\}, \tag{26}$$

and the set

$$U^\dagger \otimes V^\dagger \; \mathbf{M}_{AB} \; U \otimes V := \{U^\dagger \otimes V^\dagger (A_x \otimes B_y) \; U \otimes V\}. \tag{27}$$

The proof of this lemma is based on the cyclic property of the trace, and that the von Neumann entropy is unitarily invariant: $S(U\rho U^\dagger) = S(\rho)$.

This lemma will prove useful in the next section, where we identify U and V with the unitary representations of the symmetry groups governing A_x and B_y.

V. SYMMETRIES IN PROTOCOLS

In this section we introduce a scenario, in which the set $\mathbf{\Gamma}$ can be reduced to a set $\bar{\mathbf{\Gamma}}$, which contains only states with a certain symmetry corresponding to the symmetries of the signal states.

A. Symmetries of signal states and measurements

Let G be a group with a unitary representation $\{U_g; g \in G\}$. A set of states $\mathbf{S}$ is G-invariant if for all states $|\varphi_x\rangle \in \mathbf{S}$ and all $g \in G$ the state

$$|\varphi_{g(x)}\rangle\langle\varphi_{g(x)}| := U_g |\varphi_x\rangle\langle\varphi_x| U_g^\dagger \tag{28}$$

is also in $\mathbf{S}$. Here the index $g(x)$ denotes the index of the state $U_g|\varphi_x\rangle$. The following lemma describes the symmetry properties of the POVM elements A_x and the reduced state ρ_A in the source replacement picture [Eqs. (3) and (4)]:

Lemma 2. If the initial probability distribution $p(x)$ is uniform [$p(x) = 1/|\mathbf{S}|$ for all x] and the signal states are G-invariant, then the set of POVM elements A_x and the reduced state ρ_A are G^*-invariant; namely,

$$U_g^* A_x U_g^T = A_{g(x)}, \tag{29}$$

$$U_g^* \rho_A U_g^T = \rho_A. \tag{30}$$

The symbols $*$ and T denote the complex conjugate and the transpose with respect to the fixed Schmidt basis $\mathcal{B}$.

We prove Lemma 2 in Appendix D. Note that, with our particular definition of $*$ and T with respect to the Schmidt basis, the operators U_g^* and U_g^T are well defined.

In the following, we consider only protocols in which Bob's measurement operators B_y are equipped with the G-invariance:

$$U_g B_y U_g^\dagger = B_{g(y)}. \tag{31}$$

B. Parameter estimation with symmetries

The symmetries in the signal states alone do not guarantee that the optimal eavesdropping attack is symmetric. Moreover, the observations and the postprocessing of the measured data also need to satisfy certain symmetry criteria.

In many protocols only averaged measurement quantities are kept for the parameter estimation. For example, often only the quantum bit error rate (QBER) averaged over all signal states is monitored. In this section and for the rest of this paper, we consider the scenario where Alice and Bob only keep averaged measurement quantities and where the initial probability distribution $p(x) = 1/|\mathbf{S}|$ of the signals is uniform. In this scenario, Alice and Bob calculate a linear function Q of the probability distribution $p(x,y)$ with the invariance property

$$Q[p(x,y)] = Q[p(g(x),g(y))] \quad \forall\, g \in G, \tag{32}$$

where the distribution

$$p(g(x),g(y)) = \mathrm{tr}\{A_{g(x)} \otimes B_{g(x)} \rho_{AB}\} \tag{33}$$

is generated by relabeling the POVM elements $A_x \otimes B_y$ by $A_{g(x)} \otimes B_{g(y)}$. Later on, we will identify Q with the average error rate.

From now on, Alice and Bob's knowledge about ρ_{AB} is solely described by the average quantity Q instead of the more-detailed distribution $p(x,y)$. In the previous section the set of all states that are compatible with the measurement data was the set $\mathbf{\Gamma}$ in Def. 1. Now, since the average quantity Q is a coarse-grained version of $p(x,y)$, the set of states which are compatible with Q, $\mathbf{\Gamma}_{\mathrm{ave}}$, is a superset of $\mathbf{\Gamma}$, containing all states of the form

$$\rho_{AB}^{(U_g)} = U_g^* \otimes U_g \rho_{AB} (U_g^* \otimes U_g)^\dagger \quad \forall\; g \in G, \tag{34}$$

where $\rho_{AB} \in \mathbf{\Gamma}$. The states $\rho_{AB}^{(U_g)}$ have the properties that (i) they are compatible with Q, and (ii) their reduced state $\mathrm{tr}_B\{\rho_{AB}^{(U_g)}\}$ is equal to ρ_A.

Let us now define a map that takes a bipartite state ρ_{AB} and "symmetrizes" it with respect to the group G by averaging over all the $\rho_{AB}^{(U_g)}$. In the literature this map is commonly known as twirling,

$$\mathcal{T}^G[\rho_{AB}] \equiv \bar{\rho}_{AB} = \frac{1}{|G|} \sum_{g \in G} \rho_{AB}^{(U_g)}, \tag{35}$$

where $|G|$ is the number of group elements in G. Due to the linearity of Q, $\mathbf{\Gamma}_{\mathrm{ave}}$ also contains all the states $\bar{\rho}_{AB}$.

The twirling map $\mathcal{T}^G$ maps the set $\mathbf{\Gamma}_{\mathrm{ave}}$ to a subset $\bar{\mathbf{\Gamma}}$, which contains only states of the form $\bar{\rho}_{AB}$. Each $\bar{\rho}_{AB}$ has the property that it commutes with all $U_g^* \otimes U_g$,

$$[\bar{\rho}_{AB}, U_g^* \otimes U_g] = 0 \quad \forall\; g \in G. \tag{36}$$

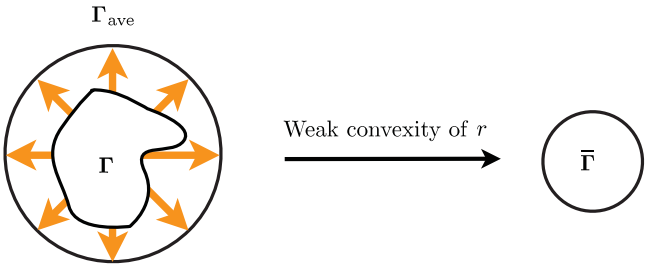

FIG. 2. (Color online) By only using averaged measurement quantities Q for parameter estimation, the set $\mathbf{\Gamma}$ is replaced by a bigger set $\mathbf{\Gamma}_{\text{ave}}$. Using the weak convexity of the key rate, the optimal attack can be chosen from a symmetrized set $\bar{\mathbf{\Gamma}}$.

The purification of a twirled state $\bar{\rho}_{AB}$ can be chosen to satisfies the following invariance:

$$U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Psi\rangle = |\Psi\rangle \quad \forall \ g \in G. \tag{37}$$

The existence of this particular choice of the purification has been proven in Ref. [17] for permutation groups, but the same proof holds for arbitrary groups as well.

C. Symmetric attack

One can restrict the search for the optimal attack ρ_{AB}^{opt} to a search over the set $\bar{\mathbf{\Gamma}}$, provided that the key rate of the particular protocol satisfies the convexity property,

$$r(\mathcal{E}(\bar{\rho}_{AB})) \leqslant \frac{1}{|G|} \sum_{g \in G} r\big(\mathcal{E}\big(\rho_{AB}^{(U_g)}\big)\big), \tag{38}$$

and the invariance property,

$$r(\mathcal{E}(\rho_{AB})) = r\big(\mathcal{E}\big(\rho_{AB}^{(U_g)}\big)\big), \tag{39}$$

under the corresponding symmetry group G. In this situation, ρ_{AB}^{opt} results from a symmetric attack and must lie in the subset $\bar{\mathbf{\Gamma}} \subset \mathbf{\Gamma}_{\text{ave}}$ with the key rate given by

$$r_{\min} = \inf_{\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}} r(\mathcal{E}(\bar{\rho}_{AB})). \tag{40}$$

In Fig. 2 we represent schematically the transition from $\mathbf{\Gamma}$ to $\bar{\mathbf{\Gamma}}$. The symmetrized states $\bar{\rho}_{AB}$ are easily characterized using tools from representation theory. In Appendix E, we show how to obtain $\bar{\rho}_{AB}$ using Schur's lemma.

In summary, in order to evaluate the key rate over the symmetrized set $\bar{\mathbf{\Gamma}}$, the protocol needs to exhibit sufficient symmetries, both in the quantum phase and in the classical phase:

(1) Symmetries in quantum phase: the set of signal states $\mathbf{S}$ and Bob's POVM elements B_y are G-invariant, and the *a priori* probability distribution $p(x)$ is uniform.

(2) Coarse-grained parameter estimation: Alice and Bob restrict themselves to averaged measurement quantities Q in the parameter estimation.

(3) Convexity and invariance of the key rate: the key rate $r(\mathcal{E}(\rho_{AB}))$ satisfies

(a) convexity $r(\mathcal{E}(\bar{\rho}_{AB})) \leqslant \frac{1}{|G|} \sum_{g \in G} r(\mathcal{E}(\rho_{AB}^{(U_g)}))$,

(b) invariance $r(\mathcal{E}(\rho_{AB})) = r(\mathcal{E}(\rho_{AB}^{(U_g)}))$.

In particular, the convexity and invariance properties depend strongly on the postselection procedure and must be checked for each protocol independently.

D. Examples of protocols with symmetric optimal attack: orthogonal bases as signal states

Let us now construct a class of protocols where the set of signal states contains only complete sets of basis states and where Alice and Bob postselect on events they measured in the same basis. This postselection is commonly referred to as sifting. We will show for this class of protocols that the convexity (38) and invariance (39) of the key rate always holds. Therefore, by choosing to keep only the average error rate Q (defined below) for the parameter estimation, the optimal attack can always be assumed to be symmetric.

First, we define the signal states and the measurements. Let us denote a basis of a d-dimensional Hilbert space by $\mathcal{B}_\beta = \{|\varphi_{(\beta,k)}\rangle : k = 0, \ldots, d-1\}$, where β is the basis index. Note that, in the following the states $|\varphi_{(\beta,k)}\rangle$ carry two independent indices (β,k) instead of only one. The set of signal states of each protocol is then identified by

$$\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_\beta : \beta \in \mathcal{L}\}, \tag{41}$$

where $\mathcal{L}$ is the set from which the bases β are drawn. For each protocol the set $\mathcal{L}$ is fixed and contains $|\mathcal{L}|$ elements. If each signal state $|\varphi_{(\beta,k)}\rangle$ is chosen with equal *a priori* probability $p(\beta,k) = 1/(d|\mathcal{L}|)$, Alice's reduced state ρ_A in Eq. (4) is proportional to the identity $\rho_A = \mathbb{1}/d$. Therefore, Alice's POVM elements in Eq. (3) reduce to the projectors

$$A_{(\beta,k)} = \frac{1}{|\mathcal{L}|} |\varphi_{(\beta,k)}^*\rangle\langle\varphi_{(\beta,k)}^*|, \tag{42}$$

with $|\varphi_{(\beta,k)}^*\rangle = \sum_i |i\rangle\langle\varphi_{(\beta,k)}|i\rangle$ defined in Eq. (5). Furthermore, we construct Bob's POVMs to be isomorphic to Alice's:

$$B_{(\beta,k)} = \frac{1}{|\mathcal{L}|} |\varphi_{(\beta,k)}\rangle\langle\varphi_{(\beta,k)}|. \tag{43}$$

Second, Alice and Bob postselect on those measurement outcomes, which they performed in the same basis. In this particular case, Alice and Bob's announcement u is the basis β.

