## Indefinite causal key distribution

Hector Spencer-Wood\*
School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, Scotland
(Dated: November 27, 2024)

We propose a quantum key distribution (QKD) protocol that is carried out in an indefinite causal order (ICO). In QKD, one considers a setup in which two parties, Alice and Bob, share a key with one another in such a way that they can detect whether an eavesdropper, Eve, has learnt anything about the key. To our knowledge, in all QKD protocols proposed until now, Eve is detected by publicly comparing a subset of Alice and Bob's key and checking for errors. We find that a consequence of our protocol is that it is possible to detect eavesdroppers without publicly comparing any information about the key. Indeed, we prove that it is not possible for eavesdroppers, performing any individual attack, to extract useful information about the shared key without inducing a nonzero probability of being detected. We also prove the security of this protocol against a class of individual eavesdropping attacks. The role ICO plays in causing unusual phenomena in quantum technologies is an important question. By considering it we find a two-way QKD protocol that exhibits a similar private detection feature, albeit with some interesting differences. After noting some implications of these differences and discussing some of the practicalities of our protocol, we conclude that this work is best considered as a first step in applying quantum cryptographic ideas in an ICO.

#### I. INTRODUCTION

In our everyday, classical world, we are used to events occurring in a well defined order: A happens before B or vice versa. However, it has been suggested that if our universe is to be governed by a quantum theory of gravity, the dynamical nature of causality in general relativity must coexist with the indefiniteness of states in quantum mechanics [1]. So, although in our classical world A comes before B or vice versa, the quantum world allows for both of these options to occur in superposition, in an *indefinite causal order* (ICO). Remarkably, without even venturing into the quantum gravitational regime, a physically realisable device, called the quantum switch, has been proposed that exhibits such an indefinite causal order [2–6]. The quantum switch has been applied in many different settings and has hinted at advantages, or interesting differences, when compared with the corresponding definite causal situations [2, 7–22]. Such differences usually present themselves when the actions of the parties within the quantum switch are incompatible (that is, when their operations do not commute with one another). This realisation has led to far reaching proposals: from quantum refrigeration [17] and battery charging [18, 19], to the violation of fundamental quantum metrological limits [10, 11]. Motivated by this relation to noncommuting operations, we explore whether another such application: quantum key distribution (QKD), can be performed in an ICO. Indeed, we ask: if it is possible, are there are any interesting consequences that follow?

QKD is concerned with the scenario in which two parties, conventionally named Alice and Bob, would like to share a private key (a string of 0s and 1s) in such a way that they are confident an eavesdropping third party, called Eve, has not been listening in. There have

been a number of protocols proposed [23–31], the first of which was by Charles Bennett and Giles Brassard in 1984 (BB84) [23]. The security of these protocols comes from the fact that Eve can be detected. This is possible because, when Eve is present, the quantum phenomenon of measurement disturbance leads to a non-zero probability of error in Bob's key, with respect to Alice's. So, if one could somehow detect these errors induced by Eve, it could be concluded that an eavesdropper had been listening in. The way that these errors are normally detected is by having Alice and Bob publicly compare a subset of their respective raw keys. Now public information, this subset is subsequently discarded regardless of whether they conclude Eve is there or not.

To our knowledge, this public comparison is a feature of all QKD protocols so far proposed. In this article, we consider how one might adapt the simplest QKD scheme: the BB84 protocol, to an indefinite causal regime. In doing so, we find that we can determine whether eavesdroppers are there or not without having to publicly compare a subset of the distributed key. Indeed, we show that this is true for any individual attack performed by eavesdroppers, at least those who cannot infiltrate the causal structure of the protocol. We also provide some understanding of the security of our protocol by proving that it is secure against a class of individual attacks. It is natural to ask whether this "private" detection is a consequence of ICO or if it is allowed by other features of quantum mechanics. As evidenced by the debate about the role of ICO in the activation of channel capacities [15, 32–34], this is an important question to ask in understanding whether indefinite causality is responsible for any given phenomenon. Indeed, we find a protocol that occurs in a well defined order which allows for this same feature of private detection. To do this, however, an extra instance of Alice's operation seems to be required, a property consistent with other discussions of indefinite versus definite causal orderings [2]. Further, motivated by a contrast in

<sup>\*</sup> hector.spencer-wood@glasgow.ac.uk

possible eavesdropping strategies, we note that there are hints of some more intriguing differences between quantum encryption in an definite causal world, and an indefinite one. Due to the practical concerns we discuss, we ultimately conclude that ICO may not offer an advantage to QKD in the way considered here. However, we note that this is just an initial step in considering this combination of topics, arguing that there are many interesting future lines of research, both from a foundational and practical standpoint.

In Sec. II we briefly discuss the general background theory of the two topics of importance in this article: indefinite causal order and quantum key distribution. In Sec. III A, we describe how a key can be distributed between Alice and Bob in an indefinite causal order when no eavesdropper is present. In Sec. IIIB we introduce a single eavesdropper to gain some intuition of their effects. One eavesdropper location being insufficient to prove the security of this protocol, in Sec. IV, a second and final eavesdropper is introduced, and we explore the security of this protocol by considering a class of individual attacks by the eavesdroppers. Also in this section, we state our main result: that eavesdroppers, performing any individual attack, cannot extract any useful information about the shared key without revealing themselves. Following this, in Sec. V we briefly discuss whether this phenomenon is truly a consequence of indefinite causal order, and whether there are any alternate differences between the definite and indefinite cases. Finally, in Sec. VI, the findings are summarised along with a discussion of the implementability and practicality of this protocol, as well as possible future lines of research.

#### II. BACKGROUND THEORY

#### A. Indefinite causal order

Suppose two parties, Alice and Bob, hope to act on some state  $\rho$  sequentially with the respective operations  $\mathcal{A}, \mathcal{B}$  (or more generally, sets of operations, i.e. quantum instruments<sup>1</sup>) defined using the Kraus operators  $\{A_i\}, \{B_j\}$ , respectively. Normally, at least from a classical perspective, this occurs, as depicted in FIG. 1, in a definite order: either Alice before Bob,

$$\rho \to \sum_{i} A_{i} \,\rho \,A_{i}^{\dagger} \to \sum_{i,j} B_{j} A_{i} \,\rho \,A_{i}^{\dagger} B_{j}^{\dagger}, \tag{1}$$

or Bob before Alice,

$$\rho \to \sum_{j} B_{j} \rho B_{j}^{\dagger} \to \sum_{i,j} A_{i} B_{j} \rho B_{j}^{\dagger} A_{i}^{\dagger}. \tag{2}$$

In quantum mechanics, however, the order in which Alice and Bob act on  $\rho$  can be indefinite - a phenomenon

known as indefinite causal order (ICO). Take the quantum switch for example<sup>2</sup>, where an extra, control qubit in the state  $\omega$  dictates the order in which Alice and Bob act on  $\rho$ . Much like a classical switch, if we turn it on and set  $\omega = |1\rangle\langle 1|$ , then Alice acts before Bob. Conversely, if we switch it off and let  $\omega = |0\rangle\langle 0|$ , then Bob would go before Alice. However, since  $\omega$  is a quantum state, it can be in a superposition of  $|0\rangle$  and  $|1\rangle$ , meaning that Alice and Bob can act on  $\rho$  in a controlled superposition of orders.

Let us write this down mathematically. As mentioned, if the control qubit is in the state  $\omega = |1\rangle\langle 1|$ , then Alice acts on the target qubit using  $\mathcal{A}$  before Bob acts on it with  $\mathcal{B}$ , and if  $\omega = |0\rangle\langle 0|$ , then  $\mathcal{B}$  occurs before  $\mathcal{A}$ . Following the notation of Ref. [16], we can therefore write the quantum switch as the following operation

$$\rho \to \mathcal{S}_{\omega}(\mathcal{A}, \mathcal{B})(\rho) = \sum_{i,j} S_{ij} \left(\rho \otimes \omega\right) S_{ij}^{\dagger}, \tag{3}$$

where the Kraus operators  $\{S_{ij}\}$  are defined as

$$S_{ij} = A_i B_j \otimes |0\rangle\langle 0| + B_j A_i \otimes |1\rangle\langle 1| \tag{4}$$

This is depicted in FIG. 1(c).

#### B. Quantum key distribution

Aside from being in an indefinite causal order with each another, Alice and Bob also like to share private keys with one other to use for various cryptographic tasks. In quantum key distribution (QKD), this is often done (for example in the original implementation: BB84 [23]) by having Alice send a key to Bob using encoded quantum systems. To do this, she prepares qubits in states that correspond to the 0s and 1s of the private key and sends them to Bob to be measured. Indeed, in BB84, Alice and Bob respectively prepare and measure, independently and randomly, in one of two mutually unbiased bases. In this work, we will use the Pauli x and z-bases:  $\{|0\rangle, |1\rangle\}$  and  $\{|+\rangle, |-\rangle\}$  respectively. If Alice (Bob) prepared (measured) the qubit to be in the state  $|0\rangle$  or  $|+\rangle$ , she (he) will have a corresponding key bit of 0. Likewise,  $|1\rangle, |-\rangle$  corresponds to the key bit 1. Once Bob has measured the qubit Alice sent him, the two parties publicly discuss which bases they chose. If they chose different bases, there is only a 50% chance of them agreeing on the corresponding key bit value, so they discard it. If, however, they chose the same basis, when no eavesdroppers are present, Bob's measurement result is guaranteed to correspond to the state prepared by Alice, assuming

<sup>&</sup>lt;sup>1</sup> Defined in Appendix B.

<sup>&</sup>lt;sup>2</sup> This is just one example of indefinite causal order, but by far the most understood, and it is what we use throughout this article. For more general discussions, see e.g. Ref. [35].

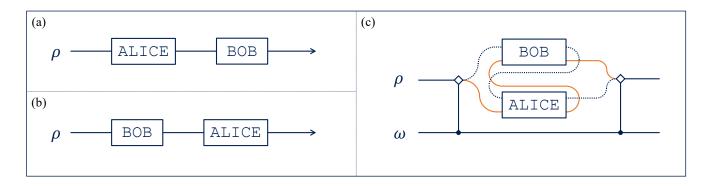


FIG. 1. Quantum mechanics allows for more freedom in the ordering of events: (a) Alice can act on a state  $\rho$  before Bob, (b) Bob before Alice, or (c) in a superposition of both orders, controlled on some quantum state  $\omega$ .

noiseless and lossless transmission, as we will do throughout. Therefore, Alice and Bob can use the corresponding ordered set of key bit values as their shared key.

The security of this protocol comes from the fact that when an eavesdropper, Eve, intercepts the transmission from Alice to Bob and tries to learn the key bit value being shared, she disturbs the quantum state being sent with non-zero probability<sup>3</sup>. This means that, even if Alice and Bob agree on the basis chosen, there is a non-zero probability that they disagree on the state of the qubit, which implies that there is a chance of an error in Bob's key with respect to Alice's. To detect these errors, Alice and Bob take a subset of their sifted keys and compare them *publicly*. Since it has to be done publicly, this subset must subsequently be discarded, regardless of whether errors, and therefore Eve, were detected or not. Let us now see how this protocol can be adapted to an indefinite causal setting.

## III. QUANTUM KEY DISTRIBUTION IN AN INDEFINITE CAUSAL ORDER

# A. Indefinite causal key distribution with no eavesdroppers

In BB84, Alice would prepare the qubits to be sent to Bob in a certain state. When considering an indefinite causal ordered scheme, Alice is simultaneously sending and receiving the qubit from Bob (and vice versa). So having one party be the "preparer" of the state, and the other the "measurer" makes little sense. To avoid this, we let both Alice and Bob measure the qubit being used, which, because of how states are updated following

projective measurements, allows them to both be the preparer and measurer of the shared qubit. This method has similarities to how a key is generated in protocols like E91 [24]. Taking this approach, each bit of the key would be the result of projective measurements performed by Alice and Bob on the shared qubit, initially in the state  $\rho$ , but only when Alice and Bob agree they had performed the *same* measurement. Due to the projective nature of these measurements, Alice and Bob would obtain identical measurement outcomes and therefore share an identical key bit (assuming noiseless and lossless channels).

Thinking of the key generation in this way, we can consider a scheme in which a key is distributed in an indefinite causal order. Here, we send a state  $\rho$  to two parties, Alice and Bob, in a controlled superposition of two orders: Alice before Bob and Bob before Alice. As shown in FIG. 2, and as discussed in Sec. II A, this superposition is controlled by the qubit state  $\omega$ . Alice and Bob then both make a random choice to measure either in the Pauli z-basis:  $\{|0\rangle, |1\rangle\}$ , or x-basis:  $\{|+\rangle, |-\rangle\}$ . We can think of Alice and Bob as acting on the state with quantum channels  $\mathcal{A}, \mathcal{B} \equiv \mathcal{A}$  respectively<sup>4</sup>, defined by the respective sets of Kraus operators  $\{A_i\}, \{B_j\}$ , such that

$$A_0 \equiv B_0 = \frac{1}{\sqrt{2}} |0\rangle\langle 0|, \tag{5a}$$

$$A_1 \equiv B_1 = \frac{1}{\sqrt{2}} |1\rangle\langle 1|, \tag{5b}$$

$$A_{+} \equiv B_{+} = \frac{1}{\sqrt{2}} |+\rangle \langle +|, \qquad (5c)$$

$$A_{-} \equiv B_{-} = \frac{1}{\sqrt{2}} |-\rangle \langle -|. \tag{5d}$$

Here, the factors of  $1/\sqrt{2}$  arise because we are assuming Alice and Bob are both equally likely to measure

<sup>&</sup>lt;sup>3</sup> This is a consequence of quantum measurement disturbance: to learn which state Alice prepared the system in, Eve must measure it. Since she has no idea which of the mutually unbiased bases Alice chose to prepare the state in, she cannot choose a measurement that will always leave the state undisturbed.

<sup>&</sup>lt;sup>4</sup> We denote Alice and Bob's channels using different letters for clarity, but they are identical and can be interchanged whenever it is useful.

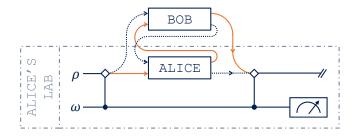


FIG. 2. Indefinite causal key distribution with no eavesdroppers. A key is shared between Alice and Bob by sending a state  $\rho$  to them in a superposition of orders controlled by the state  $\omega$ . Alice and Bob perform projective measurements randomly in either the Pauli x or z-basis. After discarding cases in which Alice and Bob measured in different bases, they are left with identical keys. Regardless of the initial state  $\omega$  of the control qubit,  $\omega$  never changes when there are no eavesdroppers, a phenomenon we see not to be true when an eavesdropper is introduced.

in the x or z-basis<sup>5</sup>. It should be made clear that Alice and Bob are not just putting  $\rho$  through some quantum channel, they are indeed performing the stated measurements. They could, for example, store their measurement results in a four dimensional ancillary register R (available only in their respective laboratories) initially in the state  $|m_0\rangle^R$ . The corresponding Kraus operators that would achieve this would have the form  $A_i' \equiv B_i' = |i\rangle\langle i| \otimes |m_i\rangle^R\langle m_0|^R/\sqrt{2}$ , where  $|m_i\rangle$  encode the four possible measurement outcomes  $i \in \{0, 1, +, -\}$  in orthogonal states:  $\langle m_i|m_j\rangle = \delta_{ij}$ . Having said this, since these ancillary systems factor out, we can take  $A_i, B_i$  to have the form given in Eq. (5).

Following their measurements, Alice and Bob then publicly discuss the basis they chose for each measurement and only keep the measurement outcomes in which they measured  $\rho$  in the same basis. Assuming no errors occur between Alice and Bob's measurements, their keys, made up of the measurement outcomes they kept, should be identical. In what follows, similarly to what we discussed earlier, a measurement outcome of 0 and + will correspond to a 0 in the key. Likewise, 1 and - correspond to a 1 in the key.

