Security of two-way quantum key distribution

Normand J. Beaudry,[1] Marco Lucamarini,[2] Stefano Mancini,[3] and Renato Renner[1]

[1]*Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland*

[2]*Cambridge Research Laboratory, Toshiba Research Europe Ltd., 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom*

[3]*School of Science and Technology, University of Camerino, Camerino 62032, Italy*

Quantum key distribution protocols typically make use of a one-way quantum channel to distribute a shared secret string to two distant users. However, protocols exploiting a two-way quantum channel have been proposed as an alternative route to the same goal, with the potential advantage of outperforming one-way protocols. Here we provide a strategy to prove security for two-way quantum key distribution protocols against the most general quantum attack possible by an eavesdropper. We utilize an entropic uncertainty relation, and only a few assumptions need to be made about the devices used in the protocol. We also show that a two-way protocol can outperform comparable one-way protocols.

I. INTRODUCTION

Quantum key distribution (QKD) research has been primarily focused on one-way protocols: One party, Alice, prepares states, sends them through an insecure quantum channel, and then another party, Bob, does a measurement [1,2]. However, in the last decade, two-way protocols have been proposed where Bob prepares states, sends them to Alice through an insecure quantum channel, Alice does an encoding on the states, sends them backwards through the same quantum channel, and then Bob performs a measurement [3–7]. Paradigmatic examples of these kind of protocols are the so-called "Ping-Pong" protocol [6] and the LM05 protocol [7]. The former uses entangled states, while the latter uses nonorthogonal states. They have also been experimentally realized [8–11].

It is not yet clear what the full potential of two-way protocols is, but there are at least several reasons why they are interesting. One motivation is that some two-way protocols are deterministic, that is, they do not require any sifting of the raw keys generated due to a mismatch of basis choices. For example, the LM05 protocol [7] has this advantage. The Ping-Pong protocol, which is based on super dense coding (SDC) [12], has no basis choices and therefore is also deterministic. Moreover, this protocol is conceptually interesting, as SDC can be turned into a QKD protocol.

One implementation of two-way protocols is to use polarization encoding of photons in fiber optics. The polarization drift caused by the fiber then needs to be actively corrected [13–15]. However, if signals are sent backwards through the same channel, then the polarization drift is passively corrected by the use of a Faraday mirror at Alice's side. This means that there may be experimental situations in which one-way QKD does not succeed because the error rate is too high but two-way QKD may still be possible. One QKD protocol that exploits this fact is the "Plug & Play" BB84 protocol [16,17].

This implementation ideally yields one raw key bit for each qubit signal sent from Bob to Alice and then from Alice to Bob. From SDC we know that two bits can be communicated by only sending one qubit in this manner. Therefore, another motivation is that the key rate can be increased by using the SDC protocol instead of Plug & Play BB84 by using the same channel resources and without the need of higher dimensional states or more complicated measurements.

A major difficulty when studying the security of two-way protocols is that the eavesdropper, Eve, can attack each signal twice: once on the way from Bob to Alice, and later on its way back from Alice to Bob. This gives her more strategies than in a one-way QKD protocol. In fact, the Ping-Pong protocol has been shown to be insecure [18,19], while recently the LM05 protocol was proven secure, but by assuming the use of qubits and the full characterization of all of the devices [20,21]. In addition, the Plug & Play protocol was proven secure [22,23] but by using strong assumptions (e.g., an intensity monitor, phase randomizer, and attenuator are required, and all devices, except the source, are fully characterized).

Unlike these previous approaches, we propose a general security proof strategy through which devices used in the protocol only need to be characterized by a few assumptions. Our assumptions are on the same level as one-way QKD security proofs that use uncertainty and complimentarity, such as the proofs by Mayers [24] and Koashi [25]. This is in contrast to device-independent security proofs where no assumptions are made about devices used in the protocol. However, they require loophole free Bell tests, which are not possible with current technology [26–28]. Our assumptions lie between the device-dependent scenario, where devices are completely characterized, and the device-independent scenario. For example, a device may be characterized by a single constant that can be experimentally bounded.

Our proof strategy consists of two main steps. First we show how to "purify" prepare and measure protocols into entanglement-based protocols. Second, we apply the entropic uncertainty relation proposed as a tool for security proofs of one-way protocols to the purified protocols [29]. An entanglement-based or purified protocol is one where Eve prepares a state, sends a part of the state to Alice and another

part to Bob, and then Alice and Bob perform measurements. The uncertainty relation we use states [29]: Given a tripartite quantum state ρ_{ABE} and two measurements on system A, F_X, and F_Z, described by elements of a positive-operator valued measure (POVM) $\{F_X^i\}_i$ and $\{F_Z^i\}_i$ with classical outcomes X and Z, respectively, then

$$H(Z|B) + H(X|E) \geqslant \log_2 1/\gamma, \tag{1}$$

where $H(A|B)$ is the conditional von Neumann entropy, $\gamma = \max_{i,j} \|\sqrt{F_X^i} \sqrt{F_Z^j}\|_\infty^2$ (which we call the overlap between the measurements F_X and F_Z). Given an operator F acting on a Hilbert space $\mathcal{H}$ such that $F \geqslant 0$, then $\|F\|_\infty := \max\{\langle\phi|F|\phi\rangle : \phi \in \mathcal{H}, \langle\phi|\phi\rangle = 1\}$ is the operator norm on positive operators. Using this uncertainty relation and the Devetak-Winter security bound [30], we demonstrate how to prove security against the most general type of attacks for two-way protocols.

Actually we use this method to prove security for two example protocols: a super dense coding (SDC) protocol similar to the Ping-Pong protocol [6] and a protocol similar to LM05 (which we will also refer to as LM05) [7]. For the LM05 protocol we show an improvement of the key rate of [20]. Furthermore, we provide a comparison among relevant two-way and one-way protocols showing that the former can outperform the latter.

Our proof clarifies the analysis of two-way QKD protocols and provides an important step towards device-independent security of quantum cryptography in this framework. In addition, our results illustrate that the uncertainty relation Eq. (1) can be useful to prove security of QKD protocols other than BB84.

We proceed by first defining the SDC and LM05 protocols in the scenario where only qubits are used. Second, we describe purified versions of these protocols in order to apply the uncertainty relation Eq. (1). Third, we list the assumptions that are needed for the application of this security proof to implementations of these protocols. Fourth, we prove the security of the protocols. Lastly, we compare the key rates to different implementations of the BB84 protocol.

II. PROTOCOL DEFINITIONS

In the descriptions of the SDC and LM05 protocols below we assume that the states are deterministically prepared and all devices are completely characterized. This is for the ease of describing the protocols and this assumption is not necessary for the security proofs.

