Foiling zero-error attacks against coherent-one-way quantum key distribution

Marcos Curty
Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain

To protect practical quantum key distribution (QKD) against photon-number-splitting attacks, one could measure the coherence of the received signals. One prominent example that follows this approach is coherent-one-way (COW) QKD, which is commercially available. Surprisingly, however, it has been shown very recently that its secret key rate scales quadratically with the channel transmittance, and, thus, this scheme is unsuitable for long-distance transmission. This result was derived by using a zero-error attack, which prevents the distribution of a secure key without introducing any error. Here, we study various countermeasures to foil zero-error attacks against COW-QKD. They require to either monitor some additional available detection statistics, or to increase the number of quantum states emitted. We obtain asymptotic upper security bounds on the secret key rate that scale close to linear with the channel transmittance, thus suggesting the effectiveness of the countermeasures to boost the performance of this protocol.

I. INTRODUCTION

Quantum key distribution (QKD) allows two remote users (typically called Alice and Bob) to share a symmetric key with information-theoretic security [1–3]. This key is the essential resource of the one-time-pad cryptosystem [4], the only known solution that guarantees confidential communication without resorting to computational complexity assumptions.

Since its first theoretical proposal [5, 6], several QKD protocols have been introduced [7–22] and implemented [23–36] in the last two decades, each of them with their own merits. Recent experimental advances in QKD include, for instance, the deployment of QKD networks based on trusted nodes [37–40], the distribution of secret keys over 600 km of optical fibre [41], and the demonstration of satellite-based QKD links [42, 43].

Distributed-phase-reference (DPR) QKD [8–10, 29–32] is a type of QKD protocols in which Alice and Bob check the coherence of the received optical pulses. This approach has triggered great attention in recent years because it held the promise to provide a secret key rate that scales linearly with the system’s transmittance, $\eta_{\text{sys}}$, by using a simple experimental setup. This is the best possible scaling for point-to-point QKD links [44, 45]. DPR-QKD includes the commercially available [46] coherent-one-way (COW) QKD scheme [10, 30, 31], which has been demonstrated over 300 km of optical fibre [32]. Surprisingly, however, very recently it has been shown that COW-QKD provides a secret key rate that scales quadratically with $\eta_{\text{sys}}$ [47, 48], which implies that all of its experimental implementations reported so far in the scientific literature are insecure. This matches the scaling of the lower security bounds against general attacks presented in [49], and renders COW-QKD unsuitable for long-distance QKD transmission.

The results in [47, 48] use a special type of zero-error attack [50, 51], in which the eavesdropper (Eve) measures out all the signals sent by Alice one by one, and then resends Bob new signals (whose state might depend on all her measurement results) that do not introduce any error. For this, Eve exploits two special properties of the signals emitted in COW-QKD. First, they are linearly independent, which means that they can be identified with an unambiguous state discrimination (USD) measurement [52–54]. And, second, they include vacuum pulses, which naturally break the coherence between adjacent pulses. Such attack transforms the quantum channel into an entanglement breaking channel and, therefore, it does not allow the distribution of a secure key [55].

In this paper, we evaluate the effectiveness of three possible countermeasures to foil zero-error attacks against COW-QKD and, thus, boost the performance of this protocol. For this, we consider the zero-error attack introduced in [48], which is optimal when Eve measures Alice’s signals one by one, and it outperforms previous approaches [47, 50, 51]. For each countermeasure analyzed, we derive asymptotic upper security bounds and compare our results with those corresponding to the original COW-QKD scheme.

The first two countermeasures do not require to modify the experimental setup of COW-QKD. Instead, Alice and Bob need to monitor additional detection statistics of Alice’s signals at Bob’s side, besides the standard quantum bit error rate (QBER) and the visibilities prescribed in the original COW-QKD scheme. This includes the monitoring of the number of coincidences (i.e., those detection events in which Bob observes a simultaneous “click” both in his data and monitoring lines), as well as the detection rates of Alice’s signals at Bob’s data line. This is so because zero-error attacks typically modify these quantities greatly, when compared to their expected values in the absence of Eve. The third countermeasure contemplates the scenario in which Alice increases the number of emitted signals by adding a vacuum signal [50]. In doing so, it now becomes harder for Eve to unambiguously identify the state of the signals emitted. We show that these countermeasures could be quite effective to protect COW-QKD against zero-error attacks.