Let's see in more detail out what happens to the state  $\rho$  when it is put through the setup in FIG. 2. Repeating what was written in Sec. II A, the channel that  $\rho$  goes through, is given by

$$S_{\omega}(\mathcal{A}, \mathcal{B})(\rho) = \sum_{i \ j \in \mathcal{I}} S_{ij} \rho \otimes \omega S_{ij}^{\dagger}, \tag{6}$$

where

$$S_{ij} = A_i B_j \otimes |0\rangle\langle 0| + B_j A_i \otimes |1\rangle\langle 1|, \tag{7}$$

and we define the set containing the Kraus operator indices by

$$\mathfrak{I} := \{0, 1, +, -\}. \tag{8}$$

After some algebra, it follows that Eq. (6) can be rewritten as follows:

$$S_{\omega}(\mathcal{A}, \mathcal{B})(\rho) = \frac{1}{4} \sum_{i,j \in \mathfrak{I}} \left( \{A_i, B_j\} \rho \{A_i, B_j\}^{\dagger} \otimes \omega + [A_i, B_j] \rho [A_i, B_j]^{\dagger} \otimes \sigma_z \omega \sigma_z \right), \quad (9)$$

where  $\sigma_z$  is the z Pauli operator.

Now, recall that, after public discussion, Alice and Bob only keep the cases in which they performed a measurement in the same basis. Therefore, following this discussion, the state becomes

$$S_{\omega}(\mathcal{A}, \mathcal{B})(\rho) \to \frac{1}{2} \sum_{\mathfrak{B} \in \mathsf{C}} \sum_{i, j \in \mathfrak{B}} \left( \{A_i, B_j\} \rho \{A_i, B_j\}^{\dagger} \otimes \omega + [A_i, B_j] \rho [A_i, B_j]^{\dagger} \otimes \sigma_z \omega \sigma_z \right), \quad (10)$$

where the prefactor is found by requiring normalisation,  $C = \{\{0,1\}, \{+,-\}\}$ , and  $\mathfrak{B}$  labels the elements of C. Noting the form of  $A_k, B_k$  given in Eq. (5), the terms in these sums have the following properties

$$\{A_i, B_j\} = \sqrt{2}A_i\delta_{ij},$$
  

$$[A_i, B_j] = 0,$$
(11)

for all i, j from the same basis, where  $\delta_{ij}$  is the Kronecker delta. This confirms that Alice and Bob must agree on their measurement outcomes, meaning we can successfully share a key in an ICO. Overall, we have that

$$S_{\omega}(\mathcal{A}, \mathcal{A})(\rho) \to \sum_{i \in \mathfrak{I}} A_i \rho A_i^{\dagger} \otimes \omega.$$
 (12)

So, when there are no eavesdroppers present, the control state  $\omega$  stays in its original state and this situation is ultimately no different from when the causal order is definite. Let us introduce an eavesdropper to see what changes.

#### B. Introducing an eavesdropper

Notice that, unlike in BB84, there are multiple places an eavesdropper can reside (see FIG. 4). Having said this, to gain some intuition about the effects of eavesdroppers, let us first consider introducing just a single eavesdropper, Eve. In the original BB84 protocol, Eve interacts with the qubit when in transit between Alice and Bob, regardless of who the sender/receiver was:

$$\rho \xrightarrow{\text{Alice}} \sum_{i,j,k} B_k E_j A_i \, \rho \, A_i^{\dagger} E_j^{\dagger} B_k^{\dagger}, \tag{13a}$$

$$\rho \xrightarrow{\text{Bob}} \sum_{i,j,k} A_i E_j B_k \rho B_k^{\dagger} E_j^{\dagger} A_i^{\dagger}. \tag{13b}$$

<sup>&</sup>lt;sup>5</sup> This is not always the case in practical QKD, often, one basis is taken to be heavily biased over the other [36].

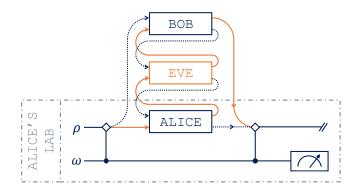


FIG. 3. Indefinite causal key distribution with a single eavesdropper, Eve, between Alice and Bob.

Here, for simplicity<sup>6</sup>, denote the channel corresponding to Eve's measurement by  $\mathcal{E}$ , defined by the Kraus operators  $\{E_i\}$ .

Now, suppose Alice and Bob carry out the indefinite causal QKD method described in the previous subsection

and Eve takes motivation from the definite causal case, setting herself up in between Alice and Bob. This scenario is depicted in FIG.3. As before, allowing a state  $\rho$  to be acted on by Alice, Eve and Bob in an indefinite causal order controlled by  $\omega$ , the channel  $\rho$  passes through is given by

$$S_{\omega}(\mathcal{A}, \mathcal{E}, \mathcal{B})(\rho) = \sum_{i,j,k} S_{ijk} \rho \otimes \omega S_{ijk}^{\dagger}, \qquad (14)$$

where

$$S_{ijk} := A_i E_j B_k \otimes |0\rangle\langle 0| + B_k E_j A_i \otimes |1\rangle\langle 1|$$

$$= \frac{1}{2} \{A_i, E_j, B_k\} \otimes \mathbb{1} + \frac{1}{2} [A_i, E_j, B_k] \otimes \sigma_z \qquad (15)$$

such that

$${A_i, E_j, B_k} := A_i E_j B_k + B_k E_j A_i,$$
 (16a)

$$[A_i, E_j, B_k] := A_i E_j B_k - B_k E_j A_i.$$
 (16b)

After some algebra, and following the basis comparison,

$$S_{\omega}(\mathcal{A}, \mathcal{E}, \mathcal{B})(\rho) \to \frac{1}{2} \sum_{j} \sum_{\mathfrak{B} \in \mathcal{C}} \sum_{i, k \in \mathfrak{B}} \left( \{A_i, E_j, B_k\} \rho \{A_i, E_j, B_k\}^{\dagger} \otimes \omega + [A_i, E_j, B_k] \rho [A_i, E_j, B_k]^{\dagger} \otimes \sigma_z \omega \sigma_z \right). \tag{17}$$

From this, we can see that, as before, the  $\omega$  terms survive. But more interestingly, notice that the  $\sigma_z \omega \sigma_z$  terms can survive too. For example, suppose Alice and Bob measure in the z-basis and Eve measures in the x-basis, then it is possible for Alice to obtain an outcome of 0, and Bob an outcome of 1. This combination allows for  $[A_0, E_{\pm}, B_1] \neq 0$ .

We may therefore hypothesise that if Eve attempts to extract information about the state when in between Alice and Bob, she induces a nonzero  $\sigma_z \omega \sigma_z$  term. So, if we were to let  $\omega = |+\rangle \langle +|$  (and therefore  $\sigma_z \omega \sigma_z = |-\rangle \langle -|$ ), if someone were to perform the measurement  $\{|+\rangle \langle +|,|-\rangle \langle -|\}$  on the control state  $\omega$ , and obtain an outcome of -, they could conclude that there was an eavesdropper in between Alice and Bob. Moreover, since Alice can keep and measure the control qubit in her own lab, this would mean that no subset of the distributed key need be publicly compared and discarded to determine the presence of Eve. Let us now explore how robust this hypothesis is.

# IV. SECURITY AGAINST INDIVIDUAL ATTACKS

As alluded to earlier, there are two possible positions eavesdroppers can exist: in between, or outwith Alice and Bob's encoding operations. Let's see what happens when two eavesdroppers, Eve and Yves, are introduced. In particular, in this work, we consider *individual* attacks where Eve and Yves act on each distributed state separately [30] and we leave more general attacks for future work. There being more than one eavesdropper allows for cooperative strategies, the most general of which utilise both quantum and classical correlations between Eve and Yves's operations. Possible correlations include everything from shared entangled ancilla states, to quantum channels, to more general indefinite causal structures and can be described mathematically by Eve and Yves sharing a process matrix  $W^{\tilde{E}\tilde{Y}}$ , as depicted in FIG.4. We discuss this scenario, which we will often call the "fully correlated" case, in more depth in Appendix C.

In this section, we consider a subclass of these individual eavesdropping strategies where Eve and Yves's ancilliary systems (that they use to aid in their attack) are separable but jointly measurable, and we prove the security of our protocol (which is summarised in Protocol 1) against them. Investigation into the full security proof of this protocol is beyond the scope of this work. This

<sup>&</sup>lt;sup>6</sup> More generally, Eve has access to a quantum instrument. This is discussed in more detail in Appendix C.

- 1. Alice prepares the state  $\rho=1/2$  to be distributed along with a control qubit state  $\omega=|+\rangle\langle+|$  that remains in her lab.
- 2. The state  $\rho$  is distributed to Alice and Bob's measuring devices in an indefinite causal order, controlled on  $\omega$ .
- 3. Alice and Bob non-destructively measure  $\rho$  in either the x or z-basis, chosen randomly with probability 1/2. Measurement outcomes 0, + correspond to a key bit 0, and outcomes 1, correspond to a key bit of 1.
- 4. Alice and Bob compare the bases they chose and only keep the cases in which they agree.
- 5. For each (sifted) state  $\rho$  distributed, Alice measures the corresponding control qubit state  $\omega$  in the x-basis. If an outcome + is obtained, carry on. If an outcome is found, Alice concludes eavesdroppers are present after which, she either aborts the key distribution, or she and Bob go ahead with privacy amplification and error correction (not discussed in this work).

Protocol 1. Summary of the proposed indefinite causal key distribution protocol.

being said, the attacks considered in this section provide us with some useful understanding about the security of this protocol. The methods used follow closely those used in [28] where the authors consider a two-way deterministic quantum communications protocol in which quantum states are sent back and forth between Alice and Bob. Although they are working in a definite causal order, in this protocol, the eavesdropper has access to the state at two different points, which is why the same techniques used can be applied to our protocol.

#### A. Problem setup

Let S denote the distributed qubit, initially prepared in the state  $\rho$ . In the scenario we consider, we assume that Alice and Bob would like their shared key to contain, on average, equal numbers of 0s and 1s. Therefore, we can make a natural choice for the initial state of S:  $\rho = (1/2) \sum_{\psi} |\psi\rangle\langle\psi| = 1/2$ , where  $\{|\psi\rangle\}$  is some complete basis of the Hilbert space corresponding to S. Now, if Alice is in the lab in which the state  $\rho$  is created and where  $\omega$  resides, there are two places eavesdroppers, who we call Eve and Yves, can be located. This setup is shown in FIG. 4. In addition to the state  $\rho$  being sent between Alice and Bob, Eve and Yves also have access to independent ancilliary quantum systems  $\tilde{E}, \tilde{Y}$  (respectively) initially in the states  $\varepsilon := |\varepsilon\rangle\langle\varepsilon|$  and  $\eta := |\eta\rangle\langle\eta|$ 

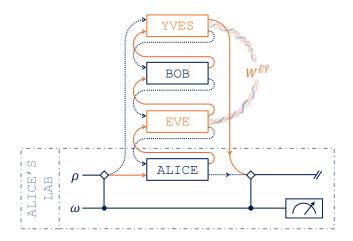


FIG. 4. Indefinite causal quantum key distribution with two eavesdroppers Eve and Yves. The fact there are now two eavesdroppers means correlated attacks are possible. All possible correlations are described mathematically by a process matrix  $W^{\tilde{E}\tilde{Y}}$  shared by Eve and Yves.

respectively<sup>7</sup>. Eve and Yves perform the respective unitaries  $U_E^{(S\check{E})} =: U_E, \, U_Y^{(S\check{Y})} =: U_Y$  on the joint space of the distributed state  $\rho$  and the spaces of their respective ancillae  $\varepsilon, \eta$ . Following this, the eavesdroppers perform some joint measurement on the ancillae to try and gain some information about Alice and Bob's shared key. Note that Eve and Yves do, therefore, cooperate in this scenario, although not in the most general way possible.

For  $k \in \{0, 1, +, -\}$ , the eavesdroppers' unitaries are performed most generally as follows [28]:

$$U_E^{(SE)}|k\rangle^{(S)}|\varepsilon\rangle^{(E)} = |k\rangle|\varepsilon_{kk}\rangle + |\bar{k}\rangle|\varepsilon_{k\bar{k}}\rangle,$$
 (18a)

$$U_Y^{(SY)}|k\rangle^{(S)}|\eta\rangle^{(Y)} = |k\rangle|\eta_{kk}\rangle + |\bar{k}\rangle|\eta_{k\bar{k}}\rangle,$$
 (18b)

where  $|\varepsilon_{mn}\rangle$  and  $|\eta_{mn}\rangle$  are, in general, unnormalised and non-orthogonal, and  $\bar{k}$  is taken to mean "not k". Note that we, from now on, will drop the superscripts unless it is unclear which space is which. Note also, that<sup>8</sup>

$$|\varepsilon_{\pm\pm}\rangle = \frac{1}{2}(|\varepsilon_{00}\rangle \pm |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle),$$
 (19a)

$$|\varepsilon_{\pm\mp}\rangle = \frac{1}{2}(|\varepsilon_{00}\rangle \mp |\varepsilon_{01}\rangle \pm |\varepsilon_{10}\rangle - |\varepsilon_{11}\rangle),$$
 (19b)

 $<sup>^7</sup>$  Note that we are not here considering the fully general case of Eve and Yves sharing an arbitrary process matrix  $W^{\tilde{E}\tilde{Y}}$ .

<sup>&</sup>lt;sup>8</sup> To see this explicitly, we perform  $U_E|\pm\rangle|\epsilon\rangle = U_E(|0\rangle|\epsilon\rangle \pm |1\rangle|\epsilon\rangle)/\sqrt{2}$  using Eq. (18a). This results in  $(|0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \pm |1\rangle|\epsilon_{11}\rangle \pm |0\rangle|\epsilon_{10}\rangle)/\sqrt{2} = [|0\rangle(|\epsilon_{00}\rangle \pm |\epsilon_{10}\rangle) + |1\rangle(|\epsilon_{01}\rangle \pm |\epsilon_{11}\rangle)]/\sqrt{2}$ , which can be rewritten (ignoring the global phase  $\pm 1$ ) as  $[|\pm\rangle(|\epsilon_{00}\rangle \pm |\epsilon_{01}\rangle \pm |\epsilon_{10}\rangle + |\epsilon_{11}\rangle) + |\mp\rangle(|\epsilon_{00}\rangle \mp |\epsilon_{01}\rangle \pm |\epsilon_{10}\rangle + |\epsilon_{11}\rangle)]/2$ . The form of  $|\epsilon_{\pm\pm}\rangle$  and  $|\epsilon_{\pm\mp}\rangle$  follow from this.

and

$$|\eta_{\pm\pm}\rangle = \frac{1}{2}(|\eta_{00}\rangle \pm |\eta_{01}\rangle \pm |\eta_{10}\rangle + |\eta_{11}\rangle),$$
 (20a)

$$|\eta_{\pm\mp}\rangle = \frac{1}{2}(|\eta_{00}\rangle \mp |\eta_{01}\rangle \pm |\eta_{10}\rangle - |\eta_{11}\rangle).$$
 (20b)

When  $k \in \{0, 1\}$ , we define  $\langle \varepsilon_{kk} | \varepsilon_{kk} \rangle = F$ ,  $\langle \varepsilon_{k\bar{k}} | \varepsilon_{k\bar{k}} \rangle = D$  and  $\langle \eta_{kk} | \eta_{kk} \rangle = F'$ ,  $\langle \eta_{k\bar{k}} | \eta_{k\bar{k}} \rangle = D'$ , which can all be taken to be positive real numbers. These values relate to the probability that Eve and Yves leave the distributed state unaffected. In order to ensure unitarity.

$$F + D = 1 = F' + D',$$
 (21a)

$$\langle \varepsilon_{00} | \varepsilon_{10} \rangle + \langle \varepsilon_{01} | \varepsilon_{11} \rangle = 0 = \langle \eta_{00} | \eta_{10} \rangle + \langle \eta_{01} | \eta_{11} \rangle.$$
 (21b)

This allows us, without loss of generality [28], to set

 $\langle \varepsilon_{kk} | \varepsilon_{k\bar{k}} \rangle = \langle \varepsilon_{kk} | \varepsilon_{\bar{k}k} \rangle = 0 = \langle \eta_{kk} | \eta_{k\bar{k}} \rangle = \langle \eta_{kk} | \eta_{\bar{k}k} \rangle, \forall k \in \{0,1\}.$  Also,  $|\varepsilon_{kl}\rangle, |\varepsilon_{\bar{k}\bar{l}}\rangle$  are generally non-orthogonal (likewise for  $|\eta_{kl}\rangle$ ). So, we take

$$\langle \varepsilon_{00} | \varepsilon_{11} \rangle = F \cos x,$$
 (22a)

$$\langle \varepsilon_{01} | \varepsilon_{10} \rangle = D \cos y,$$
 (22b)

$$\langle \eta_{00} | \eta_{11} \rangle = F' \cos x', \tag{22c}$$

$$\langle \eta_{01} | \eta_{10} \rangle = D' \cos y', \tag{22d}$$

where  $x, y, x', y' \in [0, \pi/2]$ . We can think of x, y (x', y') as dictating the distinguishability between Eve's (Yves's) possible ancilla states.