There are some similarities between both protocols: They have two quantum channels between Alice and Bob, Q_1 and Q_2, which can be attacked by the eavesdropper, Eve, using any strategy allowed by quantum mechanics. Alice and Bob will also be performing some X- and Z-basis measurements. These refer to the projections onto the eigenvectors of the Pauli operators σ_X and σ_Z, respectively. In addition, Alice and Bob will do parameter estimation, error correction, and privacy amplification on their raw data after the steps outlined below. They abort their protocol if during parameter estimation they find that one of their relevant error rates is beyond a certain threshold.
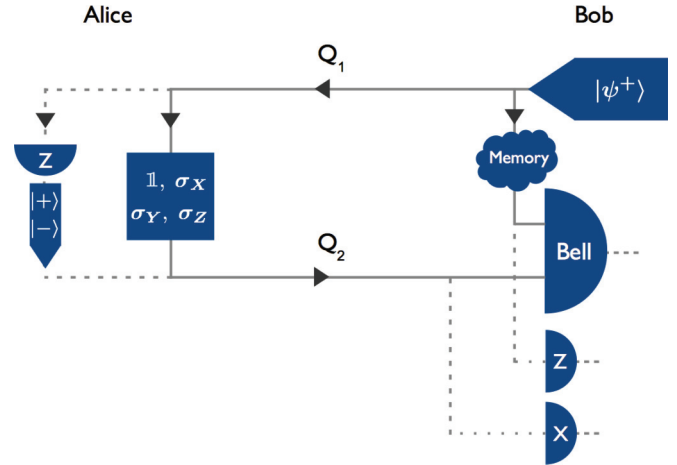

FIG. 1. (Color online) Depiction of the ideal qubit SDC protocol. Bob prepares the Bell state $|\psi^+\rangle$, and keeps half of it in a quantum memory. He sends the other half to Alice who either does an encoding (with probability c, solid line) or does the Z-basis measurement which indicates whether she prepares $|+\rangle$ or $|-\rangle$ (with probability $1-c$, dashed line). Alice sends this state to Bob who does a Bell measurement with his stored qubit and the qubit from Alice (with probability c, solid line) or does a $Z \otimes X$-basis measurement (with probability $1-c$, dashed line).

A. Qubit SDC protocol

Bob's preparation. Bob prepares a maximally entangled state $|\psi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and keeps one-half of it in a quantum memory. He sends the other half to Alice through channel Q_1 (see Fig. 1).

Alice. With probability $c \approx 1$ Alice applies one of the four Pauli operators $\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z$ (choosing each with probability $1/4$) to the state from the channel Q_1. She records her choice by storing two classical bits: $00, 10, 11, 01$, respectively. Alice then sends this state into channel Q_2 back to Bob. With probability $1-c$ Alice measures the state from channel Q_1 in the Z basis. She then prepares $|+\rangle$ with probability $1/2$ or $|-\rangle$ with probability $1/2$, where $|\pm\rangle := 1/\sqrt{2}(|0\rangle \pm |1\rangle)$, and sends it into channel Q_2 to Bob.

Bob's measurement. With probability c Bob performs a Bell measurement jointly on his stored qubit and his received qubit from the channel Q_2. He gets possible outcomes $|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$, and then will store the bits $00, 01, 10, 11$, respectively. With probability $1-c$ he measures his stored qubit in the Z basis and his received qubit in the X basis.

Postprocessing. Alice and Bob repeat the above procedure N times. Their raw key is the concatenation of all of their two-bit strings together, respectively. Alice publicly announces which signals she encoded and which signals she measured.

B. Qubit LM05 protocol

In the LM05 protocol [7] Alice and Bob will have the choice to perform either an X- or Z-basis measurement. We use a parameter p to denote the probability that Alice and Bob choose the Z basis, so $1-p$ is the probability that they choose the X basis. We will consider two possible versions of the protocol for the simplicity of presentation. Version 1 is
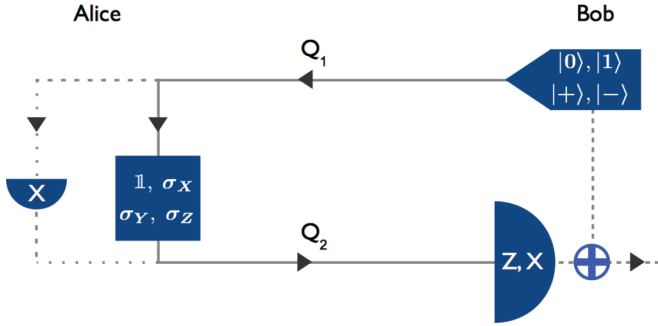
FIG. 2. (Color online) Version 1 of the ideal qubit LM05 protocol. Bob prepares one of the four BB84 states and sends it Alice. Alice performs an encoding (with probability c, solid line), or a measurement in the X basis followed by the sending of the postmeasurement state (with probability $1 - c$, dashed line). Bob performs a measurement in the Z or X basis whenever he prepared states in the Z or X basis, respectively. Bob then does an XOR of his measured bit and his preparation bit corresponding to his prepared state.

when $p \approx 1$, and Alice and Bob will only use their X-basis measurement for parameter estimation (see Fig. 2). Version 2 is when $p = 1/2$ and then they will use both X- and Z-basis measurements for parameter estimation and key generation. Note that the choice of p will not affect the key rate.

Bob's preparation. Bob prepares one of the four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. He chooses $|0\rangle$ or $|1\rangle$ each with probability $p/2$, and $|+\rangle$ or $|-\rangle$ each with probability $(1 - p)/2$. When he picks either $|0\rangle$ or $|+\rangle$ he classically stores a 0, when he picks either $|1\rangle$ or $|-\rangle$, he stores a 1 (we refer to this bit as the preparation bit). Bob also stores the basis the state is in. He sends the state to Alice through channel Q_1 (see Fig. 2).

Alice. With probability $c \approx 1$ Alice applies one of $\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z$ (choosing each with probability $1/4$) to the state from the channel Q_1. She records her choice of encoding. With probability $1 - c$ she applies an X-basis measurement (Version 1), or randomly chooses either an X- or Z-basis measurement (Version 2). Alice then takes the postmeasurement state (when a measurement was performed) or the encoded state (where a Pauli operator was applied) and sends it to Bob through channel Q_2.

Bob's measurement. Bob does a measurement in the same basis he prepared his state in: If he prepared $|0\rangle$ or $|1\rangle$ then he measures in the Z basis; if he prepared $|+\rangle$ or $|-\rangle$ then he measures in the X basis.

