Two-time state formalism for quantum eavesdropping

Kieran Flatt,[*] Sarah Croke, and Stephen M. Barnett
School of Physics and Astronomy, University of Glasgow, Glasgow, G12 8QQ, UK

The key piece of knowledge which quantum eavesdroppers can access is the correlation between prior and future events, i.e. the post-selected results of the legitimate preparations and measurements. We present a method for optimising eavesdropping strategies which is closely related to the two-time state formalism, the natural way to analyse such scenarios; it converts the task of optimisation into an eigenvalue problem. Our framework is applied to the familiar BB84 and B92 protocols as well as to the largely unexplored three-state scheme, which has a remarkable feature: the best eavesdropping strategy does not extract any information about the sent state.

I. INTRODUCTION

Quantum key distribution (QKD) is a set of protocols that share a key between two legitimate communicating parties and use the quantum mechanical concept of measurement disturbance to ensure that any eavesdropping is flagged to the legitimate users [1, 2]. In a typical strategy, one of these parties will produce a quantum state, the signal, and send it through a quantum channel to a second party who measures the state. We shall follow standard procedure in naming these actors Alice and Bob respectively. After Bob's measurement, one of the two publically shares information which allows for a pre-determined subset of send-measure correlations to be saved. This process is called sifting. Finally, logical bit values are assigned. According to the principle of measurement disturbance, any interlocutor hoping to know which states were exchanged will leave a measurable trace of their activity: Alice and Bob could in principle uncover them by examining the final set of logical bits. Nonetheless, this illegitimate party (Eve) will attempt to hide behind systemic noise and quantum cryptanalysis partly involves calculating her best strategy.

In designing an eavesdropping strategy, one wants to take into account information from both the past (from the interlocutor's perspective, i.e. the signal sent by Alice) and future (the post-measurement sifting process). This approach contrasts with quantum mechanics as it is often presented, as a predictive theory in which a state is modified by a sequence of measurements. In a recent paper [3] we developed a framework, closely linked to that of two-time states, more suitable to the task at hand. In that work, we consider physical processes in which a quantum state is prepared and subsequently measured twice. Probabilities are calculated using the inner product of two vectors: one associated with the first measurement and one associated with everything else (preparation, second measurement, post-selection at any point). There is a clear analogy between this and our QKD eavesdropper, who now becomes an ideal case study for examining joint probabilities as inner products. On a formal level, it is also similar to expressions for probability found in the literature on measurement-device-independent QKD [4–6] and hence may find some utility in extending the security proofs of that research programme such that the more traditional single-transmitter, single-receiver protocols are also covered.

We introduce operator space and show how it can be used to represent sequences of measurements, linking our results with the related formalisms of two-time states [7] and quantum combs [8]. In the following section, we use this to find the optimum eavesdropping strategies for three different QKD protocols: BB84, B92 and three-state. Our results are translated into the language of Kraus operators. While a large literature is dedicated to the proof of security against *a*rbitrary attacks (in particular for the former two protocols), it should be emphasised that exploring specific forms of attack can still lead to new insights. This will be seen especially for the three-state scheme.

II. BACKGROUND

A mathematical result with many applications in quantum information theory is the Choi-Jamiołkowski isomorphism. Choi's isomorphism [9] is a correspondence between channels and states. It may be thought of as arising from a mapping between the set of operators on a Hilbert space H and the set of vectors on the space $\mathcal{H} \otimes \mathcal{H}$; Jamiołkowski's [10] is similar though replaces the latter space with $\mathcal{H} \otimes \mathcal{H}^\dagger$ (the dagger indicating the dual space). One way of interpreting these two theorems is in terms of gate teleportation though a number of recent works have emphasised a different reading in terms of conditional probabilities [11]. Related to this are a pair of other works which will help to contexualise our method.

Firstly, Silva et al [7] have examined the roles of pre- and post-selection in reconstructing two-time states. A state $|\psi\rangle$ is prepared by a single party who sends this on to an observer that performs any measurement before returning the state to the preparer. Finally, the first party performs a measurement; if the desired result $|\phi\rangle$ is the outcome then the state is kept, else the second party forgets their result. The scheme is analogous to quantum key distribution, if Alice and Bob are consid-

[*] k.flatt.1@research.gla.ac.uk

ered a single party. The two-time state interpretation of this process is that $|\psi\rangle$ is a forwards evolving "ket" state and that $|\phi\rangle$ is a backwards evolving "bra" state; the tensor product of these two is the two-time state. Probabilities are then calculated by taking the inner product of this object with a suitably defined "Kraus density vector".

Secondly, there exists a body of work concerning quantum networks, combinations of quantum channels and POVMs e.g. [8, 12]. A quantum comb, the main analytical tool in the theory of quantum networks, is defined as the Choi-Jamiołkowski operator for a given network. As will be seen, this is very closely related to our original, reconstructions-inspired, route to this formulation in which we were led from the positivity of inner products on Liouville space to the complete positivity of operators on the dual space $\mathcal{H}\otimes\mathcal{H}^\dagger$.

The experimental scenario of quantum key distribution does not require use of the full range of description offered by either of these frameworks. That the two states (associated with Alice's signal and Bob's measurement) are pure means that we need only use a subset of all possible two-time states. That the legitimate parties are connected by a single channel means that we do not need to consider the full range of quantum combs, which can include maps between any number of Hilbert spaces, or the "link product" operation which concatenates multiple channels. Two-time states and quantum networks are thus generalisations of the framework we will use and is now presented.

Consider that a quantum state is observed twice in series. We can separate this out into three processes: a preparation which leaves the state with a density operator ρ and two measurements associated with positive operator-valued measures (POVMs) $\pi_i^{(1)} = \sum_\nu A_i^{\nu\dagger} A_i^\nu$ and $\pi_j^{(2)} = \sum_\lambda B_j^{\lambda\dagger} B_j^\lambda$. According to the standard rules of quantum mechanics [13, 14] the joint probability of outcomes i and j respectively will be given by

$$P(i,j|\rho) = \sum_{\lambda\nu} \mathrm{Tr}(A_i^\nu \rho A_i^{\nu\dagger} B_j^{\lambda\dagger} B_j^\lambda). \tag{1}$$

The sets A_i^ν and B_j^λ are Kraus operators [15]: they encode information both about the probability distribution of outcomes as well as the associated state transformation for a given measurement.

In a recent article [3] inspired by quantum reconstructions [16, 17], we were interested in the minimal set of physical principles which make Eq. (1) unique. This led us to employ the framework of operator space [18, 19]. By the Choi-Jamiołkowski isomorphism [9, 10], operators in the Hilbert space $\mathcal{H}$ are associated with vectors (written as $|\cdot\rangle\rangle$) in the related space $\mathcal{H}\otimes\mathcal{H}^\dagger$: $|i\rangle\langle j| \leftrightarrow |ij^\dagger\rangle\rangle$. For a generic operator A we have

$$A = \sum_{ij} a_{ij}|i\rangle\langle j| \leftrightarrow \sum_{ij} a_{ij}|ij^\dagger\rangle\rangle. \tag{2}$$

The labels i and j here are the basis vectors on the two spaces used, where the superscript dagger on the j is meant to indicate that this piece of the vector lies in the dual space, $\mathcal{H}^\dagger$. Liouville space is equipped with an inner product denoted by the trace rule, so that $\langle\langle A|B\rangle\rangle = \mathrm{Tr}(A^\dagger B)$. This final point is what allowed our axiomatic approach to work, and in the field of quantum reconstructions one often finds a close link between probabilities and inner products.