Similarly to in the previous section, following the basis comparison step, the state of the entire system is updated as follows:

$$\rho \otimes \varepsilon \otimes \eta \otimes \omega \to \rho_{\text{sifted}} = \frac{1}{2} \sum_{\mathfrak{B} \in \mathsf{C}} \sum_{j,k \in \mathfrak{B}} \left( \{ U_Y, B_j, U_E, A_k \} \rho \otimes \varepsilon \otimes \eta \{ U_Y, B_j, U_E, A_k \}^{\dagger} \otimes \omega \right.$$

$$+ \left. [U_Y, B_j, U_E, A_k] \rho \otimes \varepsilon \otimes \eta [U_Y, B_j, U_E, A_k]^{\dagger} \otimes \sigma_z \omega \sigma_z \right.$$

$$+ \left. \{ U_Y, B_j, U_E, A_k \} \rho \otimes \varepsilon \otimes \eta [U_Y, B_j, U_E, A_k]^{\dagger} \otimes \omega \sigma_z \right.$$

$$+ \left. [U_Y, B_j, U_E, A_k] \rho \otimes \varepsilon \otimes \eta \{ U_Y, B_j, U_E, A_k \}^{\dagger} \otimes \sigma_z \omega \right), \quad (23)$$

where

$$\{U_Y, B_j, U_E, A_k\} := U_Y B_j U_E A_k + A_k U_E B_j U_Y,$$
 (24a)  
 $[U_Y, B_j, U_E, A_k] := U_Y B_j U_E A_k - A_k U_E B_j U_Y.$  (24b)

Denoting Eve and Yves's joint strategy using  $\mathcal{Z}$ , we are now equipped to calculate the following:

- 1. Minimum probability of detection: d.
- 2. Eavesdroppers and Alice's [Bob's] mutual information:  $H(\mathcal{Z}:\mathcal{A})$  [ $H(\mathcal{Z}:\mathcal{B})$ ].
- 3. Alice and Bob's mutual information: H(A : B).

## B. Minimum probability of detection

Let us first calculate the eavesdropper detection probability. Recall that, in this protocol, this corresponds to measuring the control qubit to be in the state  $|-\rangle\langle-|$  given that it was initially prepared in the state  $|+\rangle\langle+|$ . Therefore, using  $\rho = 1/2 = (1/2) \sum_{\psi} |\psi\rangle\langle\psi|$ , the probability of detection is given by

$$P_{\text{detect}} = \frac{1}{4} \sum_{\psi} \sum_{\mathfrak{B} \in \mathsf{C}} \sum_{j,k \in \mathfrak{B}} \langle \psi \varepsilon \eta | [U_Y, B_j, U_E, A_k]^{\dagger} \times [U_Y, B_j, U_E, A_k] | \psi \varepsilon \eta \rangle, \quad (25)$$

where  $|\psi \varepsilon \eta\rangle := |\psi\rangle^{(S)} \otimes |\varepsilon\rangle^{(\tilde{E})} \otimes |\eta\rangle^{(\tilde{Y})}$ . Now, noting that,

$$U_{Y}B_{j}U_{E}A_{k}|\psi\varepsilon\eta\rangle = \frac{1}{2}\delta_{\psi k}\left(\delta_{jk}|\varepsilon_{kk}\rangle + \delta_{j\bar{k}}|\varepsilon_{k\bar{k}}\rangle\right)$$

$$\left(|j\rangle|\eta_{jj}\rangle + |\bar{j}\rangle|\eta_{j\bar{j}}\rangle\right), (26a)$$

$$A_{k}U_{E}B_{j}U_{Y}|\psi\varepsilon\eta\rangle = \frac{1}{2}|k\rangle\left(\delta_{kj}|\varepsilon_{jj}\rangle + \delta_{k\bar{j}}|\varepsilon_{j\bar{j}}\rangle\right)$$

$$\left(\delta_{j\psi}|\eta_{\psi\psi}\rangle + \delta_{j\bar{\psi}}|\eta_{\psi\bar{\psi}}\rangle\right), (26b)$$

where, in the first equation, the order of the qubits was changed for convenience, we can calculate  $P_{\rm detect}$  to be

$$P_{\text{detect}} = \frac{1}{2} - \frac{1}{8} \left[ FF'(3 + \cos x \cos x') + DD'(1 + 3\cos y \cos y') + FD'(\cos x + \cos y') + DF'(\cos y + \cos x') \right].$$
(27)

Recalling that D=1-F and D'=1-F', and minimising  $P_{\rm detect}$  over F,F', we find there are two<sup>9</sup> possibilities when minimising the probability of detection

<sup>&</sup>lt;sup>9</sup> There are actually 4 possibilities, but the two options not written explicitly: F = 0 = D' and F = 1 = D', result in larger detection probabilities than the F = 1 = F' case  $\forall x, x', y, y'$ .

 $d:=P_{\mathrm{detect}}^{\min}.$  Note that we can take this approach since D,F,D',F' can be chosen independently of x,x',y,y'.

Option 1: F = 0 = F'. Here,

$$d = \frac{3}{8}(1 - \cos y \cos y'). \tag{28}$$

Option 2: F = 1 = F'. Here,

$$d = \frac{1}{8}(1 - \cos x \cos x'). \tag{29}$$

Since there are values of x, y, x', y' such that each option is smaller, we must consider both options when calculating the various mutual information values.

#### C. Eavesdroppers - Alice/Bob mutual information

It can be shown that  $H(\mathcal{Z}:\mathcal{A})=H(\mathcal{Z}:\mathcal{B}).$  So, in what follows, we only look at  $H(\mathcal{Z}:\mathcal{A})$  explicitly. With the setup we're considering, after Eve and Yves have both carried out their unitaries, they perform some joint measurement on both of their ancillae that best distinguishes between a 0 and a 1 in Alice's key. In order to do this, they should utilise all public information, which means waiting for Alice to reveal her basis choice before choosing which joint measurement to perform on their ancillae. Therefore, in order to find the maximum mutual information (subject to a minimal probability of detection), two optimal measurements must be constructed: one to distinguish  $\{\Psi_0^{AZ}, \Psi_1^{AZ}\}$ , and one to distinguish  $\{\Psi_0^{AZ}, \Psi_1^{AZ}\}$  which are the possible states of the eavesdroppers' ancillae when the z and x-bases were chosen by Alice and Bob, respectively.

For both cases, the states to be distinguished are found using

$$\Psi_l^{AZ} = \frac{1}{\mathcal{N}} \operatorname{Tr}_{S,C} \left( \rho_{\text{sifted}} \Big|_{k=l} \right), \tag{30}$$

where  $\mathcal{N}$  is a normalisation constant, and S,C indicate that the trace is being carried out over the distributed and control qubit respectively. Further,  $\rho_{\text{sifted}}|_{k=l}$  denotes the terms in  $\rho_{\text{sifted}}$  [Eq. (23)] in which Alice's measurement outcome is l. Let's consider the two options we found in the previous subsection.

*Option 1:* F = 0 = F'.

In this case, when  $l \in \{0, 1\}$ ,

$$\Psi_l^{AZ} = \frac{1}{2} (\varepsilon_{01} \otimes \eta_{10} + \varepsilon_{10} \otimes \eta_{01}), \tag{31}$$

and when  $l \in \{+, -\}$ ,

$$\Psi_l^{AZ} = \frac{1}{4} (\varepsilon_{10} + \varepsilon_{01}) \otimes (\eta_{10} + \eta_{01}). \tag{32}$$

Note that  $\Psi_0^{AZ}=\Psi_1^{AZ}$  and  $\Psi_+^{AZ}=\Psi_-^{AZ}$  which implies Eve and Yves's best strategy is to just guess. Therefore, the mutual information between the eavesdroppers and Alice is  $H(\mathcal{Z}:\mathcal{A})=0$  when F=0=F'.

Option 2: F = 1 = F'.

In this case, when  $l \in \{0, 1\}$ ,

$$\Psi_l^{AZ} = \varepsilon_{ll} \otimes \eta_{ll}, \tag{33}$$

and, when  $l \in \{+, -\}$ ,

$$\Psi_l^{AZ} = \frac{1}{4} (\varepsilon_{00} + \varepsilon_{11}) \otimes (\eta_{00} + \eta_{11}). \tag{34}$$

This means that, although  $\Psi_+^{AZ}=\Psi_-^{AZ}$ , as in the previous case (and therefore no information can be gained here), unlike in Option 1,  $\Psi_0^{AZ}\neq\Psi_1^{AZ}$  and information about Alice's key can thus be accessed.

Now, as mentioned earlier, in order to maximise the mutual information between Alice and the eavesdroppers, we must find the optimal measurement that distinguishes  $\{\Psi_0^{AZ}, \Psi_1^{AZ}\}$ . We can do this by noticing that these states can be written as  $\Psi_l^{AZ} = |\Psi_l^{AZ}\rangle\langle\Psi_l^{AZ}|$ , such that

$$\begin{split} |\Psi_l^{AZ}\rangle &= \frac{1}{\sqrt{2}} \bigg[ \sqrt{1 + |\langle \Psi_0^{AZ} | \Psi_1^{AZ} \rangle|} |a\rangle \\ &+ (-1)^l \sqrt{1 - |\langle \Psi_0^{AZ} | \Psi_1^{AZ} \rangle|} |b\rangle \bigg], \quad (35) \end{split}$$

where  $|a\rangle, |b\rangle$  are some orthonormal vectors in Eve and Yves's shared ancilla space. In our case,  $|\langle \Psi_0^{AZ} | \Psi_1^{AZ} \rangle|$  =  $\cos x \cos x'$ . The optimal measurement to distinguish these states is known to be made up of the following operators [37]:

$$\pi_l = \frac{1}{2} \left[ |a\rangle + (-1)^l |b\rangle \right] \left[ \langle a| + (-1)^l \langle b| \right]. \tag{36}$$

To calculate the mutual information in the z-basis case, we use

$$H_{0/1}(\mathcal{Z}:\mathcal{A}) = -\sum_{i \in \{0,1\}} P(z_i) \log P(z_i)$$

$$-\sum_{j \in \{0,1\}} P(a_j) \log P(a_j)$$

$$+\sum_{i,j \in \{0,1\}} P(z_i, a_j) \log P(z_i, a_j),$$
(37)

where the subscript 0/1 is used to highlight that this is the mutual information *only* in the z-basis case. Here, the outcome  $z_i$  corresponds to Eve and Yves performing their joint optimal measurement  $\{\pi_k\}$ , with outcome k=i, and  $a_j$  corresponds to Alice measuring j, or equivalently (and perhaps more usefully for the calculation),  $a_j$  can be thought of as the preparation of the state  $\Psi_j^{AZ}$ . After some algebra, it turns out that

$$H_{0/1}(\mathcal{Z}:\mathcal{A}) = 1 - h \left[ \left( 1 + \sqrt{1 - \cos^2 x \cos^2 x'} \right) / 2 \right], (38)$$

where  $h(q) = -q \log(q) - (1-q) \log(1-q)$  is the binary entropy function [38]. Using Eq. (29), this can be rewritten in terms of the minimum detection probability as

$$H_{0/1}(\mathcal{Z}:\mathcal{A}) = 1 - h \left[ \left( 1 + 4\sqrt{d[1 - 4d]} \right) / 2 \right],$$
 (39)

such that  $0 \le d \le 1/8$ .

#### D. Alice - Bob mutual information

The calculation of the mutual information between Alice and Bob,  $H(\mathcal{A}:\mathcal{B})$ , is less involved than that of  $H(\mathcal{Z}:\mathcal{A})$  since Alice and Bob's measurements are fixed. The key thing to note is that the probabilities required for the calculations are found using

$$P(a_l, b_m) = \text{Tr}\left(\rho_{\text{sifted}}\big|_{k=l, j=m}\right),$$
 (40)

where, similarly to before,  $\rho_{\text{sifted}}|_{k=l,j=m}$  is made up from the k=l, j=m terms in Eq. (23).

Carrying out all the algebra, we find that, when Alice and Bob measure in the z-basis, the mutual information between them is

$$H_{0/1}(\mathcal{A}:\mathcal{B}) = 1. \tag{41}$$

When Alice and Bob measure in the x-basis however.

$$H_{\pm}(\mathcal{A}:\mathcal{B}) = 1 - h[(1+\cos x)/2].$$
 (42)

Intuitively, this can be understood when we realise that any errors between Alice and Bob's keys are induced purely by Eve's intervention and not Yves's (this is discussed slightly more in the following subsection). We may therefore expect to see a  $\cos x$  dependence but not a  $\cos x'$  one.

The form of Eq. (42) means we cannot directly determine  $H_{\pm}(\mathcal{A}:\mathcal{B})$  [and therefore  $H(\mathcal{A}:\mathcal{B})$ ] using the probability of detection d. However, we can use d to put some bounds on  $H_{\pm}(\mathcal{A}:\mathcal{B})$ . To do this, we look at how Eve and Yves maximise  $H_{0/1}(\mathcal{Z}:\mathcal{A})$  [and therefore  $H(\mathcal{Z}:\mathcal{A})$ ] for any given value of d. Plotting  $H_{0/1}(\mathcal{Z}:\mathcal{A})$  with respect to x,x', it can be seen that this maximisation occurs along either the x=0 or x'=0 axis. This results in

$$H_{+}(\mathcal{A}:\mathcal{B})|_{x=0} = 1,$$
 (43a)

$$H_{\pm}(\mathcal{A}:\mathcal{B})|_{x'=0} = 1 - h(4d),$$
 (43b)

where, as before,  $0 \le d \le 1/8$ . Thus, if Eve and Yves are aiming to minimise the probability of being detected whilst maximising their knowledge of the shared key,

$$H_{0/1}(\mathcal{A}:\mathcal{B}) = 1,\tag{44a}$$

$$H_{+}(\mathcal{A}:\mathcal{B}) \in [1 - h(4d), 1].$$
 (44b)

It is interesting to note that, since  $H(\mathcal{Z}:\mathcal{A})|_{x=0}$  and  $H(\mathcal{Z}:\mathcal{A})|_{x'=0}$  take the same range of values [as can be seen from Eq. (38)], the eavesdroppers can choose whether or not they want to induce errors in Alice and Bob's shared key whilst extracting information about it<sup>10</sup>. This effectively corresponds to how much impact they allow Eve to have (regardless of Yves).