Postprocessing. Alice and Bob repeat this procedure N times. If they perform reverse reconciliation then Bob publicly reveals which basis he used for each signal, and Alice reveals which signals she measured and which she encoded. In Version 2 Alice also reveals which basis she measured in for each signal and then Alice and Bob discard their measurement results wherever they measure in different bases. Bob's raw key is the result of the XOR of his measurement outcomes with his preparation bits. Alice's raw key is made up of one of the two classical bits $00, 10, 11, 01$ corresponding to the encodings $\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z$, respectively. Whenever Bob measured in the Z basis Alice keeps her first bit, and when Bob measured in the X basis Alice keeps the second bit.

In direct reconciliation, Bob does not reveal his basis choice and instead Alice reveals whether she applied one of the

encodings from the set $S_0 := \{\mathbb{1}, \sigma_Y\}$ or the set $S_1 := \{\sigma_X, \sigma_Z\}$. Alice corresponds the encodings $\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z$ with the bits $0, 1, 1, 0$, respectively. Bob then needs to flip his raw bit for each signal that he used the X basis and Alice announces she applied an encoding from S_1.

We now purify these two prepare and measure QKD protocols by showing that they are equivalent to protocols that start with entangled states distributed by Eve followed by measurements by Alice and Bob.

III. PURIFIED PROTOCOLS

We introduce two purified protocols that are structured such that a pure state is shared between Alice, Bob, and Eve; then Alice and Bob perform measurements on this state. These purified protocols are equivalent to the prepare and measure protocols described above. However, fewer assumptions are needed about the devices used. In the next section we will explain exactly which assumptions about the devices in the prepare and measure protocol are necessary in order to apply our security proofs. Afterwards we will prove the security of the purified protocols.

We can purify Alice's encoding operation in both protocols by finding an equivalence to a POVM acting on the input of the encoding and half of a pure state such that the other half of the pure state is the same as the output from Alice's encoding (see Fig. 3). In addition, the outcome of the POVM is two random bits independent of the input and therefore is the same as Alice's choice of encoding operation using a random string. We use the following lemma to achieve this equivalence (see the Appendix for the proof). For the lemma, we define the set of normalized positive semidefinite operators on a Hilbert space $\mathcal{H} : S(\mathcal{H}) := \{\tau \in \mathcal{P}(\mathcal{H}) : \text{Tr}(\tau) = 1\}$, where $\mathcal{P}(\mathcal{H})$ is the set of positive semidefinite operators on $\mathcal{H}$.

Lemma 1. Let $\{\mathcal{E}_i\}_{i=1..n}$ be a set of n completely positive trace-preserving maps from Hilbert space $\mathcal{H}_A$ to Hilbert space $\mathcal{H}_D$ and $\sigma_D \in S(\mathcal{H}_D)$ be a fixed density operator on $\mathcal{H}_D$ such
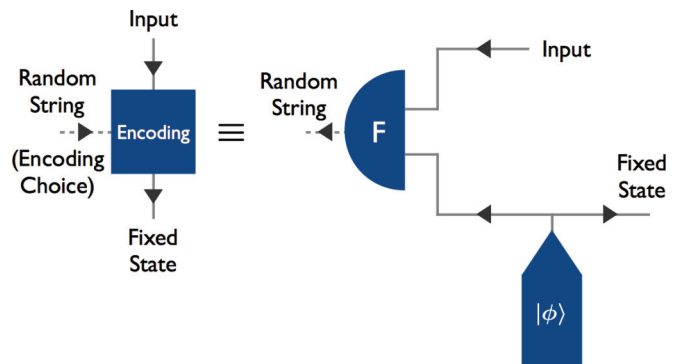

FIG. 3. (Color online) A depiction of Lemma 1. An encoding that takes a quantum state and a random string as input, which is used to choose which encoding to perform, always outputs a fixed state (averaged over all encoding choices). This encoding is equivalent to the scenario where a measurement F acts jointly on the same quantum state input as the encoding and half of a bipartite pure state $|\phi\rangle$. The output of the measurement is a random string, and the other half of $|\phi\rangle$ is then the same fixed state output from the encoding, averaged over all measurement outcomes of F.

that

$$1/n \sum_{i=1}^{n} \mathcal{E}_i(\rho_A) = \sigma_D \; \forall \rho_A \in S(\mathcal{H}_A). \tag{2}$$

Then there exists a fixed pure state $|\phi\rangle_{CD}$ in $\mathcal{H}_{CD} := \mathcal{H}_C \otimes \mathcal{H}_D$, where $\dim \mathcal{H}_C = \dim \mathcal{H}_D$, and a complete set of POVM elements $\{F_{AC}^i\}_{i=1..n}$ on $\mathcal{H}_{AC}$ (so $\sum_i F_{AC}^i = \mathbb{1}_{AC}$), such that $\forall i, \forall \rho_A \in S(\mathcal{H}_A)$ we have

$$n \mathrm{Tr}_{AC}\big(F_{AC}^i \rho_A \otimes |\phi\rangle_{CD}\langle\phi|\big) = \mathcal{E}_i(\rho_A). \tag{3}$$

In the prepare and measure protocol there were four encodings that Alice could do, and therefore $n = 4$ for the application of this lemma. Now that the encoding is purified, we purify all of the preparations of both protocols.

In the perfect qubit version of both protocols, Alice and Bob's preparations are equivalent to starting with a maximally entangled state $|\psi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ followed by a Z- or X-basis measurement (or probabilistic distribution over the choice of the two measurements). More generally, if we only assume that the preparations are of qubits then they are equivalent to the maximally entangled state $|\psi^+\rangle$, followed by a measurement on one of the two qubits. The nonmeasured qubit is then the same as the prepared qubit [31]. It only makes Eve more powerful to prepare both entangled states from Alice's encoding and from the purifications of the preparations, so we can let her prepare these states.

Now the protocols can be described as follows. Eve prepares a state ρ_{ABE} and sends A to Alice and B to Bob, and keeps part E. Alice and Bob perform one of two measurements on each of their systems. Then Alice and Bob do postprocessing as in the prepare and measure protocol. Before we prove the purified protocol's security, we outline which assumptions we will make for the security proof to hold.

IV. ASSUMPTIONS

To specify exactly when our security proofs will apply, we explicitly state the assumptions we will make about the devices used in the protocols. Afterward we will discuss how these assumptions can be justified.

(1) The states prepared are qubits. This assumption can be avoided if instead an arbitrary bipartite state is prepared and a measurement is performed on one-half of it, while sending the other half into the appropriate channel. It can be assumed that Eve holds a purification of this prepared bipartite state.

(2) The output state of Alice's encoding operation is independent of the input state, when averaged over all encodings. Mathematically, this means that the encoding satisfies Eq. (2) in Lemma 1.

(3) Measurements detect each signal independently. This means that the POVM elements have an i.i.d. form.