We are now able to recast our probability rule, Eq. (1), in operator space. It suffices to consider only the limited case in which the prepared state is pure and the second measurement is a projective measurement. In such a case the former is $\rho = \sum_i \lambda_i \lambda_j^* |i\rangle\langle j|$, and the latter can be written in the same basis, $\pi_j^{(2)} = \sum_{kl} c_k^{(j)} c_l^{(j)*} |k\rangle\langle l|$. We introduce a vector

$$|\Psi_j\rangle\rangle = \sum_{ik} \lambda_i c_k^{(j)*} |ik^\dagger\rangle\rangle, \tag{3}$$

which encodes both the preparation and final measurement. The other objects required to describe a series of measurements are the relevant Kraus operators, associated with the first measurement. Using the same basis, we write $A_i^\nu = \sum_{lm} \alpha_{lm}^{(i\nu)} |l\rangle\langle m|$. In our framework this is represented by the Choi-Jamiołkowski vector of the Hermitian conjugate,

$$|A_i^\nu\rangle\rangle = \sum_{lm} \alpha_{lm}^{(i\nu)*} |lm^\dagger\rangle\rangle. \tag{4}$$

Outer products $|A_i^\nu\rangle\rangle\langle\langle A_i^\nu|$ of these objects are the superoperators for a given channel. The latter are closely related to quantum combs, which can be understood as the Choi operators associated with a given channel versus our Jamiołkowski operators. Both $|\Psi_j\rangle\rangle$ and $|A_i^\nu\rangle\rangle$ are analogous to similar objects which appear in the theory of two-time states.

A natural interpretation of the two vectors from Eqs. (3) and (4) is in terms of Bayesian statistics for the first measurement. The former, Eq. (3), includes prior information concerning the pre- and post-selected state; the latter, Eq. (4), is written in terms of posterior information related to the probability of a given outcome and the method by which the measurement is performed. This contrasts with both standard quantum mechanics, in which we have a knowledge about a state at a given time and ask how future measurements are impacted, and retrodictive quantum mechanics, in which we have knowledge of a measurement outcome and want to know which state was prepared [20, 21]. The link with measurement-device-independent QKD [4–6] is apparent in the process of combining initial and final information, associated with Alice and Bob's activities, to produce a two-time state. In measurement-device-independent QKD both Alice and Bob produce light pulses in selected states to send to a central untrusted server. Our treatment of an intercept-resend strategy produces an analogous state formed from Alice's preparation and Bob's measurement and challenges Eve to derive as much information as possible from this without being detected.

Eq. (1) can now be written as

$$P(i,j|\rho)=\sum_{\nu}\langle\langle A_i^{\nu}|\Psi_j\rangle\rangle\langle\langle\Psi_j|A_i^{\nu}\rangle\rangle. \qquad (5)$$

This tells us that pre- and post-selection has the same form as a superoperation, in contrast with the first measurement which would usually play this role. Conditional rather than joint probabilities can of course be calculated from this using Bayes's rule.

Readers familiar with entanglement-based QKD analyses may find it useful to make links between that formalism and the one we make. In entanglement-based QKD, Alice and Bob share a maximally entangled Bell state $|\phi^+\rangle$. Each party then performs a measurement on it, corresponding to the preparation and measurement states of the equivalent measurement-based scheme. If we restrict our attention to pure states, then we can assign $|\psi_A\rangle$ to Alice's measurement and $|\psi_B\rangle$ to Bob's. The probability distribution of their outcomes is then given by $P(A,B)=|\langle\psi_A|\langle\psi_B|\phi^+\rangle|^2$. It is already seen that the joint Alice-Bob measurements appear as a bipartite state in this scheme, and in fact by the Choi-Jamiolkowski isomorphism already discussed we have $|\Psi_j\rangle\rangle\leftrightarrow|\psi_A\rangle|\psi_B\rangle$ (where the j subscript is associated with Bob's outcome). With this in mind we can also associate the Kraus vector, Eq. 4, with an equivalent bipartite state $A_{i\nu}^{\dagger}\otimes I|\phi^+\rangle$. Our probability rule Eq. 5 is then equivalent to the expression $P(i,j|\rho)=\sum_{\nu}|\langle\psi_A\psi_B|A_{i\nu}^{\dagger}\otimes I|\phi^+\rangle|^2$. That there are two bipartite states here, one associated with Alice and Bob's actions and the other with Eve's, is the key mathematical tool which we have used.

III. KEY DISTRIBUTION EAVESDROPPING

As discussed earlier, QKD is a pre- and post-selecting process that correlates the former with the latter. This gives some initial knowledge to Eve, who will take advantage of these correlations in optimising her eavesdropping strategy. This is the task we now turn to.

There are a number of senses in which the quality of a given strategy could be measured and here two figures of merit are considered. Both seek to quantify the amount of information Eve has extracted from a single bit, in which we are motivated by the fact that, choosing to demonstrate our method instead of performing a complete security analysis, we restrict our attention to incoherent attacks in which she intercepts and measures each system independently from the others. One figure of merit is the probability that all three parties finish up with the same bit value, $P(A=E=B)$. The other is this probability conditioned upon the fact that Alice and Bob share the bit, $P(A=E=B|A=B)$, which can of course be derived from the former as a conditional probability:

$$\mathrm{P}(A=E=B|A=B)=\frac{\mathrm{P}(A=E=B)}{\mathrm{P}(A=B)}. \qquad (6)$$

In realistic implementations, a set of post-measurement privacy amplification procedures will occur such that this latter figure is often more relevant for individual attacks. A useful third parameter is the induced quantum bit error rate, the probability $P(A\neq B)$ that Eve's actions cause Alice and Bob to end the protocol with different logical bits, which we will also calculate for each scheme. If this is too high, Alice and Bob will abort the protocol. In realistic quantum communications systems it is impossible to avoid noise. Security proofs thus provide a different quantum bit error rate, Q, which is the number of logical bits which are assigned different values by the two legitimate users. We will also provide this value for context.

In order to make Eve's attack minimally disturbing, we can let her associate a single Kraus operator with each bit value. We will also use that there is symmetry between logical bits: given the high level of symmetry in the protocols under consideration, it should hold that if all three parties relabel which measurement outcomes correspond to which bit values then all probabilities are invariant (for example, the probability that all three bit values are 0 is equal to the probability that all three bit values are 1). Indeed, for each of the figures of merit we are considering, there will always exists a strategy which is bit symmetric and achieves the same value as one which does not have this structure. We can thus restrict attention to such attacks, as discussed in [22]. This set of operations is subject to a constraint that the overall measurement must be trace-preserving, which is typically represented by the requirement that the POVM elements sum to the identity. In our formalism, this corresponds to

$$\sum_{ij}\langle i^{\dagger}|A_j\rangle\rangle\langle\langle A_j|i^{\dagger}\rangle=I, \qquad (7)$$

where i represents any complete set of basis vectors. Each term $\sum_i\langle i^{\dagger}|A_j\rangle\rangle\langle\langle A_j|i^{\dagger}\rangle$ in the sum on the left hand side of this equation corresponds to the relevant POVM element, associated with a given Kraus operator vector. Eq. (7) can be derived by summing Eq. (5) over all i,j (and assuming a single value for ν). If we consider the limited case of a pure state $\rho=|\rho\rangle\langle\rho|$, then applying that the second POVM satisfies $\sum_i\pi_i^{(2)}=I$ leads one to the form

$$\sum_{ij}\langle\langle\rho i^{\dagger}|A_j\rangle\rangle\langle\langle A_j|\rho i^{\dagger}\rangle\rangle=1. \qquad (8)$$

This equation is of the form $\langle\rho|A|\rho\rangle=1$ and we require that it holds for all ρ; this implies that $A=I$ and Eq. (7) follows.