In FIG. 5, we plot these various different mutual information functions with respect to the minimum detection probability d. Notice the difference between the x and z-basis cases in these plots. This is purely an artifact of how the eavesdroppers' unitaries, and therefore measurements, were set up in a basis dependent way. By an appropriate redefinition of these measurements, we could flip these results and have the eavesdroppers learn something about the x cases but not the z ones, or some combination of both. These plots make it clear that in both cases of Alice and Bob's basis choice, the mutual information between the eavesdroppers and Alice (or Bob) is less than or equal to the mutual information shared by Alice and Bob. Therefore, the normal post processing protocols can be undertaken to obtain a secure key between Alice and Bob, at least in the class of attacks considered here [30].

#### E. Example

Let us consider a simple example to gain some intuition as to how this protocol differs from its definite causal counterpart. Before we do so, let us write down the probability of error  $P_{\text{error}}$  between Alice and Bob's keys in the case of F, F' = 1. Using  $P_{\text{error}} = \text{Tr}\left(\rho_{\text{sifted}}\big|_{j=\bar{k}}\right)$ , it can be shown that

$$P_{\text{error}} = \frac{1}{4}(1 - \cos x). \tag{45}$$

Note once again that the errors are caused purely by Eve and not Yves. Similarly to in the previous subsection, we can use the maximisation of  $H(\mathcal{Z}:\mathcal{A})$  to put bounds on  $P_{\text{error}}$ . Recall that to do this, we let either x=0 or x'=0, from which it follows that

$$P_{\text{error}} \in [0, 2d]. \tag{46}$$

So, let's consider the case in which Eve performs the measurement  $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ . This corresponds to  $x=\pi/2$ . Using Eq. (29) and Eq. (45), we can see that  $P_{\rm error}=1/4$ , but d=1/8. This differs from the analogous case in BB84 where the error rate of 1/4 is used as the detection probability. This is because the effects of the eavesdroppers are not solely contained in the terms used to calculate  $P_{\rm detect}$  (that is, the  $\sigma_z\omega\sigma_z$  terms). Some

<sup>&</sup>lt;sup>10</sup> Note that here, we have ignored the subscripts in the mutual entropy notation since  $H(\mathcal{Z}:\mathcal{A})=H_{0/1}(\mathcal{Z}:\mathcal{A})$ .

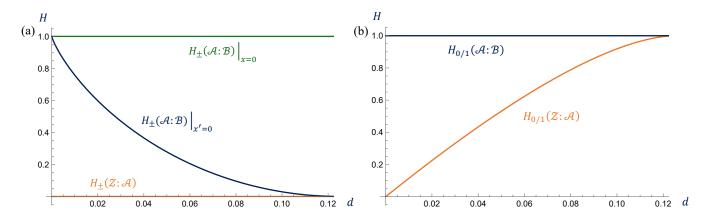


FIG. 5. When eavesdroppers Eve and Yves carry out individual (not fully correlated) attacks, the mutual information,  $H(\mathcal{Z}:\mathcal{A})$ , they share with Alice (or Bob) compares to the mutual information between Alice and Bob  $H(\mathcal{A}:\mathcal{B})$  as plotted. In (a), this is shown for the case in which Alice and Bob measure in the *z*-basis, and in (b), Alice and Bob measure in the *z*-basis.

of them lie in the  $\omega, \omega \sigma_z$  and  $\sigma_z \omega$  terms. It is possible that a different measurement on the control qubit could result in better odds. However, we do not attempt to optimise this measurement here.

It is interesting to note that the location of the eavesdroppers (performing  $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ) dictates the errors induced between Alice and Bob's key. For example, if only Yves is present, there will be no errors found. If, however, Eve is present, regardless of whether Yves is there or not, the probability of error (in this example) between Alice and Bob's key is 1/4, similarly to what is observed in BB84. This phenomenon is true beyond this example: if only Eve is present, every detection event implies an error between Alice and Bob's corresponding key bit, since  $[A_k, U_E, A_k] = 0 \ \forall k$ . If, however, only Yves is present, there are never any errors induced, since  $[U_Y, A_k, A_{\bar{k}}] = 0 \ \forall k$ . This is a contrasting point to BB84, where errors are required to detect eavesdroppers. Here, they need not introduce errors to be detected. All in all, this means that, if the location of the eavesdropper(s) is (are) unknown, whether or not errors occur is unknown. These ideas were hinted at in the previous subsection where we saw that the eavesdroppers had the ability to affect how much mutual information Alice and Bob shared.

#### F. Correlated individual attacks and beyond

As noted before, the strategies considered until now have not allowed Eve and Yves's operations to be correlated prior to the measurement of their ancillae. It turns out that the presence of eavesdroppers, performing individual attacks<sup>11</sup>, can be privately detected regardless of the correlations they share. Assuming that the eavesdroppers do not have access to Alice's lab, and therefore cannot alter the causal structure of the protocol by tampering with the control qubit, we let Eve and Yves do anything permitted by quantum mechanics within their respective labs. We therefore allow them to perform correlated quantum instruments<sup>12</sup>. To describe this situation we use the process matrix formalism [3] introduced in Appendix B. Indeed, to account for correlations shared between Eve and Yves, we allow them to act jointly on the state being shared via the quantum switch process matrix, together with their own, separate ancillary process matrix. This process matrix is taken to be arbitrary. meaning it describes any possible set of correlations: Eve and Yves could share entangled states; send quantum and classical information to each other; or even utilise their own indefinite causal structure.

Full details of all of this can be found in Appendix C, but for clarity, we state our main result here.

**Result IV.1.** Define the probability of detection  $P_{detect} = P(\omega = |-\rangle \langle -|)$  as the probability of measuring the control qubit to be in the state  $|-\rangle \langle -|$ , and assume eavesdroppers perform arbitrary individual attacks without access to  $\omega$ . Writing Alice and Bob's measurement outcomes as i, j respectively, and Eve and Yves's joint measurement outcome as  $\mathbf{x}$ , if  $P_{detect} = 0$ , then

$$P(\mathbf{x}, i, j) = \begin{cases} \frac{|\langle i|\psi\rangle|^2}{2} \left( |r_{\mathbf{x}}^0 + r_{\mathbf{x}}^3|^2 \delta_{ij} + |r_{\mathbf{x}}^1 + r_{\mathbf{x}}^2|^2 \delta_{i\bar{j}} \right), & i, j \in \{0, 1\} \\ \frac{|\langle i|\psi\rangle|^2}{2} \left( |r_{\mathbf{x}}^0 + r_{\mathbf{x}}^1|^2 \delta_{ij} + |r_{\mathbf{x}}^2 + r_{\mathbf{x}}^3|^2 \delta_{i\bar{j}} \right), & i, j \in \{+, -\}, \end{cases}$$

$$(47)$$

<sup>&</sup>lt;sup>11</sup> Recall that by individual attacks, we mean that Eve and Yves act on each distributed state separately.

<sup>&</sup>lt;sup>12</sup> Quantum instruments are defined in Appendix B.

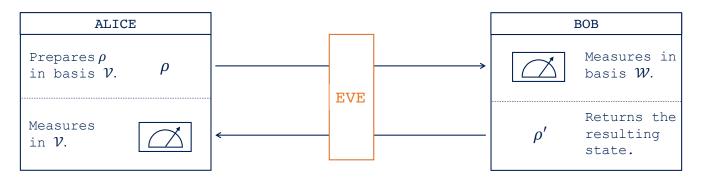


FIG. 6. Two way QKD protocol in a definite causal order that realises private detection. The bases V, W are independently and randomly chosen between the x and z-bases.

where  $|\psi\rangle\langle\psi|=\rho$  is the initial state of the target system  $S,\ r_{\mathbf{x}}^0,r_{\mathbf{x}}^1,r_{\mathbf{x}}^2,r_{\mathbf{x}}^3\in\mathbb{C},\ and\ \bar{j}\ means\ "not\ j".$ 

Notice that when undetected (i.e.  $P_{\rm detect}=0$ ), Eve and Yves can therefore learn something about Alice and Bob's copies of the keys, but nothing useful. They can learn something about which basis was chosen, which is already publicly known, as well as whether errors have occurred between Alice and Bob's keys. Notice also that, similarly to in the previous subsection, Eve and Yves can choose to induce errors in Alice and Bob's key without being detected. But the fact remains that the information the eavesdroppers have access to has no use when it comes to learning about Alice and Bob's key.

## V. PRIVATE DETECTION IN A DEFINITE CAUSAL ORDER

In this section, we consider whether this same phenomena of private detection could be achieved without the help of indefinite causal order. Indeed, we provide here evidence that it is possible. However an extra measurement by Alice is required, and as we shall discuss, some attacks possible here are not possible in the indefinite causal case we have considered. This indicates a more subtle relationship between definite and indefinite causal quantum key distribution protocols.

Suppose, as depicted in FIG. 6, Alice prepares a state  $\rho \in \mathcal{L}(\mathcal{V})$  that is either the x or z-basis (with corresponding key bits as before). Suppose she then sends  $\rho$  to Bob, who measures in the basis  $\mathcal{W}$  which, again, is chosen randomly between the x and z-bases. Following this, Bob returns the updated state back to Alice who measures it in the same basis that she prepared the state in:  $\mathcal{V}$ . As they did in the other sections of this chapter, Alice and Bob then compare which bases they chose, and only use the cases in which they agree for their shared key. Now, by counting how often she measures a different state from the one she prepared, a scenario that we call an error, Alice can monitor for eavesdroppers. This is possible since she knows two things when there are no eavesdroppers:

- 1. When  $V=\mathcal{W}$ , the probability of error  $P_{\text{error}}^{\text{same}}$  is zero.<sup>13</sup>
- 2. When  $\mathcal{V} \neq \mathcal{W}$ , the probability of error  $P_{\mathrm{error}}^{\mathrm{diff}}$  is  $1/2.^{14}$

Let's consider an example showing how an eavesdropper's intervention affects at least one of these probabilities.

Suppose an eavesdropper, Eve, attempts to keep  $P_{\rm error}^{\rm same}$  at its expected value of zero. As depicted in FIG. 7, she can do this by sending out a probe state  $\xi$  to Bob, whilst returning Alice's qubit state  $\rho$  back to her, unaffected<sup>15</sup>. In this scheme, Eve can access as much information as possible about Bob's key without affecting  $P_{\rm error}^{\rm same}$ . However, this strategy would also result in  $P_{\rm error}^{\rm diff} = 0 \neq 1/2$ , thereby allowing Alice to detect Eve. This is, of course, an extreme case: Eve could attempt to find out which measurement Bob performed and induce errors using some operation  $\mathcal E$  on  $\rho$  to increase  $P_{\rm error}^{\rm diff}$ . But it doesn't seem as though she could ever increase it to 1/2.

To see this, suppose Eve thinks she knows which measurement Bob chose, for example,  $\{|\pm\rangle\langle\pm|\}$ . Then she can introduce errors in at most 50% of the bits by acting on  $\rho$  with  $\sigma_x$ : if Alice prepared  $|\pm\rangle$ , no errors are induced (as

<sup>&</sup>lt;sup>13</sup> For example, suppose Alice prepares the state  $|-\rangle\langle-|$  and Bob measures it in the basis  $\{|\pm\rangle\langle\pm|\}$ . Since  $\langle+|-\rangle=0$ , Bob is guaranteed to obtain an outcome of -, and therefore send the state  $|-\rangle\langle-|$  back to Alice. So, when Alice goes on to measure this state in the basis she prepared it in:  $\{|\pm\rangle\langle\pm|\}$ , she will always obtain a result of -. In other words, she will never register an error.

<sup>&</sup>lt;sup>14</sup> For example, suppose Alice prepares the state  $|0\rangle\langle 0|$  and Bob measures in the basis:  $\{|\pm\rangle\langle\pm|\}$ . Then the state Alice receives from Bob is 1/2, meaning that when Alice measures this in her original basis  $\{|0/1\rangle\langle 0/1|\}$ , the probability she measures the state to be different to the one she prepared is  $\langle 1|1|1\rangle\langle 2=1/2$ .

 $<sup>^{15}</sup>$  In FIG. 7 this would correspond to setting the operation  $\mathcal E$  equal to the identity  $\mathcal I.$ 

Alice would expect if Bob measured in the x-basis), if Alice prepared in  $|0/1\rangle$ , Eve induces an error. The problem is, Bob is choosing randomly between mutually unbiased bases, meaning Eve can only be sure which basis he chose some proportion p<1 of the time<sup>16</sup>. It follows that, if Eve wants to preserve  $P_{\rm error}^{\rm same}=0$ , the attack proposed in FIG. 7 results in, at most,  $P_{\rm error}^{\rm diff}=p/2<1/2$ . We discuss this situation more explicitly in Appendix A. Of course, more general correlations between Eve's probe state  $\sigma$ , and how she acts on Alice's state  $\rho$  are possible. That being said, we found no strategy that allowed for Eve to extract information whilst leaving both  $P_{\rm error}^{\rm same}$  and  $P_{\rm error}^{\rm diff}$  unaltered. We leave the full analysis of this scenario for future work.

So, it may seem as though there is no difference between the indefinite and definite causal cases. However, one thing to notice here is that the attacks discussed here (depicted in FIG. 7) are not ones that are possible in our indefinite causal protocol. In order for undetected eavesdroppers to send  $\rho$  back to Alice without going via Bob, Eve and Yves would need to do so coherently in the superposition induced by  $\omega$ . Doing so requires them to have access to the control qubit  $\omega$ . We discuss possible implications of this realisation in the following section.

#### VI. CONCLUSION AND DISCUSSION

In this work we explored the idea of performing the QKD protocol BB84 in an indefinite causal regime. We defined a protocol that achieves this by performing projective measurements in an indefinite causal order. In doing so, we found that it is possible to detect eavesdroppers during a QKD task without publicly comparing any subset of a shared private key between the two parties involved, Alice and Bob. We found that this could be achieved using a second system that acts as the control in inducing the indefinite causal ordering. In contrast to one-way QKD protocols, but similarly to two-way protocols, there are two locations eavesdroppers can reside, allowing for cooperative attacks. These have both been considered and the security against a class of individual attacks by the eavesdroppers was proven. Further, it was shown (in Appendix C) that eavesdroppers, who do not have access to the qubit controlling the causal order of the protocol, cannot extract any useful information about the key without inducing a non-zero detection probability, at least when they act on each distributed state individually. Indeed, we showed that this was true for any cooperative strategy the eavesdroppers used. In Sec. V, we discussed a possible way of privately detecting eavesdroppers using a two-way protocol in a definite causal order. To do this, an extra instance of Alice's operation was required,

This ICO QKD protocol could be challenging to realise experimentally due to the requirement to preserve coherence between the two causal orderings over the distance of communication. Further, one might expect projective measurements of  $\rho$ , performed in an indefinite causal order, to be unattainable. However, as discussed in Appendix D, the results of this protocol could be simulated using linearly polarised light, a Sagnac interferometer and some polarising filters. The Sagnac interferometer would create the indefinite causal order and the polarising filters would be orientated in various different ways to correspond to each of Alice and Bob's measurement outcomes. More promising is with regards to recent work by H. Cao et al [6], who experimentally performed quantum instruments in an indefinite causal order. This indicates that a full experimental implementation of this protocol could be possible in the not-too-distant future.

When it comes to practicality, consider using a Sagnac interferometer or something similar to create an indefinite causal ordering of operations. In order for the ICO to be legitimate, the coherence length of the light used must be considerably larger than the path length of the interferometer [4], perhaps indicating a limit to how practical such a protocol would be. Another limitation becomes apparent when we notice that two qubits are required to distribute one key bit securely, compared to BB84's one qubit. Perhaps this second, control state could find a secondary use beyond determining the presence of eavesdroppers, but we leave this consideration for future work. Finally, we note that the effects of noise and loss in this protocol have not been considered here. Indeed, being similar in nature to two-way protocols, they are likely to have a substantial impact (in comparison to one-way protocols). Having said this, there is evidence that the effects of noise can be evaded in certain indefinite causal scenarios [13, 15, 16, 20] which could make this an interesting line of future research<sup>17</sup>.