We show three properties in Appendix F for these protocols under postselection, which we will use to prove the convexity and the invariance of the effective key rate $r(\mathcal{E}(\rho_{AB}))$: (i) The measurements conditioned on u are simply renormalized versions of the original POVMs:

$$\mathbf{M}_A^u = \{|\mathcal{L}|A_{(\beta,k)} : \beta = u\}, \tag{44}$$

$$\mathbf{M}_B^u = \{|\mathcal{L}|B_{(\beta,k)} : \beta = u\}, \tag{45}$$

(ii) the filtered states are independent of u and satisfy $\rho_{AB}^u = \rho_{AB}$, and (iii) the probability distribution $p(u) = 1/|\mathcal{L}|$ is uniform. Additionally, since $\rho_A = \mathbb{1}/d$ and the $\mathbf{M}_A^u$ is a von Neumann measurement, the marginals $p_u(x) := \text{tr}\{|\varphi_{(\beta,k)}^*\rangle\langle\varphi_{(\beta,k)}^*|\rho_A\} = 1/d$ are uniform.

Using the uniform marginals $p_u(x)$ in combination with Theorem 1, each term $I(\rho_{AB}, \mathbf{M}_{AB}^u)$ is convex in ρ_{AB}. Moreover, due to the uniform distribution of $p(u)$, the convexity

property immediately transfers to the convex sum

$$\bar{I}(\mathcal{E}(\rho_{AB})) = \frac{1}{|\mathcal{L}|}\sum_u I\left(\rho_{AB}, \mathbf{M}^u_{AB}\right). \tag{46}$$

Similarly, from Theorem 2 we conclude that each term $\chi(\bar{\rho}_{AB}, \mathbf{M}^u_A)$ is concave in ρ_{AB}, which transfers also to

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) = \frac{1}{|\mathcal{L}|}\sum_u \chi\left(\rho_{AB}, \mathbf{M}^u_A\right) \tag{47}$$

by the same argument. The convexity of the effective key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ now follows immediately from the definition in Eq. (16).

Next, we show the invariance of $\bar{r}(\mathcal{E}(\rho_{AB}))$ under the symmetry group G. Since any unitary acts like a basis transformation, the sets $\mathbf{M}^u_A$ and $\mathbf{M}^u_B$ effectively inherit the G^*- and G-invariance from the individual POVM elements $A_{(\beta,k)}$ and $B_{(\beta,k)}$. More precisely, the sets

$$\mathbf{M}^{g(u)}_A := U_g^* \mathbf{M}^u_A U_g^T, \tag{48}$$

$$\mathbf{M}^{g(u)}_B := U_g \mathbf{M}^u_B U_g^\dagger, \tag{49}$$

are again POVMs corresponding to the announcement with index $g(u)$ in the protocol.

Using the definitions (48) and (49), and applying Lemma 1, each component of $\bar{r}(\mathcal{E}(\rho_{AB}))$ transforms as follows under unitaries:

$$I\left(\rho^{(U_g)}_{AB}, \mathbf{M}^{g(u)}_{AB}\right) = I\left(\rho_{AB}, \mathbf{M}^u_{AB}\right), \tag{50}$$

$$\chi\left(\rho^{(U_g)}_{AB}, \mathbf{M}^{g(u)}_{A}\right) = \chi\left(\rho_{AB}, \mathbf{M}^u_{A}\right). \tag{51}$$

Due to the uniform distribution of $p(u)$ and the G^*- and G-invariance of the POVMs, the invariance property of the convex sums $\bar{I}(\mathcal{E}(\rho_{AB}))$ and $\bar{\chi}(\mathcal{E}(\rho_{AB}))$ as well as $\bar{r}(\mathcal{E}(\rho_{AB}))$ follows directly.

In summary, if the average error rate Q in Def. 2 is used in the parameter estimation, the optimal attack lies in the symmetric subset $\bar{\mathbf{\Gamma}}$ for this class of protocols, and the key rate $r_{\min}$ can be calculated according to Eq. (40) without loss of generality.

Definition 2. The average error rate is the probability that Alice sent the signal state $|\varphi_{(\beta,k)}\rangle$, but Bob received an orthogonal state $|\varphi_{(\beta,k')}\rangle$ $(k' \neq k)$ averaged over all k and all bases β

$$Q = \frac{1}{|\mathcal{L}|}\sum_{\beta\in\mathcal{L}} Q^\beta, \tag{52}$$

where Q^β is the average error rate found in each basis,

$$Q^\beta = \sum_{\substack{k,k'\\ k'\neq k}} \mathrm{tr}\{|\varphi^*_{(\beta,k)}\rangle\langle\varphi^*_{(\beta,k)}| \otimes |\varphi_{(\beta,k')}\rangle\langle\varphi_{(\beta,k')}|\rho_{AB}\}, \tag{53}$$

and $|\mathcal{L}|$ is the number of bases in the set $\mathcal{L}$.

The average Uhlmann fidelity of Bob's states with respect to Alice's signal state is defined as

$$F_B = \frac{1}{|\mathcal{L}|}\sum_{\beta\in\mathcal{L}}\sum_k \mathrm{tr}\{|\varphi^*_{(\beta,k)}\rangle\langle\varphi^*_{(\beta,k)}| \otimes |\varphi_{(\beta,k)}\rangle\langle\varphi_{(\beta,k)}|\rho_{AB}\}. \tag{54}$$

With the definition of Q above, F_B and Q are related by the simple relation $F_B = 1 - Q$.

VI. QUANTUM CLONERS

A quantum cloner is a map that creates two copies of quantum states $\varphi_x = |\varphi_x\rangle\langle\varphi_x|$ drawn from a set $\mathbf{S}$. Let us define three isomorphic Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_C$ each with dimension d. A cloner $\mathcal{C}$ is a completely positive and trace-preserving map $\mathcal{C} : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_C$ that takes a state $\varphi_x \in \mathcal{H}_A$ to $\mathcal{C}(\varphi_x) \in \mathcal{H}_B \otimes \mathcal{H}_C$. The quality of each copy k $(k = B, C)$ is determined by the single-clone Uhlmann fidelity $f_k(\varphi_x, \mathcal{C}(\varphi_x))$ of the copy with respect to the original state φ_x. If the states φ_x are pure, the Uhlmann fidelity reads

$$f_B(\varphi_x, \mathcal{C}(\varphi_x)) = \mathrm{tr}\{|\varphi_x\rangle\langle\varphi_x|_B \otimes \mathbb{1}_C \cdot \mathcal{C}(\varphi_x)\}, \tag{55}$$

$$f_C(\varphi_x, \mathcal{C}(\varphi_x)) = \mathrm{tr}\{\mathbb{1}_B \otimes |\varphi_x\rangle\langle\varphi_x|_C \cdot \mathcal{C}(\varphi_x)\}. \tag{56}$$

Instead of $f_k(\varphi_x, C(\varphi_x))$, it is often assumed that only the average fidelity

$$F_k = \frac{1}{|\mathbf{S}|}\sum_{\varphi_x\in\mathbf{S}} f_k(\varphi_x, \mathcal{C}(\varphi_x)) \tag{57}$$

is of interest. The cloner is called optimal if copy C emerges with maximal average fidelity (F_C), while the fidelity F_B of the copy B has a fixed value.

The cloning transformation can also be described using the Choi-Jamiolkowski isomorphism with a nonmaximally entangled state. For this purpose, let $\mathcal{C}$ act on the second half of a source state $|\Phi\rangle$ defined in Eq. (1). This relates $\mathcal{C}$ to a positive operator $\sigma_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ via the rule

$$\sigma_{ABC} = (\mathbb{1} \otimes \mathcal{C})|\Phi\rangle\langle\Phi|. \tag{58}$$

The trace-preserving property of $\mathcal{C}$ translates to $\sigma_A = \mathrm{tr}_{BC}\sigma_{ABC} = \rho_A$, where ρ_A is the reduced state of the source state $|\Phi\rangle$ given in Eq. (4). From σ_{ABC} the map $\mathcal{C}$ can be recovered through the reverse transformation realized by

$$\mathcal{C}(\varphi_x) = \frac{1}{p(x)}\mathrm{tr}_A[A_x \otimes \mathbb{1}_B \otimes \mathbb{1}_C \cdot \sigma_{ABC}], \tag{59}$$

where the A_x are the POVM elements defined in Eq. (3). The reverse transformation effectively corresponds to preparing the states $|\varphi_x\rangle$ in the source-replacement scheme for the cloner.

A. Covariant cloners

We now give a description of quantum cloners based on the work of Refs. [9,18]. Let the set of quantum states $\mathbf{S}$ be G-invariant. If the figure of merit is the average fidelity, then for every cloning map σ_{ABC}, the "rotated" maps

$$U_g^* \otimes U_g \otimes U_g \sigma_{ABC} (U_g^* \otimes U_g \otimes U_g)^\dagger, \tag{60}$$

for $g \in G$ yield the same average fidelity F_k as σ_{ABC}. Furthermore, due to the linearity of the trace, there exists a covariant cloning map

$$\bar{\sigma}_{ABC} = \sum_{g\in G} U_g^* \otimes U_g \otimes U_g \sigma_{ABC} (U_g^* \otimes U_g \otimes U_g)^\dagger, \tag{61}$$

with the same average fidelity F_k as σ_{ABC}. As a consequence, we can always choose the cloning map to be a covariant map,

without loss of generality. The covariant state in Eq. (61) satisfies the commutation relation

$$[\bar{\sigma}_{ABC}, U_g^* \otimes U_g \otimes U_g] = 0. \tag{62}$$

B. Strong covariant cloner

In this section we describe a subset of cloning maps with a stronger symmetry than the covariant cloners, called strong covariant cloners.

The unitary realization U_C of the map $\mathcal{C}$ can be uniquely described by the purification of $\bar{\sigma}_{ABC}$. In the canonical formulation, the purification of such a state lives on the extended Hilbert space $\mathcal{H}^{\otimes 6}$. Some cloners, however, can be realized with a purification on a smaller Hilbert space $\mathcal{H}^{\otimes 4}$ composed of four systems $H_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$, each system having the same dimension. In Ref. [9], the cloners with such a purification are called strong covariant cloners and are defined as follows:

Definition 3. A cloner is called strong covariant if it has a purification $|\Sigma\rangle_{ABCD}$ on $\mathcal{H}_{ABCD}$ with the property

$$U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Sigma\rangle_{ABCD} = |\Sigma\rangle_{ABCD} \quad \forall \quad g \in G. \tag{63}$$

It is easy to see that the strong covariant cloners are a subset of the covariant cloners: for every strong covariant cloner $|\Sigma\rangle$, tracing over the fourth system returns a covariant state $\bar{\sigma}_{ABC}$.