We further note that here we have considered that the input space is a qubit, for which Eq. (7) implies that

$$\sum_i\mathrm{Tr}\left(|A_i\rangle\rangle\langle\langle A_i|\right)=2. \qquad (9)$$

For just two symmetric Kraus operators we thus find $\langle\langle A_0|A_0\rangle\rangle = \langle\langle A_1|A_1\rangle\rangle = 1$, and hence are searching for normalised Kraus vectors. This simplifies our optimisation task below.

To help readers follow the calculations below, we will briefly outline our process for finding the optimal eavesdropping strategies in each case. The initial step is to construct the superoperators, $|\Psi_j\rangle\rangle\langle\langle\Psi_j|$ in Eq. 5, which correspond to Alice and Bob sharing a bit value in a given timeslot. For example, if Alice sending the pure state $|0\rangle$ and Bob measuring the state $|1\rangle$ in a routine results in a shared bit value, we will associate to such an event the superoperator $|01^\dagger\rangle\rangle\langle\langle 01^\dagger|$. In a general routine, there will be more than one correlation associated with a bit value and an overall superoperator is then constructed by summing over the relevant cases. The next step is to associate with Eve's interventions a Kraus operator; in what follows we investigate the simplest case in which one measurement outcome is associated with each bit value. Then, using Eq. 5, an overall probability rule is found for each of our figures of merit. By examination these can then be maximised and, typically, we find that the task of finding optimal eavesdropping strategies is rewritten as an eigenvalue problem.

A. BB84

To illustrate our approach, we consider first the most prevalent protocol in QKD literature, BB84 [23, 24]. This uses the set of four qubit states $|0\rangle$, $|1\rangle$, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice chooses with equal probability between these and sends the state to Bob, who measures using a POVM corresponding to projections onto each state before announcing which of the two orthogonal bases ($|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$) he measured. In the case that Alice sent a state not in the relevant set, it is discarded; in the remaining cases the two parties now share knowledge of a quantum state and assign bit values: 0 for $|0\rangle$ or $|+\rangle$ and 1 otherwise. BB84's security has been demonstrated in a number of different context [25, 26], and with a slight modification is found to be secure with an error rate below $Q = 18.9\%$ [27].

An eavesdropper's task in a given time-slot is to identify the correlations between Alice's sent state and Bob's measured state without giving themselves away. Our basic eavesdropping model is to associate with Eve a single Kraus operator for each logical bit value which we label $|E_i\rangle\rangle$. Then, by Eq. (5), the probability that all three parties have the same bit value, given that the bit is not discarded during sifting, is

$$\begin{aligned}
&\mathrm{P}(A = E = B) \\
&= \mathrm{P}(A = 0)\mathrm{P}(B = 0, E = 0|A = 0) \\
&+ \mathrm{P}(A = +)\mathrm{P}(B = +, E = 0|A = +) + ... \\
&= \frac{1}{4}(\langle\langle E_0| \left(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |++^\dagger\rangle\rangle\langle\langle ++^\dagger|\right) |E_0\rangle\rangle \\
&+ \langle\langle E_1| \left(|11^\dagger\rangle\rangle\langle\langle 11^\dagger| + |--^\dagger\rangle\rangle\langle\langle --^\dagger|\right) |E_1\rangle\rangle). \quad (10)
\end{aligned}$$

The factor of $1/4$ here is the probability that Alice sends a given state [28]. One can see straightforwardly that this figure will be maximised if we let the eavesdropper's Kraus operator vectors be proportional to the eigenvector with the largest eigenvalue for the relevant superoperator. We next require that the overall measure satisfy bit symmetry and trace preservation, Eq. (7), and find rather straightforwardly the optimal measurement

$$\begin{aligned}
|E_0\rangle\rangle &= \frac{1}{\sqrt{3}}\left(|00^\dagger\rangle\rangle + |++^\dagger\rangle\rangle\right) \\
|E_1\rangle\rangle &= \frac{1}{\sqrt{3}}\left(|11^\dagger\rangle\rangle + |--^\dagger\rangle\rangle\right). \quad (11)
\end{aligned}$$

Each of these vectors has an eigenvalue of $3/2$ with the relevant superoperator taken from Eq. 10 and so we have found that $\mathrm{P}(A = E = B) = 3/4$ is the maximum value that this figure of merit can take.

It is useful to know the quantum bit error rate for such a measurement. In the BB84 strategy, the two legitimate parties will disagree on the value of their logical bit value if the receiver's measured state is orthogonal to that which was sent. We have

$$\begin{aligned}
\mathrm{P}(A \neq B) = \frac{1}{4}\sum_i \langle\langle E_i| &\left(|01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger|\right. \\
&\left.+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger| + |-+^\dagger\rangle\rangle\langle\langle -+^\dagger|\right) |E_i\rangle\rangle. \quad (12)
\end{aligned}$$

This is evaluated using the above measurement vectors (Eq. 11). Taking just one outcome for example, we find

$$\begin{aligned}
&\left(|01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger|\right. \\
&\left.+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger| + |-+^\dagger\rangle\rangle\langle\langle -+^\dagger|\right) |E_0\rangle\rangle \\
&= \frac{1}{2\sqrt{3}}\left(|01^\dagger\rangle\rangle + |10^\dagger\rangle\rangle + |+-^\dagger\rangle\rangle + |-+^\dagger\rangle\rangle\right). \quad (13)
\end{aligned}$$

From this, the overlap is found to be

$$\begin{aligned}
&\langle\langle E_0| \left(|01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger|\right. \\
&\left.+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger| + |-+^\dagger\rangle\rangle\langle\langle -+^\dagger|\right) |E_0\rangle\rangle = \frac{1}{3} \quad (14)
\end{aligned}$$

The same result is found for the equivalent expression involving $|E_1\rangle\rangle$. Hence, the total probability that Alice and Bob's bit values disagree in a given timeslot is

$$\mathrm{P}(A \neq B) = \frac{1}{4} \times \frac{2}{3} = \frac{1}{6}. \quad (15)$$

Finally, by Eq. 6, the above two results give $\mathrm{P}(A = E = B|A = B) = (3/4)/(5/6) = 9/10$ as the fraction of cases for which all three parties share a bit value, conditioned upon agreement between the two legitimate users, for this strategy. Using Eq. (4) we can write the measurement Eq. (11) in terms of Kraus operators:

$$\begin{aligned} E_0 &= \frac{1}{\sqrt{3}}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right) \\ &= \frac{1}{2\sqrt{3}}\left(2I + \sigma_x + \sigma_z\right), \qquad (16) \\ E_1 &= \frac{1}{\sqrt{3}}\left(|1\rangle\langle 1| + |-\rangle\langle -|\right) \\ &= \frac{1}{2\sqrt{3}}\left(2I - \sigma_x - \sigma_z\right). \qquad (17) \end{aligned}$$

Here, $\sigma_x = |+\rangle\langle +| - |-\rangle\langle -|$ and $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ are the usual Pauli matrices and I the identity.

