Optimized attacks on twin-field quantum key distribution

STEPHEN M. BARNETT[1,*], THOMAS BROUGHAM[1], SARAH CROKE[1], AND SIMON J. D. PHOENIX[2]

[1] School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, UK
[2] Department of Physics, Khalifa University, P.O. Box 127788, Abu Dhabi, UAE
[*] Corresponding author: stephen.barnett@glasgow.ac.uk

Compiled January 11, 2019

In twin-field quantum key distribution the two communicating parties, Alice and Bob, each send a weak coherent pulse to a third party stationed between them. The key bits are generated by interference between these pulses, with the results communicated to Alice and Bob. We consider optimized strategies for eavesdropping on the communication built upon state discrimination and quantum non-demolition measurements. We find that the best strategy comprises a two-step process but that even this does not compromise the security of the protocol.

http://dx.doi.org/10.1364/ao.XX.XXXXXX

1. INTRODUCTION

Quantum key distribution (QKD), the most mature of the fledgling quantum technologies, has been demonstrated in a variety of technical settings [1–7]. Practical implementations include communication using optical fiber [8–11], free-space line of sight communications [12–14] and, most recently, satellite-based quantum communication [15, 16]. A strong motivation for developing satellite QKD is the necessarily limited range of terrestrial schemes: the use of optical fiber, in particular, is inevitably constrained by absorption losses that, due to the nature of quantum states, cannot be compensated by amplification. Attempts to overcome this difficulty have inspired lively activity in the development of quantum repeaters [17, 18] and quantum memories [19, 20].

Protocols for QKD follow a variety of patterns. In the earliest and simplest scheme one party, Alice, sends light pulses along a quantum channel to a receiving party, Bob. The light will usually be in the form of weak coherent pulses or heralded photons, although other schemes are also possible. Another possibility is to use a third party positioned between Alice and Bob who either prepares entangled photons for transmission to Alice and Bob, who receive one each or, as suggested for measurement-device-independent QKD, receives and measures light sent by Alice and Bob [21–23]. Networks with multiple communicating parties are also possible [24, 25].

In twin-field QKD both Alice and Bob prepare and send weak coherent pulses of light, each with a mean photon number of significantly less than one, to a central point operated by a central server [26]. This character was named 'Charlie' in the original paper but we prefer 'Severus' as Charlie has already been assigned numerous other roles in QKD protocols. In contrast to measurement-device-independent schemes, Severus needs to record just a *single* photocount and relay the result of this detection to Alice and Bob. The concept is that Alice and Bob each sends 'half a photon', or rather a corresponding probability amplitude, to Severus who combines these and performs a simple measurement, the result of which he sends to Alice and Bob. Naturally the scheme will be secure only if Severus and any other eavesdropper cannot access the shared key generated by Alice and Bob. To demonstrate this it suffices to consider just the strategies available to a dishonest S *Eve* rus, who plays the role traditionally assigned to the eavesdropper, Eve.

An important advantage of this scheme is that each of Alice and Bob's pulses travels only half the distance between them and hence suffers a significantly smaller loss than it would in a single-transmission scheme in which Alice sends pulses of light to Bob [26].

We present, first, an idealized account of a somewhat simplified twin-field QKD protocol and the principles on which the security is based. Ultimately, a security proof must allow for a technologically advanced Severus to perform the best eavesdropping strategy allowed by quantum theory. Security proofs to date have been based on information theory and evaluating key rates [26–28]. We complement these by determining a range of optimized strategies and evaluate their efficacy. In particular, we obtain an optimal single-shot measurement, i.e. the best attack when Severus is not able to make multi-mode, joint measurements. The result sheds new light on the security of the protocol. It also fits with a growing interest in security analysis under various restrictions on an eavesdropper [29, 30]. We also give an upper bound on the information gain when joint measurements are allowed. The approach given is rather different from security arguments based on entanglement purification. It is an open

question whether there is any connection. We conclude with some important practical considerations that might affect an experimental realization of the protocol.

2. TWIN-FIELD PROTOCOL

Let us turn to the basic protocol for twin-field QKD and start with operation as intended with no eavesdropping and an honest Severus. We neglect also, at this stage, the losses that occur in transmission and due to the finite efficiency of Severus's detectors. Alice and Bob, in each time slot for communication, prepare a weak coherent pulse of light and imprint upon it the phase 0, $\pi/2$, π or $3\pi/2$, chosen at random and with equal probabilities. They send these pulses to Severus through optical fibers. The lengths of these fibers need to be carefully controlled both so that the pulses arrive at Severus at the same time and also so that the phases acquired by the pulses on propagation are known and can be adjusted by Severus. This means that Severus receives from each party and in each time slot a coherent-state pulse for the form $|\alpha e^{in\pi/2}\rangle$, with mean photon number $|\alpha|^2 \ll 1$. We note that such a scheme has been employed successfully for quantum fingerprinting [31, 32] and to establish quantum digital signatures [33]. The use of such states has been considered, also, for direct (Alice to Bob) QKD [34]. Twin-field QKD as originally introduced uses global phase randomization between Alice and Bob [26]; other techniques such as decoy states are also discussed elsewhere [27, 28]. The simplified version of the protocol discussed here is sufficient for our purposes.

Severus is required to combine the two weak pulses on a 50:50 beam splitter as depicted in Figure 1. He then records photodetection events either at detector A (agree) or D (disagree). Owing to the weakness of the pulses, many time slots will produce no detections, but on those occasions when an event is recorded, Severus announces A or D to Alice and Bob. Very occasionally both of Severus's detectors will register counts but such events are simply discarded , as they cannot be used to construct shared bits.