(4) Bob's devices (when reverse reconciliation is performed) or Alice's devices (when direct reconciliation is performed) are characterized by a constant overlap γ, defined after Eq. (1).

(5) There are no losses in the channels or detectors.

Assumption 1 is needed in order to purify the preparation process. Assumption 2 is needed in order for the encoding to have a purified form. Assumption 3 is needed so that we can an-

alyze the measurement outcomes in an i.i.d. way. Assumption 4 is needed to apply the uncertainty relation Eq. (1). Assumption 5 is made for the convenience of the security analysis, but can be removed if Alice and Bob randomly assign a bit value for their measurement in a time where a signal was sent but they did not receive a measurement outcome.

Assumption 1 is valid if the preparations are done in a purified way. Assumptions 2 and 3 are idealized assumptions necessary for our security proof method. However, Assumption 3 is common for both device-independent and device-dependent security proofs [26–28]. Assumption 2 requires knowledge about Alice's encoding device, and could be justified to a good approximation. Such assumptions are typical for device-dependent security proofs [1]. However, Assumption 2 is not necessary if the purified protocol is implemented directly.

The overlap γ that characterizes the devices in Assumption 4 cannot be obtained without a description of the POVMs for the measurements (if reverse reconciliation is performed), or a description of the encoding map (if direct reconciliation is performed). However, Alice and Bob can put a bound on a so-called "effective overlap": γ^*. This effective overlap is defined differently than the overlap in Eq. (1) (see Definition 7.2 in [32]), but it satisfies the same uncertainty relation:

$$H(Z|B) + H(X|E) \geqslant \log_2 1/\gamma^*. \tag{4}$$

The effective overlap has the advantage that it can be upper bounded by measuring a CHSH value [33] if the measurements have binary outcomes. We now define the CHSH value and then we will describe the upper bound on the effective overlap. Given a bipartite system, let M and N be random variables representing the measurement outcomes from choosing one of two measurements randomly on one part of the system, and let R and S be random variables representing the measurement outcomes from choosing one of two measurements randomly on the other half of the system. Then the CHSH value β is defined as

$$\beta := 2[\Pr(M = R) + \Pr(N = R) \\ + \Pr(M = S) + \Pr(N \neq S)] - 4.$$

Since the LM05 protocol measurements and encoding choice are binary, the CHSH value provides an upper bound for the effective overlap. It is not yet known if the same relation between the effective overlap and a CHSH value holds for more than two measurement outcomes [34]. Therefore, it is not known how the effective overlap may be upper bounded by the CHSH value for the SDC protocol since there are four measurement outcomes and four encoding choices in this protocol.

For the LM05 protocol, as long as preparations are done in a purified way, Alice and Bob can run Version 2 of the LM05 QKD setup and find the CHSH value between Alice's encoding choice and Bob's measurement outcomes. More precisely, Bob's XOR of his Z- and X-basis measurement outcomes with his preparation bit define the random variables R and S, while Alice's bit values that correspond to the encoding sets S_0 and S_1 define M and N. Despite Alice not performing a measurement we can still define the CHSH value this way, since from Assumption 2 we are guaranteed that Alice's encoding corresponds to a measurement via Lemma 1, where her encoding choice corresponds to the measurement's outcomes.

The effective overlap is bounded by

$$\gamma^* \leqslant \frac{1}{2} + \frac{\beta}{8}\sqrt{8 - \beta^2}. \tag{5}$$

Note that no additional devices are needed to put a bound on the effective overlap. In addition, if desired, Alice or Bob (depending on whether direct or reverse reconciliation is performed) can measure the CHSH value by themselves by using another measurement device on their side. Alice can measure her CHSH value in the same way as Alice and Bob did it jointly. Bob can measure his CHSH value by running the purified QKD setup. In summary, Assumption 4 can be justified by an experimental test on the devices used in the LM05 protocol (see [32,34] for more details).

For the security proofs below we fix the overlap in Assumption 4 for each protocol. The overlap for the SDC protocol, when reverse reconciliation is performed, between Bob's two measurements is assumed to be 1/4 (which is true for the ideal Bell and $Z \otimes X$-basis measurements). For the LM05 protocol, where Bob's preparations are done with a bipartite state and a measurement, we assume that there are two measurements that have an overlap of 1/2 with Bob's measurements followed by an XOR of the outcomes. The first is his measurement on half of his prepared pure state in the other basis and the second is his measurement in the other basis on channel Q_2. Note that this overlap occurs between the ideal $Z \otimes Z$-basis measurement followed by an XOR of the outcomes and the X-basis measurement on his prepared pure state and his X-basis measurement on the input from channel Q_2. In the case of direct reconciliation this assumption changes to the overlap between Alice's POVM associated with her encoding (via Lemma 1) and her measurement tensored with her purified preparation measurement. While we have made these rigid assumptions for the security proofs, we can relax the assumption that this overlap is exactly 1/2 for the LM05 protocol and instead use the CHSH value bound on the effective overlap [32,34].

Assumption 5 is clearly not experimentally justifiable. However, it can be removed if, whenever there is a missing measurement outcome at Alice or Bob's detector, Alice and Bob randomly assign a bit value. The error rates will be increased, decreasing the key rate significantly. We leave a more detailed analysis of loss as future work, which could follow along similar lines as [31].

It is important to note that no assumptions are necessary about the Hilbert space that the signals of the protocols are in (except, possibly, qubit preparations). In addition, no assumptions need to be made about the internal structure of the measurements on each signal, descriptions of the preparations of bipartite states, or the quantum memory used in the SDC protocol.

V. SECURITY PROOFS

The security proofs of the purified protocols can be found via the Devetak-Winter rate [30], followed by the application of the uncertainty relation of Eq. (1) [29]. The security proofs can then be applied to the nonpurified SDC and LM05 protocols since they are equivalent to the purified protocols. This equivalence is guaranteed under Assumptions 1 and 2 of the previous section.