For reasons stemming from this article, we argue that further exploration into the crossover between quantum cryptography and indefinite causal structures is warranted. Recall that in Sec. V we discussed a definite causal protocol that exhibited similar phenomena to our indefinite causal one. Here, we considered various eavesdropping attacks, in particular the one depicted in FIG. 7. We noted that these attacks are not possible in our indefinite causal protocol: undetected eavesdroppers can't send  $\rho$  straight back to Alice without having access to the control qubit state  $\omega$ . This hints at an intriguing thought: do eavesdroppers have to be able to "hack into" and alter the causal structure of a protocol to realise their full, cryptanalytic potential? Indeed, if so,

a property consistent with other discussions of indefinite versus definite causal orderings [2].

<sup>&</sup>lt;sup>16</sup> As is done in Appendix A, unambiguous quantum state discrimination can be used to analyse this tactic more concretely [37, 39, 40].

<sup>&</sup>lt;sup>17</sup> Regardless of whether this phenomenon is a unique to indefinite causal order or not [32].

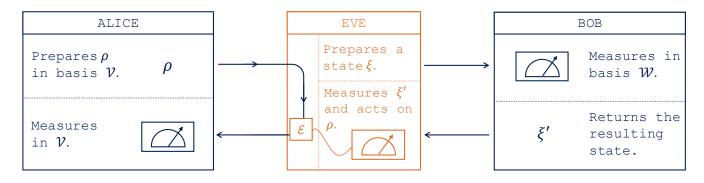


FIG. 7. Eavesdropping strategy allowing for Alice's state to be returned to her unaffected whilst letting Eve learn something about Bob's key. If the probability  $P_{\text{error}}^{\text{same}}$  is left unaltered at its expected value of zero, we found no strategy that allowed the probability  $P_{\text{error}}^{\text{diff}}$  to remain at its expected value of 1/2.

could this mean that the security of a key sharing protocol is bolstered by obscuring its causal structure? It's plausible that eavesdroppers may be able to somehow gain access to the control qubit in the quantum switch scenario we considered, but how about when different, more obscure, causal structures are used? Related to these questions, how do the ideas of device-independent QKD [41, 42] translate into a setting where eavesdroppers may be infiltrating the causal structure of the protocol? We therefore consider this work as just an initial step in studying quantum cryptographic protocols within indefinite causal structures.

#### ACKNOWLEDGMENTS

The author would like to thank Sarah Croke and John Jeffers for the invaluable discussions. The author acknowledges The Engineering and Physical Sciences Research Council and the UK National Quantum Technologies Programme via the QuantIC Quantum Imaging Hub (EP/T00097X/1). This work benefitted from network activities through the INAQT network, supported by the Engineering and Physical Sciences Research Council (grant number EP/W026910/1). This research was supported in part by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development and by the Province of Ontario through the Ministry of Colleges and Universities.

#### Appendix A: A definite causal QKD attack

In Sec. V, we considered an attack, depicted in FIG. 7 and discussed how  $P_{\rm error}^{\rm same}=0, P_{\rm error}^{\rm diff}=1/2$ , cannot seem to be simultaneously achieved. We expand on this argument in this short appendix.

Suppose Eve sends the probe state  $\xi$  to Bob. Depending on Bob's measurement choice, he would send back

one of the following two states:

$$\xi_z = \langle 0|\xi|0\rangle|0\rangle\langle 0| + \langle 1|\xi|1\rangle|1\rangle\langle 1|, \tag{A1a}$$

$$\xi_x = \langle +|\xi|+\rangle |+\rangle \langle +|+\langle -|\xi|-\rangle |-\rangle \langle -|. \tag{A1b}$$

Eve's aim is to use these returned states to introduce or avoid errors in the relevant places. Since she doesn't want to induce any errors when Alice and Bob agree on their basis choice, only when they disagree, she must be sure which basis Bob chose. She could therefore perform unambiguous quantum state discrimination [37, 39, 40] to distinguish  $\{\xi_z, \xi_x\}$ . To do this, she uses the following POVM

$$\pi_z = \alpha \xi_x^{\perp}, \tag{A2a}$$

$$\pi_x = \beta \xi_z^{\perp}, \tag{A2b}$$

$$\pi_? = \mathbb{1} - \pi_x - \pi_z, \tag{A2c}$$

where  $\alpha, \beta \geq 0$ ,  $\text{Tr}(\xi_w^{\perp} \xi_w) = 0$  for w = x, z, and  $\pi$ ? corresponds to the inconclusive outcome.

Now, since  $\pi_x=\pi_z=0$  would make for an uninformative measurement, we assume, without loss of generality, that  $\xi_z^\perp\neq 0$ . It follows that the support of  $\xi_z$  is not  $\mathbb{C}^2$ , and so, from Eq. (A1),  $\exists!\,i\in\{0,1\}$  such that  $\langle i|\xi|i\rangle=0$ . Again without loss of generality, let  $\langle 1|\xi|1\rangle=0$  and thus  $\xi=|0\rangle\langle 0|$ . This means that  $\xi_z=|0\rangle\langle 0|,\xi_x=1/2,$  and therefore

$$\pi_z = 0, \tag{A3a}$$

$$\pi_x = \beta |1\rangle \langle 1|,\tag{A3b}$$

$$\pi_? = |0\rangle\langle 0| + (1-\beta)|1\rangle\langle 1|. \tag{A3c}$$

Minimising the probability of an inconclusive outcome results in  $\beta=1$ , meaning the probability that Eve is sure Bob measured in the x-basis is p=1/4<1 (assuming Bob picks the x-measurement 1/2 of the time). So, by acting on the state  $\rho$ , being sent back to Alice, with  $\sigma_x$  whenever she measures  $\pi_x$ , Eve induces an error  $P_{\rm error}^{\rm diff}=1/8<1/2$ .

### Appendix B: Quantum operations, instruments, the Choi-Jamiołkowski isomorphism and process matrices

#### 1. Quantum operations and instruments

We begin this appendix by defining a quantum operation. In what follows we take  $\mathcal{L}(\mathcal{V})$  to be the space of linear operators on  $\mathcal{V}$ , and we will label out quantum system by S.

**Definition B.1.** A quantum operation is a map  $\mathcal{E}$ :  $\mathcal{L}(\mathcal{H}^S) \to \mathcal{L}(\mathcal{H}^{S'})$  satisfying the following three conditions:

- 1. For any density operator  $\rho \in \mathcal{L}(\mathcal{H}^S)$ ,  $Tr\mathcal{E}(\rho) \in [0,1]$ .
- 2. It is convex-linear. That is, for any convex combination of density operators  $\sum_{i} p_{i} \rho_{i}$ ,

$$\mathcal{E}\left(\sum_{i} p_{i} \rho_{i}\right) = \sum_{i} p_{i} \mathcal{E}(\rho_{i}).$$

3. It is completely-positive (CP).

One particularly important class of quantum operations are called quantum channels. These are subject to the additional constraint that they are trace-preserving. That is,  $\mathcal{E}_c: \mathcal{L}(\mathcal{H}^S) \to \mathcal{L}(\mathcal{H}^{S'})$  is a quantum channel if it is a quantum operation and, for any density operator  $\rho \in \mathcal{L}(\mathcal{H}^S)$ ,  $\operatorname{Tr} \mathcal{E}_c(\rho) = 1$ . Therefore, quantum channels are often called completely-positive trace-preserving (CPTP) maps.

An alternative, but equivalent, way of describing a quantum operation  $\mathcal{E}$  mathematically is to use a set of operators  $\{E_i\}$  called Kraus operators, named after K. Kraus who first noted this equivalence [43, 44]. As before, let  $\rho$  be a density operator in the input space of  $\mathcal{E}$ , then there exists a set of operators  $\{E_i\}$ , subject to

$$\sum_{i} E_i^{\dagger} E_i \le \mathbb{I}, \tag{B1}$$

that allow us to write

$$\mathcal{E}(\rho) = \sum_{i} E_{i} \rho E_{i}^{\dagger}. \tag{B2}$$

Being a sum of positive operators, the condition in Eq. (B1) corresponds to the first axiom of quantum operations:  $\operatorname{Tr} \mathcal{E}(\rho) \in [0,1]$ . If  $\mathcal{E}$  is CPTP (i.e. a quantum channel), then this condition becomes an equality.

We are now able to define the mathematical structure we use to describe everything allowed by quantum mechanics within a closed lab: a quantum instrument [3, 45].

**Definition B.2.** A quantum instrument is a set of quantum operations  $\mathcal{M} = \{\mathcal{M}_i : \mathcal{L}(\mathcal{H}^S) \to \mathcal{L}(\mathcal{H}^{S'})\}$ , such that  $\sum_i \mathcal{M}_i$  is CPTP.

When performing the instrument  $\mathcal{M} = \{\mathcal{M}_i\}$ , an outcome "i" is registered which tells us that the quantum operation  $\mathcal{M}_i$  has occurred. The probability of obtaining an outcome i, given that S was prepared in the state  $\rho$ , is given by the (generalised) Born rule:  $P(i|\rho) = \text{Tr } \mathcal{M}_i(\rho)$ .

Quantum instruments can rewritten in the Kraus representation. That is, for each outcome i of  $\mathcal{M}$ , the corresponding operation  $\mathcal{M}_i$  can be decomposed as follows:

$$\mathcal{M}_i(\rho) = \sum_j M_{ij} \rho M_{ij}^{\dagger}, \tag{B3}$$

such that the Kraus operators  $\{M_{ij}\}$  satisfy

$$\sum_{i,j} M_{ij}^{\dagger} M_{ij} = \mathbb{I}. \tag{B4}$$

This corresponds to the requirement that  $\sum_i \mathcal{M}_i$  be CPTP in order to ensure that the probabilities  $P(i|\rho) = \text{Tr } \mathcal{M}_i(\rho)$  sum to unity. If this wasn't the case, there would be some other possible outcome unaccounted for. Note that it follows that

$$\sum_{i} M_{ij}^{\dagger} M_{ij} \le \mathbb{I}, \tag{B5}$$

which corresponds to the definition of a quantum operation, as we'd hope since  $\mathcal{M}_i$  is one.

## 2. The Choi-Jamiołkowski isomorphism and process matrices

In the following appendix, we aim to consider Eve and Yves who can work together with the help of classical, quantum and (indefinite) causal correlations to perform individual attacks. In order to do this, it is convenient to use the *process matrix formalism* [35]. This formalism essentially only insists that quantum mechanics is obeyed *locally*. Indeed, no assumptions are made about the causal structure between parties.

To utilise this formalism, we employ the *Choi-Jamiołkowsi isomorphism* [46–48] to reinterpret quantum instruments as sets of positive semi-definite operators. More specifically, suppose some system  $X_I$  with Hilbert space  $\mathcal{H}^{X_I}$  is input to some closed lab and is evolved via some CP map  $\mathcal{X}: \mathcal{L}(\mathcal{H}^{X_I}) \to \mathcal{L}(\mathcal{H}^{X_O})$  resulting in the system  $X_O$ , with corresponding Hilbert space  $\mathcal{H}^{X_O}$ , being output<sup>18</sup>. The Choi-Jamiołkowski (CJ) isomorphism details a correspondence between such CP maps  $\mathcal{X}$  and positive semi-definite operators  $M^X \in \mathcal{L}(\mathcal{H}^{X_I}) \otimes \mathcal{L}(\mathcal{H}^{X_O})$ , which we call CJ operators. As we have done here, we will often use the abbreviation  $X := X_I X_O$ . Explicitly,

$$M^{X} = (\mathcal{I} \otimes \mathcal{X})(|\mathbb{1}\rangle)^{X_{I}X'_{I}}\langle\langle\mathbb{1}|^{X_{I}X'_{I}}\rangle,$$
(B6)

 $<sup>^{18}</sup>$  For our purposes, this could be the lab of Alice, Bob, Eve or  $\mathbf{Y}_{\mathbf{Ves}}$ 

where  $|1\rangle\rangle^{X_IX_I'} = \sum_j |jj\rangle^{X_IX_I'}$  for some *choice* of complete basis  $\{|j\rangle\} \subset \mathcal{H}^{X_I}$  and the primed superscript  $X_I'$  indicates that the space  $\mathcal{H}^{X_I'}$  is a copy of  $\mathcal{H}^{X_I}$ . For Alice and Bob, we will use  $j \in \{0,1\}$ . The map  $\mathcal{X}$  can be recovered using

$$\mathcal{X}(\rho) = \operatorname{Tr}_{X_I} \left[ (\rho^T \otimes \mathbb{1}) M^X \right] \tag{B7}$$

for some state  $\rho$ , where the superscript T denotes the transpose with respect to the chosen basis  $\{|j\rangle\}$ .

Since quantum instruments are made up of quantum operations (maps which are CP, among other things), we can use the Choi-Jamiołkowski isomorphism to describe quantum instruments as sets of CJ operators. So, suppose two parties, Alice and Bob perform the respective instruments  $\mathcal{M}^A = \{\mathcal{M}_i^A: \mathcal{L}(\mathcal{H}^{A_I}) \to \mathcal{L}(\mathcal{H}^{A_O})\}, \mathcal{M}^B = \{\mathcal{M}_j^B: \mathcal{L}(\mathcal{H}^{B_I}) \to \mathcal{L}(\mathcal{H}^{B_O})\}$  on some system that passes through their labs<sup>19</sup>. The probability that Alice obtains an outcome i and Bob j, is given by what we call a process [3]:

$$P(i,j) = \text{Tr}\left[\left(M_i^A \otimes M_j^B\right)^T W^{AB}\right], \tag{B8}$$

where  $M_i^A, M_j^B$  are the CJ operators corresponding to  $\mathcal{M}_i^A, \mathcal{M}_j^B$  respectively, and T is the transpose with respect to the chosen bases in the definitions of  $M_i^A, M_j^B$ . Also in this expression is the process matrix  $W^{AB}$  ( $\equiv W^{A_I A_O B_I B_O}$ ) which details all the possible correlations between Alice and Bob's outcomes. It is defined as a linear operator on  $\mathcal{H}^{A_I} \otimes \mathcal{H}^{A_O} \otimes \mathcal{H}^{B_I} \otimes \mathcal{H}^{B_O}$  satisfying

$$W^{AB} \ge 0,$$
 (B9a)

$$\operatorname{Tr}\left[\left(M^{A}\otimes M^{B}\right)^{T}W^{AB}\right]=1\tag{B9b}$$

for all CJ operators  $M^A = \sum_i M_i^A$ ,  $M^B = \sum_j M_j^B$  corresponding to the CPTP maps  $\sum_i \mathcal{M}_i^A$ ,  $\sum_j \mathcal{M}_j^B$  respectively.

#### Appendix C: Fully correlated eavesdroppers

The aim of this appendix is to see if our protocol withstands eavesdroppers who can work together, as depicted in FIG.4. In particular, eavesdroppers, performing individual attacks, who cannot alter the indefinite causal structure of the key sharing device. In other words, we do not allow them access to the control qubit  $\omega$  of FIG. 4. Let's begin by setting up the problem.

## 1. Problem setup

In this setup, we have multiple labs: first, Bob, labelled by B who performs the same channel as always  $\mathcal{B}$  with Kraus operators  $\{B_j\}$  defined in Eq. (5). Second, Alice,

who we can think of as having two "sublabs": the one we've discussed before, labeled by A where she performs the channel A with Kraus operators  $\{A_i\}$ , again defined in Eq. (5). But, following [35, 49], she also has another sublab, labeled by C that takes in the target and control states at the end. That is, we think of this final system, with Hilbert space  $\mathcal{H}^{C_t} \otimes \mathcal{H}^{C_c}$ , composed from a target component and control component  $C_t$ ,  $C_c$  respectively, as residing within Alice's lab.