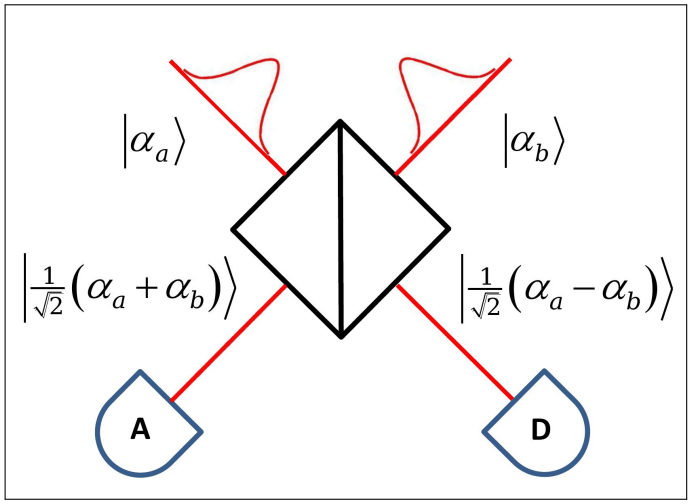

Fig. 1. Severus combines Alice and Bob's coherent pulses on a beamsplitter. If Alice and Bob have used the same basis then one of the outputs will be in the vacuum state, with all of the light going to the other output.

Alice and Bob generate a random key from the sequence of As and Ds announced by Severus as follows. Alice and Bob assign a bit value to their encoding phases: $n = 0, 1$ and $n = 2, 3$ corresponding, respectively, to the bit values 0 and 1. Alice and Bob announce in each time slot for which Severus has announced A or D, whether the real, $|\alpha\rangle$ or $|-\alpha\rangle$, or the imaginary, $|i\alpha\rangle$ or $|-i\alpha\rangle$, basis was used and they keep only those slots for which they have both chosen the real or the imaginary basis. Finally, Alice and Bob's bit values should agree if Severus has announced A and disagree if Severus announced D. When Severus announces D one of the communicating parties, Bob, simply flips the corresponding bit value and the two key strings generated by Alice and Bob should now agree. These possibilities are summarized in Table 1. The secrecy of the communication between Alice and Bob is then established, in common with existing protocols, by checking for errors, followed by a process of privacy amplification. As in other QKD protocols, the existence of errors is associated with dishonest or eavesdropping activity.

Table 1. The possible outcomes for ideal operation of the protocol. Only those cases in which Alice and Bob agree on their choice of basis are included, the remaining eight possibilities are simply discarded.

Alice	Bob	Severus	Bit value agreed
$\|\alpha\rangle$	$\|\alpha\rangle$	A	0
$\|\alpha\rangle$	$\|-\alpha\rangle$	D	0
$\|i\alpha\rangle$	$\|i\alpha\rangle$	A	0
$\|i\alpha\rangle$	$\|-i\alpha\rangle$	D	0
$\|-\alpha\rangle$	$\|-\alpha\rangle$	A	1
$\|-\alpha\rangle$	$\|\alpha\rangle$	D	1
$\|-i\alpha\rangle$	$\|-i\alpha\rangle$	A	1
$\|-i\alpha\rangle$	$\|i\alpha\rangle$	D	1

A crucial question to address is whether a dishonest Severus can defeat the protocol by sharing the key bits without introducing errors into his announcements to Alice and Bob of A and D. To understand the problem facing Severus, let us write the product states for Alice and Bob's pulses in the photon number basis, recalling that the mean photon number is very much less than one. It suffices to consider only those states in which both Alice and Bob chose the real basis ($n = 0, 2$) or the imaginary basis ($n = 1, 3$) as only these can contribute to the final key. We find

$$\begin{aligned} |\alpha e^{in\pi/2}, \alpha e^{in\pi/2}\rangle &\approx |0,0\rangle + e^{in\pi/2}\sqrt{2}\alpha|+\rangle \\ |\alpha e^{in\pi/2}, -\alpha e^{in\pi/2}\rangle &\approx |0,0\rangle + e^{in\pi/2}\sqrt{2}\alpha|-\rangle, \end{aligned} \quad (1)$$

where $|0,0\rangle$ is the two-pulse vacuum state and $|\pm\rangle$ are the single-photon entangled states $2^{-1/2}(|1,0\rangle \pm |0,1\rangle)$. To announce correctly A or D, Severus needs to perform a measurement in the $|\pm\rangle$ basis, but the required key-bit is contained in the incompatible basis given by the superposition of these states with the two-mode vacuum. It follows, in common with other approaches to QKD, that a dishonest Severus has to fight against complementarity.

Furthermore, keeping double click events will not help Severus. Firstly, these events are very rare. Secondly, these events are not useful for constructing shared bits. Moreover, for Severus to try and use the double clicks, he would need to

risk incorrectly announcing agree or disagree, which would necessarily introduce errors into the announcements to Alice and Bob.

The argument presented in the preceding paragraph is indicative of security and information-theoretic security proofs exist in the literature [26, 27]. Nevertheless, an analysis of the attacks available to Severus can offer some insight into the security and assumptions of the protocol. We address this point more fully in the following section, but give here a further indication of Severus's difficulties. We might start by conceding that if there are two or more photons present then this could be used to Severus's advantage. The probability for two or more photons to be present is, for small mean photon number, simply $2|\alpha|^4$, which is proportional to square of the mean photon number. We can make this arbitrarily small by reducing the intensities of Alice and Bob's pulses. Privacy amplification will suppress the small amount of information leaked to Severus in this way. The remaining task for Severus is to do as well as possible in discriminating between the eight states in Equation (1). We may note that these are a multiply symmetric set of states [35] and hence we know that a square-root measurement [7, 36–39] will identify the state with the minimum probability of error, $P_{\text{error}} \approx \frac{7}{8} - \frac{|\alpha|}{2}$ which for small $|\alpha|$ is only marginally better than guessing.