A. SDC protocol

Now we define some states useful for the security proof. The state that Alice, Bob, and Eve share after Alice and Bob have done their measurements is

$$\tau_{Z_A Z_B E} = F_A \otimes F_B(\rho_{ABE}), \tag{6}$$

where Z_A and Z_B are the classical strings that result from Alice and Bob's measurements, F_A and F_B, which are represented as completely positive trace-preserving (CPTP) maps. We assume that the measurements F_A and F_B act independently on each signal, so that we can apply the uncertainty relation to each measurement independently. Using Assumption 3 from the previous section, the measurement's POVM elements have the form $\{\bigotimes_j F_A^{i_j}\}_i$ and $\{\bigotimes_j F_B^{i_j}\}_i$, where $i = i_1 i_2 i_3 \ldots$. We also define another state ξ, where we only change Alice's measurement. This state has the important property that $H(Z_B|E)_\tau = H(Z_B|E)_\xi$. Intuitively this means that Eve's information about Bob's string does not depend on Alice's measurement. The state ξ is defined as

$$\xi_{X_A Z_B E} = G_A \otimes F_B(\rho_{ABE}), \tag{7}$$

where X_A is the classical string output from the measurement G_A on Alice's side. We do not characterize G_A. However, we assume that the POVM elements of G_A are independent, and therefore have the form $\{\bigotimes_j G_A^{i_j}\}_i$ (Assumption 3). We now define a third state that will be used for the application of the uncertainty relation [29]:

$$\sigma_{X_A X_B E} = G_A \otimes G_B(\rho_{ABE}), \tag{8}$$

where G_B have POVM elements of the form $\{\bigotimes_j G_B^{i_j}\}_i$ (Assumption 3) and its classical output is denoted as X_B. In addition, the only characterization we make for any of the measurements is that the overlap between G_B and F_B is $\max_{ij} \|F_B^{i_k} G_B^{j_k}\|_\infty^2 = 1/4 \; \forall \; k$ (Assumption 4).

If Alice and Bob do one-way classical communication for the postprocessing after the protocol from Alice to Bob and Bob's measurement outcomes are used as the raw key (which we call reverse reconciliation), then we can write the Devetak-Winter rate [30] as

$$r \geqslant H(Z_B|E)_\tau - H(Z_B|Z_A)_\tau \tag{9}$$

$$\geqslant H(Z_B|E)_\xi - h_4(q_F) \tag{10}$$

$$\geqslant 2 - H(X_B|X_A)_\sigma - h_4(q_F) \tag{11}$$

$$\geqslant 2 - h_4(q_G) - h_4(q_F), \tag{12}$$

where h_d is the d-ary Shannon entropy, q_F is the error rate probability distribution generated from Z_A and Z_B, and q_G is the error rate probability distribution generated from X_A and X_B. Specifically, these error rate probability distributions consist of the probability that both bits are the same, both bits are different, only the first bit is different, and only the second bit is different.

In going from Eq. (9) to Eq. (10) we use the fact that $H(Z_B|E)_\tau = H(Z_B|E)_\xi$ and we upper bound the entropy $H(Z_B|Z_A)_\tau$ by $h_4(q_F)$ by using the method of types (Lemma II.2 of [35]). From Eq. (10) to Eq. (11) we use the uncertainty relation Eq. (1) with the measurements F_B and G_B. In Eq. (12) we use the method of types to bound $H(X_B|X_A)_\sigma$ by $h_4(q_G)$.

Alice and Bob estimate the error rates q_G and q_F by revealing X_A and X_B as well as a small fraction of their Z_A and Z_B strings in jointly specified positions chosen uniformly at random. Alice and Bob have access to these strings in the prepare and measure SDC protocol because Bob actually performs F_B and G_B (these are the Bell and $Z \otimes X$ measurements in the perfect qubit scenario, respectively); Alice uses her encoding bits (which correspond to her string Z_A in the purified protocol via Lemma 1); and her measurement and her resending of the postmeasurement state correspond to X_A.

We have permutation invariance of the two-bit outcomes and so we can apply the quantum de Finetti theorem of Renner [36] to the protocol. Therefore the key rate Eq. (12) is applicable for the most general type of attacks by Eve. Due to the symmetry of the purified protocol we could equivalently do direct reconciliation, where Alice uses her classical string as the key and Bob corrects his raw string. In this case the key rate is the same.

B. LM05 protocol

The security proof of this protocol follows the same method as the proof for the SDC protocol, however, there are two differences that need to be taken into account. The first is that Bob chooses a different basis for each of his individual inputs from the channel Q_2 according to a classical string Θ. When a bit of Θ is 0, Bob will measure in the Z basis, and when a bit of Θ is 1, Bob will measure in the X basis. The other difference is that there are two different measurements that have the desired overlap with Bob's measurement F_B in the uncertainty relation Eq. (1) in the main text. In the perfect purified protocol, Bob's measurement is a $Z \otimes Z$-basis measurement followed by an XOR of the two measurement outcomes. Note that this measurement only has a one-bit outcome, and therefore the minimum overlap it can have with another measurement is $1/2$. The $Z \otimes Z$ measurement with an XOR has two measurements with overlap $1/2$, as can be easily verified: measuring the first qubit in the X basis and discarding the second qubit or measuring the second qubit in the X basis and discarding the first qubit.

Now we define three states as we did in the SDC protocol's security proof. We consider the case where reverse reconciliation is performed and we discuss the case of direct reconciliation at the end of this section. The state that Alice and Bob share after they have done their measurements, Bob has publicly announced his basis choices, and Alice has done the sifting of her encoding bits is

$$\tau_{W_A W_B E} = \sum_{\Theta} F_A^{\Theta} \otimes F_B^{\Theta}(\rho_{\mathrm{ABE}}) \otimes |\Theta\rangle\langle\Theta|. \qquad (13)$$

The classical outcomes of the measurements for Alice and Bob are written as W_A and W_B, respectively. We assume (Assumption 3) that F_A^{Θ} and F_B^{Θ} have POVM elements that are independent on each signal so that the uncertainty relation can be applied to each individual measurement. They have the form $\{\bigotimes_k F_A^{\Theta,j_k}\}_j$ and $\{\bigotimes_k F_B^{\Theta,j_k}\}_j$, where $j = j_1 j_2 j_3 \dots$.

For the second state, we change Alice's measurement to be $G_A^{\Theta,i}$, which has classical outcome V_A^i, and $i \in \{0,1\}$ is a bit denoting two different measurements Alice could choose. As with the SDC protocol, we do not specify the measurements

$G_A^{\Theta,i}$. However, we do require that $G_A^{\Theta,i}$ has POVM elements of the form $\{\bigotimes_k G_A^{\Theta,i,j_k}\}_j$ (Assumption 3). This gives the state,

$$\xi_{V_A^i W_B E}^i = \sum_{\Theta} G_A^{\Theta,i} \otimes F_B^{\Theta}(\rho_{\mathrm{ABE}}) \otimes |\Theta\rangle\langle\Theta|. \qquad (14)$$

Now we also define another state (which we'll use for the uncertainty relation), where we change the measurement on Bob's side to be $G_B^{\Theta,i}$, that is,

$$\sigma_{V_A^i V_B^i E}^i = \sum_{\Theta} G_A^{\Theta,i} \otimes G_B^{\Theta,i}(\rho_{\mathrm{ABE}}) \otimes |\Theta\rangle\langle\Theta|. \qquad (15)$$

The measurement $G_B^{\Theta,i}$ has classical outcome V_B^i. The measurement $G_B^{\Theta,i}$ acts independently on each signal, and so its POVM elements have the form $\{\bigotimes_k G_B^{\Theta,i,j_k}\}_j$ (Assumption 3). In addition, F_B^{Θ} and $G_B^{\Theta,i}$ must satisfy $\max_{jk} \|F_B^{\Theta,j_l} G_B^{\Theta,i,k_l}\|_{\infty}^2 = 1/2 \; \forall \; i,l$ (Assumption 4).