Eve and Yves, on the other hand, are only required to obey quantum mechanics locally within their labs, and so can perform quantum instruments  $\mathcal{E}, \mathcal{Y}$  respectively. What's more, since they are allowed to work together, not only do they have access to the state being distributed (with the system passing through their labs labeled by E, Y respectively), but they also share some ancillary process matrix  $W^{\tilde{E}\tilde{Y}}$  detailing all possible correlations between the outcomes of their quantum instruments. We therefore write their quantum instruments as follows:

$$\mathcal{E} = \left\{ \mathcal{E}_l : \mathcal{L}(\mathcal{H}^{E_I} \otimes \mathcal{H}^{\tilde{E}_I}) \to \mathcal{L}(\mathcal{H}^{E_O} \otimes \mathcal{H}^{\tilde{E}_O}) \right\}_l, \quad \text{(C1a)}$$

$$\mathcal{Y} = \left\{ \mathcal{Y}_p : \mathcal{L}(\mathcal{H}^{Y_I} \otimes \mathcal{H}^{\tilde{Y}_I}) \to \mathcal{L}(\mathcal{H}^{Y_O} \otimes \mathcal{H}^{\tilde{Y}_O}) \right\}_n, \quad \text{(C1b)}$$

where  $E_I, Y_I$  ( $E_O, Y_O$ ) are the systems received (sent), by Eve and Yves from (to) Alice and Bob. And  $\tilde{E}_I, \tilde{Y}_I$  ( $\tilde{E}_O, \tilde{Y}_O$ ) are the input (output) ancillary systems of Eve and Yves respectively. These instruments can be described by the sets of Kraus operators

$$\{E_{lm}: \mathcal{H}^{E_I} \otimes \mathcal{H}^{\tilde{E}_I} \to \mathcal{H}^{E_O} \otimes \mathcal{H}^{\tilde{E}_O}\}_{l,m},$$
 (C2a)

$$\{Y_{pq}: \mathcal{H}^{Y_I} \otimes \mathcal{H}^{\tilde{Y}_I} \to \mathcal{H}^{Y_O} \otimes \mathcal{H}^{\tilde{Y}_O}\}_{p,q},$$
 (C2b)

respectively such that  $\sum_m E_{lm}^{\dagger} E_{lm} \leq \mathbb{I}^{E_I \tilde{E}_I}$ ,  $\sum_{l,m} E_{lm}^{\dagger} E_{lm} = \mathbb{I}^{E_I \tilde{E}_I}$ , and similarly for  $\{Y_{pq}\}$ . Further, it will be useful rewrite these Kraus operators using the operator-Schmidt decomposition [50, 51]:

$$E_{lm} = \sum_{\alpha} E_{lm}^{\alpha} \otimes \tilde{E}_{lm}^{\alpha}, \tag{C3a}$$

$$Y_{pq} = \sum_{\lambda} Y_{pq}^{\lambda} \otimes \tilde{Y}_{pq}^{\lambda}, \tag{C3b}$$

where  $\{E_{lm}^{\alpha}: \mathcal{H}^{E_I} \to \mathcal{H}^{E_O}\}_{\alpha}$ ,  $\{\tilde{E}_{lm}^{\alpha}: \mathcal{H}^{\tilde{E}_I} \to \mathcal{H}^{\tilde{E}_O}\}_{\alpha}$  are sets of orthogonal operators, and  $Y_{pq}^{\lambda}, \tilde{Y}_{pq}^{\lambda}$  are defined analogously.

Building off of Refs. [35, 49], if we input a pure state  $\rho_{\psi} = |\psi\rangle\langle\psi|$  to our quantum switch, controlled on the state  $\omega = |+\rangle\langle+|$ , the causal structure of the setup shown in FIG. 4 is described by the process matrix

$$W_{\psi} = W_{\text{ab}}^{ABEYC} \otimes W^{\tilde{E}\tilde{Y}}. \tag{C4}$$

Here,  $W_{\psi}^{ABEYC} = |w_{\psi}\rangle\langle w_{\psi}|$ , defined via

$$|w_{\psi}\rangle = \frac{1}{\sqrt{2}} (|\psi\rangle^{Y_I} |\mathbb{1}\rangle^{Y_O B_I} |\mathbb{1}\rangle^{B_O E_I} |\mathbb{1}\rangle^{B_O E_I} |\mathbb{1}\rangle^{A_O C_t} |0\rangle^{C_c} + |\psi\rangle^{A_I} |\mathbb{1}\rangle^{A_O E_I} |\mathbb{1}\rangle^{E_O B_I} |\mathbb{1}\rangle^{B_O Y_I} |\mathbb{1}\rangle^{Y_O C_t} |1\rangle^{C_c}), \quad (C5)$$

is the process matrix of the quantum switch containing Alice, Bob Yves and Eve. Further, as mentioned,  $W^{\bar{E}\bar{Y}}$  is some arbitrary process matrix shared between Eve and Yves detailing all of their possible correlations. Notice the separable nature of  $W_{\psi}$ . This is because we are assuming Eve and Yves do not, in some sense, have access to the causal structure of the quantum switch: that is, they do not have access to the control qubit. Therefore, their correlations (and instruments) cannot depend on whether  $\rho$  is being sent along the  $|0\rangle$  path, or the  $|1\rangle$  path.

Let us now write down the CJ operators that describe each lab's operations. For Alice and Bob, being independent, these are given by

$$M_k^X = (\mathcal{I} \otimes \mathcal{X}_k) (|\mathbb{1}) \langle \langle \mathbb{1}|^{X_I X_I'})$$

$$= \sum_{i,j=0}^1 (|i\rangle \langle j|)^{X_I} \otimes (X_k |i\rangle \langle j| X_k^{\dagger})^{X_O}$$

$$= (|X_k^*\rangle) \langle \langle X_k^*|^X \rangle^T,$$
(C7)

where

$$|X_k^*\rangle^X := (\mathbb{1} \otimes X_k^*)|\mathbb{1}\rangle^X. \tag{C8}$$

Note that here we are taking  $X \equiv X_I X_O \in \{A, B\}$ ,  $X_k \in \{A_k, B_k\}$  to be the Kraus operators defining the channel  $\mathcal{X} \in \{\mathcal{A}, \mathcal{B}\}$ , and we select  $\{|i\rangle\} = \{|j\rangle\} = \{|0\rangle, |1\rangle\}$  as our chosen basis for defining  $|1\rangle\rangle^{X_I X_I'}$ .

Let's now move onto the operations making up Eve and Yves's instruments, given in Eq. (C1). To find the corresponding CJ operators, we choose a basis for their respective Hilbert spaces:

$$\{|b_{e\tilde{e}}\rangle := |e\rangle^{E_I}|\tilde{e}\rangle^{\tilde{E}_I}\}_{e,\tilde{e}} \subset \mathcal{H}^{E_I} \otimes \mathcal{H}^{\tilde{E}_I},$$
 (C9a)

$$\{|c_{y\tilde{y}}\rangle := |y\rangle^{Y_I}|\tilde{y}\rangle^{\tilde{Y}_I}\}_{y,\tilde{y}} \subset \mathcal{H}^{Y_I} \otimes \mathcal{H}^{\tilde{Y}_I},$$
 (C9b)

where  $\{|e\rangle^{E_I} \mid e=0,1\}, \{|\tilde{e}\rangle^{\tilde{E}_I}\}_{\tilde{e}}$  are our chosen bases for  $\mathcal{H}^{E_I}, \mathcal{H}^{\tilde{E}_I}$  respectively, and  $\{|y\rangle^{Y_I} \mid y=0,1\}, \{|\tilde{y}\rangle^{\tilde{Y}_I}\}_{\tilde{y}}$  are our chosen bases for  $\mathcal{H}^{Y_I}, \mathcal{H}^{\tilde{Y}_I}$  respectively<sup>20</sup>. This allows

us to define

$$|1\rangle\rangle^{E_{I}\tilde{E}_{I},E'_{I}\tilde{E}'_{I}} = \sum_{b_{e\tilde{e}}} |b_{e\tilde{e}}b_{e\tilde{e}}\rangle^{E_{I}\tilde{E}_{I},E'_{I}\tilde{E}'_{I}}$$

$$= \sum_{e,\tilde{e}} |ee\rangle^{E_{I}E'_{I}} |\tilde{e}\tilde{e}\rangle^{\tilde{E}_{I}\tilde{E}'_{I}}$$

$$= |1\rangle\rangle^{E_{I}E'_{I}} |1\rangle\rangle^{\tilde{E}_{I}\tilde{E}'_{I}}, \qquad (C10a)$$

$$|1\rangle\rangle^{Y_{I}\tilde{Y}_{I},Y'_{I}\tilde{Y}'_{I}} = |1\rangle\rangle^{Y_{I}Y'_{I}} |1\rangle\rangle^{\tilde{Y}_{I}\tilde{Y}'_{I}}, \qquad (C10b)$$

where the second expression follows from the same argument of the first. Using the operator-Schmidt decomposition given in Eq. (C3), the corresponding CJ operators are therefore given by

$$M_{l}^{E\tilde{E}} = (\mathcal{I} \otimes \mathcal{E}_{l}) \left( |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{E_{I}\tilde{E}_{I},E'_{I}\tilde{E}'_{I}} \right)$$

$$= \sum_{m} \sum_{\alpha,\beta} \left( |E_{lm}^{\alpha*}\rangle\rangle\langle\langle E_{lm}^{\beta*}|^{E} \otimes |\tilde{E}_{lm}^{\alpha*}\rangle\rangle\langle\langle\tilde{E}_{lm}^{\beta*}|^{\tilde{E}} \right)^{T},$$
(C11a)

$$\begin{split} M_{p}^{Y\tilde{Y}} &= (\mathcal{I} \otimes \mathcal{Y}_{p}) \Big( |\mathbb{1}\rangle\!\rangle \langle\!\langle \mathbb{1}|^{Y_{I}\tilde{Y}_{I},Y'_{I}\tilde{Y}'_{I}} \Big) \\ &= \sum_{q} \sum_{\lambda,\mu} \Big( |Y_{pq}^{\lambda*}\rangle\!\rangle \langle\!\langle Y_{pq}^{\mu*}|^{Y} \otimes |\tilde{Y}_{pq}^{\lambda*}\rangle\!\rangle \langle\!\langle \tilde{Y}_{pq}^{\mu*}|^{\tilde{Y}} \Big)^{T}, \end{split}$$
(C11b)

where

$$|E_{lm}^{\alpha*}\rangle\rangle^{E} = (\mathbb{1} \otimes E_{lm}^{\alpha*})|\mathbb{1}\rangle\rangle^{E_{I}E'_{I}},$$
 (C12a)

$$|\tilde{E}_{lm}^{\alpha*}\rangle\rangle^{\tilde{E}} = (\mathbb{1}\otimes\tilde{E}_{lm}^{\alpha*})|\mathbb{1}\rangle\rangle^{\tilde{E}_{I}\tilde{E}_{I}'},$$
 (C12b)

$$|Y_{nq}^{\lambda*}\rangle^{Y} = (\mathbb{1} \otimes Y_{nq}^{\lambda*})|\mathbb{1}\rangle^{Y_{I}Y_{I}'}, \tag{C12c}$$

$$|\tilde{Y}_{pq}^{\lambda*}\rangle\rangle^{\tilde{Y}} = (\mathbb{1}\otimes\tilde{Y}_{pq}^{\lambda*})|\mathbb{1}\rangle\rangle^{\tilde{Y}_{I}\tilde{Y}_{I}'}.$$
 (C12d)

We are therefore equipped to see how the initial state of our system  $\rho_{\psi} \otimes \omega$  evolves with respect to the process matrix  $W_{\psi}$ , along with the actions of Alice, Bob, Eve and Yves that we just defined. Following the basis comparison of Alice and Bob,

<sup>19</sup> They could be acting on the same system that is shared between them through some quantum channel, they could be acting on their respective parts of an entangled state, and so on - no as-

sumptions are made here.

Note that no restrictions are put on the choice of bases for the ancilla systems to preserve generality.

$$\rho_{\psi} \otimes \omega \to 2 \sum_{l,p} \sum_{\mathfrak{B} \in \mathcal{C}} \sum_{i,j \in \mathfrak{B}} \operatorname{Tr}_{\bar{C}} \left[ \left( M_{i}^{A} \otimes M_{j}^{B} \otimes M_{l}^{E} \otimes M_{p}^{Y} \otimes \mathbb{I}^{C} \right)^{T} W_{\psi} \right]$$

$$= 2 \sum_{l,p} \sum_{m,q} \sum_{\mathfrak{B} \in \mathcal{C}} \sum_{i,j \in \mathfrak{B}} \sum_{\alpha,\beta} \sum_{\lambda,\mu} \left( \langle \langle A_{i}^{*} | \langle \langle B_{j}^{*} | \langle \langle E_{lm}^{\alpha*} | \langle \langle Y_{pq}^{\lambda*} | W_{\psi}^{ABEYC} | A_{i}^{*} \rangle \rangle | B_{j}^{*} \rangle \rangle | E_{lm}^{\beta*} \rangle | Y_{pq}^{\mu*} \rangle$$
(C13)

$$\times \langle \langle \tilde{E}_{lm}^{\alpha*} | \langle \langle \tilde{Y}_{pq}^{\lambda*} | W^{\tilde{E}\tilde{Y}} | \tilde{E}_{lm}^{\beta*} \rangle \rangle | \tilde{Y}_{pq}^{\mu*} \rangle \rangle, \qquad (C14)$$

where the factor of two comes from the normalisation of the state following basis comparison and  $\operatorname{Tr}_{\bar{C}}$  means we are tracing out all systems but  $C=C_tC_c$ . This is a rather complicated expression. However, it contains information (about Yves and Eve's correlations) that we don't require for the result of this appendix. To simplify the problem, note first that the positivity of  $W^{\tilde{E}\tilde{Y}}$  allows us to write  $W^{\tilde{E}\tilde{Y}}=\sum_s|s|^2|s\rangle\langle s|$  such that  $|s\rangle\in\mathcal{H}^{\tilde{E}}\otimes\mathcal{H}^{\tilde{Y}}$ . We can use this to define the Kraus operators  $Z_{\mathbf{x}}:\mathcal{H}^{E_I}\otimes\mathcal{H}^{Y_I}\to\mathcal{H}^{E_O}\otimes\mathcal{H}^{Y_O}$  by

$$Z_{\mathbf{x}} = \sum_{\alpha,\lambda} s(\langle \langle \tilde{E}_{lm}^{\alpha*} | \langle \langle \tilde{Y}_{pq}^{\lambda*} | \rangle | s \rangle E_{lm}^{\alpha} \otimes Y_{pq}^{\lambda}, \tag{C15}$$

where  $\mathbf{x} = (l, m, p, q, s) \in \mathbf{X}$ , is an index that holds the

instrument (measurement) outcome of Eve and Yves and  $\mathbf{X}$  is the set containing all such outcomes. In what follows, we forget the structure of these operators and take Eve and Yves's joint action to be some arbitrary set of Kraus operators  $\{Z_{\mathbf{x}}: \mathcal{H}^{E_I} \otimes \mathcal{H}^{Y_I} \to \mathcal{H}^{E_O} \otimes \mathcal{H}^{Y_O}\}$ . Doing so means that anything that we find, also holds for the actual situation we have been considering up until this point.