There is a far better strategy that is open to a technologically advanced Severus, one who can perform a first measurement to decide whether to announce A or D and a second to determine the bit-value only *after* Alice and Bob have revealed their basis choice. The best initial measurement available to Severus is a three-element POVM (or POM) with the probability operators

$$\begin{aligned} \hat{\pi}_A &= K|0,0\rangle\langle 0,0| + |+\rangle\langle +| \\ \hat{\pi}_D &= K|0,0\rangle\langle 0,0| + |-\rangle\langle -| \\ \hat{\pi}_X &= (1-2K)|0,0\rangle\langle 0,0|, \end{aligned} \tag{2}$$

for which Severus announces A, D or nothing respectively. Here K is a positive number between 0, corresponding to the behavior of an honest Severus, and $\frac{1}{2}$, for which Severus makes an announcement for every time slot. Adopting this strategy necessarily introduces errors into the announcements made by Severus, with each such announcement, of A or D, being incorrect with probability

$$P_{DA\,\text{error}} = \frac{K}{2(K+|\alpha|^2)} \tag{3}$$

and so to avoid detection by Alice and Bob, K needs to be small, ideally much less than $|\alpha|^2$.

Following Severus's announcement of A or D Alice and Bob announce their basis choices and Severus can then use this additional information to inform his subsequent measurement of the bit value. For definiteness let us consider a case in which Severus has announced (correctly) A and Alice and Bob selected the real basis. This leaves Severus with the task of discriminating between the two states

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{K+2|\alpha|^2}}(\sqrt{K}|0,0\rangle + \sqrt{2}\alpha|+\rangle) \\ |\psi_1\rangle &= \frac{1}{\sqrt{K+2|\alpha|^2}}(\sqrt{K}|0,0\rangle - \sqrt{2}\alpha|+\rangle), \end{aligned} \tag{4}$$

as modified from the states given in Equation (1) by Severus's measurement. The minimum probability of error in distinguishing between these two states is

$$P_{\text{error}} = \frac{1}{2} - \frac{\sqrt{2K}|\alpha|}{K+2|\alpha|^2}. \tag{5}$$

This takes the value zero if $K = 2|\alpha|^2$. In this case Severus will have the potential key bit, but will necessarily reveal his activity through significant errors in the announcements made to Alice and Bob: $P_{DA\,\text{error}} = \frac{1}{3}$.

A more complete assessment of the possible strategies available to Severus requires the introduction of a range of generalized measurements, in particular, unambiguous measurement [7, 38–42], which we consider in the following section.

3. OPTIMIZED MEASUREMENTS AVAILABLE TO SEVERUS

The security of any QKD protocol must be tested against the best measurements possible, ideally to a technologically advanced eavesdropper and establishing this requires the introduction of generalized measurements [43]. In pursuit of the best strategy it suffices to treat, simply, the actions open to a dishonest Severus, as Severus can perfom any action that is also open to an eavesdropper. We note that treating Severus as an unreliable agent is an essential feature of this study, for if Alice and Bob fully trust Severus then a simpler procedure would be to establish separate keys between Alice and Severus and between Bob and Severus. We consider four optimized strategies and for each determine the way in which Severus's probability for success scales with the mean photon number.

A. Minimum error discrimination between the signal states

The simplest strategy, at least conceptually, is for Severus to attempt to discriminate, with minimum error, between the states sent by Alice and Bob. He might try simply measuring Alice and Bob's pulses separately. We note that a single-shot measurement of such phase-shifted coherent states, albeit a non-optimal one, has been reported recently [44]. This means discriminating between the four coherent states, $|\alpha\rangle$, $|i\alpha\rangle$, $|-\alpha\rangle$ and $|-i\alpha\rangle$. These form a symmetric set and it follows that the minimum-error measurement is the square-root measurement [37], with the POVM comprising the four elements

$$\begin{aligned} \pi_n &= \frac{1}{4}\rho^{-1/2}|\alpha e^{in\pi/2}\rangle\langle\alpha e^{in\pi/2}|\rho^{-1/2} \\ \rho &= \frac{1}{4}\sum_{n=0}^{3}|\alpha e^{in\pi/2}\rangle\langle\alpha e^{in\pi/2}|. \end{aligned} \tag{6}$$

For this measurement strategy we find that the probability of correctly determining the state is

$$P_{\text{error}} = 1 - \sum_{n=0}^{3}\frac{1}{16}\langle\alpha e^{in\pi/2}|\pi_n|\alpha e^{in\pi/2}\rangle \approx \frac{3}{4} - \frac{|\alpha|}{2}, \tag{7}$$

to lowest order in $|\alpha|$. It follows that the probabilty for Severus to correctly identify *both* of the pulses is $(\frac{1}{4} + \frac{|\alpha|}{2})^2 \approx \frac{1}{16} + \frac{|\alpha|}{4}$. Clearly this strategy results in a high probability of error and will result in numerous occasions on which Severus will send to Alice and Bob the incorrect assignment, A or D.

A somewhat superior minimum-error strategy would be to ignore those situations in which Alice and Bob used different bases for their pulses and to concentrate on the remaing eight two-pulse signal states that Alice and Bob would seek to use to establish a secret key. These are the states listed in Table 1. For this multiply-symmetric set the square-root measurement is again optimal [35] and we find that the minimum-error probability is

$$P_{\text{error}} = \frac{7}{8} - \frac{|\alpha|}{2}, \tag{8}$$

as may be found simply by applying the square-root measurement to the eight approximate states given in Equation 1. Equivalently the probability that Severus correctly identifies the state and so both sends the correct signal to Alice and to Bob and also learns the bit value is only $\frac{1}{8} + \frac{|\alpha|}{2}$.

B. Unambiguous discrimination between the signal states

A more subtle approach to the problem is to use unambiguous state discrimination, which gives only correct answers at the cost of giving, sometimes, an ambiguous but clearly identified answer [7, 38–42]. The advantage of this approach for a dishonest Severus is that he can simply send a no detection statement to Alice and Bob on those occasions when his measurement gives an inconclusive result. The use of such strategies for quantum eavesdropping was suggested long ago by Peres [45].