As previously mentioned, we will also derive the measurement (again assuming that Eve has two possible measurement outcomes $|E_i\rangle\rangle$) that maximises the latter figure of merit. We can use Eq. (6); the numerator will be given by Eq. (10) and the denominator will be

$$\begin{aligned} \mathrm{P}(A = B) = \sum_i \langle\langle E_i| \big(&|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |11^\dagger\rangle\rangle\langle\langle 11^\dagger| \\ &+ |++^\dagger\rangle\rangle\langle\langle ++^\dagger| + |--^\dagger\rangle\rangle\langle\langle --^\dagger| \big) |E_i\rangle\rangle. \qquad (18) \end{aligned}$$

We can apply the principle of bit symmetry to write this in terms of $|E_0\rangle\rangle$ only:

$$\begin{aligned} &\mathrm{P}(A = E = B|A = B) = \\ &\frac{\langle\langle E_0| \left(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |++^\dagger\rangle\rangle\langle\langle ++^\dagger|\right) |E_0\rangle\rangle}{S} \\ &S = \langle\langle E_0| \big(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |++^\dagger\rangle\rangle\langle\langle ++^\dagger| \\ &+ |11^\dagger\rangle\rangle\langle\langle 11^\dagger| + |--^\dagger\rangle\rangle\langle\langle --^\dagger|\big) |E_0\rangle\rangle \qquad . \quad (19) \end{aligned}$$

It is seen by inspection that this expression maximises to the case of definite agreement between all three parties if we enforce the constraint

$$\langle\langle E_0| \left(|11^\dagger\rangle\rangle\langle\langle 11^\dagger| + |--^\dagger\rangle\rangle\langle\langle --^\dagger|\right) |E_0\rangle\rangle = 0, \quad (20)$$

and are led to the form

$$|E_0\rangle\rangle = a|0+^\dagger\rangle\rangle + b|+0^\dagger\rangle\rangle. \quad (21)$$

By symmetry the other measurement outcome must be associated with a Kraus vector

$$|E_1\rangle\rangle = a|1-^\dagger\rangle\rangle + b|-1^\dagger\rangle\rangle. \quad (22)$$

a and b in the above equations are two variables which we are free to vary subject to the constraint

$$a^2 + ab + b^2 = 1; \quad (23)$$

a requirement which follows from trace preservation. Any measurement which satisfies the three previous equations will form a valid POVM and ensure that Eve, Alice and Bob all agree on a bit value given that the latter pair do. As one example, we choose $a = 1$ and $b = 0$, giving $|E_0\rangle\rangle = |0+^\dagger\rangle\rangle$ and $|E_1\rangle\rangle = |1-^\dagger\rangle\rangle$, corresponding to the Kraus operators $E_0 = |+\rangle\langle 0|, E_1 = |-\rangle\langle 1|$. The first of these outcomes cannot occur if the signal state is $|1\rangle$; otherwise it will leave the qubit in state $|+\rangle$. If the state $|0\rangle$ is sent then this outcome is retained and if $|-\rangle$ is sent then the bit values disagree, which is not a member of the set of outcomes under consideration. Thus all three parties agree on a bit value 0. However, for this arbitrarily chosen measurement we can calculate $\mathrm{P}(A \neq B) = 1/2$. It is sensible of Eve to ask that this final variable be minimised (equivalently, the converse probability be maximised), subject to our previously derived constraints. One arrives at

$$\mathrm{P}(A = B) = \frac{1}{2}(a + b)^2, \quad (24)$$

derived from Eq. (18). The maximum value that this function can take within the domain given by Eq. (23) is $2/3$, corresponding to the point $a = b = \pm 1/\sqrt{3}$. If we take only the positive value (ignoring the overall phase, irrelevant for Kraus operators) our set of Kraus vectors is

$$\begin{aligned} |E_0\rangle\rangle &= \frac{1}{\sqrt{3}}\left(|0+^\dagger\rangle\rangle + |+0^\dagger\rangle\rangle\right) \\ |E_1\rangle\rangle &= \frac{1}{\sqrt{3}}\left(|1-^\dagger\rangle\rangle + |-1^\dagger\rangle\rangle\right). \qquad (25) \end{aligned}$$

We can understand how to physically implement this attack by writing it in the more familiar form of Kraus operators acting on Hilbert space, done using the isomorphism Eq. (4). We find

$$\begin{aligned} E_0 &= \frac{1}{\sqrt{3}}\left(|+\rangle\langle 0| + |0\rangle\langle +|\right) \\ &= \frac{1}{\sqrt{6}}\left(\sigma_x + \sigma_z + I\right), \\ E_1 &= \frac{1}{\sqrt{3}}\left(|-\rangle\langle 1| + |1\rangle\langle -|\right) \\ &= \frac{1}{\sqrt{6}}\left(\sigma_x + \sigma_z - I\right). \qquad (26) \end{aligned}$$

In order to physically implement a pair of Kraus operators, one may perform a controlled-NOT gate acting in the basis in which they diagonalise. Here, that role is played by the Breidtbart states $|0_B\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|1_B\rangle = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle$. Eve uses a suitable initialised qubit probe as the gate's target and the Alice-Bob qubit as the control. This is the well-known Fuchs-Peres-Brandt attack [22, 29–31], which has emerged as here as the solution to a simple eigenvalue problem.

B. B92

Our second illustration is the B92 protocol developed by Bennett, who realised that it was possible to modify the protocol such that it is performed using just two states [32]. Alice sends either $|0\rangle$ or $|+\rangle$ and Bob measures using the same POVM as in the BB84 protocol. The two outcomes $|0\rangle$ or $|+\rangle$ are consistent with both possible signal states; they are sifted out. The outcome $|-\rangle$ can only occur if $|0\rangle$ is sent and the outcome $|1\rangle$ can only occur if $|+\rangle$ is sent. These two outcomes are thus kept and associated with the bit values 0 or 1 respectively. This is (one variation of) the B92 protocol, which is provably secure [33, 34] up for noise below $Q = 3.4\%$.