# 2. Correlated eavesdroppers cannot learn anything useful using individual attacks

The conclusion of the previous subsection was that we take to the state  $\rho_{\psi} \otimes \omega$  to evolve in the following way during this protocol:

$$\rho_{\psi} \otimes \omega \to 2 \sum_{\mathbf{x} \in \mathbf{X}} \sum_{\mathfrak{B} \in \mathcal{C}} \sum_{i,j \in \mathfrak{B}} \langle \langle A_i^* | A_i^* \langle \langle B_j^* | A_j^* \rangle \langle Z_{\mathbf{x}}^* | A_j^* \rangle \langle A_i^* \rangle \langle A_i^* \rangle \langle A_i^* \rangle \langle A_j^* \rangle \langle A_i^* \rangle \langle$$

Here,

$$|Z_{\mathbf{x}}^*\rangle = (\mathbb{I} \otimes Z_{\mathbf{x}}^*)|\mathbb{1}\rangle^{E_I E_I'}|\mathbb{1}\rangle^{Y_I Y_I'}$$

$$= \sum_{e,y \in \{0,1\}} |ey\rangle^{E_I Y_I} (Z_{\mathbf{x}}^*|ey\rangle)^{E_O Y_O}, \qquad (C18)$$

where we followed an analogous argument to Eq. (C10) in order to use  $|1\rangle\rangle^{E_IY_I,E_I'Y_I'} = |1\rangle\rangle^{E_IE_I'} |1\rangle\rangle^{Y_IY_I'}$ . Now, using Eq. (C5) for  $W_{\psi}^{ABEYC} = |w_{\psi}\rangle\langle w_{\psi}|$ , we can see explicitly, that after some algebra,

$$\rho_{\psi} \otimes \omega \to \sum_{\mathbf{x} \in \mathbf{X}} \sum_{\mathfrak{B} \in \mathbf{C}} \sum_{i,j \in \mathfrak{B}} |f_{\mathbf{x}ij}\rangle \langle f_{\mathbf{x}ij}|^{C_t C_c}, \qquad (C19)$$

where,

$$|f_{\mathbf{x}ij}\rangle^{C_t C_c} = \sum_{n \in \{0,1\}} \left[ (\langle n | \otimes \mathbb{1})(B_j \otimes A_i) Z_{\mathbf{x}} |\psi\rangle |n\rangle^{C_t} |0\rangle^{C_c} + (\mathbb{1} \otimes \langle n |) Z_{\mathbf{x}}(B_j \otimes A_i) |n\rangle^{C_t} |\psi\rangle |1\rangle^{C_c} \right]. \quad (C20)$$

We can quickly check our sanity by considering the case when Eve and Yves are not present. That is, when

 $Z_{\mathbf{x}} \propto \mathbb{1} \otimes \mathbb{1}, \ \forall \mathbf{x} \in \mathbf{X}.$  Here, it turns out that

$$|f_{\mathbf{x}ij}\rangle^{C_t C_c} \propto \frac{1}{\sqrt{2}} \left( A_i B_j |\psi\rangle^{C_t} |0\rangle^{C_c} + B_j A_i |\psi\rangle^{C_t} |1\rangle^{C_c} \right)$$
(C21)

which is what we'd expect from a quantum switch with two operations [4].

Recall that earlier, we found that when no eavesdroppers are present, measuring the state of the control qubit  $C_c$  at the end in the  $\{|\pm\rangle\}$  basis would always result in +. In other words, the probability of measuring -, denoted  $P(-C_c)$ , is zero. The question now is, if a correlated Eve and Yves are present, what form must  $Z_{\mathbf{x}}$  have in order to ensure  $P(-C_c) = 0$ ? And further, with this form of  $Z_{\mathbf{x}}$ , can Eve and Yves extract information about the key being shared between Alice and Bob?

**Theorem C.1.** For any input state  $|\psi\rangle$ ,  $P(-^{C_c}) = 0$  if and only if

$$Z_{\mathbf{x}} = \sum_{\mu=0}^{3} r_{\mathbf{x}}^{\mu} \sigma_{\mu} \otimes \sigma_{\mu}, \tag{C22}$$

where  $r_{\mathbf{x}}^{\mu} \in \mathbb{C} \ \forall \mu \in \{0, 1, 2, 3\}, \mathbf{x} \in \mathbf{X} \ and \ (\sigma_0, \sigma_1, \sigma_2, \sigma_3) = (\mathbb{1}, \sigma_x, \sigma_y, \sigma_z).$ 

*Proof.* First, assume that  $P(-C_c) = 0$ . This means that

$$\sum_{\mathbf{x} \in \mathbf{X}} \sum_{\mathfrak{B} \in \mathcal{C}} \sum_{i,j \in \mathfrak{B}} \sum_{m \in \{0,1\}} \left| \left( \langle m |^{C_t} \langle -|^{C_c} \rangle | f_{\mathbf{x}ij} \rangle^{C_t C_c} \right|^2 = 0,$$
(C23)

where the sum over m comes about because no measurement is being performed on the target qubit  $C_t$ . This implies that  $(\langle m|^{C_t}\langle -|^{C_c}\rangle|f_{\mathbf{x}ij}\rangle^{C_tC_c}=0 \ \forall i,j\in\mathfrak{B},\in\mathsf{C},m\in\{0,1\}$  and  $\forall\mathbf{x}\in\mathbf{X}$ . From here on, unless stated otherwise, let  $\mathfrak{B}\in\mathsf{C},\,i,j\in\mathfrak{B},\,\mathbf{x}\in\mathbf{X},\,m\in\{0,1\}$  be arbitrary. Using Eq. (C20), it follows that

$$\sum_{n \in \{0,1\}} \left( \langle n | \langle m | (B_j \otimes A_i) Z_{\mathbf{x}} | \psi \rangle | n \rangle - \langle m | \langle n | Z_{\mathbf{x}} (B_j \otimes A_i) | n \rangle | \psi \rangle \right) = 0. \quad (C24)$$

Suppose we have an arbitrary, pure input state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , where  $\alpha, \beta \in \mathbb{C}$  subject to  $|\alpha|^2 + |\beta|^2 = 1$ . If we show the theorem to be true for this case, it follows that it is true for any mixed state  $\rho = \sum_{\psi} p_{\psi} |\psi\rangle \langle\psi|$  by the linearity of the theory. In order to achieve this, we first of all take  $|\psi\rangle \neq |0\rangle, |1\rangle$ , that is,  $\alpha, \beta \neq 0$ .

Note that Eq. (C24) must hold for both  $i, j \in \{0, 1\}$  and  $i, j \in \{+, -\}$ . Let us first see what we can find out about  $Z_{\mathbf{x}}$  when we take  $i, j \in \{0, 1\}$ . In this case, Eq. (C24) has the following form:

$$\delta_{im} \left( \alpha \langle jm | Z_{\mathbf{x}} | 0j \rangle + \beta \langle jm | Z_{\mathbf{x}} | 1j \rangle \right)$$

$$= \left( \alpha \delta_{i0} + \beta \delta_{i1} \right) \langle mj | Z_{\mathbf{x}} | ji \rangle. \quad (C25)$$

When  $i \neq m$ , we can quickly see that  $\langle 00|Z_{\mathbf{x}}|01\rangle$ ,  $\langle 01|Z_{\mathbf{x}}|11\rangle$ ,  $\langle 10|Z_{\mathbf{x}}|00\rangle$ ,  $\langle 11|Z_{\mathbf{x}}|10\rangle=0$ . Next, when  $m=i, Z_{\mathbf{x}}$  is constrained by

$$\alpha \langle jm|Z_{\mathbf{x}}|0j\rangle + \beta \langle jm|Z_{\mathbf{x}}|1j\rangle = (\alpha \delta_{m0} + \beta \delta_{m1}) \langle mj|Z_{\mathbf{x}}|jm\rangle. \quad (C26)$$

When (j,m)=(0,0),(1,1) we find that  $\langle 00|Z_{\mathbf{x}}|10\rangle$ ,  $\langle 11|Z_{\mathbf{x}}|01\rangle=0$  respectively. And, defining  $e_{\mathbf{x}}=\langle 10|Z_{\mathbf{x}}|01\rangle$ ,  $d_{\mathbf{x}}=\langle 01|Z_{\mathbf{x}}|10\rangle$ , when (j,m)=(0,1), it turns out that  $\langle 01|Z_{\mathbf{x}}|00\rangle=\frac{\beta}{\alpha}(e_{\mathbf{x}}-d_{\mathbf{x}})$ , and when  $(j,m)=(1,0),\,\langle 10|Z_{\mathbf{x}}|11\rangle=\frac{\alpha}{\beta}(e_{\mathbf{x}}-d_{\mathbf{x}})$ . Here we can see why we have not allowed  $\alpha=0$  or  $\beta=0$ .

Taking stock so far,  $Z_{\mathbf{x}}$  has the form

$$Z_{\mathbf{x}} = \begin{cases} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{cases} \begin{pmatrix} a_{\mathbf{x}} & 0 & 0 & b_{\mathbf{x}} \\ \frac{\beta}{\alpha} (e_{\mathbf{x}} - d_{\mathbf{x}}) & c_{\mathbf{x}} & d_{\mathbf{x}} & 0 \\ 0 & e_{\mathbf{x}} & f_{\mathbf{x}} & \frac{\alpha}{\beta} (e_{\mathbf{x}} - d_{\mathbf{x}}) \\ g_{\mathbf{x}} & 0 & 0 & h_{\mathbf{x}} \end{cases},$$
(C27)

where all entries can be complex numbers. This can be simplified further by summing Eq. (C24) over i and j. This results in

$$\sum_{n \in \{0,1\}} \langle nm|Z_{\mathbf{x}}|\psi n \rangle = \sum_{n \in \{0,1\}} \langle mn|Z_{\mathbf{x}}|n\psi \rangle, \qquad \text{(C28)}$$
 which implies

$$\sum_{n \in \{0,1\}} \alpha \left( \langle nm | Z_{\mathbf{x}} | 0n \rangle - \langle mn | Z_{\mathbf{x}} | n0 \rangle \right)$$

$$= \sum_{n \in \{0,1\}} \beta \left( \langle mn | Z_{\mathbf{x}} | n1 \rangle - \langle nm | Z_{\mathbf{x}} | 1n \rangle \right), \quad (C29)$$

which must be true for all  $m \in \{0, 1\}$ . Choosing m = 0 and using Eq. (C27), we find that  $d_{\mathbf{x}} = e_{\mathbf{x}}$ . So, we therefore have

$$Z_{\mathbf{x}} = \begin{pmatrix} a_{\mathbf{x}} & 0 & 0 & b_{\mathbf{x}} \\ 0 & c_{\mathbf{x}} & d_{\mathbf{x}} & 0 \\ 0 & d_{\mathbf{x}} & f_{\mathbf{x}} & 0 \\ g_{\mathbf{x}} & 0 & 0 & h_{\mathbf{x}} \end{pmatrix}. \tag{C30}$$

To finish the derivation, we use the fact that Eq. (C24) must also hold for  $i, j \in \{+, -\}$ . To utilise this, we keep  $i, j \in \{0, 1\}$  and use the Hadamard operator  $H = (\sigma_x + \sigma_z)/\sqrt{2} = H^{\dagger}$  to relate the x and z-bases: that is, by replacing  $B_j \otimes A_i$  in Eq. (C24) with  $(H \otimes H)(B_j \otimes A_i)(H \otimes H)$ . After some rearranging, we find that

$$\sum_{n \in \{0,1\}} [\delta_{j0} + (-1)^n \delta_{j1}] \langle ji | (H \otimes H) Z_{\mathbf{x}} | \psi n \rangle = \frac{1}{2} \frac{(\alpha + \beta) \delta_{i0} + (\alpha - \beta) \delta_{i1}}{\delta_{i0} + (-1)^m \delta_{i1}} \sum_{n \in \{0,1\}} [\delta_{j0} + (-1)^n \delta_{j1}] \langle mn | Z_{\mathbf{x}} (H \otimes H) | ji \rangle.$$
(C31)

Straight away, we can see that the RHS has a dependence on m but the LHS does not. So we can equate the m=0 and m=1 cases of the RHS. Doing this, the four cases that come from  $i,j\in\{0,1\}$  result in

$$a_{\mathbf{x}} = h_{\mathbf{x}},$$
  
 $g_{\mathbf{x}} = b_{\mathbf{x}} + c_{\mathbf{x}} - f_{\mathbf{x}}.$  (C32)

Updating  $Z_{\mathbf{x}}$  and looking at Eq. (C31) when (i, j, m) = (0, 0, 0) results in  $c_{\mathbf{x}} = f_{\mathbf{x}}$  and  $b_{\mathbf{x}} = g_{\mathbf{x}}$ . Therefore we have

$$Z_{\mathbf{x}} = \begin{pmatrix} a_{\mathbf{x}} & 0 & 0 & b_{\mathbf{x}} \\ 0 & c_{\mathbf{x}} & d_{\mathbf{x}} & 0 \\ 0 & d_{\mathbf{x}} & c_{\mathbf{x}} & 0 \\ b_{\mathbf{x}} & 0 & 0 & a_{\mathbf{x}} \end{pmatrix}$$
(C33)

which can be rewritten as

$$Z_{\mathbf{x}} = \frac{1}{2} \left[ (a_{\mathbf{x}} + c_{\mathbf{x}}) \mathbb{1} \otimes \mathbb{1} + (d_{\mathbf{x}} + b_{\mathbf{x}}) \sigma_x \otimes \sigma_x + (d_{\mathbf{x}} - b_{\mathbf{x}}) \sigma_y \otimes \sigma_y + (a_{\mathbf{x}} - c_{\mathbf{x}}) \sigma_z \otimes \sigma_z \right].$$
(C34)

Further, since the mapping

$$\begin{cases} r_{\mathbf{x}}^{0} = a_{\mathbf{x}} + c_{\mathbf{x}}, \\ r_{\mathbf{x}}^{1} = d_{\mathbf{x}} + b_{\mathbf{x}}, \\ r_{\mathbf{x}}^{2} = d_{\mathbf{x}} - b_{\mathbf{x}}, \\ r_{\mathbf{x}}^{3} = a_{\mathbf{x}} - c_{\mathbf{x}} \end{cases}$$
(C35)

is invertible and linear,  $a_{\mathbf{x}}, b_{\mathbf{x}}, c_{\mathbf{x}}, d_{\mathbf{x}} \in \mathbb{C}$  being independent from one another implies that  $r_{\mathbf{x}}^{\mu} \in \mathbb{C}$  are independent from one another. Therefore,

$$Z_{\mathbf{x}} = \sum_{\mu=0}^{3} r_{\mathbf{x}}^{\mu} \sigma_{\mu} \otimes \sigma_{\mu}. \tag{C36}$$

At this stage, one might notice that we didn't consider all the combinations of i,j in Eq. (C31). It turns out that these give us no further constraints on  $Z_{\mathbf{x}}$ . To confirm this, we just need to prove the reverse implication of the if and only if statement. If it turns out that we missed some constraints on  $Z_{\mathbf{x}}$ ,  $P(-^{C_c})$  would be nonzero in general when using Eq. (C36) for  $Z_{\mathbf{x}}$ .

So, suppose that  $Z_{\mathbf{x}}$  is given by Eq. (C36). Substituting this into  $(\langle m|^{C_t}\langle -|^{C_c}\rangle|f_{\mathbf{x}ij}\rangle^{C_tC_c}$  and carrying out the sum over n results in

$$(\langle m|^{C_t}\langle -|^{C_c})|f_{\mathbf{x}ij}\rangle^{C_tC_c}$$

$$= \sum_{\mu=0}^3 r_{\mathbf{x}}^{\mu}\langle m|[A_i, \sigma_{\mu}B_j\sigma_{\mu}]|\psi\rangle = 0 \quad (C37)$$

for all  $i, j \in \mathfrak{B}, \mathfrak{B} \in \mathsf{C}, m \in \{0, 1\}$  and  $\forall \mathbf{x} \in \mathbf{X}$  since  $[A_i, \sigma_{\mu} B_j \sigma_{\mu}] = 0 \ \forall i, j, \mu$ .

Finally, for the cases in which  $|\psi\rangle \in \{|0\rangle, |1\rangle\}$ , notice that what we have shown so far holds for  $|\psi\rangle \in \{|+\rangle, |-\rangle\}$ . Now, the process matrix defined using Eq. (C5) can equivalently be formulated in the x-basis, and Alice and Bob's channels are invariant under this basis change. So, after converting everything to the x-basis, what was the situation in which  $|\psi\rangle = |+/-\rangle$  becomes that of when  $|\psi\rangle = |0/1\rangle$ . Thus, since  $Z_{\mathbf{x}}$  [Eq. (C36)] has the same form when it is changed from the z-basis to the x-basis, the result also holds for this case.