We can now consider the Devetak-Winter rate [30]:

$$r \geqslant H(W_B|E\Theta)_{\tau} - H(W_B|W_A\Theta)_{\tau} \qquad (16)$$

$$\geqslant H(W_B|E\Theta)_{\tau} - H(W_B|W_A)_{\tau} \qquad (17)$$

$$\geqslant H(W_B|E\Theta)_{\xi^i} - h(q_F) \qquad (18)$$

$$\geqslant 1 - H\left(V_B^i \middle| V_A^i\right)_{\sigma^i} - h(q_F) \qquad (19)$$

$$\geqslant 1 - h(q_{G^i}) - h(q_F). \qquad (20)$$

The error rates q_{G^i} are generated from V_A^i and V_B^i, and q_F is generated from W_A and W_B. In addition, the binary entropy is defined as $h(q) := q \log_2 q + (1-q) \log_2 (1-q)$. From Eq. (16) to Eq. (17) we use the data processing inequality on the second term to trace out Θ. From Eq. (17) to Eq. (18) we use the fact that $H(W_B|E\Theta)_{\tau} = H(W_B|E\Theta)_{\xi^i}$, as well as the method of types to bound the entropy $H(W_B|W_A)$ by $h(q_F)$ (Lemma II.2 of [35]). In going from Eq. (18) to Eq. (19) we apply the uncertainty relation Eq. (1) of the main text using the overlap of $1/2$ between the measurements $G_B^{\Theta,i}$ and F_B^{Θ}. In the last line, Eq. (20), we use the method of types to bound $H(V_B^i|V_B^i)_{\sigma^i}$ by $h(q_{G^i})$. Since Eqs. (16)–(20) hold for $i = 0$ or $i = 1$ we can choose which lower bound on the rate r we would like to use. We would like to have a high lower bound and therefore we pick the minimum of the two binary entropies:

$$r \geqslant 1 - \min_i h(q_{G^i}) - h(q_F). \qquad (21)$$

To estimate the error rates q_{G^i} and q_F for Version 1 of the LM05 protocol, Alice and Bob reveal V_A^i and V_B^i as well as a small fraction of their W_A and W_B strings in jointly specified positions chosen uniformly at random. In Version 2, Alice and Bob reveal a small fraction of both their V^i strings and W strings in jointly specified uniformly random positions. Alice and Bob have access to these strings in the prepare and measure LM05 protocol because V_A^0 is the string of Alice's measurement outcomes and V_B^0 is the string of Bob's preparation bits, while V_A^1 is the string of Alice's preparation bits (i.e., from her postmeasurement state) and V_B^1 is the string of Bob's measurement outcomes before doing his XOR. W_A and W_B come from Alice's encoding bit (see Lemma 1), and Bob's XOR of his measurement outcomes and preparation bits. In both versions, the resulting key rate is the same.

It is important to note that since there is a minimization in Eq. (21) Alice can choose to either not do a measurement or not do a preparation and then the key rate loses the minimization, and instead she just uses the error rate that is estimated (q_{G^1} for the former choice and q_{G^0} in the latter).

In addition, we have permutation invariance of the outcomes (due to the i.i.d. form of the measurements from Assumption 3) and so we can apply the quantum de Finetti theorem of [36] to this protocol. Therefore the key rate Eq. (21) is applicable for the most general type of attacks by Eve.

In addition, we could have chosen to do direct reconciliation instead of reverse reconciliation. In this case, the string Θ would represent Alice's choice of encoding from the set S_0 or S_1. The proof continues in the same manner and the resulting key rate is the same.

VI. COMPARISON WITH BB84

If we set the quantum channels to be fixed resources, then we can use two BB84 protocol implementations to compare with the SDC and LM05 protocols. The first is two one-way BB84 protocols from Alice to Bob (with an asymmetric basis choice so that basis sifting is negligible in the infinite key limit). The second is the Plug & Play version of BB84 using strong laser pulses (see [2] and references therein). Note that Plug & Play BB84 does not have the same level of security as one-way BB84 [22,23], LM05, or SDC as the measurement devices need to be characterized. If we model the two channels as depolarizing independent identical channels [8,9,11] $\mathcal{E} : \rho \mapsto q\frac{\mathbb{1}}{d} + (1-q)\rho$, where q is the probability of depolarizing and d the dimension of the Hilbert space on which ρ acts, then we see the key rates of Fig. 4 (top). The error rate plotted is $q/2$: The probability of having an error when measuring a signal sent through one of the channels, since with probability q the state is maximally mixed. Since the channels are independent, the probability of being depolarized after passing through both channels in succession is $2q - q^2$.

If instead only one channel is used for communication from Alice to Bob and Bob to Alice, with the polarization drift on the forward channel partially corrected by going back through the channel [37], then the key rates follow Fig. 4 (bottom); that is, the probability of a state being depolarized after passing through the channel is q and the probability of a state being depolarized after passing through the channel one way and then being sent backwards through the same channel is then only q (which is less than $2q - q^2$, which would be the error rate if the channels were independent). In Fig. 4 (bottom) the error rate of the x axis is also $q/2$ for easy comparison with Fig. 4 (top).