There is an added complexity in this protocol, compared to BB84, which we must be careful of. Due to the non-orthogonality of the post-selected states, Eve's measurements have the ability to change the proportion of bits which are sifted. Taking this into account, our first variable to optimise is

$$\begin{aligned}&P(A=E=B)\\&=\frac{\langle\langle E_0|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|E_0\rangle\rangle+\langle\langle E_1|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|E_1\rangle\rangle}{T}\\&T=\sum_i\langle\langle E_i|\left(|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|+|01^\dagger\rangle\rangle\langle\langle 01^\dagger|\right.\\&\left.+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger|+|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|\right)|E_i\rangle\rangle\qquad,\end{aligned}\tag{27}$$

where T is the probability that a given bit value is not sifted from the protocol. This will occur whenever one of the relevant measurement outcomes occurs whether the desired signal state correlation has occured or not. Furthermore, Alice and Bob of course are unaware of Eve's results and hence we sum over those two outcomes. We again take advantage of the bit symmetry previously discussed. This leaves us with a form entirely in terms of $|E_0\rangle\rangle$:

$$\begin{aligned}&P(A=E=B)\\&=\frac{\langle\langle E_0|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|E_0\rangle\rangle}{T'}\\&T'=\langle\langle E_0|\left(|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|+|01^\dagger\rangle\rangle\langle\langle 01^\dagger|\right.\\&\left.+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger|+|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|\right)|E_0\rangle\rangle\quad,\end{aligned}\tag{28}$$

By inspection it is seen that this maximises for $P(A = E = B) = 1$ if

$$\begin{aligned}\langle\langle E_0|\left(|01^\dagger\rangle\rangle\langle\langle 01^\dagger|+|+-^\dagger\rangle\rangle\langle\langle +-^\dagger|\right.\\\left.+|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|\right)|E_0\rangle\rangle=0.\end{aligned}\tag{29}$$

The only set of vectors which satisfy this are those of the form

$$|E_0\rangle\rangle = A|-0^\dagger\rangle\rangle,\tag{30}$$

and, by symmetry,

$$|E_1\rangle\rangle = A|1+^\dagger\rangle\rangle,\tag{31}$$

where A is a constant which is to be found, such that the derived measurement is trace preserving. In the Hilbert space formulation of quantum mechanics, this measurement is represented by the Kraus operators $E_0 = A|0\rangle\langle-|$ and $E_1 = A|+\rangle\langle1|$, which replace the states $|-\rangle$ and $|1\rangle$ with $|0\rangle$ and $|+\rangle$ respectively. As neither pair of states is orthogonal, we can see that the measurement does not span the state space. This can be seen alternatively by substituting these two vectors into (7):

$$A^2\left(|1\rangle\langle1|+|-\rangle\langle-|\right)=I.\tag{32}$$

Clearly there exists no value of A which satisfies this and hence the measurement defined by Eqs. (30) and (31) cannot be complete in itself. We can, however, propose a third outcome $|E_2\rangle\rangle$ such that our trace preservation condition is fulfilled. Our task then becomes to maximise A such that the condition

$$\begin{aligned}A^2\left(|1\rangle\langle1|+|-\rangle\langle-|\right)+\langle0^\dagger|E_2\rangle\rangle\langle\langle E_2|0^\dagger\rangle\\+\langle1^\dagger|E_2\rangle\rangle\langle\langle E_2|1^\dagger\rangle=I\end{aligned}\tag{33}$$

can still hold for some $|E_2\rangle\rangle$. We can begin by defining an operator $X = \langle0^\dagger|E_2\rangle\rangle\langle\langle E_2|0^\dagger\rangle + \langle1^\dagger|E_2\rangle\rangle\langle\langle E_2|1^\dagger\rangle$. Optimising the measurement is equivalent to finding the maximum A such that this operator is positive semi-definite. Rearranging the above constraint, one finds

$$\begin{aligned}X=(1-A^2/2)|0\rangle\langle0|-(A^2/2)\left(|0\rangle\langle1|+|1\rangle\langle0|\right)\\+(1-3A^2/2)|1\rangle\langle1|.\end{aligned}\tag{34}$$

This operator's two eigenvalues are found to be $1 - A^2 \pm (A^2/\sqrt{2})$; we only need ensure that the lower value is positive and this holds if $A^2 = 2 - \sqrt{2}$. This choice gives a single non-zero eigenvector, $|\psi\rangle = (\sqrt{2-\sqrt{2}}/2)((-1-\sqrt{2})|0\rangle + |1\rangle)$, and any $|E_2\rangle\rangle$ that satisfies

$$X=\langle0^\dagger|E_2\rangle\rangle\langle\langle E_2|0^\dagger\rangle+\langle1^\dagger|E_2\rangle\rangle\langle\langle E_2|1^\dagger\rangle=|\psi\rangle\langle\psi|\tag{35}$$

is consistent with this maximum value of A, that which ensures that Alice, Eve and Bob have a shared bit value given the occurence of outcomes $|E_0\rangle\rangle$ and $|E_1\rangle\rangle$. Our choice here is the usual freedom found in measurement theory that a number of Kraus operators are consistent with a given POVM element.

The measurement we have derived can be identified with unambiguous state discrimination [35–38]: by themselves, $|E_0\rangle\rangle$ and $|E_1\rangle\rangle$ will not preserve the trace and this implies that Eve measures the qubit without resending. Introducing a third measurement outcome has given us cases for which she does not have a logical bit however in all other cases eavesdropping will be successful. This is well known to be the weakness of B92: Eve is able to hide behind the losses in the quantum channel [39].

We now move on to consider our second figure of merit, which is conditional on Alice and Bob's agreement. Again we use Bayes's rule, the probability of agreement between those two parties this time being

$$\begin{aligned}&\mathrm{P}(A=B) \\ &=\sum_i(\langle\langle E_i|(|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|+|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|)|E_i\rangle\rangle.\end{aligned} \tag{36}$$

We now renormalize Eq. (27) and take advantage of bit symmetry to simplify the expression to

$$\begin{aligned}&\mathrm{P}(A=E=B|A=B) \\ &=\frac{\langle\langle E_0|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|E_0\rangle\rangle}{U} \qquad (37)\\ &U=\langle\langle E_0|(|0-^\dagger\rangle\rangle\langle\langle 0-^\dagger|+|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|)|E_0\rangle\rangle \quad . \qquad (38)\end{aligned}$$

Following the procedure from previous calculations, we note that $\mathrm{P}(A=E=B|A=B)=1$ if

$$\langle\langle E_0|+1^\dagger\rangle\rangle\langle\langle +1^\dagger|E_0\rangle\rangle=0, \tag{39}$$

for which we can parameterise the relevant set of vectors by

$$|E_0\rangle\rangle=a|-\psi^\dagger\rangle\rangle+b|\phi 0^\dagger\rangle\rangle \tag{40}$$

with a, b two free parameters (up to normalisation) and ϕ, ψ two states which again are free up to some constraints. Requiring symmetry between the two attacks implies next that we have

$$|E_1\rangle\rangle=c|1\lambda^\dagger\rangle\rangle+d|\rho+^\dagger\rangle\rangle. \tag{41}$$

There are a large number of parameters here (the four complex variables and four states) however they are not all free, given the bit symmetry and trace preservation that we are enforcing for all measurements. We choose to focus first on the former condition, from which we obtain the requirements

$$\begin{aligned}&|a\langle -^\dagger|\psi^\dagger\rangle+b\langle 0|\phi\rangle|^2=|c\langle 1^\dagger|\lambda^\dagger\rangle+d\langle +|\rho\rangle|^2 \\ &|a\langle 1^\dagger|\psi^\dagger\rangle|^2=|c\langle -^\dagger|\lambda^\dagger\rangle|^2 \\ &|b\langle +|\phi\rangle|^2=|d\langle 0|\rho\rangle|^2.\end{aligned} \tag{42}$$