It is difficult to have any intuition about what Eve and Yves's measurement would look like physically. This is because, in the previous subsection, in anticipation of simplifying this proof, we ignored the correlations shared by Eve and Yves through their ancillary process matrix  $W^{\bar{E}\bar{Y}}$ . A little intuition can be gained, however, by considering what happens when only one of the coefficients  $r_{\mathbf{x}}^{\mu}$  is nonzero for each  $\mathbf{x}$ . In this scenario, if one of Eve or Yves performs  $\sigma_{\mu}$ , then the other eavesdropper must do the same if they want to go undetected.

As discussed earlier, an ancillary process matrix shared between Eve and Yves is likely necessary to understand what is happening here physically with regards to the correlations between the eavesdroppers' measurements. Either way, and to reiterate, since the approach taken here considers no physical constraints on the correlations between Eve and Yves, operations with physical correlations should exist as a subset of the ones we have derived here.

So, can Eve and Yves gain any information about Alice and Bob's shared key using Eq. (C36)? To answer this, we calculate  $P(Z_{\mathbf{x}}, A_i, B_j) = \langle f_{\mathbf{x}ij} | f_{\mathbf{x}ij} \rangle$  for  $i, j \in \{0, 1\}$  and  $i, j \in \{+, -\}$ . These are given by:

$$P(Z_{\mathbf{x}}, A_i, B_j) = \begin{cases} \frac{|\langle i|\psi\rangle|^2}{2} \left( |r_{\mathbf{x}}^0 + r_{\mathbf{x}}^3|^2 \delta_{ij} + |r_{\mathbf{x}}^1 + r_{\mathbf{x}}^2|^2 \delta_{i\bar{j}} \right), & i, j \in \{0, 1\} \\ \frac{|\langle i|\psi\rangle|^2}{2} \left( |r_{\mathbf{x}}^0 + r_{\mathbf{x}}^1|^2 \delta_{ij} + |r_{\mathbf{x}}^2 + r_{\mathbf{x}}^3|^2 \delta_{i\bar{j}} \right), & i, j \in \{+, -\}, \end{cases}$$
(C38)

where  $\bar{j}$  denotes "not j". At first glance, it appears that Eve and Yves have access to some information about Alice and Bob's key. However, note first that distinguishing between the two cases of  $i,j\in\{0,1\}$  and  $i,j\in\{+,-\}$  is of no use as Alice and Bob publicly discuss which basis they measured in after they have done so. Secondly, although Eve and Yves could alter  $r_{\mathbf{x}}^{\mu}$  however they like, the only additional information they could gain is about whether each bit of Alice and Bob's key agree or not. Therefore, they can still do no better than a guess to determine the key. This intuitive argument is backed up by a calculation of the mutual information between the eavesdroppers and either Alice or Bob. In both cases, this turns out to be zero.

Finally, it should be noted this protocol has a weakness if we allow the eavesdroppers alter the causal structure set up by Alice. That is, if they had access to the control qubit that dictates the indefinite causal order of the quantum switch. In this case, Eve and Yves could perform a similar attack to the one described in Sec. V. That is, if the eavesdroppers return Alice's qubit unaffected, and in an indefinite causal order, whilst, independently sending out a probe state to Bob, they can learn about Bob's key bit, without inducing any " - " measurement results in the control mode. Having said this, it seems as though this eavesdropping strategy can be detected by monitoring  $\omega$  in the cases when Alice and Bob disagree on their basis choice. The analysis of such attacks, in

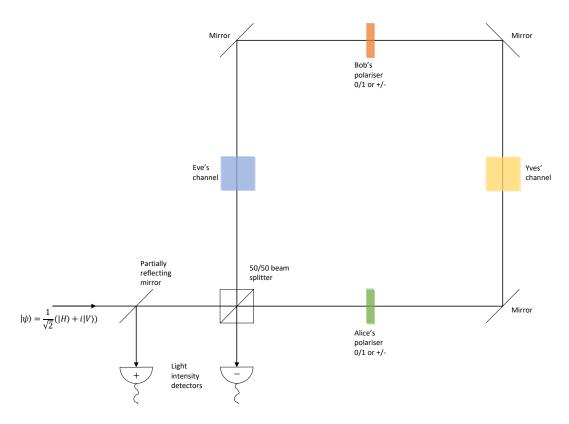


FIG. 8. The results derived in this work can be simulated using polarised light to share a key between Alice and Bob, and a Sagnac interferometer to induce the indefinite causal order. Within the interferometer, polarising filters are orientated to correspond to all the valid measurement outcomes Alice and Bob obtain during the protocol.

which eavesdroppers can infiltrate the causal structure of the protocol, is beyond the scope of this paper.

#### Appendix D: Experimental simulation

Figure 8 shows a possible experimental setup to simulate some of the results derived. The idea is to use photon polarisation (in the horizontal-vertical basis, with  $|H\rangle =: |0\rangle, |V\rangle =: |1\rangle$  as the target state  $\rho$ , initially in the state  $|\psi\rangle\langle\psi|$ , that is acted on by Alice, Bob, Eve and Yves. As is mentioned in the main text, if we wanted Alice and Bob to have approximately equal numbers of Os and 1s, we can take our input state to be 1/2. This can be achieved by taking it to be  $|i\rangle$  half of the time and  $|-i\rangle$  the remainder of the time. These correspond to left and right circularly polarised light respectively:  $|\psi\rangle \in \{|\pm i\rangle = (|H\rangle \pm i|V\rangle)/\sqrt{2}\}$ . The control state  $\omega$ is taken to be the path degree of freedom induced by a beamsplitter. Using a 50/50 beamsplitter corresponds to taking  $\omega = |+\rangle\langle +|$  with  $|0\rangle$  corresponding to reflection and  $|1\rangle$  to transmission.

Recall that Alice and Bob perform projective measurements in either the x or z-basis. This is difficult to do non-destructively and even more difficult to do while keeping the photon continuing around the Sagnac interferometer in its original superposition of paths. That

being said, there has been recent progress along these lines [6]. In this appendix, however, we just consider a simulation of projective measurements using polarisers. This means we can simulate the statistics that the measurements of Alice, Bob, Eve and Yves would produce.

Explicitly, when Alice and Bob measure in the z-basis, we use polarisers orientated at 0 and  $\pi/2$  which correspond to measurement outcomes of 0 and 1 respectively. Likewise, when measuring in the x-basis, polarisers being orientated at  $\pm \pi/4$  correspond to measurement outcomes of  $\pm$  respectively. The probability of Alice and Bob measuring i,j can be taken to be the ratio of the total intensity  $I_{\text{exit}}(i,j)$  of light exiting the interferometer to that of it entering  $I_{\text{enter}}$ :

$$P(A_i, B_j) = \frac{I_{\text{exit}}(i, j)}{I_{\text{enter}}}.$$
 (D1)

Here, the dependence of  $I_{\rm exit}(i,j)$  on i,j highlights that the interferometer is setup with Alice and Bob's polarisers being orientated correspondingly to the measurement outcomes i,j respectively. Since Alice and Bob only keep measurement results when they have publicly confirmed that they measured in the same basis, there are eight permutations when ignoring Eve and Yves. These are given in the Table I.

The key feature of this protocol involves the measurement of the control state in the  $\pm$  basis. Noticing that,

TABLE I. Table detailing the eight polariser orientations that correspond to the possible measurement outcomes that Alice and Bob can obtain when they measure in the same basis.

Bob polariser orientation
0
$\frac{\pi}{2}$
Ō
$\frac{\pi}{2}$
$\frac{\pi}{4}$
$-\frac{\pi}{4}$
$\frac{\pi^4}{4}$
$-\frac{\pi}{4}$

after going through the main part of the Sagnac interferometer, the path that the light exits the 50/50 beam-splitter along, is controlled by the path qubit in the x-

basis. That is, the  $|+\rangle$  component is transmitted through the beamsplitter, whereas the  $|-\rangle$  component is reflected. Therefore, placing a detector in the reflected arm corresponds to the - outcome and, after a partially reflecting mirror, a detector in the transmitted arm corresponds to the + outcome. The probability of measuring the eavesdroppers comes from the probability of measuring the control qubit state to be -. Therefore, for each run of the experiment (each permutation of polariser angles). the ratio of the intensity in the – arm to the total intensity exiting the interferometer is what is required. As a sanity check, this should always be zero when Eve and Yves are not present. As mentioned before, in order to exploit the features of indefinite causal order, the coherence length of the light used should be significantly longer than the path length of the interferometer. A laser can be used to achieve this.

- L. Hardy, Towards quantum gravity: a framework for probabilistic theories with non-fixed causal structure, J. Phys. A: Math. Theor. 40, 3081 (2007).
- [2] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Quantum computations without definite causal structure, Phys. Rev. A 88, 022318 (2013).
- [3] O. Oreshkov, F. Costa, and C. Brukner, Quantum correlations with no causal order, Nat. Commun. 3, 1092 (2012).
- [4] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. G. White, Indefinite causal order in a quantum switch, Phys. Rev. Lett. 121, 090503 (2018).
- [5] G. Rubino, L. A. Rozema, A. Feix, M. Araújo, J. M. Zeuner, L. M. Procopio, Č. Brukner, and P. Walther, Experimental verification of an indefinite causal order, Sci. Adv. 3, e1602589 (2017).
- [6] H. Cao, J. Bavaresco, N.-N. Wang, L. A. Rozema, C. Zhang, Y.-F. Huang, B.-H. Liu, C.-F. Li, G.-C. Guo, and P. Walther, Semi-device-independent certification of indefinite causal order in a photonic quantum switch, Optica 10, 561 (2023).
- [7] G. Chiribella, Perfect discrimination of no-signalling channels via quantum superposition of causal structures, Phys. Rev. A 86, 040301 (2012).
- [8] M. Araújo, F. Costa, and C. Brukner, Computational advantage from quantum controlled ordering of gates, Phys. Rev. Lett. 113, 250402 (2014).
- [9] P. A. Guérin, A. Feix, M. Araújo, and Č. Brukner, Exponential communication complexity advantage from quantum superposition of the direction of communication, Phys. Rev. Lett. 117, 100502 (2016).
- [10] X. Zhao, Y. Yang, and G. Chiribella, Quantum metrology with indefinite causal order, Phys. Rev. Lett. 124, 190503 (2020).
- [11] P. Yin, X. Zhao, Y. Yang, Y. Guo, W.-H. Zhang, G.-C. Li, Y.-J. Han, B.-H. Liu, J.-S. Xu, G. Chiribella, et al., Experimental super-heisenberg quantum metrology with indefinite gate order, Nat. Phys. 19, 1122 (2023).
- [12] M. Frey, Indefinite causal order aids quantum depolariz-

- ing channel identification, Quantum Inf. Process. 18, 96 (2019).
- [13] D. Ebler, S. Salek, and G. Chiribella, Enhanced communication with the assistance of indefinite causal order, Phys. Rev. Lett. 120, 120502 (2018).
- [14] S. Salek, D. Ebler, and G. Chiribella, Quantum communication in a superposition of causal orders, arXiv preprint arXiv:1809.06655 (2018).
- [15] N. Loizeau and A. Grinbaum, Channel capacity enhancement with indefinite causal order, Phys. Rev. A 101, 012340 (2020).
- [16] G. Chiribella, M. Banik, S. S. Bhattacharya, T. Guha, M. Alimuddin, A. Roy, S. Saha, S. Agrawal, and G. Kar, Indefinite causal order enables perfect quantum communication with zero capacity channels, New J. Phys. 23, 033039 (2021).
- [17] D. Felce and V. Vedral, Quantum refrigeration with indefinite causal order, Phys. Rev. Lett. 125, 070603 (2020).
- [18] Y. Chen and Y. Hasegawa, Indefinite causal order in quantum batteries, arXiv preprint arXiv:2105.12466 (2021).
- [19] G. Zhu, Y. Chen, Y. Hasegawa, and P. Xue, Charging quantum batteries via indefinite causal order: Theory and experiment, Phys. Rev. Lett. 131, 240401 (2023).
- [20] A. Z. Goldberg, K. Heshami, and L. L. Sánchez-Soto, Evading noise in multiparameter quantum metrology with indefinite causal order, Phys. Rev. Res. 5, 033198 (2023).
- [21] K. Simonov, G. Francica, G. Guarnieri, and M. Paternostro, Work extraction from coherently activated maps via quantum switch, Phys. Rev. A 105, 032217 (2022).
- [22] L. A. Rozema, T. Strömberg, H. Cao, Y. Guo, B.-H. Liu, and P. Walther, Experimental aspects of indefinite causal order in quantum mechanics, Nat. Rev. Phys. 6, 483 (2024).
- [23] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings* of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE,

- New York, 1984).
- [24] A. K. Ekert, Quantum cryptography based on bell's theorem, Phys. Rev. Lett. 67, 661 (1991).
- [25] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. 91, 057901 (2003).
- [26] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92, 057901 (2004).
- [27] M. Koashi and N. Imoto, Quantum cryptography based on split transmission of one-bit information in two steps, Phys. Rev. Lett. 79, 2383 (1997).
- [28] M. Lucamarini and S. Mancini, Secure deterministic communication without entanglement, Phys. Rev. Lett. 94, 140501 (2005).
- [29] K. Boström and T. Felbinger, Deterministic secure direct communication using entanglement, Phys. Rev. Lett. 89, 187902 (2002).
- [30] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).
- [31] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al., Advances in quantum cryptography, Adv. Opt. Photonics 12, 1012 (2020).
- [32] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard, Communication through coherent control of quantum channels, Quantum (2020).
- [33] P. A. Guérin, G. Rubino, and Č. Brukner, Communication through quantum-controlled noise, Phys. Rev. A 99, 062317 (2019).
- [34] H. Kristjánsson, G. Chiribella, S. Salek, D. Ebler, and M. Wilson, Resource theories of communication, New Journal of Physics 22, 073014 (2020).
- [35] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, Witnessing causal nonseparability, New J. Phys. 17, 102001 (2015).
- [36] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptology 18, 133 (2005).

- [37] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photonics 1, 238 (2009).
- [38] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (American Association of Physics Teachers, 2002).
- [39] J. A. Bergou, Discrimination of quantum states, J. Mod. Opt. 57, 160 (2010).
- [40] U. Herzog and J. A. Bergou, Optimum unambiguous discrimination of two mixed quantum states, Phys. R. A 71, 050301 (2005).
- [41] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, arXiv preprint arXiv:0911.3814 (2009).
- [42] H.-K. Lo, M. Curty, and B. Qi, Measurement-deviceindependent quantum key distribution, Phys. Rev. Lett. 108, 130503 (2012).
- [43] K. Kraus, States, effects, and operations: fundamental notions of quantum theory (Springer Verlag, 1983).
- [44] S. Croke, S. M. Barnett, and S. Stenholm, Linear transformations of quantum states, Ann. Phys. 323, 893 (2008).
- [45] E. B. Davies and J. T. Lewis, An operational approach to quantum probability, Commun. Math. Phys. 17, 239 (1970).
- [46] J. de Pillis, Linear transformations which preserve hermitian and positive semidefinite operators, Pac. J. Math. 23, 129 (1967).
- [47] M.-D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Its Appl. 10, 285 (1975).
- [48] A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, Rep. Math. Phys. 3, 275 (1972).
- [49] E. Castro-Ruiz, F. Giacomini, and Č. Brukner, Dynamics of quantum causal structures, Phys. Rev. X 8, 011047 (2018)
- [50] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines, Quantum dynamics as a physical resource, Phys. Rev. A 67, 052301 (2003).
- [51] M. A. Nielsen, Quantum information theory, arXiv preprint quant-ph/0011036 (2000).