Since the set of covariant cloning maps $\bar{\sigma}_{ABC}$ is a convex set and the fidelity is a linear functional of the cloning map, the cloning problem is a convex optimization problem [9]. The optimal cloner is an extremal point of the convex set, which means a map that cannot be written as a convex sum of other maps in the set. We want to find the extremal map with the maximal clone fidelity. In Ref. [9], two theorems about extremal maps are given:

Theorem 3 (Chiribella et al. [9]). Let U_g be an irreducible representation of the group G, and let $K = \{\bar{\sigma}_{ABC}\}$ denote the set of covariant cloning maps with respect to G according to Eq. (62). Then, every cloning map $\bar{\sigma}_{ABC}$, which allows a strong covariant purification is an extremal point of the convex set K.

This theorem states that the strong covariant maps are a subset of the extremal maps. The converse—that the extremal maps are a subset of the strong covariant maps—is not true in general. The next theorem, however, describes a special case in which the set of extremal maps and the set of strong covariant maps coincide:

Theorem 4 (Chiribella et al. [9]). If the set of states **S** to be cloned is G-invariant under the generalized Pauli group Π_d, then the set of strong covariant cloning maps is equal to the set of extremal maps.

Theorem 4 allows us to restrict the search of the optimal cloner to strong covariant maps based on the symmetries of the signal states alone. In Sec. VII A we give the definition of the generalized Pauli group.

VII. CONNECTION BETWEEN OPTIMAL CLONERS AND OPTIMAL ATTACKS

We identify the optimal attack in QKD with an optimal cloner if Eve's interaction U_E^{opt} coincides with the optimal cloning transformation U_C^{opt} or, in terms of the purifications, if $|\Psi\rangle^{\text{opt}} = |\Sigma\rangle^{\text{opt}}$. The optimal attack is always chosen from the set of purifications $\mathbf{\Delta}$ defined as follows:

Definition 4. We define by $\mathbf{\Delta}$ the set that contains the purifications $|\Psi\rangle$ of the symmetrized states in $\bar{\mathbf{\Gamma}}$. All states in $\mathbf{\Delta}$ satisfy the symmetry condition $U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Psi\rangle = |\Psi\rangle$ for all $g \in G$, and they are compatible with the averaged quantity Q and fixed ρ_A.

We observe that all eavesdropping attacks represented by the set $\mathbf{\Delta}$ correspond to representations of strong covariant cloners. We can therefore make the following conclusion:

Observation. The optimal cloner can only be the optimal attack if it is strong covariant. Otherwise, one can already conclude that $|\Psi\rangle^{\text{opt}} \neq |\Sigma\rangle^{\text{opt}}$.

At this point, the strong covariance property alone does not uniquely determine if the optimal attack is an optimal cloner. Even if the optimal cloner is strong covariant, we can only conclude that the optimal attack is an optimal cloner if the set $\mathbf{\Delta}$ contains exactly one state. Otherwise, in order to compare the optimal attack with the optimal cloner, we must perform the optimization.

A. Pauli-invariant signal states

As mentioned in Theorem 4, a sufficient requirement for a cloning map to allow a strong covariant realization is the Pauli-invariance of the set of states to be cloned. Hence, if the signal states of a QKD protocol are Pauli-invariant, the corresponding cloning attack on that protocol is certainly realized by a strong covariant cloner. Therefore, we will focus our attention on protocols with signal states that are Pauli-invariant.

First, let us define the generalized Pauli group.

Definition 5. The generalized Pauli group Π_d in d dimensions has d^2 elements. The set of unitaries

$$U_{r,s} = \sum_{k=0}^{d-1} \omega^{ks} |k+r\rangle\langle k|, \quad \omega = e^{2\pi i/d}, \tag{64}$$

for $r, s = 0, \ldots, d-1$ form an irreducible unitary representation of Π_d on a d-dimensional Hilbert space. The group has two generators

$$Z := U_{0,1}, \quad X := U_{1,0}, \tag{65}$$

which generate the entire group by the following relation:

$$U_{r,s} = X^r Z^s, \quad r, s = 0, \ldots, d-1. \tag{66}$$

A state ρ_{AB} that commutes with all $U_{r,s}^* \otimes U_{r,s}$ is Bell-diagonal:

$$\rho_{AB} = \sum_{r,s=0}^{d-1} u_{r,s} |U_{r,s}\rangle\langle U_{r,s}|, \tag{67}$$

with eigenvalues $u_{r,s} \geqslant 0$ that satisfy $\sum_{r,s} u_{r,s} = 1$. The eigenvectors

$$|U_{r,s}\rangle = \frac{1}{\sqrt{d}} \sum_k \omega^{ks} |k+r\rangle|k\rangle \tag{68}$$

are called Bell states and form a maximally entangled basis of $\mathcal{H}^{\otimes 2}$. As shown in Refs. [4,9], the general form of the purification of ρ_{AB} is given by $|\Psi\rangle = \sum_{r,s} \sqrt{u_{r,s}} |U_{r,s}\rangle|U_{r,d-s}\rangle$.

Since $U_{r,s}$ is an irreducible representation, we can use Schur's lemma in Appendix E to characterize the reduced state $\rho_A = \mathbb{1}/d$, which is proportional to the identity.

VIII. EXAMPLES WITH MUTUALLY UNBIASED BASES

Mutually unbiased bases (MUBs), which were first introduced in Refs. [19,20], are a common choice for the signal states of QKD protocols. For example, in the qubit space, the BB84 and the 6-state protocol use 2 and 3 MUBs, respectively. In higher-dimensional Hilbert spaces, MUB protocols have been studied in Refs. [4–6,12,21,22].

MUBs are orthonormal bases $\mathcal{B}_\alpha = \{|\psi_1^\alpha\rangle, |\psi_2^\alpha\rangle, \ldots, |\psi_{d-1}^\alpha\rangle\}$ on d-dimensional Hilbert spaces with the property $|\langle\psi_k^\alpha|\psi_{k'}^{\alpha'}\rangle| = 1/\sqrt{d}$ for all $k, k' = 0, \ldots, d-1$ and $\alpha \neq \alpha'$. In Ref. [23], it was shown that, when d is a prime number, there exist exactly $d+1$ MUBs. Throughout this section, we assume that d is a prime number. The eigenbases of the generalized Pauli operators Z and XZ^β for $\beta = 0, \ldots, d-1$ form MUBs, as shown in Ref. [24]. The eigenbasis of the operator Z is denoted by the standard basis with the index Z,

$$\mathcal{B}_Z = \left\{\left|\psi_1^Z\right\rangle, \left|\psi_2^Z\right\rangle, \ldots, \left|\psi_{d-1}^Z\right\rangle\right\}, \tag{69}$$

$$\left|\psi_k^Z\right\rangle = |k\rangle, \tag{70}$$

and the eigenbases of the operators XZ^β with indices $\beta = 0, \ldots, d-1$ by

$$\mathcal{B}_\beta = \left\{\left|\psi_1^\beta\right\rangle, \left|\psi_2^\beta\right\rangle, \ldots, \left|\psi_{d-1}^\beta\right\rangle\right\}, \tag{71}$$

$$\left|\psi_k^\beta\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-kj} \omega^{-\beta s_j} |j\rangle, \tag{72}$$

where $s_j = \frac{1}{2}(d-j)(d+j-1)$, $\omega = e^{2\pi i/d}$, and where $|j\rangle$ are the basis vectors of the standard basis $\mathcal{B}_Z$.

Let us now consider protocols where the set of signal states $\mathbf{S}_\mathcal{L}$ contains any subset of these $d+1$ eigenbases. In a slight generalization of the result of Theorem 2.2 in Ref. [24], we can show that the action of any Pauli operator $U_{r,s}$ on the eigenstates of the Pauli eigenbasis $\mathcal{B}_\alpha$ for $\alpha \in \{Z, 0, 1, \ldots, d-1\}$ permutes the eigenstates without changing the basis index α. Using this invariance, the set of signal states $\mathbf{S}_\mathcal{L}$ of any such protocol are also Pauli-invariant.

Unfortunately, the full symmetry groups of the sets $\mathbf{S}_\mathcal{L}$ are not known explicitly. Thus, one cannot simply write down the general form of the symmetrized states $\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}$. However, in a first step, we can exploit the invariance of the set $\mathbf{S}_\mathcal{L}$ with respect to the generalized Pauli group. This partial symmetry implies that the optimal attack ρ_{AB}^{opt} must lie in the subset $\mathbf{\Gamma}_{\text{Bell}}$ containing only Bell-diagonal states defined in Eq. (67).

Let us, therefore, calculate the key rate (16) for MUB protocols with Bell-diagonal states ρ_{AB}. For this purpose, we require the eigenvalue spectrum of each conditional state on Bob's side $\rho_B^{(\alpha,k)}$ for $\alpha \in \{Z, 0, 1, \ldots, d-1\}$, given that Alice obtained the measurement outcome corresponding to the state $|\psi_k^\alpha\rangle$. We project Alice's system of the Bell state onto $|\psi_k^{*\alpha}\rangle$ and divide the result by a normalization constant N:

$$\rho_B^{(\alpha,k)} = \sum_{r,s} u_{r,s} \left\langle\psi_k^{*\alpha}\right| U_{r,s} \left\rangle\left\langle U_{r,s}\right| \left.\psi_k^{*\alpha}\right\rangle / N. \tag{73}$$

In the following, all operations are modulo d and, in particular, the indices are to be understood modulo d. The overlaps in Eq. (73) are found to be

$$\left\langle\psi_k^{*Z}\right| U_{r,s}\left\rangle = \tfrac{1}{\sqrt{d}} \omega^{(k-r)s} |k-r\rangle, \tag{74}$$

$$\left\langle\psi_k^{*\beta}\right| U_{r,s}\left\rangle = \frac{1}{\sqrt{d}} \omega^{-kr-\frac{\beta}{2}(r-r^2)} \left|\psi_{k-(s+\beta r)}^\beta\right\rangle, \tag{75}$$

for Z and for $\beta \in \{0, \ldots, d-1\}$. After reinserting the overlaps into Eq. (73) and using by $N = 1/d$, we do an index substitution $y = s + \beta r$ in Eq. (75) to obtain the following expressions for the conditional states for $\alpha \in \{Z, 0, 1, \ldots, d-1\}$:

$$\rho_B^{(\alpha,k)} = \sum_y \lambda_y^\alpha \left|\psi_{k-y}^\alpha\right\rangle\left\langle\psi_{k-y}^\alpha\right|. \tag{76}$$

The set of eigenvalues $\mathbf{\Lambda}^\alpha = \{\lambda_0^\alpha, \lambda_1^\alpha, \ldots, \lambda_{d-1}^\alpha\}$ for each $\rho_B^{(\alpha,k)}$ is independent of the index k with the specific values

$$\lambda_y^Z = \sum_{r=0}^{d-1} u_{y,r} \quad \text{for} \quad Z, \tag{77}$$

$$\lambda_y^\beta = \sum_{r=0}^{d-1} u_{r,y-\beta r} \quad \text{for} \quad \beta \in \{0, \ldots, d-1\}. \tag{78}$$