The first of these constraints is derived from the probabilities that all three parties agree; the second from the case in which only Alice and Eve agree; the third from that in which only Eve and Bob agree. The fourth possibility (that Alice and Bob agree with each other but not Eve) is of course automatically satisfied given the figure of merit under consideration. Given the freedom still available, we can choose to consider just a subset of all possible measurements. It can be seen that all three requirements above hold if we let $|\psi\rangle=|-\rangle, |\phi\rangle=|0\rangle, |\lambda\rangle=|1\rangle, |\rho\rangle=|+\rangle$. Furthermore, we can require that the measurement is complete with just two outcomes, i.e. that it does not involve unambiguous state discrimination, as in the previous result. In terms of our parameterisation, this involves letting $a=c$ and $b=d$ and making sure that all four are nonzero. Finally, we require that the signal state's trace is preserved by Eve's attack, for which Eq. (7) is used to fix the two remaining degrees of freedom. A calculation reveals

$$\begin{aligned}&\sum_{ij}\langle i^\dagger|E_j\rangle\rangle\langle\langle E_j|i^\dagger\rangle= \\ &\left(\frac{a^2}{2}+\frac{3b^2}{2}+ab\right)|0\rangle\langle 0| \\ &+\frac{(b^2-a^2)}{2}(|0\rangle\langle 1|+|1\rangle\langle 0|) \\ &+\left(\frac{3a^2}{2}+\frac{b^2}{2}+ab\right)|1\rangle\langle 1|,\end{aligned} \tag{43}$$

in which the contraction has been performed in the $|0\rangle, |1\rangle$ basis, and the requirement is that expression on the left hand side is the identity matrix. It is easy to see that this can only be satisfied if $a=b=\sqrt{1/3}$, so that the measurement is

$$\begin{aligned}|E_0\rangle\rangle&=\frac{1}{\sqrt{3}}\left(|--^\dagger\rangle\rangle+|00^\dagger\rangle\rangle\right) \\ |E_1\rangle\rangle&=\frac{1}{\sqrt{3}}\left(|11^\dagger\rangle\rangle+|++^\dagger\rangle\rangle\right) \qquad .\end{aligned} \tag{44}$$

One finds that a probability of one for the current figure of merit comes at a cost of introducing an error rate of $P(A\neq B)=1/5$ between Alice and Bob. As with previous results we can evaluate the Kraus operators:

$$\begin{aligned}E_0&=\frac{1}{\sqrt{3}}\left(|0\rangle\langle 0|+|-\rangle\langle -|\right) \\ &=\frac{1}{2\sqrt{3}}\left(2I+\sigma_z-\sigma_x\right) \\ E_1&=\frac{1}{\sqrt{3}}\left(|1\rangle\langle 1|+|+\rangle\langle +|\right) \\ &=\frac{1}{2\sqrt{3}}\left(2I-\sigma_z+\sigma_x\right).\end{aligned} \tag{45}$$

Let's consider the specific case in which Alice signals the state $|0\rangle$ in order to aid understanding of the measurement. In one-sixth of cases Eve's outcome will correspond to the Kraus operator E_1, meaning that she has failed to identify the correct bit value. With this result, the qubit is left in the state $|+\rangle$ which ensures that Bob disagrees with Alice as to which logical bit is set in that timeslot: in order for him to arrive at the bit value 0, he must get the result $|-\rangle$, which Eve has made impossible. This explains why our measurement results maximise the relevant figure of merit. There is still a chance of disagreement in the remaining five-sixths of cases and those lead to the above calculated probabilities.

C. Three-state QKD

The preceding examples are but two of a large set of QKD protocols that have been considered. We complement these with the example of three-state QKD, sometimes referred to as PBC00 [40]. While this protocol has been demonstrated experimentally [41], and security proofs for arbitrary intercept-resend attacks provided [42, 43] which show that the protocol is secure up to a noise level of $Q = 9.81\%$, individual eavesdropping strategies have been less thoroughly explored. We find particularly surprising results for the optimal eavesdropping strategies for this protocol.

Trine states are the three symmetric qubit states on the Bloch sphere, which we can parameterise as

$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i2\pi k/3}|1\rangle), \tag{46}$$

with i taking the values 0, 1 or 2 corresponding, for example, to three linear polarisations of a single photon separated by $\pi/3$. The anti-trine ensemble are the three states orthogonal to each of these which we label $|\overline{\psi}_k\rangle$. Three-state QKD is a protocol which utilises this set of states. Alice chooses one of the three trine states with equal probability; it is then sent to Bob, who measures with a POVM consisting of projections onto the three anti-trine states suitably weighted so that the overall set is trace-preserving. In the absence of an eavesdropper, he has zero probability of measuring the state orthogonal to that which was sent and equal probability of measuring either of the other two. Alice now announces publically one of the states which she didn't send. There are two possibilities: Bob knows this already (which he announces, causing the bit to be discarded) or this is new information for Bob (in which case he now knows what the sent state is). Logical bit values are assigned as such: if Alice announces that she didn't send the state one step clockwise of that which she did, the bit value is 0. If the former is one step anti-clockwise of the latter, the bit value is 1.

As an example, consider that Alice sends the state $|\psi_0\rangle$ and Bob's outcome is $|\overline{\psi}_1\rangle$. If it is announced that Alice did not send $|\psi_1\rangle$ then Bob still does not know whether she sent $|\psi_0\rangle$ or $|\psi_2\rangle$ and so the bit is discarded. If instead Alice announces that she did not send $|\psi_2\rangle$ then Bob knows that she could only have sent $|\psi_0\rangle$. As $|\psi_2\rangle$ is anti-clockwise of $|\psi_0\rangle$, the bit value 1 is assigned to this run.

As in the previous cases, Eve's task is to uncover the relevant bit value without giving away that she is doing this. We begin our calculation by introducing three superoperators:

$$\begin{aligned}
&A_0 = |\psi_0\overline{\psi}_2^\dagger\rangle\rangle\langle\langle\psi_0\overline{\psi}_2^\dagger| + |\psi_1\overline{\psi}_0^\dagger\rangle\rangle\langle\langle\psi_1\overline{\psi}_0^\dagger| \\
&+ |\psi_2\overline{\psi}_1^\dagger\rangle\rangle\langle\langle\psi_2\overline{\psi}_1^\dagger| \\
&= \frac{3}{4}\Big(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger| \\
&+|11^\dagger\rangle\rangle\langle\langle 11^\dagger| - e^{-i2\pi/3}|00^\dagger\rangle\rangle\langle\langle 11^\dagger| - e^{i2\pi/3}|11^\dagger\rangle\rangle\langle\langle 00^\dagger|\Big)
\end{aligned} \tag{47}$$

$$\begin{aligned}
&A_1 = |\psi_0\overline{\psi}_1^\dagger\rangle\rangle\langle\langle\psi_0\overline{\psi}_1^\dagger| + |\psi_1\overline{\psi}_2^\dagger\rangle\rangle\langle\langle\psi_1\overline{\psi}_2^\dagger| \\
&+ |\psi_2\overline{\psi}_0^\dagger\rangle\rangle\langle\langle\psi_2\overline{\psi}_0^\dagger| \\
&= \frac{3}{4}\Big(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger| \\
&+|11^\dagger\rangle\rangle\langle\langle 11^\dagger| - e^{i2\pi/3}|00^\dagger\rangle\rangle\langle\langle 11^\dagger| - e^{-i2\pi/3}|11^\dagger\rangle\rangle\langle\langle 00^\dagger|\Big)
\end{aligned} \tag{48}$$