Let us begin, as with the minimum-error strategies above, with a direct attempt to determine which of the four possible coherent states were sent by Alice and Bob. The problem, then, is to determine, without error, which of the four coherent states, $|\alpha\rangle$, $|i\alpha\rangle$, $|-\alpha\rangle$ and $|-i\alpha\rangle$, is present. To construct such a measurement we need to find a state-vector for each of these states that is orthogonal to each of the others; the measurement operators (POVM elements) are constructed from these, completed by a fifth measurement operator corresponding to the ambiguous or undetermined result. There is a known least upper bound for the probability, P_D, of successfully determining, amongst a symmetric set, the state without error [46]. For the case at hand this reduces to

$$P_D \leq \min_r \sum_{n=0}^{3} (-i)^{nr} e^{|\alpha|^2(i^n-1)}, \tag{9}$$

where $r = 0, 1, 2, 3$. For our case, it suffices to consider the limit of small $|\alpha|$ for which this expression simplifies to

$$P_D \leq \frac{2}{3}|\alpha|^6, \tag{10}$$

which is proportional to the third power of the mean photon number and hence is very small. We can trace this dependence on $|\alpha|$ to the need to construct four orthogonal states, one corresponding to unambiguously identifying each of the four states. It follows that we need to work with the four-dimensional space spanned by the first four photon number states and the probability associated with the last of these, $|3\rangle$, is proportional to $|\alpha|^6$.

Instead of determining, unambiguously, both Alice and Bob's signal states, it might be better to restrict the set to the eight two-pulse states, given in Equation (1), that can contribute to the key generated by Alice and Bob. The fact that there are eight states to discriminate between tells us that we we need measurement operators corresponding to orthogonal states in an eight-dimensional state space. There is one two-pulse state with no photons, two states with a single photon, and three with two photons. To reach the required eight dimensional space we require, as a minimum, two further states and these must come from the three-photon states. The latter arise with probability proportional to $|\alpha|^6$ and it follows that a successful unambiguous discrimination among these eight states occurs with a probability proportional to $|\alpha|^6$.

It is clear that measuring Alice and Bob's pulses separately, either with minimum error probability or unambiguously, does not provide an effective eavesdropping strategy.

C. Two-stage measurements

Let us consider a more technologically advanced, but dishonest, Severus, one who can perform a first non-destructive measurement with which to decide whether to send to Alice and Bob A or D, then store the light and perform a second measurement, to determine the key bit only *after* Alice and Bob have revealed the basis used.

The first measurement carried out by Severus is to determine which signal, A or D, to send to Alice and Bob. From the setup in Figure 1 it is clear that the natural way to achieve this is by measuring the photon number, for it is detection of light in output A (D) accompanied by the absence of light in output D (A) that correctly identifies the signal to be sent to Alice and Bob. The minimum action required by Severus is to measure, in each of the outputs from the beamsplitter, the vacuum projector and its complement. If this measurement is a quantum non-demolition measurement [47–50] then the light pulse remains available for further measurement and, indeed, a measurement performed after Alice and Bob have announced the basis used.

On those occasions when Alice and Bob have used the same basis the outputs from the beamsplitter, depicted in Figure 1, will be of the form $|\sqrt{2}\alpha e^{in\pi/2}\rangle \otimes |0\rangle$ if Alice and Bob chose the same phase for their pulses and $|0\rangle \otimes |\sqrt{2}\alpha e^{in\pi/2}\rangle$ if they chose phases differing by π. The quantum non-demolition measurement required by Severus, thus, has four measurement operators:

$$\begin{aligned} \pi_0 &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ \pi_A &= (\mathbb{1} - |0\rangle\langle 0|) \otimes |0\rangle\langle 0| \\ \pi_D &= |0\rangle\langle 0| \otimes (\mathbb{1} - |0\rangle\langle 0|) \\ \pi_{AD} &= (\mathbb{1} - |0\rangle\langle 0|) \otimes (\mathbb{1} - |0\rangle\langle 0|). \end{aligned} \tag{11}$$

These correspond, respectively, to the absence of photons, photons in the agree output but none in the disagree output, photons in the disagree output but none in the agree output and, finally, photons in both outputs. For these measurement results, Severus announces 'no detections', A, D or multiple detections, respectively. The measurement on each output is thus a measurement of the vacuum state or its complement; although this is difficult to arrange, we note that a reasonable scheme for such a measurement has been proposed in the context of cavity quantum electrodynamics [51]. It is clear that, ideally realized, this measurement will introduce no errors into Alice and Bob's shared bit string and hence will leave no detectable trace of Severus's subtle attack.

Once Alice and Bob have announced their agreed basis, Severus can perform a second measurement on the stored light pulse. For definiteness, let us consider the case in which Alice and Bob both chose the real basis and sent to Severus the same state (the analysis for the others possible states follows the same line of reasoning). This means that Severus will have announced A and will now have to discriminate between the states $|\sqrt{2}\alpha\rangle$ and $|-\sqrt{2}\alpha\rangle$ or, more precisely, these states with their vacuum components removed. His remaining task, then, is to discriminate between the two states

$$\begin{aligned} |\psi_0\rangle &= \left(1 - e^{-2|\alpha|^2}\right)(\mathbb{1} - |0\rangle\langle 0|)|\sqrt{2}\alpha\rangle \\ |\psi_1\rangle &= \left(1 - e^{-2|\alpha|^2}\right)(\mathbb{1} - |0\rangle\langle 0|)|-\sqrt{2}\alpha\rangle, \end{aligned} \tag{12}$$

corresponding, respectively, to Alice and Bob assigning the key bit 0 or 1.