The average error rate, the mutual information and the Holevo quantity (46), (47), and (52) can now be calculated using the eigenvalue spectrum

$$Q = 1 - \frac{1}{|\mathcal{L}|} \sum_{\alpha\in\mathcal{L}} \lambda_0^\alpha, \tag{79}$$

$$\bar{I}(\mathcal{E}(\rho_{AB})) = \log_2 d - \frac{1}{|\mathcal{L}|} \sum_{\alpha\in\mathcal{L}} H(\mathbf{\Lambda}^\alpha), \tag{80}$$

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) = S(\rho_{AB}) - \frac{1}{|\mathcal{L}|} \sum_{\alpha\in\mathcal{L}} H(\mathbf{\Lambda}^\alpha), \tag{81}$$

with the Shannon entropy $H(\mathbf{\Lambda}^\alpha) = -\sum_y \lambda_y^\alpha \log_2(\lambda_y^\alpha)$ and the von Neumann entropy $S(\rho) = -\text{tr}\rho \log_2 \rho$. The key rate (16) follows straightforwardly,

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \log_2 d - S(\rho_{AB}). \tag{82}$$

For the special protocols with 2, d, and $d+1$ MUBs, we further confine our search for the optimal attack to smaller subsets $\tilde{\mathbf{\Gamma}} \subset \mathbf{\Gamma}_{\text{Bell}}$. The procedure is essentially the same as the one we used in Sec. V to reduce to the subset $\bar{\mathbf{\Gamma}}$ from the set $\mathbf{\Gamma}_{\text{ave}}$. For each state ρ_{AB} in $\mathbf{\Gamma}_{\text{Bell}}$, we generate an equivalence class of states $\{\rho_{AB}^{(P_i)}; i = 1, \ldots, n\}$ by applying permutations P_i to the eigenvalues of ρ_{AB}. In contrast to the states $\rho_{AB}^{(U_g)}$ in Eq. (34), the states $\rho_{AB}^{(P_i)}$ are not generated using the symmetry group of the signal states. However, since the key rate (82) is proportional to $S(\rho_{AB})$, all permuted states satisfy the invariance property $\bar{r}(\mathcal{E}(\rho_{AB})) = \bar{r}(\mathcal{E}(\rho_{AB}^{(P_i)}))$. Furthermore, we chose the permutations in such a way, that the $\rho_{AB}^{(P_i)}$ give the same error rate as ρ_{AB}. This ensures that the $\rho_{AB}^{(P_i)}$ are again in $\mathbf{\Gamma}_{\text{Bell}}$. Consequently, since the convexity property (38) of the key rate holds for protocols with MUBs, we can conclude that the optimal attack is found in the subset $\tilde{\mathbf{\Gamma}} \subset \mathbf{\Gamma}_{\text{Bell}}$ containing only convex combinations,

$$\tilde{\rho}_{AB} = \frac{1}{n} \sum_i \rho_{AB}^{(P_i)} \in \tilde{\mathbf{\Gamma}}.$$

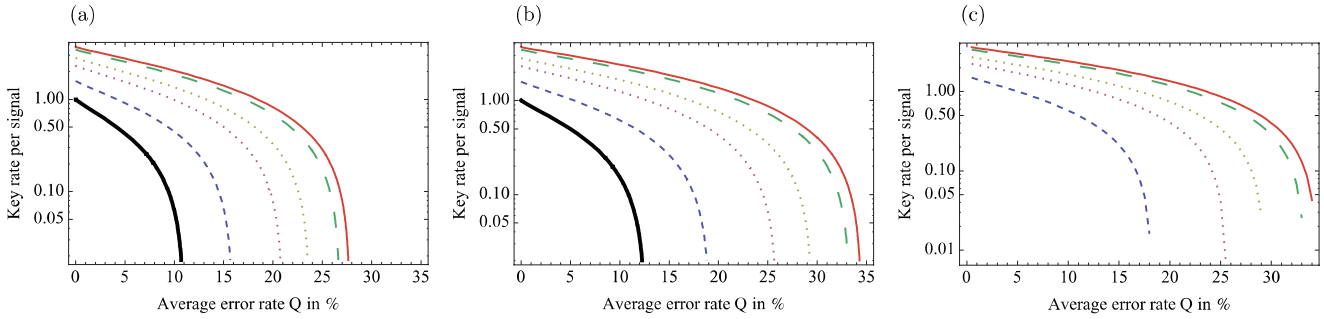

FIG. 3. (Color online) Key rates of protocols with (a) 2, (b) $d+1$, and (c) d MUBs for $d=2$ (thick bottom line, black), $d=3$ (dashed line, blue), $d=5$ (dotted line, purple), $d=7$ (dash-dotted line, yellow), $d=11$ (large dashed line, green), and $d=13$ (solid top line, red). These plots do not serve as a comparison of the performance of the different protocols.

Note that it suffices to check that the states $\rho_{AB}^{(P_i)}$ have the same average error rate Q as ρ_{AB} in order to be in the set $\mathbf{\Gamma}_{\text{Bell}}$. We do not need to monitor the condition on ρ_A, because $\rho_A = \mathbb{1}/d$ is automatically satisfied for any Bell-diagonal state.

A. 2 MUBs

We describe here how to obtain the states $\tilde{\rho}_{AB} \in \tilde{\mathbf{\Gamma}}$ for the example of the 2-MUB protocol with the signal states $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_0, \mathcal{B}_Z\}$: given Bell-diagonal states ρ_{AB}. As mentioned above, we generate the (Bell-diagonal) permuted states $\rho_{AB}^{(P_i)}$ by keeping the error rate (79) of ρ_{AB} invariant:

$$\begin{aligned} Q &= 1 - \frac{1}{2}\left(\lambda_0^0 + \lambda_0^Z\right) \\ &= 1 - \frac{1}{2}\left(2u_{0,0} + \sum_{r=1}^{d-1}(u_{r,0} + u_{0,r})\right). \end{aligned} \tag{83}$$

The invariance of Q is guaranteed if the permutations P_i leave the sets $\mathbf{U}_a = \{u_{0,0}\}$, $\mathbf{U}_b = \{u_{0,r}, u_{r,0};\ r = 1, \ldots, d-1\}$, and $\mathbf{U}_c = \{u_{r,s};\ r, s = 1, \ldots, d-1\}$ invariant. Such permutations P_i are, for example, independent permutations of the eigenvalues in each set. Therefore, in the convex combination $\tilde{\rho}_{AB}$, the average over all eigenvalues in each set will appear. In this particular case, $\tilde{\rho}_{AB}$ has three different types of independent eigenvalues a, b, and c corresponding to the three sets $\mathbf{U}_a$, $\mathbf{U}_b$, and $\mathbf{U}_c$,

$$\begin{aligned} \tilde{\rho}_{AB} = a|U_{0,0}\rangle\langle U_{0,0}| + c\sum_{r,s=1}^{d-1}|U_{r,s}\rangle\langle U_{r,s}| \\ + b\sum_{r=1}^{d-1}(|U_{r,0}\rangle\langle U_{r,0}| + |U_{0,r}\rangle\langle U_{0,r}|). \end{aligned} \tag{84}$$

Now we can use the average error rate condition $Q = (d-1)b + (d-1)^2 c$ and the normalization condition $a + 2(d-1)b + d^2 c = 1$ to further reduce the number of independent eigenvalues to only one. Through an (analytical) optimization of the key rate over the free eigenvalue, we find the following values for a, b, and c that describe the optimal attack:

$$a = (1-Q)^2, \quad b = \frac{Q(1-Q)}{d-1}, \quad c = \frac{Q^2}{(d-1)}. \tag{85}$$

These are exactly the same coefficients that are found to describe the optimal phase-covariant cloner in d dimensions Ref. [4]. The connection between optimal cloning and the optimal attack for 2 MUBs was already conjectured in Ref. [4]. The key rates for these protocols, which were independently obtained in Ref. [13], are given by

$$r_{\min} = \log_2 d + 2(1-Q)\log_2(1-Q) + 2Q\log_2\left(\frac{Q}{d-1}\right).$$

They are plotted for $d = 2, 3, 5, 7, 11, 13$ in Fig. 3. Note that this plot is not intended to compare the performances of the different protocols. For a fair comparison, one must specify the channel model for which the key rates are drawn.

Note that the results of this subsection for protocols with two MUBs hold also if the dimension d of the systems is not prime. The reason to restrict initially to prime dimension is that this guarantees that we have a description of the MUBs as in Eq. (72). However, for two MUBs the choices of $\mathcal{B}_0$ and $\mathcal{B}_Z$ are still valid MUBs for any dimension. That suffices to derive the results in this section.

B. $d+1$ MUBs

Consider protocols with the signal states $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_Z, \mathcal{B}_0, \mathcal{B}_1, \ldots \mathcal{B}_{d-1}\}$. In contrast to the case with 2 MUBs, these protocols are tomographically complete. With the same strategy as for 2 MUBs, we construct the set $\tilde{\mathbf{\Gamma}}$ for this situation: The error rate (79) of a Bell-diagonal state in this scenario is given by

$$Q = 1 - \frac{1}{d+1}\left((d+1)u_{0,0} + \sum_{(r,s)\neq(0,0)} u_{r,s}\right), \tag{86}$$

where we used the relation that, for $r \neq 0$, the sum $\sum_{\beta=0}^{d-1} u_{r,-\beta r} = \sum_{\gamma=0}^{d-1} u_{r,\gamma}$. The error rate defines the sets $\mathbf{U}_a = \{u_{0,0}\}$ with one eigenvalue, and $\mathbf{U}_b = \{u_{r,s};\ (r,s) \neq (0,0)\}$ with the remaining $d^2 - 1$ eigenvalues. Again, $\mathbf{U}_a$ and $\mathbf{U}_b$ determine the form of the states in the set $\tilde{\mathbf{\Gamma}}$, after averaging over all permutations P_i:

$$\tilde{\rho}_{AB} = a|U_{0,0}\rangle\langle U_{0,0}| + b\sum_{(r,s)\neq(0,0)}|U_{r,s}\rangle\langle U_{r,s}|. \tag{87}$$

In this situation, the average eigenvalues a and b are uniquely defined by the error rate $Q = d(d-1)b$ and the trace condition

$a + (d^2 - 1)b = 1$:

$$a = 1 - \frac{d+1}{d}Q, \quad b = \frac{Q}{d(d-1)}. \tag{88}$$

As there is only one state in $\tilde{\mathbf{\Gamma}}$ for this protocol, the optimization of the key rate becomes trivial, and we can conclude that the optimal cloner and the optimal attack are equal. This connection was already conjectured in Ref. [4]. The cloner in this case is the optimal universal cloner in d dimensions [25,26]. For $d = 2$, we recover the the 6-state protocol, where the optimal cloner is the universal cloner [3,27], which clones all the states on the Bloch sphere equally well. The key rates of these protocols are given by

$$r_{\min} = \log_2 d + \frac{d+1}{d}Q\log_2\left(\frac{Q}{d(d-1)}\right) + \left(1 - \frac{d+1}{d}Q\right)\log_2\left(1 - \frac{d+1}{d}Q\right), \tag{89}$$

as independently shown in Ref. [13]. We plot the key rates for $d = 2, 3, 5, 7, 11, 13$ in Fig. 3. Again, the plot is not intended to compare the performance of the protocols.