The paper is organized as follows. In Sec. II, we introduce COW-QKD. In Sec. III, we review briefly the opti-
FIG. 1: Alice uses a laser, together with an intensity modulator (IM), to randomly prepare the signals \(|\varphi_0\rangle = |0\rangle|\alpha\rangle\), \(|\varphi_1\rangle = |\alpha\rangle|0\rangle\) and \(|\varphi_2\rangle = |\alpha\rangle|\alpha\rangle\). At Bob’s side, a beamsplitter (BS) of transmittance \(t_B\) distributes the incoming signals between the data and the monitoring lines. The latter consists of a Mach-Zehnder interferometer. In the figure: \(|0\rangle\) (|\alpha\rangle\) is a vacuum state (coherent state); \(\Delta t\) denotes the time delay the two pulses within a signal; \(D_d\), \(D_M_1\) and \(D_M_2\) are single-photon detectors.

II. COHERENT-ONE-WAY QKD

Fig. 1 shows the basic setup of the original COW-QKD scheme [10, 30]. Alice sends Bob a sequence of signals \(|\varphi_0\rangle = |0\rangle|\alpha\rangle\), \(|\varphi_1\rangle = |\alpha\rangle|0\rangle\) and \(|\varphi_2\rangle = |\alpha\rangle|\alpha\rangle\) that she selects at random each given time, where \(|0\rangle\) (|\alpha\rangle\) represents a vacuum (coherent) state. The signals \(|\varphi_i\rangle\), with \(i = 0, 1\), encode a bit value \(i\) and are used for key generation. The decoy signal \(|\varphi_2\rangle\), on the other hand, is used to test for eavesdropping. These signals are generated by Alice with a priori probabilities

\[
p_{|\varphi_0\rangle} = p_{|\varphi_1\rangle} = \frac{1-f}{2}, \quad p_{|\varphi_2\rangle} = f,
\]

with \(0 < f < 1\).

At Bob’s receiver, he uses a beamsplitter of transmittance \(t_B\) to randomly distribute the incoming signals into two possible lines: the data line and the monitoring line. The former measures the signals with a single-photon detector \(D_d\). Bob can distinguish the two key generation signals \(|\varphi_i\rangle\), with \(i = 0, 1\), based on the time slot in which \(D_d\) reports a detection “click”. Precisely, if he observes a “click” in the first (second) time slot of a signal, then he considers that it is \(|\varphi_0\rangle\) (|\varphi_1\rangle). If there is a double “click” (i.e., a “click” in both time slots), Bob assigns a random bit value to it. The monitoring line tests the coherence between adjacent pulses. This is done by means of a Mach-Zehnder interferometer followed by two single-photon detectors \(D_M_1\) and \(D_M_2\). The interferometer is arranged such that say \(D_M_2\) never produces a detection “click” when the state of the two adjacent pulses is |\alpha\rangle.

Once the quantum phase of the protocol ends, Bob announces over an authenticated classical channel which signals produced a “click” in his data line. Also, Alice announces which detected signals correspond to key generation signals (but without revealing their state |\varphi_i\rangle). The respective bit values associated to such signals form Alice and Bob’s sifted key. In addition, they estimate the QBER in the sifted key, as well as the visibilities \(V_j\) observed in the monitoring line. These visibilities are defined as

\[
V_j = \frac{p_{\text{click}}(D_{M1}|j) - p_{\text{click}}(D_{M2}|j)}{p_{\text{click}}(D_{M1}|j) + p_{\text{click}}(D_{M2}|j)},
\]

where the index \(j\) is \{“01”, “02”, “10”, “11”\} identifies the five possible signal combinations in which there are two adjacent coherent states |\alpha\rangle. For instance, \(V_2\) refers to the interference between the two adjacent states |\alpha\rangle in |\varphi_2\rangle = |\alpha\rangle|\alpha\rangle\), \(V_0\) considers the interference between the two adjacent states |\alpha\rangle in |\varphi_0\rangle|\varphi_1\rangle = |0\rangle|\alpha\rangle|0\rangle\), and the other cases are defined similarly. In Eq. (2), \(p_{\text{click}}(D_{M1}|j)\) denotes the conditional probability to observe a “click” in \(D_{M1}\) that corresponds to the interference of two adjacent coherent states |\alpha\rangle when they are situated within a signal combination \(j\).

When the QBER (the visibilities \(V_j\) is (are) above (below) a certain threshold, no secret key can be distilled from the sifted key [32, 49], being the ideal noiseless case that where QBER = 0 and \(V_j = 1\) for all \(j\).