The two states, $|\psi_0\rangle$ and $|\psi_1\rangle$ are not orthogonal and so perfect discrimination between them is not possible. This means

that Severus has to choose between maximizing the probability of getting the bit value and learning some of the bits for certain but learning nothing about the others. These correspond to the minimum error and the unambiguous discrimination measurements. It is also possible, of course, to adopt an intermediate strategy in which we seek to minimize the error for a given probability of an inconclusive result [52].

The optimal strategies for discriminating between two equiprobable non-orthogonal pure states, either with minimum error or via unambiguous state discrimination are well known [7, 38, 39]. The minimum achievable error is

$$\begin{aligned} P_{\text{error}} &= \frac{1}{2}\left(1-\sqrt{1-|\langle\psi_0|\psi_1\rangle|^2}\right) \\ &= \frac{1}{2}\left(1-\sqrt{1-e^{-4|\alpha|^2}}\right) \\ &\approx \frac{1}{2}-|\alpha|. \end{aligned} \tag{13}$$

This is a significant improvement on the single-step error probability but Severus's information can still be reduced by lowering the mean photon number. For example if $|\alpha|^2 = 0.05$, corresponding to Alice and Bob together contributing on average 0.1 photons per time slot, then this minimum error probability is approximately 0.28 so that Severus will have a 28% error rate in his final key.

An unambiguous measurement will produce either the correct key bit or an inconclusive result and the minimum achievable probability for the inconclusive result is

$$\begin{aligned} P_? &= |\langle\psi_0|\psi_1\rangle| \\ &= e^{-2|\alpha|^2} \approx 1-2|\alpha|^2. \end{aligned} \tag{14}$$

Equivalently, Severus will know a proportion $2|\alpha|^2$ for certain but have to guess the remaining bits. For the example given above, with $|\alpha|^2 = 0.05$, Severus will know 10% of the bits but have to guess the remaining key bits.

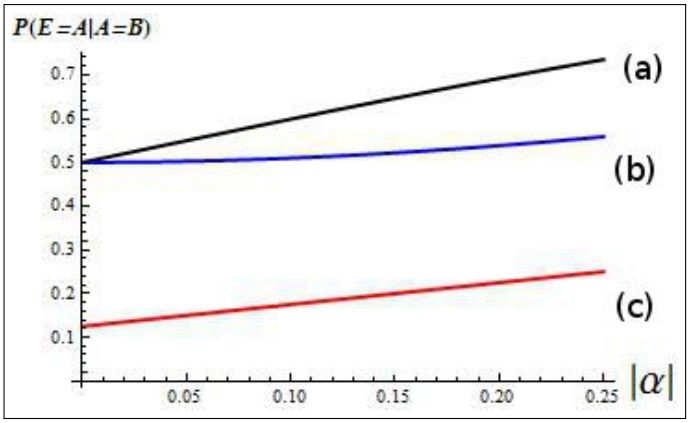

Fig. 2. A plot of $P(E = A|A = B)$, the probability for Severus to gain a bit when Alice and Bob agree on the bit, against the amplitude $|\alpha|$. The plot shows several different attacks. The black line, (a), shows the two-stage attack with an final minimum error measurement. The blue line, (b), is for the two-stage measurement with an unambiguous measurement. The red line, (c) shows a single-stage minimum error attack, which was described in equation (10).

The results are illustrated in figure 2, were we plot $P(E = A|A = B)$, the probability for Severus to gain bit conditioned on Alice and Bob both sharing the bit. The probability $P(E = A|A = B)$ is plotted against the amplitude $|\alpha|$, for: (a) the optimal two-stage attack, (b) a two-stage attack with an unambiguous measurement, and (c) the single-stage attack outlined at the end of section 3A, i.e. in equation (8). We see that for each of the attacks, Severus' probability to gain the bit increases with $|\alpha|$. Furthermore, the plot illustrates the significant advantage of the two-stage attack. Nevertheless, we again see that if we make the amplitude sufficiently small, then we ensure that Severus will have a large error rate in his final key.

The minimum error measurement is also the measurement that extracts the maximum information (i.e. the accessible information) from an ensemble of two equiprobable non-orthogonal pure states [53]. In certain cases, however, one can extract more information by storing the states and making complicated, multimode joint measurement. This approach is optimal for decoding channels, where one can control the input states [54]. Joint measurements also provide an advantage when we have multiple copies of the same state [55]. Whether it provides an advantage in the current situation is an open question. For example, it is know that joint measurements would not help with the problems of minimum error and unambiguous state discrimination [39][1]. Nevertheless, we will give an upper bound on the accessible information, when Severus saves N copies of the output and then makes a joint measurement.

The Holevo bound gives an upper limit on the accessible information, although it is not clear that this value is achievable in our case. For an ensemble of pure states, the Holevo bound is just the von Neumann entropy of the ensemble. For the case of the real basis, one makes a joint measurement on $(\frac{1}{2}|\alpha\rangle\langle\alpha| + \frac{1}{2}|-\alpha\rangle\langle-\alpha|)^{\otimes N}$. The accessible information per pulse, I_S, is found to be upper bounded by

$$I_S \leq -x\log_2(x) - (1-x)\log_2(1-x), \tag{15}$$

where

$$\begin{aligned} x &= \frac{1}{2}(1+|\langle\psi_0|\psi_1\rangle|) \\ &= \frac{1}{2}(1+e^{-2|\alpha|^2}) \approx 1-|\alpha|^2. \end{aligned} \tag{16}$$

The results for a joint measurement on the imaginary basis are identical. In figure 3 we plot this upper bound as a function of $|\alpha|$ and compare it to the information that one can extract by making individual, minimum error measurements. By making $|\alpha|$ small, we again see that one can limit the information that Severus obtains.

4. PRACTICAL CONSIDERATIONS

The protocol described above is much idealized and takes no account of experimental practicalities. Some of these will be specific to a given realization, but others are likely to affect any experiment and we consider, briefly, just three of these: phase stability, detector efficiency and fiber losses.