C. d MUBs

The signal states of protocols using d MUBs are $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_0, \mathcal{B}_1, \ldots \mathcal{B}_{d-1}\}$. Unlike the protocols with d MUBs, the protocols analyzed here are not tomographically complete. The error rate

$$Q = 1 - \frac{1}{d}\left(d\, u_{0,0} + \sum_{r=0}^{d-1}\sum_{s=1}^{d-1} u_{r,s}\right) \tag{90}$$

defines three sets $\mathbf{U}_a = \{u_{0,0}\}$, $\mathbf{U}_b = \{u_{r,s};\, r = 0, \ldots, d-1, s = 1, \ldots, d-1\}$, and $\mathbf{U}_c = \{u_{0,s};\, s = 1, \ldots, d-1\}$, which determine the form of $\tilde{\rho}_{AB} \in \tilde{\mathbf{\Gamma}}$

$$\tilde{\rho}_{AB} = a|U_{0,0}\rangle\langle U_{0,0}| + c\sum_{s=1}^{d-1}|U_{0,s}\rangle\langle U_{0,s}| + b\sum_{r=0}^{d-1}\sum_{s=1}^{d-1}|U_{r,s}\rangle\langle U_{r,s}|. \tag{91}$$

The eigenvalues a, b, and c are further constricted by the normalization condition $a + d(d-1)b + (d-1)c = 1$, and the error rate condition for $\tilde{\rho}_{AB}$ $Q = (d-1)^2 b + (d-1)c$. We can express two of the three eigenvalues by

$$a = 1 + c - \frac{dQ}{d-1}, \quad b = \frac{Q - (d-1)c}{(d-1)^2}. \tag{92}$$

We perform an optimization of the key rate over the free eigenvalue c and plot the numerically obtained key rates $r_{\min}$ in Fig. 3 for different dimensions.

We compare the optimal attack to the optimal multiple phase-covariant (MPC) cloner U_{MPC} given in Ref. [28]. This cloner copies all states of the form $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi_j}|j\rangle$ for $\phi_j \in [0, 2\pi)$ optimally. If it is known that the eavesdropper performed an attack based on the optimal MPC cloner, Alice and Bob can expect some key rate r_{MPC}. Numerical optimizations for $d = 3, 5, 7, 11, 13$ show that r_{MPC} is always bigger (or equal) than the key rate $r_{\min}$. Therefore, the optimal MPC cloner is not the optimal attack: $U_{\mathrm{MPC}} \neq U_E^{\mathrm{opt}}$. In Fig. 4 we plot the difference between the key rates, $r_{\mathrm{MPC}} - r_{\min}$. We denote Eve's average fidelity of the optimal MPC cloner by F_E^{MPC} calculated according to Eq. (57). Since each transformation U can be viewed as a (nonoptimal) cloner, we can calculate the fidelity of the transformation corresponding to the optimal attack U_E^{opt} from the pure state $|\Psi^{\mathrm{opt}}\rangle$. This fidelity we define as F_E^{attack}. We plot the difference $F_E^{\mathrm{MPC}} - F_E^{\mathrm{attack}}$ for $d = 3$ in Fig. 4.

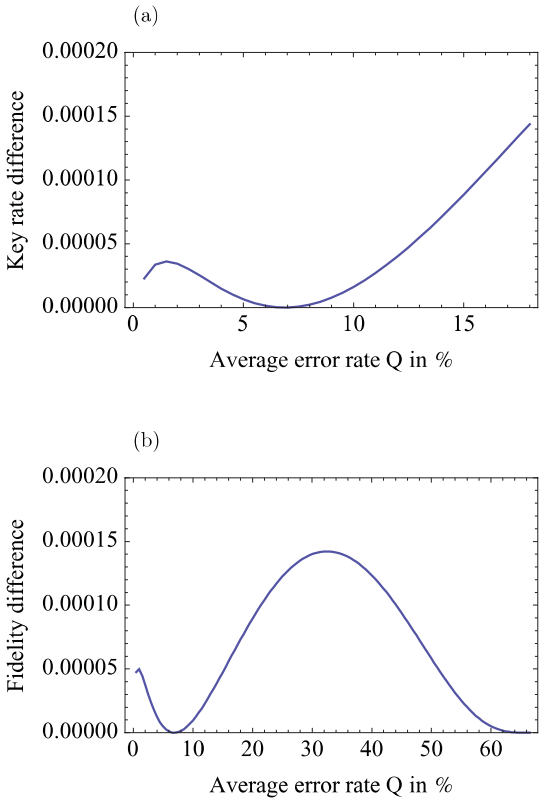

FIG. 4. (Color online) (a) Plot of difference of key rates $\delta r = r_{\mathrm{MPC}} - r_{\min}$ for scenarios where Eve uses the optimal cloner (r_{MPC}), and where she uses the optimal attack ($r_{\min}$) for $d = 3$. (b) Plot of the difference of the fidelities $\delta F_E = F_E^{\mathrm{MPC}} - F_E^{\mathrm{attack}}$ for scenarios where Eve uses the optimal MPC cloner (F_E^{MPC}) and where she uses the optimal attack (F_E^{attack}) for $d = 3$.

We would like to remark that the U_{MPC} produces optimal copies of more than just the necessary d MUBs. It is possible that there exists a cloner U_d that provides copies of the d MUBs with a higher fidelity F_E^d (for fixed error rate) than U_{MPC}: $F_E^d \geqslant F_E^{\mathrm{MPC}}$. This raises the question of whether the cloner U_d could be the optimal attack U_E^{opt}. To answer this, we turn the question around and ask it from the cloning point of view: whether the optimal attack U_E^{opt} can play the role of the optimal cloner U_d. For this purpose, we compare Eve's fidelity F_E^{attack}, when she used the optimal attack to the fidelity F_E^d, when she used U_d. We know from our numerical optimization how F_E^{attack} compares to F_E^{MPC}: we plotted the difference $F_E^{\mathrm{MPC}} - F_E^{\mathrm{attack}}$ in Fig. 4. From this plot we see that, in general, $F_E^{\mathrm{MPC}} > F_E^{\mathrm{attack}}$. However, we know by construction of U_d that the fidelity $F_E^d \geqslant F_E^{\mathrm{MPC}}$. By transitivity it follows that $F_E^d > F_E^{\mathrm{attack}}$, which

TABLE I. Summary of optimal attacks of protocols using MUBs in d dimensions. For the protocols where the optimal attack is an optimal cloner we put a check mark ($\surd$). Where the optimal attack is not an optimal cloner we put a cross ($\times$). The numerical optimizations cover the cases of d MUBs up to $d = 13$.

	Number of MUBs							
Dimension	2 MUBs	3 MUBs	4 MUBs	5 MUBs	6 MUBs	$\cdots$	d MUBs	$d+1$MUBs
2	$\surd$	$\surd$						
3	$\surd$	$\times$	$\surd$					
5	$\surd$			$\times$	$\surd$			
$\vdots$	$\vdots$						$\ddots$	
d	$\surd$							$\surd$

proves that the optimal attack is not equivalent to the optimal cloner U_d either.

In Table I we summarize the results obtained for the MUB protocols. It turns out that, in general, the intuition that the optimal attack is always an optimal cloner proves wrong, as can be seen for the protocols with d MUBs.

IX. CLASSES OF PROTOCOLS WITH THE SAME OPTIMAL ATTACK

We observe that, for certain protocols with different signal states, the same attack ρ_{AB}^{opt} is found to be optimal. Consider two protocols P and P' with sets of signal states $\mathbf{S}$ and $\mathbf{S}'$ that are G- and G'-invariant, respectively. We consider only protocols where the signal states are orthogonal bases, and where Alice and Bob postselect on events in the same basis. These protocols were already described in Sec. V D. We denote the average error rate of each protocol by Q and Q'. Let us denote Alice and Bob's POVM elements by A_x and B_y for the protocol P and by $A'_{x'}$ and $B'_{y'}$ for the protocol P' which are given in Eqs. (42) and (43). The POVMs conditioned on the basis announcement u given in Eqs. (44) and (45) are denoted by $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ for protocol P and by $\mathbf{M}'^{u'}_A$ and $\mathbf{M}'^{u'}_B$ for protocol P'. The sets characterizing the possible symmetric attacks are denoted by $\bar{\mathbf{\Gamma}}$ and $\bar{\mathbf{\Gamma}}'$. We also define the set of twirled states as follows:

Definition 6. The set of all twirled bipartite states $\bar{\rho}_{AB}$ with respect to the group G is

$$\mathbf{T}_G = \{\mathcal{T}^G[\rho_{AB}] | \rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B\}.$$

The following theorem states the criteria under which two protocols have the same optimal attack.

Theorem 5. If the following three conditions are satisfied, the protocols P and P' have the same optimal attack:

(I) $\mathbf{T}_G = \mathbf{T}_{G'}$.

(II) The average measurement quantities Q and Q' provide the same constraints on all $\bar{\rho}_{AB}$ in $\mathbf{T}_G$ and $\mathbf{T}_{G'}$.

(III) There exists a third group H with a representation $\{W_h; h \in H\}$, such that G and G' are subgroups of H, with the following properties:

(a) $\mathbf{T}_H = \mathbf{T}_G = \mathbf{T}_{G'}$, and

(b) for all POVM elements $A_x \in \mathbf{M}_A$ and $A'_{x'} \in \mathbf{M}'_A$ there exists a $W_{h(x,x')}$ in H such that

$$|\mathcal{L}|^2 W^*_{h(x,x')} A_x W^T_{h(x,x')} = |\mathcal{L}'|^2 A'_{x'}. \tag{93}$$

Note that (III b) automatically implies the relation $|\mathcal{L}|^2 W_{h(x,x')} B_x W^\dagger_{h(x,x')} = |\mathcal{L}'|^2 B'_{x'}$ for Bob's measurement operators B_y defined in Eq. (43).

Proof. We show that the optimization of the key rate in Eq. (40) leads to the same optimal ρ_{AB}^{opt} for both protocols. There are two parts to the proof. First, from (I) and (II) it follows that $\bar{\mathbf{\Gamma}} = \bar{\mathbf{\Gamma}}'$ by definition. Therefore, the set over which the key rate is optimized is identical for the two protocols. Second, we show that the mutual information $\bar{I}(\mathcal{E}(\bar{\rho}_{AB}))$ and the Holevo quantity $\bar{\chi}(\mathcal{E}(\bar{\rho}_{AB}))$ in Eqs. (46) and (47) are identical for both protocols for all states in the set $\bar{\mathbf{\Gamma}}$. We show this for the example of the mutual information, but the same arguments apply to the Holevo quantity as well.