Note that the error rates used to calculate the key rate of the SDC protocol depend upon the probability of getting errors in the first bit only, the second bit only, and both bits of the two-bit measurement outcomes. This means that these error rates for the G-measurement basis (the $Z \otimes X$ basis in the perfect implementation) are $q/2(1-q/2), (1-q/2)q/2$, and $q^2/4$, respectively, for the situations in Fig. 4. For the F-measurement basis (the Bell-basis measurement in the perfect implementation) the error rates are all $(2q - q^2)/4$ for the situation in Fig. 4 (top) and $q/4$ for the situation in Fig. 4 (bottom).
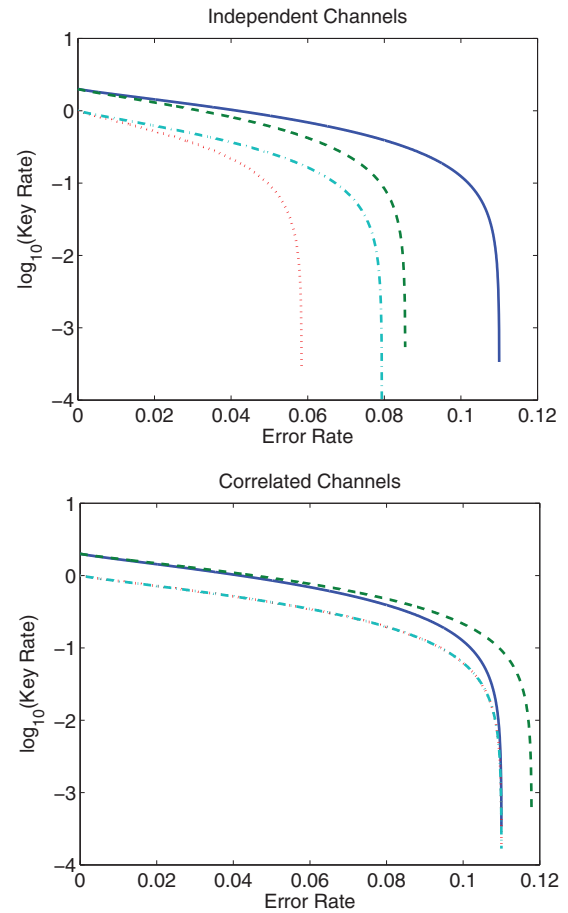

FIG. 4. (Color online) (Top) Log base 10 of the key rates vs the error rate (i.e., half the probability of having a state depolarized) for uncorrelated independent identical depolarizing channels. (Bottom) Log base 10 of the key rates vs the error rate (i.e., half the probability of having a state depolarized) in one channel, where the channels are correlated such that the probability of becoming depolarized through one channel is the same as the probability of being depolarized when going forwards and backwards through the same channel. The plotted key rates are as follows: two copies of the one-way BB84 protocol performed from Alice to Bob and from Bob to Alice (blue, solid), the SDC protocol (green, dashed), the LM05 protocol (cyan, dot dashed), and the Plug & Play protocol (red, dotted).

Importantly, the SDC protocol key rate exceeds both BB84 key rates in the scenario of Fig. 4 (bottom), and it can also tolerate a higher error rate of 11.8%. This is because the correlation between the forward and backward channel makes the error rate in the F-measurement basis lower. This advantage increases if the error rate of passing forwards and then backwards through the channel is smaller.

VII. CONCLUSION

We have shown a general method to prove security of two-way QKD protocols. We have applied this proof method to two such protocols, namely one based on super dense coding (SDC), and another based on a previously proposed two-way protocol (LM05) [7]. These two protocols are secure against

the most general types of attacks by an eavesdropper and provide the following key rates:

$$\text{SDC: } r_{\text{SDC}} \geqslant 2 - h_4(q_G) - h_4(q_F),$$
$$\text{LM05: } r_{\text{LM05}} \geqslant 1 - \min_i h(q_{G^i}) - h(q_F), \tag{22}$$

where in the later $i = 0,1$ denotes two possible measurements Alice could choose. Importantly, few assumptions are needed about the devices used. This is a step towards device independence for two-way QKD protocols. We make the following assumptions to apply our security proof: Preparations are done in a purified way (i.e., an arbitrary bipartite state is prepared and half of it is measured, while the other half is used as the preparation), Alice's encoding output is a fixed state, measurements are done independently on each signal, and a fixed overlap constant characterizes either Bob or Alice's devices (depending on whether reverse or direct reconciliation is performed). The first assumption can instead be the assumption that qubits are prepared. Interesting future work could be to remove some of these assumptions while still providing the same rates of security.

We have shown that these protocols have comparable performance to different implementations of the BB84 protocol, and can even exceed the BB84 rate in certain relevant parameter regimes. In addition, the key rate we obtain for the LM05 protocol is higher than that of [20].

The determinism of two-way protocols in the infinite-key case is not an advantage since an asymmetrical basis choice in the BB84 protocol makes it deterministic as well. However, in the finite-key regime, the BB84 protocol is not deterministic [31]. Therefore both the SDC and LM05 protocols will have an advantage over BB84 implementations when finite keys are used.

In addition, an advantage that the LM05 protocol has, which is not apparent in the infinite key limit, is that there is a higher fraction of key bits per signal sent compared to the BB84 and SDC protocols. If the basis bias for BB84 and the SDC protocol used for parameter estimation is p, then $2p(1 - p)$ fraction of the signals are lost due to basis sifting. However, in the LM05 protocol, if c is the probability that Alice does her measurement, and p is the probability that Alice and Bob use the Z basis, then only $2p(1 - p)c$ fraction of the signals are lost. This advantage would have a positive effect on the finite-key rate.

Our work paves the way for fully exploiting the potential of entropic uncertainty relations in two-way QKD with finite-key sizes for any possible implementation. We did not evaluate the finite-key regime here, but the techniques of [31,38] could be used to show security for two-way protocols. We leave this as future work.

APPENDIX

Here we provide the proof of Lemma 1 that purifies Alice's encoding operation. It establishes an equivalence between a POVM acting on half of a pure state and a CPTP map of a particular form.

Lemma 1. (POVM equivalent to a CPTP map). Let $\{\mathcal{E}_i\}_{i=1..n}$ be a set of n completely positive trace-preserving maps from Hilbert space $\mathcal{H}_A$ to Hilbert space $\mathcal{H}_D$ and σ_D be a fixed density operator on $\mathcal{H}_D$ such that $1/n \sum_{i=1}^{n} \mathcal{E}_i(\rho_A) = \sigma_D \ \forall \rho_A \in S(\mathcal{H}_A)$.

Then there exists a fixed pure state $|\phi\rangle_{CD}$ in $\mathcal{H}_{CD} := \mathcal{H}_C \otimes \mathcal{H}_D$, where $\dim \mathcal{H}_C = \dim \mathcal{H}_D$, and a complete set of POVM elements $\{F_{AC}^i\}_{i=1..n}$ on $\mathcal{H}_{AC}$ (so $\sum_i F_{AC}^i = \mathbb{1}_{AC}$), such that $\forall i, \forall \rho_A \in S(\mathcal{H}_A)$ we have

$$n \text{Tr}_{AC}\left(F_{AC}^i \rho_A \otimes |\phi\rangle_{CD}\langle\phi|\right) = \mathcal{E}_i(\rho_A). \tag{A1}$$

Proof. Summing over i in Eq. (A1) implies that we require $\text{Tr}_C(|\phi\rangle_{CD}\langle\phi|) = \sigma_D$, and therefore we fix $|\phi\rangle_{CD}$ to be a purification of σ_D. Now we can constructively determine what the POVM elements F_{AC}^i are in terms of σ_D and the maps $\mathcal{E}_i$. Then we will show that this construction of the POVM satisfies all necessary requirements above.