A. Phase stability

The interference between the weak coherent pulses sent by Alice and Bob lies at the very heart of the protocol and it is essential that the path lengths between Alice and Severus and between Bob and Severus are matched, both so that their pulses arrive at

[1]Joint measurements can help if we have multiple *copies* of a state. But in this case we have multiple copies of identical, but independent ensembles.

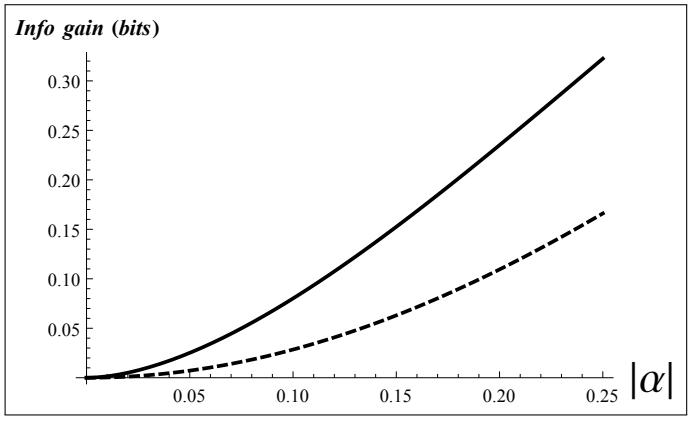

Fig. 3. A plot of the information gain (in bits) or accessible information plotted against the amplitude $|\alpha|$. The solid black line is the upper bound on the accessible information per pulse, obtained using a joint measurement. The dashed black line shows the accessible information for a individual measurement made one each combined pulse, from Alice and Bob.

the same time, but also in order for the combined pulses to combine and end up in the correct photodetector, A or D. Clearly some active stabilization and monitoring will be required. One possibility is that Alice and Bob punctuate the transmission of their weak pulses with more intense pulses with which Severus can make small adjustments to the path lengths as suggested in [26]. There is no doubt, however, that this will be technically demanding and adds to the complexity of the scheme. Failure to control the phases adequately will introduce errors into Alice and Bob's shared bit strings and these will have to be detected and corrected but also, treated as though evidence of eavesdropping with the consequent reduction in key generation rate. It is encouraging, however, that high visibility interference has been demonstrated over 550 km albeit under laboratory conditions [26].

B. Detector efficiency

No photodetector is 100% efficient. This means that Severus will report fewer measurement results than would be expected on the basis of the photon statistics of Alice and Bob's pulses. Ideally, the probability that Severus will record a photon count at one of his detectors given a pulse in the coherent state $|\sqrt{2}\alpha e^{in\pi/2}\rangle$ is, for low photon number, approximately $2|\alpha|^2$. For a photodetector with quantum efficiency η, however, this becomes $2\eta|\alpha|^2$.

A technologically advanced Severus could replace the photodetectors provided by Alice and Bob with prefect ones (at least in principle) with quantum efficiency $\eta = 1$ and in doing so exploit this to obtain additional key data. To see how this works we can compare the operation of the channel by an honest Severus with detectors of efficiency η with a technologically advanced Severus, able to carry out the two-stage strategy employing unambiguous state discrimination, as outlined above. For an honest Severus, the probability that he will make a detection and send to Alice and Bob either A or D, given that they have chosen the same basis is simply

$$P_{\text{honest}} = 2\eta|\alpha|^2. \tag{17}$$

Let us compare this with the operation of a dishonest and technologically advanced Severus. In this case, the probability that Severus's ideal quantum non-demolition measurement shows the presence of photons in one the A or D channels is, for small mean photon number, simply $2|\alpha|^2$. As we have seen, an unambiguous state discrimination measurement following the announcement by Alice and Bob of the bases they used is $P_D = 1 - P_? = 2|\alpha|^2$. It follows that the probability Severus learns the key bit is

$$P_{\text{dishonest}} = 2|\alpha|^2 \times 2|\alpha|^2 = 4|\alpha|^4. \tag{18}$$

By adopting this approach while pretending to be using the inefficient detectors, Severus can gain an advantage by simply announcing an outcome preferentially when his unambiguous measurement clearly identified the state sent. If $\eta < 2|\alpha|^2$ then this procedure will provide Severus with the whole key. Clearly it is highly desirable to provide Severus with high-efficiency detectors and essential to use pulse energies such that $2|\alpha|^2 \ll \eta$.

We note that a related security issue arose in connection with the B92 protocol, built on two non-orthogonal signal states [45, 56] and it is possible that some of the counter measures proposed to deal with this might be adapted to the protocol proposed here. In particular, it has been shown that B92 is secure if one has the ability to perform QND measurements that descriminate between the vacuum, a single photon or multiple photons [57]. Alternatively, one might use an adapted decoy state approach as illustrated in [58].

C. Fiber losses

The optical fibers used to transport the pulses from Alice and Bob to Severus introduce losses associated with absorption. If L is the distance along these fibers between Alice and Bob and κ is the absorption coefficient, then the coherent states of the pulses reaching Severus will be $|\alpha e^{in\pi/2} e^{-\kappa L/4}\rangle$. If a technologically advanced Severus can replace some or all of the optical fiber with a very low-loss channel (ideally lossless) then this would provide him with more light to work with than either Alice or Bob assume. The principle of his attack follows that in our discussion of detector efficiency, with η replaced by $\eta e^{-\kappa L/2}$. If this has to be taken into account then the average energy in Alice and Bob's pulses will have to be further reduced such that

$$2|\alpha|^2 \ll \eta e^{-\kappa L/2}. \tag{19}$$

For large distances this may lead to unacceptably low key rates.