As a starting point, we switch to the language where the unitaries act on the sets $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ instead of the individual elements A_x and B_y. The action of each unitary U on the A_x and B_y defines uniquely the action of the same unitary U on $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ by the relation in Eqs. (25) and (26). This correspondence allows us to uniquely relabel $W_{h(x,x')}$ by $W_{h(u,u')}$, where u and u' are the basis announcements found in P and P', respectively. We can now restate (III a) and say that there exists unitaries $W_{h(u,u')}$ for all pairs (u,u') such that

$$W^*_{h(u,u')} \mathbf{M}_A^u W^T_{h(u,u')} = \mathbf{M}'^{u'}_A, \tag{94}$$

$$W_{h(u,u')} \mathbf{M}_B^u W^\dagger_{h(u,u')} = \mathbf{M}'^{u'}_B. \tag{95}$$

Furthermore, for a fixed u_0 in P, there exist unitaries $W_{h(u_0,u)} = W_{h(u,u')} W_{h(u',u_0)}$, connecting all u in P to the fixed u_0. Similarly, there exist unitaries $W_{h(u'_0,u')}$ connecting a fixed u'_0 to all u' in P'. Using the invariance $\bar{\rho}_{AB} = W_h^* \otimes W_h \bar{\rho}_{AB} (W_h^* \otimes W_h)^\dagger$ for all $W_h \in H$ and Lemma 1, the total mutual information of P and P' satisfies the following:

$$\bar{I}(\mathcal{E}(\bar{\rho}_{AB})) = \frac{1}{|\mathcal{L}|} \sum_{u=1}^{|\mathcal{L}|} I\left(\bar{\rho}_{AB}, \mathbf{M}_{AB}^u\right) = I\left(\bar{\rho}_{AB}, \mathbf{M}_{AB}^{u_0}\right),$$

$$\bar{I}(\mathcal{E}'(\bar{\rho}_{AB})) = \frac{1}{|\mathcal{L}'|} \sum_{u'=1}^{|\mathcal{L}'|} I\left(\bar{\rho}_{AB}, \mathbf{M}'^{u'}_{AB}\right) = I\left(\bar{\rho}_{AB}, \mathbf{M}'^{u'_0}_{AB}\right).$$

A similar statement can be made for the Holevo quantity as well.

Since there exists also a unitary $W_{h(u_0,u'_0)}$, we can conclude that

$$I\left(\bar{\rho}_{AB}, \mathbf{M}_{AB}^{u_0}\right) = I\left(\bar{\rho}_{AB}, \mathbf{M}'^{u'_0}_{AB}\right), \tag{96}$$

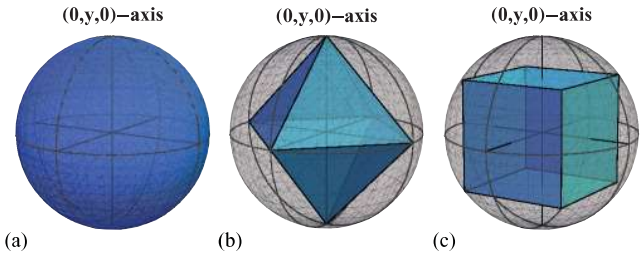

FIG. 5. (Color online) Representation of sets of signal states on the Bloch sphere related to the 6-state protocol. (a) States that are invariant under SU(2), (b) States of the 6-state protocol (octahedron), invariant under O-symmetry. (c) States of the cube protocol, invariant under O-symmetry.

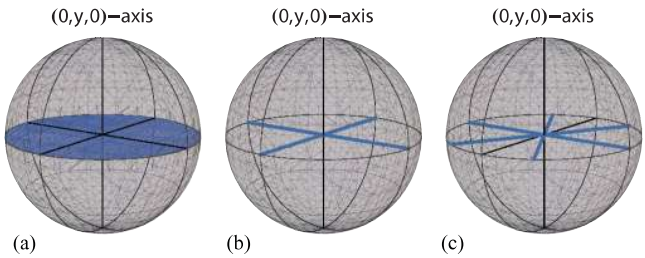

FIG. 6. (Color online) Representation of signal states on the Bloch sphere for protocols related to the BB84 protocol. (a) States that are invariant under D_∞. (b) States of the BB84 protocol, D_4-symmetry. (c) States of the $2n$-protocol for $n = 3$, D_6 symmetry.

from which we conclude that $\bar{I}(\mathcal{E}(\bar{\rho}_{AB})) = \bar{I}(\mathcal{E}'(\bar{\rho}_{AB}))$. Again, a similar statement holds for the Holevo quantity.

It follows now that the same function $\bar{r}(\mathcal{E}(\rho_{AB})) = \bar{r}(\mathcal{E}'(\rho_{AB}))$ appears in the optimization of protocols P and P'. Since these are now identical optimization problems, they must have the same solution, and therefore the same optimal attack. ■

We will give some examples of protocols with the same optimal attack in the next section. We analyze qubit protocols, where we can make use of the point group symmetries, which are commonly used and well studied in the field of crystallography.

A. Protocols with same optimal attack as 6-state protocol

The signal states of the 6-state protocol form a regular octahedron in the Bloch sphere representation. The symmetry group G that maps an octahedron onto itself is the discrete group O with a unitary irreducible representation on the qubit space. A symmetry group G' that satisfies the criterium (I) in Theorem 5 is, for example, the icosahedron group I [29,30].

We can now construct protocols with signal states that are invariant under O- or I-symmetry. There are many sets of signal states that are invariant under these symmetries. For example, we choose to examine protocols, where the signal states form a cube (O-symmetry), a dodecahedron (I-symmetry), or an icosahedron (again I-symmetry) on the Bloch sphere, consisting of 8, 20, and 12 states, respectively. For each state there exists an orthogonal state on the opposite side of the Bloch sphere. See Fig. 5 for a representation of the signal states of the 6-state and the cube protocol.

The average error rate adopts the same form for all these protocols; namely, $Q = 2b$, where b is defined in Eq. (87). Therefore, condition (II) in Theorem 5 is also satisfied, and we conclude that the sets $\bar{\mathbf{\Gamma}}$ for these protocols are identical to the set given in the case of the 6-state protocol. Since there is only one state in $\bar{\mathbf{\Gamma}}$ for the 6-state protocol, we can already conclude that the optimal attack of the 6-state, the cube, the icosahedron and the dodecahedron protocols are the same, which was already established to be the optimal universal cloner.

B. Protocols with same optimal attack as BB84 protocol

We analyze protocols with $2n$ ($n \geqslant 2$) signal states $|\varphi_x\rangle$, that are distributed equally in the equatorial plane of the Bloch sphere, represented by the Bloch vectors

$$s_x^{(2n)} = (\sin(\pi x/n), 0, \cos(\pi x/n)), \quad x = 0, \ldots, 2n-1. \tag{97}$$

For each state $|\varphi_x\rangle$ there exists an orthogonal state $|\bar{\varphi}_x\rangle$ on the opposite side of the Bloch sphere, which together form a basis. For $n = 2$, we recover the signal states of the BB84 protocol. In Fig. 6 the signal states of the $2n$-protocol for $n = 2, 3$ are represented on the Bloch sphere.

The symmetry group of the signal states of the $2n$-protocol is called the dihedral group denoted by D_{2n}. In the multiplication tables of Refs. [29,30], we find the form of the set $\mathbf{T}_{D_{2n}}$ for $n = 2, 3$. It turns out that $\mathbf{T}_{D_6} = \mathbf{T}_{D_4}$, where $\mathbf{T}_{D_4}$ contains the symmetrized states of the BB84 protocol given in Eq. (84) for $d = 2$. The error rate $Q = b + c$ of the $2n$-protocol with $n = 3$ is the same as for the BB84 protocol, where b and c are defined in Eq. (84). Thus we can conclude that $\bar{\mathbf{\Gamma}}_6 = \bar{\mathbf{\Gamma}}_4 \equiv \bar{\mathbf{\Gamma}}_{\mathrm{BB84}}$.

Let us define Alice's POVM elements of the BB84 and the $2n$-protocol by $A_x^{(BB84)}$ for $x = 1, \ldots 4$ and $A_{x'}^{(2n)}$ for $x' = 1, \ldots, 2n$. In both cases, the POVM elements are projectors onto the signal states. We can identify the group H in Theorem 5 by the phase-covariant symmetry group $D_\infty = \mathrm{U}(1) \times \Pi_2$, where Π_2 is the Pauli group of dimension 2 and U(1) is the unitary group. In the tables of Ref. [30], we find that the set $\mathbf{T}_{D_\infty}$ is identical to $\mathbf{T}_{D_4}$ and $\mathbf{T}_{D_6}$. The phase-covariant group contains all rotations about the axis $(0, 1, 0)$ on the Bloch sphere, as well as rotations by π about all axes lying in the (x, z)-plane. Thus, it also contains group elements that satisfy (III b) of Theorem 5 for any pair $A_x^{(BB84)}$ and $A_{x'}^{(2n)}$. Since all criteria of (III) are satisfied by D_∞, the optimal attack for the $2n$-protocol for $n = 3$ can be identified by the optimal phase-covariant cloner, which is also the optimal attack of the BB84 protocol.

C. Cuboid protocol

For some protocols with tomographically complete measurement settings the set $\bar{\mathbf{\Gamma}}$ contains more than one state. This has to do with loss of information during the symmetrization process. Recall that Alice and Bob only keep the averaged quantity Q, but otherwise ignore the measurement outcomes completely. This means that introducing symmetries to a problem can come at the expense of increasing the number of states in $\bar{\mathbf{\Gamma}}$.

As an example consider a qubit protocol where the signal states lie on the corners of a rectangular cuboid. The signal states are specified by the Bloch vectors

$$s_x = (\pm \sin\theta, \pm \cos\theta, 0), \tag{98}$$
$$s_z = (0, \pm \cos\theta, \pm \sin\theta), \tag{99}$$

where θ describes the angle between the $(0, y, 0)$-axis of the Bloch sphere and the corners of the cuboid. This protocol is composed of 4 bases. For each state $|\varphi_x\rangle$ there exists an orthogonal state $|\bar{\varphi}_x\rangle$ on the opposite side of the Bloch sphere.

The symmetry group of this protocol is the same as that of the BB84 protocol (D_4). Although (I) in Theorem 5 is satisfied, the error rate of the cuboid protocol is given by $Q = \frac{1}{2}[3b + c + (b - c)\cos(2\theta)]$, which is different from the BB84 error definition. Moreover, we could not find a group H to satisfy the condition (III). We performed numerical optimizations and found that the optimal attack of the cuboid protocol is not equal to the optimal attack on the BB84 protocol. It is also not the optimal cloner.

Note that, for $\theta = \frac{\pi}{2}$, we recover the BB84 protocol. For $\theta = \frac{\pi}{4}$ the signal states span a cube, which we already discussed in Sec. IX A.

X. CONCLUSION

In this paper we analyze the connection between the optimal attack on a QKD protocol and the optimal cloning attack in which the eavesdropper uses an optimal cloner to attack the protocol. We analyze protocols that have sufficient symmetries in the signal states and the postprocessing of the classical data, so that the optimal attack is, without loss of generality, a symmetric attack in the framework of the security proof of Refs. [1,2].

We compare the optimal symmetric attack to optimal covariant cloners. It turns out that a necessary condition for the cloning transformation to be an optimal attack is the strong covariance condition, which guarantees that the optimal attack and the optimal cloner are chosen from the same set. However, this condition is not sufficient to uniquely identify the optimal attack with the optimal cloner, except in the case where only one state is found in the set from which the optimal attack and the optimal cloner are chosen. Protocols which use $d + 1$ MUBs fall into this category.