$$\begin{aligned}
&A_X = |\psi_0\overline{\psi}_0^\dagger\rangle\rangle\langle\langle\psi_0\overline{\psi}_0^\dagger| + |\psi_1\overline{\psi}_1^\dagger\rangle\rangle\langle\langle\psi_1\overline{\psi}_1^\dagger| \\
&+ |\psi_2\overline{\psi}_2^\dagger\rangle\rangle\langle\langle\psi_2\overline{\psi}_2^\dagger| \\
&= \frac{3}{4}\big(|00^\dagger\rangle\rangle\langle\langle 00^\dagger| + |01^\dagger\rangle\rangle\langle\langle 01^\dagger| + |10^\dagger\rangle\rangle\langle\langle 10^\dagger| \\
&+|11^\dagger\rangle\rangle\langle\langle 11^\dagger| - |00^\dagger\rangle\rangle\langle\langle 11^\dagger| - |11^\dagger\rangle\rangle\langle\langle 00^\dagger|\big) \qquad .
\end{aligned} \tag{49}$$

The first two of these correspond to the cases in which Alice and Bob share a bit value of 0 or 1; the final case is those for which Alice and Bob are left with mismatched bit values. We note that all three objects depart from the identity only in the $|00^\dagger\rangle\rangle, |11^\dagger\rangle\rangle$ subspace. In this notation, the first figure of merit which we seek to maximise is

$$\mathrm{P}(A = E = B) = \frac{\frac{1}{2}\left(\langle\langle E_0|A_0|E_0\rangle\rangle + \langle\langle E_1|A_1|E_1\rangle\rangle\right)}{\sum_i \langle\langle E_i|\left(A_X + \frac{1}{2}(A_0 + A_1)\right)|E_i\rangle\rangle}. \tag{50}$$

The denominator arises from normalising over cases which aren't sifted: this will never happen when Alice and Bob disagree but will happen in half of the remaining cases (when Alice announces a state that Bob already knows was not sent).

In the $|0\rangle, |1\rangle$ basis this object is

$$\begin{aligned}
&A_X + \frac{1}{2}(A_0 + A_1) \\
&= \frac{3}{2}\left(I - \frac{1}{4}\left(|00^\dagger\rangle\rangle\langle\langle 11^\dagger| + |11^\dagger\rangle\rangle\langle\langle 00^\dagger|\right)\right) \quad .
\end{aligned} \tag{51}$$

As with A_0 and A_1, this superoperator differs from the identity only due to a term in the $|00^\dagger\rangle\rangle, |11^\dagger\rangle\rangle$ subspace. The optimal strategy must therefore depend only on these two vectors as any other contributions will lead to a reduced constant of normalisation without contributing to an increased probability. The bit-symmetric set of vectors consistent with this is

$$\begin{aligned}
|E_0\rangle\rangle &= \frac{1}{\sqrt{2}}\left(|00^\dagger\rangle\rangle + e^{i\phi}|11^\dagger\rangle\rangle\right) \\
|E_1\rangle\rangle &= \frac{1}{\sqrt{2}}\left(|00^\dagger\rangle\rangle + e^{-i\phi}|11^\dagger\rangle\rangle\right).
\end{aligned} \tag{52}$$

It is interesting to note that these correspond to two *unitary transformations*: the former a rotation by ϕ anti-clockwise around the Bloch sphere and the latter the anti-clockwise rotation. (The corresponding Kraus operators are $E_0 = (|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|)/\sqrt{2}$ and $E_1 = (|0\rangle\langle 0| + e^{-i\phi}|1\rangle\langle 1|)/\sqrt{2}$, both of which can be seen to satisfy the usual condition $UU^\dagger = U^\dagger U = I$ for a unitary operation, up to a factor of 1/2, which represents Eve's probability of choosing each one.) The unitarity of this operation implies the remarkable result that Eve gains *no information* about Alice's state from her intervention! This is because, in the three-state protocol, no bit value is associated with the signal state itself: rather it is assigned only when Alice makes her later announcement. Eve's best strategy is to change the state Bob receives and in this manner choose which signal states are subsequently sifted.

Substituting the measurement Eq. (52) into Eq. (50) we obtain the single parameter equation

$$\mathrm{P}(A = E = B) = \frac{1 - \cos(\frac{2\pi}{3} - \phi)}{4 - \cos(\phi)}. \tag{53}$$

One can straightforwardly maximise this; we find that $\mathrm{P}(A = E = B) = 3/5$ for the rotation angle $\phi = -\sin^{-1}(5\sqrt{3}/14) \approx -0.21\pi$, which has an associated error rate of 2/15. This is an unexpected result, but can be rationalised somewhat. There is a $\pi/6$ phase difference between the probability that a given qubit being either sifted or positively post-selected. The angle ϕ lies somewhere between the two.

We can now move onto our second figure of merit, the same probability conditional on Alice and Bob's agreement. We find

$$\mathrm{P}(A = E = B|A = B) = \frac{\langle\langle E_0|A_0|E_0\rangle\rangle + \langle\langle E_1|A_1|E_1\rangle\rangle}{\sum_i \langle\langle E_i|(A_0 + A_1)|E_i\rangle\rangle} \tag{54}$$

a form that again depends only on the coefficients of $|00^\dagger\rangle\rangle$ and $|11^\dagger\rangle\rangle$. Our optimal measurement will again be the unitary given in Eq. 52 with ϕ now taking a different value. In terms of this parameter, we find

$$\mathrm{P}(A = E = B|A = B) = \frac{1 - \cos(\frac{2\pi}{3} - \phi)}{2 + \cos(\phi)}, \tag{55}$$

which maximises at $\phi = -2\pi/3$ to give $\mathrm{P}(A = E = B|A = B) = 1$; that is, for such an attack, Eve will always know the bit value when Alice and Bob agree. This attack thus corresponds to Eve choosing the bit value through her choice of unitary transformation: if she chooses 0, the signal qubit is rotated $2\pi/3$ clockwise around the Bloch sphere and oppositely for bit value 1. Of course, the trine ensemble also satisfies a $2\pi/3$ rotation, which allows us to understand why this is an optimal measurement. Let's consider a concrete example of the protocol. Alice sends the signal state $|\psi_0\rangle$ and Eve chooses the unitary $|E_0\rangle\rangle$, a rotation $2\pi/3$ around the Bloch sphere which thus leaves the qubit in the state $|\psi_1\rangle$. There is now no chance that Bob's outcome is $|\bar{\psi}_1\rangle$. This is the reason that Eve is able to achieve such a high conditional probability: the only two outcomes possible now are either that the legitimate parties disagree or that all three parties agree. The latter occurs when Bob measures $|\bar{\psi}_2\rangle$ and Alice announces that she did not send $|\psi_1\rangle$. The former will occur in all other cases. To see this better, we have displayed all possible outcomes conditioned upon Alice sending the state $|\psi_0\rangle$ in Table I. As can be seen our eavesdropper pays a high price for this attack, which introduces an error rate of 2/3.