We should note that the issue of transmission losses is common to all protocols based on weak coherent pulses. Consider, for example, the original BB84 protocol [1–7]. In this, Alice sends to Bob weak coherent pulses with the information encoded on the polarization of the pulse. Let the coherent amplitude of the pulse prepared by Alice be $\sqrt{2}\alpha$, so that the mean photon number is the same as in the two pulses prepared by Alice and Bob in our scheme. The mean number of photons in each pulse reaching Bob will be $2|\alpha|^2 e^{-\kappa L}$. If Eve can replace the channel with a lossless one, then she can extract a photon only from those pulses prepared by Alice that contain more than one photon and each time this occurs she can store the photon and measure if after the preparation basis is revealed. The probability for a pulse to contain more than one photon is approximately $2|\alpha|^4$. Thus security against this mode of attack requires that each pulse has a mean photon number

$$2|\alpha|^2 \ll e^{-\kappa L}. \tag{20}$$

Apart from the detector efficiency, this requirement is exponentially more demanding in the losses than the condition given

in Equation (19). It is possible that measures developed to deal with this feature of BB84 may be applicable, also, to the simplified scheme presented here. In particular, the decoy method [4, 59] could be used in a fashion similar to that described in [26–28]. However, it is not clear that a standard decoy state protocol would entirely solve this issue, both for the simplified approach presented here or for more standard twin-field QKD protocols [26]. In particular, a recent attack on twin-field QKD has been proposed that exploits channel losses [60]. The robustness of the protocol to detector inefficiency and fiber losses thus require further investigation.

5. CONCLUSION

Quantum key distribution depends on a quantum channel to connect the communicating parties and the security of the process depends on the quantum nature of the light sent into the channel. Twin-field QKD is based on the interference between pairs of weak coherent pulses combined and measured by a central party. It is essential that we consider this central party as an untrusted intermediary, Severus.

The greatest technical challenge in realizing a practical scheme is probably the control of the relative phases of the pulses sent to Severus by Alice and Bob, although we note that the same difficulty has been overcome over short distances for quantum fingerprinting and quantum digital signatures [32, 33] and the results produced in the initial report are certainly encouraging [26]. The development of measurement-device-independent QKD, with it use of a central server receiving and measuring light from both Alice and Bob [21, 22] provides further cause for optimism.

Exploring the strategies open to Severus requires the use of generalized measurements and we have seen how both minimum error, and unambiguous state discrimination play a role in these strategies. A feature that is distinct from eavesdropping strategies in other QKD protocols is Severus's explicit role in the formation of the key. It is this that underlies the optimal two-step strategies in which he first communicates A or D to Alice and Bob and attempts to recover the key bit later.

The Royal Society (RP150122).

We thank John Jeffers for helpful advice and suggestions.

REFERENCES

1. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer, "Quantum cryptography," Contemp. Phys. **36**, 149-163 (1995).
2. S. J. D. Phoenix and P. D. Townsend, "Quantum cryptography: how to beat the code breakers using quantum mechanics," Contemp. Phys. **36**, 165-195 (1995).
3. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145-195 (2002).
4. G. Van Assche. "Quantum cryptography and secret-key distillation," (Cambridge University Press, 2007).
5. S. Loepp and W. K. Wootters, "Protecting information," (Cambridge University Press, 2007).
6. 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**, 1301-1350 (2009).
7. S. M. Barnett, "Quantum Information" (Oxford University Press, 2009).
8. P. D. Townsend, J. G. Rarity and P. R. Tapster, "Single photon interference in 10km long optical fibre interferometer," Elect. Lett. **29**, 634-635 (1993).
9. P. D. Townsend, J. G. Rarity and P. R. Tapster, "Enhanced single photon fringe visibility in a 10km-long prototype quantum cryptography channel," Elect. Lett. **29**, 1291-1293 (1993).
10. A. Muller, J. Breguet and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1km," Europhys. Lett. **23**, 383-388 (1993).
11. C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30km," Opt. Lett. **20**, 1695-1697 (1995).
12. B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," Opt. Lett. **21**, 1854-1856 (1996).
13. W. T. Butler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt and C. G. Peterson, "Daylight quantum key distribution," Phys. Rev. Lett. **84**, 5652-5655 (2000).
14. R. J. Hughes, W. T. Butler, P. G. Kwiat, S. K. lamoreaux, G. L. Morgan, J. E. Nordholt and C. G. Peterson, "Free-space quantum key distribution in daylight," J. Mod. Opt. **47**, 549-562 (2000).
15. J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Yu, Wang and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," Phys. rev. Lett. **119**, 200501 (2017).
16. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang Y.-M. Huang, L. Dei, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Kiodl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
17. H. J. Kimble,"The quantum internet," Nature **453**, 1023-1030 (2008).
18. N. Sangouard, C. Simon, H. de Riedmatten and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys. **83**, 33-80 (2011).
19. C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup and R. J. Young, "Quantum memories," Eur. Phys. J. D **58**, 1-22 (2010).
20. D. J. Saunders, J. H. D. Munns, T. F. M. Champion, C. Qiu, K. T. Kaczmarek, E. Poem, P. M. Ledingham, I. A. Walmsley amd J. Nunn, "Cavity-enhanced room-temperature brodband Raman memory," Phys. Rev. Lett. **116**, 090501 (2016).
21. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
22. H.-K. Lo, M. Curty and B. Qi, "Measurement-device-independent quantum key distribution," Phys. rev. Lett. **108**, 130503 (2012).
23. S. Parandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Geuring, C. S. Jacobsen and U. L. Andersen, Nature Photon. **9**, 397-402 (2015).
24. P. D. Townsend, S. J. D. Phoenix, K. J. Blow and S. M. Barnett, "Design of quantum cryptography sysetms for passive optical networks," Elect. Lett. **30**, 1875-1876 (1994).
25. S. J. D. Phoenix, S. M. Barnett, P. D. Townsend and K. J. Blow, "Multi-user quantum cryptography on optical networks," J. Mod. Opt. **42**, 1155-1163 (1995).
26. M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400-403 (2018).
27. M. Curty, K. Azuma and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," arXiv:1807.07667 [quant-ph].
28. C. Cui, Z.-Q. Yin, R. Wang, F.-Y. Lu, W. Chen, S. Wang, G.-C. Guo and Z.-F. Han, "Twin-field quantum key distribution without phase post-selection," arXiv:1807.02334 [quant-ph].
29. S. Wehner, C. Schaffner and B. M. Terhal, "Cryptography from Noisy Storage," **100**, 220502 (2008); R. König, S. Wehner and J. Wullschleger, "Unconditional Security From Noisy Quantum Storage,". IEEE Transactions on Information Theory, **58**, 1962 (2012); C. Schaffner, "Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model.", Phys. Rev. A, **82**, 032308 (2010).
30. C. Lupo, and S. Lloyd, "Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate," Phys. Rev. Lett. **113**, 160502 (2014); S.