We analyze the optimal attack of protocols using 2, d, and $d + 1$ MUBs in d-dimensional Hilbert spaces. Intuitively, one expects that the optimal attack can always be identified with an optimal cloner. We prove that this intuition is correct in the case of 2 and $d + 1$ MUBs, but for protocols using d MUBs, the connection between optimal attack and optimal cloner fails.

We show that two protocols using different signal states can be shown to give rise to the same optimal eavesdropping attack. Whether this is the case can be investigated by simple analysis of the symmetries of the signal states, and we give examples related to the 6-state and the BB84 protocol.

Note added. Recently, a related preprint [13] has appeared, where the key rates of protocols using 2 and $d + 1$ MUBs in d dimensions were calculated. In contrast to Ref. [13], our emphasis lies on establishing the general connection between optimal cloning and optimal eavesdropping.

ACKNOWLEDGMENTS

The authors would like to thank Xiongfeng Ma, Geir Ove Myhr, Tobias Moroder, Marco Piani, and Volkher Scholz for useful discussions, and especially Tobias Moroder who has provided the proof of Theorem 2. This work was supported by the European Projects SECOQC and QAP, by an NSERC Discovery Grant, OCE and Quantum Works.

APPENDIX A: POSTSELECTION

In many cases Alice and Bob share data at the end of the quantum phase of their protocol that contain unusable parts for the key generation. Typically, they postselect on a set of useful data. The postselection which we describe here applies, for example, to basis sifting, or to the case where Alice and Bob discard data points because Bob did not receive a signal.

Let us first examine the classical version of the postselection protocol, which starts with the ccq state ρ_{XYE}. In the postselection described here, an announcement is made for each individual signal. After the quantum phase, Alice and Bob identify the weakly correlated data that they want to filter out by calculating to each measurement outcome x and y some values $f(x) = v$ and $f(y) = w$ and announcing v and w publicly. Typically, the announcements v and w do not reveal any information about the key. Based on the announcements, Alice and Bob decide if they want to keep the measurement outcome or discard it. For example, they can keep only those events where $v = w \equiv u$. In particular, v and w often play the role of a basis announcement where Alice and Bob only keep those events which they measured in the same basis; namely, where $v = w \equiv u$, and discard the rest of the signals, where $v \neq w$. By identifying the values v and w, Alice and Bob effectively partition their original POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ into subsets $\mathbf{m}_A^v = \{A_x : f(x) = v\}$ and $\mathbf{m}_B^w = \{B_y : f(y) = w\}$, each containing the POVM elements labeled by the value v or w of the announcement.

The quantum version of the postselection procedure is described by the map $\mathcal{E}$, which is composed of two consecutive steps: First, the announcement and filtering, which is jointly described by a quantum operation, and second, the measurement of the remaining states.

The announcement and filtering is described by a quantum operation with Kraus operators $K_u \otimes L_u$ on $\mathcal{H}_A \otimes \mathcal{H}_B$. Since only events with $w = v \equiv u$ are kept, the Kraus operators come in paris $K_u \otimes L_u$ with the same index u. The Kraus operators satisfy $\sum_u K_u^\dagger K_u \otimes L_u^\dagger L_u \leqslant \mathbb{1}$, and they are related to the POVM elements in $\mathbf{m}_A^u$ and $\mathbf{m}_B^u$ by the rule $K_u = (\sum_{\mathbf{m}_A^u} A_x)^{1/2}$ and $L_u = (\sum_{\mathbf{m}_B^u} B_y)^{1/2}$. The probability that the state ρ_{AB} is kept during the postselection is p_{kept}. There is also a Kraus operator corresponding to the discarded events, which happens with probability $1 - p_{\text{kept}}$. For each Kraus operator, the information u is announced to all parties and stored in three classical registers $\bar{A}$, $\bar{B}$, and $\bar{E}$ held by Alice, Bob, and Eve, respectively. The state after the quantum operation held by Alice, Bob, and Eve, conditioned on kept events is given by

$$\psi = \sum_u p(u) |\Psi_u\rangle\langle\Psi_u| \otimes |u\rangle\langle u|_{\bar{A}\bar{B}\bar{E}}, \tag{A1}$$

where $|\Psi_u\rangle = K_u \otimes L_u \otimes \mathbb{1}_E|\Psi\rangle/\sqrt{\tilde{p}(u)}$ is the pure state conditioned on the announcement u with normalization $\tilde{p}(u)$, and $p(u) = \tilde{p}(u)/p_{\text{kept}}$ is the normalized probability distribution of the announcement u conditioned on events that were kept.

The announcement and filtering step is followed by a measurement to extract the remaining data. Each $|\Psi_u\rangle$ is measured with respect to new (normalized) POVMs $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ with elements conditioned on the announcement u:

$$\mathbf{M}_A^u = \{A_x^u\} = \{K_u^{-1} A_x K_u^{-1\dagger} : A_x \in \mathbf{m}_A^u\}, \tag{A2}$$

$$\mathbf{M}_B^u = \{B_y^u\} = \{L_u^{-1} B_y L_u^{-1\dagger} : B_y \in \mathbf{m}_B^u\}. \tag{A3}$$

The inverses K_u^{-1} and L_u^{-1} are defined on the nonzero subspace of K_u and L_u only. Again, the new POVMs only come in paris with the same index u.

The measurement of $|\Psi_u\rangle$ with respect to the new POVM, $\mathbf{M}^u = \mathbf{M}_A^u \otimes \mathbf{M}_B^u$, is equivalent to the measurement of $|\Psi\rangle$ with respect to the original POVM; namely, $\text{tr}_{AB}\{A_x^u \otimes B_y^u \otimes \mathbb{1}_E|\Psi_u\rangle\langle\Psi_u|\} = \frac{1}{\tilde{p}(u)}\text{tr}_{AB}\{A_x \otimes B_y \otimes \mathbb{1}_E|\Psi\rangle\langle\Psi|\}$. The measurement transforms $|\Psi_u\rangle$ into a ccq state:

$$|\Psi_u\rangle\langle\Psi_u| \to \rho_{XYE}^u = \sum_{\mathbf{M}^u} p_u(x,y)|x,y\rangle\langle x,y| \otimes \rho_E^{xy}, \tag{A4}$$

with $p_u(x,y) = \text{tr}\{A_x^u \otimes B_y^u \otimes \mathbb{1}_E|\Psi_u\rangle\langle\Psi_u|\} = p(x,y)/\tilde{p}(u)$ and the conditional states $\rho_E^{xy} = \text{tr}_{AB}\{A_x \otimes B_y \otimes \mathbb{1}|\Psi\rangle\langle\Psi|\}/p(x,y)$.

We choose to calculate the key rate from each ccq state ρ_{XYE}^u independently, which leads to the effective key rate

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \sum_u p(u) r\left(\rho_{XYE}^u\right). \tag{A5}$$

APPENDIX B: PROOF OF WEAK CONVEXITY OF CLASSICAL MUTUAL INFORMATION

In this Appendix we prove Theorem 1 of Sec. IV.

Proof. The mutual information $I(\rho_{AB}, \mathbf{M}_{AB})$ depends only on the probability distribution $p(x,y)$. For $\bar{\rho}_{AB}$ the mutual information is explicitly given by $I(\bar{\rho}_{AB}, \mathbf{M}_{AB}) = H(\bar{p}(x)) - H(X|Y)_{\bar{p}}$, where $H(p(x)) = -\sum_x p(x)\log_2 p(x)$ is the Shannon entropy, and $H(X|Y)_{\bar{p}} = \sum_{x,y}\bar{p}(x,y)\log_2(\frac{\bar{p}(x,y)}{\bar{p}(y)})$ is the conditional entropy. The first term satisfies

$$H(\bar{p}(x)) = H(p(x)) = H(q(x)), \tag{B1}$$

because $p(x) = q(x) = \bar{p}(x)$. The second term, the conditional entropy, is concave; namely,

$$H(X|Y)_{\bar{p}} \leqslant \lambda H(X|Y)_p + (1-\lambda)H(X|Y)_q, \tag{B2}$$

where $H(X|Y)_p = -\sum_{x,y} p(x,y)\log_2(\frac{p(x,y)}{p(y)})$ and similarly for $H(X|Y)_q$. The concavity of the conditional entropy is shown by applying the log-sum inequality [31],

$$\left(\sum_i a_i\right)\log_2\left(\frac{\sum_j a_j}{\sum_k b_k}\right) \leqslant \sum_i a_i \log_2\left(\frac{a_i}{b_i}\right), \tag{B3}$$

to $H(X|Y)_{\bar{p}}$. Equations (B1) and (B2) together imply the weak convexity of the classical mutual information. ■

APPENDIX C: PROOF OF CONCAVITY OF HOLEVO QUANTITY

In this Appendix we prove Theorem 2 of Sec. IV. We will use the traditional notation

$$\chi(X:E)_{\rho_{XE}} := \sum_x p(x) S\left(\rho_E^x\right)$$

to denote the Holevo quantity of the cq state $\rho_{XE} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_E^x$.

Proof. Given the states ρ_{AB} and σ_{AB} with purifications $|\Psi\rangle_{ABE'}$ and $|\Sigma\rangle_{ABE'}$ on the system $E = E'$. Alice measures the states with respect to the POVM elements A_x and stores the result in the system X. The cq states describing the situation for Alice and Eve after the measurement are

$$|\Psi\rangle \to \rho_{XE'} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_{E'}^x, \tag{C1}$$

$$|\Sigma\rangle \to \sigma_{XE'} = \sum_x q(x)|x\rangle\langle x| \otimes \sigma_{E'}^x, \tag{C2}$$

with Eve's conditional states $\rho_{E'}^x = \text{tr}_{AB}\{A_x \otimes \mathbb{1}|\Psi\rangle\langle\Psi|\}/p(x)$ and $\sigma_{E'}^x = \text{tr}_{AB}\{A_x \otimes \mathbb{1}|\Sigma\rangle\langle\Sigma|\}/q(x)$. The Holevo quantity of $\rho_{XE'}$ and $\sigma_{XE'}$ is given by

$$\begin{aligned}\chi(\rho_{AB}, \mathbf{M}_A) &= \chi(X:E')_{\rho_{XE'}},\\ \chi(\sigma_{AB}, \mathbf{M}_A) &= \chi(X:E')_{\sigma_{XE'}}.\end{aligned} \tag{C3}$$

We construct a particular purification on the joint system $E = E'F$ for the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$:

$$|\bar{\Psi}\rangle_{ABE'F} = \sqrt{\lambda}|\Psi\rangle|0\rangle_F + \sqrt{1-\lambda}|\Sigma\rangle|1\rangle_F. \tag{C4}$$