Let $\sigma_D = \sum_j \lambda_j |j\rangle_D\langle j|$, so then $|\psi\rangle_{CD} = \sum_j \sqrt{\lambda_j}|jj\rangle_{CD}$. Expanding ρ_A in an orthonormal basis $\{|\psi_m\rangle\}_m$ gives $\rho_A = \sum_{ml} r_{ml}|\psi_m\rangle_A\langle\psi_l|$, which allows us to write Eq. (A1) as

$$\sum_{jkml} n \text{Tr}_{AC}\left(F_{AC}^i r_{ml}|\psi_m\rangle_A\langle\psi_l| \otimes \sqrt{\lambda_j\lambda_k}|jj\rangle_{CD}\langle kk|\right)$$
$$= \sum_{jkml} n r_{ml}\sqrt{\lambda_j\lambda_k}\left(_{AC}\langle\psi_l k|F_{AC}^i|\psi_m j\rangle_{AC}|j\rangle_D\langle k|\right)$$
$$= \sum_{ml} r_{ml}\mathcal{E}_i(|\psi_m\rangle_A\langle\psi_l|). \tag{A2}$$

This must be true for all ρ_A and therefore we have $\forall m,l$,

$$\sum_{jk} n\sqrt{\lambda_j\lambda_k}\langle\psi_l k|F_{AC}^i|\psi_m j\rangle|j\rangle_D\langle k| = \mathcal{E}_i(|\psi_m\rangle\langle\psi_l|),$$
$$n\sqrt{\lambda_j\lambda_k}\langle\psi_l k|F_{AC}^i|\psi_m j\rangle = \langle j|\mathcal{E}_i(|\psi_m\rangle\langle\psi_l|)|k\rangle \ \forall m,l,j,k. \tag{A3}$$

Equation (A3) gives a constructive way of finding the POVM elements F_{AC}^i. If σ_D has full rank then F_{AC}^i is completely determined by this equation. If σ_D is not of full rank then F_{AC}^i can be decomposed into a part on the support of $\sigma_C := \text{Tr}_D(|\phi\rangle_{CD}\langle\phi|)$ and its kernel: $F_{AC}^i = F_{AC_{\text{supp}\sigma_C}}^i \oplus F_{AC_{\text{kern}\sigma_C}}^i$. The block on the $\text{supp}\sigma_C$ is completely specified by Eq. (A3), and the block on $\text{kern}\sigma_C$ can be chosen arbitrarily as long as $F_{AC_{\text{kern}\sigma_C}}^i \geqslant 0$, for all i and satisfy $\sum_i F_{AC_{\text{kern}\sigma_C}}^i = \mathbb{1}_{AC_{\text{kern}\sigma_C}}$. It is clear from Eq. (A3) that $\sum_i F_{AC_{\text{supp}\sigma_C}}^i = \mathbb{1}_{AC_{\text{supp}\sigma_C}}$.

Now we need to verify that the POVM elements satisfy $F_{AC}^i \geqslant 0$ for all i. We write the maps in their Choi-Jamiołkowski representation [39,40]:

$$\mathcal{E}_i(|\psi_m\rangle_A \langle\psi_l|) = \text{Tr}_A \big(J_{AD}^i (|\psi_m\rangle_A \langle\psi_l|)^T \otimes \mathbb{1}_D\big) \quad \text{(A4)}$$

$$= \langle\psi_m|J_{AD}^i|\psi_l\rangle, \quad \text{(A5)}$$

where J_{AD}^i are the Choi-Jamiołkowski matrices for the maps $\mathcal{E}_i$. Now we can write $F_{AC_{\text{supp}\sigma_C}}^i$ from Eq. (A3) as

$$F_{AC_{\text{supp}\sigma_C}}^i = \frac{1}{n}\frac{1}{\sqrt{\sigma_C}}\big(J_{AC}^i\big)^T\frac{1}{\sqrt{\sigma_C}}, \quad \text{(A6)}$$

where $J_{AC}^i := \sum_{jk} |j\rangle_{CD}\langle j|J_{AD}^i|k\rangle_{DC}\langle k|$. From this form it is clear that this block is positive, and so $F_{AC}^i \geqslant 0$ for all i. ∎

[1] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] Q.-Y. Cai and B.-W. Li, Phys. Rev. A **69**, 054301 (2004).

[4] Q.-Y. Cai and B.-W. Li, Chin. Phys. Lett. **21**, 601 (2004).

[5] F.-G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[6] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[7] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).

[8] A. Cerè, M. Lucamarini, G. Di Giuseppe, and P. Tombesi, Phys. Rev. Lett. **96**, 200501 (2006).

[9] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, and P. Tombesi, Phys. Rev. A **77**, 022304 (2008).

[10] M. Ostermeyer and N. Walenta, Opt. Commun. **281**, 4540 (2008).

[11] M. Abdul Khir, M. Mohd Zain, I. Bahari, and S. Shaari, Opt. Commun. **285**, 842 (2012).

[12] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[13] Z. L. Yuan and A. J. Shields, Opt. Exp. **13**, 660 (2005).

[14] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

[15] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

[16] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[17] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electr. Lett. **34**, 2116 (1998).

[18] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).

[19] Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).

[20] H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai, Phys. Rev. A **84**, 042344 (2011).

[21] C.-H. F. Fung, X. Ma, H. F. Chau, and Q.-Y. Cai, Phys. Rev. A **85**, 032308 (2012).

[22] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).

[23] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New J. Phys. **12**, 023024 (2010).

[24] D. Mayers, in *Proceedings of Advances in Cryptology–CRYPTO '96, Santa Barbara, California, USA, 1996*, Lecture Notes in Computer Science (Springer, New York, 1996), p. 343.

[25] M. Koashi, New J. Phys. **11**, 045018 (2009).

[26] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[27] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012).

[28] U. Vazirani and T. Vidick, arXiv:1210.1810 (unpublished).

[29] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[30] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[31] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Comm. **3**, 634 (2012).

[32] M. Tomamichel, Ph.D thesis, ETH Zurich, 2012.

[33] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[34] M. Tomamichel and E. Hänggi, J. Phys. A **46**, 055301 (2013).

[35] I. Csiszar, IEEE Trans. Inf. Theory **44**, 2505 (1998).

[36] R. Renner, Nat. Phys. **3**, 645 (2007).

[37] M. Lucamarini and S. Mancini, arXiv:1004.0157 (unpublished).

[38] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[39] M.-D. Choi, Lin. Alg. and its Appl. **10**, 285 (1975).

[40] A. Jamiolkowski, Rep. on Math. Phys. **3**, 275 (1972).