Pironio, L. Masanes, A. Leverrier, and A. Acin, “Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model.” Phys. Rev. X, **3**, 031007 (2013); N. Hosseinidehaj, N. Walk, and T. C. Ralph, “Optimal realistic attacks in continuous-variable quantum key distribution,” arXiv:1811.05562 (2018).
31. J. M. Arrazola and N. Lütkenhaus, “Quantum fingerprinting with coherent states and a constant mean number of photons," Phys. Rev. A **89**, 062305 (2014).
32. F. Xu, J. M. Arrazola, K. Wei, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus and H.K. Lo, “Experimental quantum fingerprinting with weak coherent pulses," Nature Comms. **6**, 8735 (2015).
33. P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson and G. S. Buller, “Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light,” Nature Comms. **3**, 1174 (2012).
34. P. Papanastasiou, C. Lupo, C. Weedbrook and S. Pirandola, “Quantum key distribution with phase-encoded coherent states: asymptotic security analysis in thermal-loss channels,” Phys. Rev. A **98**, 012340 (2018).
35. S. M. Barnett, “Minimum-error discrimination between multiply symmetric states," Phys. Rev. A **64**, 030303(R) (2001).
36. P. Hausladen and W. K. Wootters, “A ‘pretty good’ measurement for distinguishing quantum states,” J. Mod. Opt. **41**, 2385-2390 (1994).
37. M. Ban, K. Kurokawa, R. Momose and O. Hirota, “Optimum measurements for discrimination among symmetric quantum states and parameter estimation," Int. J. Theo. Phys. **36**, 1269-1287 (1997).
38. A, Chefles, “Quantum state discrimination,” Contemp. Phys. **41**, 201-424 (2000).
39. S. M. Barnett and S. Croke, “Quantum state discrimination,” Adv. Opt. Photon. **1**, 238-278 (2009).
40. I. D. Ivanovic, “How to differentiate between non-orthogonal states,” Phys. Lett. A **123**, 257-259 (1987).
41. D. Dieks, “Overlap and distinguishability of quantum states,” Phys. Lett. A **126**, 303-306 (1988).
42. A. Peres, “How to differentiate bewteen non-orthogonal states,” Phys. Lett. A **128**, 19-19 (1988).
43. N. Lütkenhaus, “Security against eavesdropping in quantum cryptography,” Phys. Rev. A **54**, 97-111 (1996).
44. M. DiMario, E. Carrasco, R. A. Jackson and F. E. Becerra, “Implementation of a single-shot receiver for quaternary phase-shift keyed coherent states,” J. Opt. Soc. Am. B **35**, 568-574 (2018).
45. A. Peres, “Memo on non-destructive eavesdropping,” unpublished (c.1994).
46. A. Chefles and S. M. Barnett, “Optimum unambiguous discrimination between linearly independent symmetric states,” Phys. Lett. A **250**, 223-229 (1998).
47. N. Imoto, H. A. Haus and Y. Yamamoto, “Quantum nondemolition measurement of the photon number via the optical Kerr effect,” Phys. Rev. A **32**, 2287-2292 (1985).
48. V. B. Braginsky and F. Ya. Khalili, “Quantum measurement,” (Cambridge University Press, 1992).
49. P. Grangier, J. A. Levenson and J.-P. Poizat, “Quantum non-demolition measurements in optics,” Nature **396** 537-542 (1998).
50. M. O. Scully and M. S. Zubairy, “Quantum optics,” (Cambridge University Press, 1997).
51. D. K. L. Oi, V. Potoček and J. Jeffers, “Nondemolition measurement of the vacuum state or its complement,” Phys. Rev. Lett. **110**, 210504 (2013).
52. A. Chefles and S. M. Barnett, “Strategies for discriminating between non-orthogonal quantum states,” J. Mod. Opt. **45**, 1295-1302 (1998).
53. L. B. Levitin, in Workshop on Physics and Computation: PhysComp 92, edited by D. Matzke (IEEE Computer Society Press, Los Alamitos, CA, 1993).
54. M. M. Wilde, “Quantum Information Theory,” (Cambridge University Press, 2013).
55. A. Peres and W. K. Wootters, “Optimal detection of quantum information,” Phys. Rev. Lett. **66**, 1119 (1991).
56. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett. **68**, 3121-3124 (1992).
57. K. Tamaki and N. Lütkenhaus, “Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel,” Phys. Rev. A **69**, 032316 (2004).
58. M. Lucamarini, G. Di Giuseppe and K. Tamaki, “Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states,” Phys. Rev. A **80**, 032327 (2009).
59. W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication,” Phys. Rev. Lett. **91**, 057901 (2003).
60. X.-B. Wang, X. -L. Hu and Z.-W. Yu, “Effective Eavesdropping to Twin-Field Quantum Key Distribution,” arXiv:1805.02272 (2018).