IV. CONCLUSIONS

In developing our method, a consistent assumption has been the use of a prepare-and-measure scheme for the physical implementation of the eavesdropping routine, as opposed to an entanglement-based scheme which is more common in the literature on quantum security [1]. We prefer the prepare-and-measure scheme for reasons of conceptual simplicity (e.g. it does not require ancillary qubits to be invoked) as well as noting that it allows us to make a link back to the quantum reconstructions work [3] which inspired it, detailing the principles upon which security relies.

Once our formalism is set up, the optimisation follows rather naturally, with for example the Fuchs-Peres-Brandt BB84 attack emerging from a straightforward eigenvalue problem. For B92 we recover the well-known vulnerability to an unambiguous discrimination attack. For the three state protocol, the optimum set of Kraus operators are unitary, i.e. no information is extracted from the signal qubit. That this surprising result follows directly from our method demonstrates that it is a natural way to approach problems involving pre- and post-selection. The form of this optimal attack is in the same spirit as results of Silva et al [7] who showed that projective measurements are not enough for tomography of two-time states. These results are summarised in Table II. It is interesting to note that unambiguous state discrimination, the best attack against the B92 protocol, perfectly characterises the state; this contrasts with the unitary operation which appears as the solution to optimal eavesdropping in the three-state protocol and reveals no information about the signal state there. This highlights that the attack which should be used in each case strongly depends upon how the protocol assigns a bit value to each time slot. It is also seen that all three protocols allow an eavesdropping strategy in which Eve learns all of Alice and Bob's error-free shared bits, so that no level of privacy amplification can make the scheme secure for the corresponding error rates. For the BB84 protocol, this error rate is one-third, in agreement with the point at which Eve's attack becomes entanglement breaking in an entanglement based scheme [44, 45].

A natural development of this work would be to model proccesses which occur in actual QKD protocols, for example lossy channels. This would further highlight the utility of our approach.

V. ACKNOWLEDGEMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council and by the Royal Society (RP150122).

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

[2] D. Stebila, M. Mosca, and N. Lütkenhaus, in *LNICST 36, Quantum Communication and Quantum Networking*, edited by A. Sergienko, S. Pascazio, and P. Villoresi (Springer, Berlin, 2010) pp. 283–296.

[3] K. Flatt, S. M. Barnett, and S. Croke, Phys. Rev. A **96**, 062125 (2017).

[4] S. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[6] S. Pirandola *et al.*, Nature Photonics **9**, 397 (2015).

[7] R. Silva, Y. Guryanova, N. Brunner, N. Linden, A. J. Short, and S. Popescu, Phys. Rev. A **89**, 012121 (2014).

[8] G. Chiribella, G. D'Ariano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009).

[9] M.-D. Choi, Linear Algebra and its Applications **10**, 285 (1975).

[10] A. Jamiolkowski, Rep. Math. Phys. **4**, 275 (1972).

[11] M. S. Leifer and R. Spekkens, Phys. Rev. A **88**, 052130 (2013).

[12] A. Bisio, G. Chiribella, G. D'Ariano, P. Perinotti, and S. Facchini, Phys. Rev. A **81**, 032324 (2010).

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).

[14] S. M. Barnett, *Quantum Information* (Oxford University Press, Oxford, 2009).

[15] K. Kraus, *States, Effects and Operations* (Springer, 1983).

[16] L. Hardy, "Quantum theory from five reasonable axioms," (2001), v4 used here: available from arXiv:quant-ph/0101012v4.

[17] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **84**, 012311 (2011).

[18] J. Fiutak and J. Van Kranendonk, Canadian Journal of Physics **40**, 1085 (1962).

[19] S. M. Barnett and B. J. Dalton, J. Phys. A: Math. Gen. **20**, 411 (1987).

[20] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz, Phys. Rev. **134**, B1410 (1964).

[21] D. T. Pegg and S. M. Barnett, J. Opt. B: Quantum Semiclass. Opt. **1**, 442 (1999).

[22] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[23] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **175** (1984).

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology **5**, 3 (1992).

[25] N. Lutkenhaus, Phys. Rev. A **54** (1996).

[26] P. Shor and J. Preskill, Phys. Rev. Lett. **85** (2000).

[27] D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory **49** (2003).

[28] Note1, In principle the denominator here should be replaced by another form in terms of superoperators, corresponding to the probability that the state is not sifted. However, for BB84 specifically this factor is found to be a constant number, which can be shown using Eq. (7). This feature is a relic of sifting in BB84 being conditional upon correlations between bases, not states, which is not true in general. Implicit in the above equation is thus that the probability is conditional upon the state not being sifted, and this should be assumed for all future probabilities.

[29] T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **75**, 042327 (2007).

[30] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[31] H. E. Brandt, Phys. Rev. A **71**, 042312 (2005).

[32] C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[33] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[34] K. Tamaki and N. Lutkenhaus, Phys. Rev. A. **69**, 032316 (2004).

[35] I. Ivanovic, Phys. Lett. A. **123**, 257 (1987).

[36] D. Dieks, Phys. Lett. A. **126**, 303 (1988).

[37] A. Peres, Phys. Lett. A. **128**, 19 (1988).

[38] S. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009).

[39] A. Ekert, B. Huttner, G. Palma, and A. Peres, Phys. Rev. A. **50**, 1047 (1994).

[40] S. J. D. Phoenix, S. M. Barnett, and A. Chefles, Journal of Modern Optics **47**, 507 (2000).

[41] M. Schiavon, G. Vallone, and P. Villoresi, Scientific Reports **6** (2016).

[42] J.-C. Boileau, K. Tamaki, *et al.*, Phys. Rev. Lett. **94**, 040503 (2005).

[43] J. Renes, Phys. Rev. A. **70**, 052315 (2004).

[44] H.-K. Lo and H. Chau, Science **283**, 2050 (1999).

[45] H. Chau, IEEE Trans. Inform. Theory **51**, 1451 (2005).

Alice sends	Eve attack (new state)	Bob measures	Alice announces	Alice bit	Bob bit
ψ_0	0 (ψ_1)	$\overline{\psi}_0$	$\overline{\psi}_1$	0	1
			$\overline{\psi}_2$	1	0
		$\overline{\psi}_2$	$\overline{\psi}_1$	0	0
			$\overline{\psi}_2$	SIFTED	
	1 (ψ_2)	$\overline{\psi}_0$	$\overline{\psi}_1$	0	1
			$\overline{\psi}_2$	1	0
		$\overline{\psi}_1$	$\overline{\psi}_1$	SIFTED	
			$\overline{\psi}_2$	1	1

TABLE I. All rows in this table correspond to equally likely runs of the protocol. The third and eighth rows are those in which all three parties agree, the fourth and seventh are those in which sifting occurs and the rest are those in which disagreement occurs.

Protocol	$P(A = E = B)$		$P(A = E = B \vert A = E)$			
	Type of measurement	Max. Value	Type of measurement	Max. Value	Error rate	QBER
BB84	Probe-entanglement	0.750	Probe-entaglement	1	0.333	0.189
B92	USD	1	Probe-entanglement	1	0.200	0.034
Three-state	Unitary	0.600	Unitary	1	0.666	0.098

TABLE II. Summary of optimal eavesdropping attacks derived in main body of paper. All headers should be easily understood; QBER refers to the maximal tolerable error rate below which the protocol has unconditional security.