After measuring $|\bar{\Psi}\rangle_{ABE'F}$ with respect to A_x, the state shared by Alice and Eve is

$$\bar{\rho}_{XE'F} = \sum_x \bar{p}(x)|x\rangle\langle x| \otimes \bar{\rho}_{E'F}^x, \tag{C5}$$

with Eve's conditional states $\bar{\rho}_{E'F}^x = \text{tr}_{AB}\{A_x \otimes \mathbb{1}_{BE'F}|\bar{\Psi}\rangle\langle\bar{\Psi}|\}/\bar{p}(x)$ and $\bar{p}(x) = \lambda p(x) + (1-\lambda)q(x)$. The Holevo quantity of $\bar{\rho}_{XE'F}$ is

$$\chi(\bar{\rho}_{AB}, \mathbf{M}_A) = \chi(X:E'F)_{\rho_{XE'F}}.$$

Let $\mathcal{M}: F \to F'$ be a trace-preserving quantum operation. For our purposes, we identify $\mathcal{M}$ with a measurement on F in the standard basis $\{|0\rangle, |1\rangle\}$ and write the outcome in a new register F'. By defining $\lambda_x = \lambda\frac{p(x)}{\bar{p}(x)}$, the state after the measurement is given by

$$\rho_{XE'F'} = \sum_x \bar{p}(x)|x\rangle\langle x| \otimes \left[\lambda_x \rho_{E'}^x \otimes |0\rangle\langle 0|_{F'}\right. \tag{C6}$$

$$\left. + (1-\lambda_x)\sigma_{E'}^x \otimes |1\rangle\langle 1|_{F'}\right]. \tag{C7}$$

Let us state a lemma about the Holevo quantity extracted from a state of the form $\rho_{XE'F'}$:

Lemma 3. The Holevo quantity extracted from $\rho_{XE'F'}$ satisfies

$$\chi(X:E'F')_{\rho_{XE'F'}} \geqslant \lambda\chi(X:E')_{\rho_{XE'}} + (1-\lambda)\chi(X:E')_{\sigma_{XE'}}, \tag{C8}$$

with $\chi(X:E')_{\rho_{XE'}}$ and $\chi(X:E')_{\sigma_{XE'}}$ given in Eq. (C3). Equality holds if the probabilities λ_x are independent of x, $\lambda_x = \lambda$.

Proof. From $\rho_{XE'F'}$ we calculate the Holevo quantity using the joint entropy theorem of the von Neumann entropy [32]

$$\chi(X:EF') = \lambda\chi(X:E')_{\rho_{XE'}} + (1-\lambda)\chi(X:E')_{\sigma_{XE'}} + h(\lambda) - \sum_x \bar{p}(x)h(\lambda_x), \tag{C9}$$

with the binary entropy function $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ and where $\chi(X:E')_{\rho_{XE'}}$ and $\chi(X:E')_{\sigma_{XE'}}$ are given in Eq. (C3). From the concavity of the Shannon entropy it follows that $h(\lambda) - \sum_x \bar{p}(x)h(\lambda_x) \geqslant 0$ and, in particular, if $\lambda = \lambda_x$ for all x, the equality holds. ∎

According to Ref. [32], a map of the form $\mathcal{M}: F \to F'$ can only decrease the Holevo quantity:

$$\chi(X:E'F)_{\rho_{XE'F}} \geqslant \chi(X:E'F')_{\rho_{XE'F'}}. \tag{C10}$$

Equation (C8) together with Eq. (C10) show the desired result. ∎

APPENDIX D: PROOF OF LEMMA 2

In this Appendix we prove the G^*-invariance of ρ_A and A_x for the source-replacement scheme in Sec. II if $p(x)$ is uniformly distributed and if the signal states are G-invariant.

Proof. We trace out system S from the source state $|\Phi\rangle_{AS}$ in Eq. (2) and identify Alice's reduced state ρ_A by

$$\rho_A = \sum_i \kappa_i |i\rangle\langle i| = \sum_x p(x)|\varphi_x\rangle\langle\varphi_x|. \tag{D1}$$

From the G-invariance of the signal states and the uniform distribution of $p(x)$, it follows that ρ_A is also G-invariant. Since ρ_A is diagonal in the basis $\mathcal{B}$ with real eigenvalues κ_i, it holds that

$$\rho_A^* = \rho_A.$$

Therefore, ρ_A is also G^*-invariant (where the complex conjugate is taken with respect to the Schmidt basis), as can be easily seen from $U_g^*\rho_A U_g^T = (U_g\rho_A U_g^\dagger)^* = \rho_A$.

Due to the positivity of the coefficients κ_i and the full rank of ρ_A, the square root $\sqrt{\rho_A}$ and the inverse ρ_A^{-1} are well-defined. The G- and G^*-invariance of ρ_A^{-1} can be straightforwardly verified: $U_g\rho_A^{-1}U_g^\dagger = (U_g\rho_A U_g^\dagger)^{-1} = \rho_A^{-1}$, and similarly for the G^*-invariance.

In Ref. [17], it is shown for permutation groups that, for every positive G-invariant operator ρ_A, $\sqrt{\rho_A}$ is also G-invariant. The same proof applies also here and, thus, the G- and G^*-invariance of ρ_A also implies the G- and G^*-invariance of $\sqrt{\rho_A}$.

By using the G-invariance of the signals states and the G^*-invariance of $\sqrt{\rho_A}$ and ρ_A^{-1}, the G^*-invariance of A_x follows directly from the definition in Eq. (3).

APPENDIX E: PROPERTIES OF SYMMETRIZED STATES

The symmetrized states with the commutation property (36) can be characterized using Schur's lemma. Let the unitaries $U_g^{(\mu)}$ denote the irreducible representation μ of a group G on the Hilbert spaces $\mathcal{H}_\mu$. Every reducible representation of G can be decomposed into a direct sum of irreducible representations. For example, the tensor product $U_g^{(\nu)*} \otimes U_g^{(\nu)}$ is a reducible representation of G and can be decomposed into a (block diagonal) direct sum of irreducible representations $U_{g,i}^{(\mu)}$ defined on the spaces $\mathcal{H}_i^{(\mu)}$ carrying the irreducible representations μ:

$$U_g^{(\nu)*} \otimes U_g^{(\nu)} = \bigoplus_\mu \bigoplus_{i=1}^{m_\mu} U_{g,i}^{(\mu)}. \tag{E1}$$

Each irreducible representation μ occurs with integer multiplicity m_μ indicated by the index i.

According to Schur's lemma, an operator $\tau_{i,j}^{(\mu,\nu)}: \mathcal{H}_i^{(\mu)} \to \mathcal{H}_j^{(\nu)}$ that satisfies $\tau_{i,j}^{(\mu,\nu)}U_{g,i}^{(\mu)} = U_{g,j}^{(\nu)}\tau_{i,j}^{(\mu,\nu)}$ for all $g \in G$ is either (i) the identity map from $\mathcal{H}_i^{(\mu)} \to \mathcal{H}_j^{(\mu)}$ if $\mu = \nu$, or (ii) equal to zero. Using Schur's lemma, every positive operator $\bar{\rho}_{AB}$ that commutes with all the group elements of $U_g^{(\nu)*} \otimes U_g^{(\nu)}$ is characterized by

$$\bar{\rho}_{AB} = \bigoplus_\mu \bigoplus_{i,j=1}^{m_\mu} c_{ij}^{(\mu)}\tau_{ij}^{(\mu)}, \tag{E2}$$

where the $c^{(\mu)}$ are $m_\mu \times m_\mu$ matrices with positive eigenvalues $\lambda_i^{(\mu)}$, and $\tau_{ij}^{(\mu)}$ is the identity map between the subspaces with equal representation. After diagonalizing $c^{(\mu)}$, we can rewrite $\bar{\rho}_{AB}$ in a block diagonal form on a new decomposition $\mathcal{K}_i^{(\mu)}$ of the Hilbert space by

$$\bar{\rho}_{AB} = \bigoplus_\mu \bigoplus_{i=1}^{m_\mu} \lambda_i^{(\mu)}\mathbb{1}_i^{(\mu)}, \tag{E3}$$

where $\mathbb{1}_i^{(\mu)}$ is the identity on the subspace $\mathcal{K}_i^{(\mu)}$. The block diagonal form of $U_g^{(\nu)*} \otimes U_g^{(\nu)}$ is quasi "inherited" by $\bar{\rho}_{AB}$.

APPENDIX F: POSTSELECTION ON ORTHONORMAL BASES

In this Appendix we calculate the filters K_u and L_u for the class of protocols described in Sec. V D.

Given a protocol where the set of signal states $\mathbf{S}_\mathcal{L}$ contains $|\mathcal{L}|$ complete bases. Alice and Bob announce the basis of each signal, which partitions the POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ into $|\mathcal{L}|$ disjoint sets $\mathbf{m}_A^v = \{A_{(\beta,k)} : \beta = v\}$ and $\mathbf{m}_B^w = \{B_{(\beta,k)} : \beta = w\}$. They decide to keep only those events which were measured in the same basis [e.g., those where they made the same announcement $f(x) = f(y) = u$]. Each set is associate with the filters

$$K_u = L_u = \frac{\mathbb{1}}{\sqrt{|\mathcal{L}|}}, \tag{F1}$$

which are proportional to the identity for all u.

Let Alice and Bob share a state ρ_{AB} with a purification $|\Psi\rangle$. Due to the particular form of the filters, it follows that $|\Psi_u\rangle = |\Psi\rangle$, and that the new POVMs $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ are only a rescaled version of the old ones:

$$\mathbf{M}_A^u = \{|\mathcal{L}|\ A_{(\beta,k)} : \beta = u\}, \tag{F2}$$

$$\mathbf{M}_B^u = \{|\mathcal{L}|\ B_{(\beta,k)} : \beta = u\}. \tag{F3}$$

[1] I. Devetak and A. Winter, Proc. R. Soc. London A **461**, 207 (2005).
[2] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[3] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] T. Durt, N. J. Cerf, N. Gisin, and M. Żukowski, Phys. Rev. A **67**, 012311 (2003).
[6] T. Durt, D. Kaszlikowski, J.-L. Chen, and L. C. Kwek, Phys. Rev. A **69**, 032313 (2004).
[7] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[8] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[9] G. Chiribella, G. M. D'Ariano, P. Perinotti, and N. J. Cerf, Phys. Rev. A **72**, 042336 (2005).
[10] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[11] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[12] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[13] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[14] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[15] R. Renner, Nature Physics **3**, 645 (2007).
[16] R. Renner, Ph.D. thesis, ETH Zürich, 2005.
[17] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[18] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[19] I. D. Ivanovic, Phys. Lett. A **228**, 329 (1997).
[20] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[21] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[22] F. Caruso, H. Bechmann-Pasquinucci, and C. Macchiavello, Phys. Rev. A **72**, 032340 (2005).
[23] W. Wootters and B. Fields, Ann. Phys. (NY) **191**, 363 (1989).
[24] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2008).
[25] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[26] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[27] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[28] L.-P. Lamoureux and N. J. Cerf, Quantum Inf. Comput. **5**, 32 (2005).
[29] G. Koster, J. Dimmock, R. Wheeler, and H. Statz, *The Properties of the Thirty-Two Point Groups* (M.I.T. Press, Cambridge, 1963).
[30] P. Butler, *Point Group Symmetry Applications: Methods and Tables* (Plenum Press New York, London, 1981).
[31] T. Cover and J. Thomas, *Elements of Information Theory* (John Wiley and Sons, Inc., New York, 2001).
[32] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).