III. ZERO-ERROR ATTACK AGAINST COW-QKD

Here, we briefly review the zero-error attack introduced in [48], which is optimal when Eve measures Alice’s signals one by one. The key idea is rather simple. First, Eve measures out each of Alice’s signals with an optimal USD measurement [52-54]. Afterwards, she resends Bob all those blocks of signals that contain consecutive correctly identified signals, and whose first and last optical pulses are prepared in a vacuum state. In addition, Eve replaces the states |\alpha\rangle within such blocks with coherent states |\beta\rangle with \(\beta \gg \alpha\). By selecting \(\beta\) large enough, she can guarantee that each state |\beta\rangle will produce a detection “click” at Bob’s data line with basically unit probability.

It is easy to show that this eavesdropping strategy does not introduce any error in Bob’s data line nor it decreases the visibilities in his monitoring line. Indeed, since Eve’s USD measurement never misidentifies Alice’s signals, we have that QBER = 0 and the visibilities related to the signals inside the blocks are perfect. Moreover, since the blocks start and end with correctly identified vacuum pulses, the visibilities remain perfect also in the borders of the blocks, independently of the signals that precede and follow them (and for which Eve obtained an incon-
essentially negligible even for moderate values of than cause when the intensity of Alice’s signals is small (as is block containing G of the maximum length of the blocks of signals that Eve re-
of $M$ provides a conclusive result. The quantity $p$ where
experimental implementation of COW-QKD exceeds $G_{\text{zero}}$. Alice and Bob cannot generate a secure key. This is so because the observed data could be explained as coming from an entanglement breaking channel, and thus they do not share quantum correlations [55].

The parameter $G_{\text{zero}}$ can be written as [48]

$$G_{\text{zero}} = \frac{1 - p_c}{1 - p_c^{M_{\text{max}} + 1}} \left[ \sum_{k=2}^{M_{\text{max}}} p_c^k (1 - p_c) p_{\text{click}}(k) + p_c^{M_{\text{max}}} p_{\text{click}}(M_{\text{max}}) \right],$$

where $p_c$ is the probability that Eve’s USD measurement provides a conclusive result. The quantity $M_{\text{max}}$ refers to the maximum length of the blocks of signals that Eve resends to Bob. In principle, $M_{\text{max}}$ can be chosen arbitrary large. In practice, however, even relatively small values of $M_{\text{max}}$ (e.g., say $M_{\text{max}} = 10$) are sufficient to basically achieve the maximum possible value of $G_{\text{zero}}$. This is because when the intensity of Alice’s signals is small (as is the case in COW-QKD), the probability to obtain more than $M_{\text{max}}$ consecutive conclusive measurement results is essentially negligible even for moderate values of $M_{\text{max}}$. Finally, $p_{\text{click}}(k)$ denotes the average number of “clicks” observed by Bob in his data line when Eve sends him a block containing $k$ correctly identified signals (see Fig. 2).

The quantity $p_{\text{click}}(k)$ can be written as [48]

$$p_{\text{click}}(k) = \sum_{j=0}^{2} p(j|c) p_{\text{click}}(k|j),$$

where $p(j|c)$ denotes the conditional probability that Eve obtains the result $|\varphi_j\rangle$, with $j = 0, 1, 2$, given that her USD measurement is conclusive, and $p_{\text{click}}(k|j)$ refers to the average number of “clicks” observed by Bob in his data line when Eve sends him a block with $k$ correctly identified signals and the first signal of the block is in the state $|\varphi_j\rangle$.

The probabilities $p(j|c)$ are given by

$$p(0|c) = p(1|c) = \frac{(1 - f) q_s}{2 p_c},$$

$$p(2|c) = 1 - p(0|c) - p(1|c) = 1 - \frac{(1 - f) q_s}{p_c},$$

where $q_s$ refers to the probability that Eve obtains a conclusive result when she measures a key generation signal $|\varphi_j\rangle$, with $j = 0, 1$.

By calculating $p_{\text{click}}(k|j)$ and explicitly computing Eq. (4), it has been shown in [48] that $p_{\text{click}}(k)$ can be expressed as

$$p_{\text{click}}(k) = \frac{1}{p(0|c)} \left\{ -1 + (k + 1) p(0|c) + [1 - 2 p(0|c)]^k [1 + (k - 1) p(0|c)] \right\},$$

for any $k \geq 2$.

Most experimental implementations of COW-QKD satisfy

$$\sqrt{\frac{f}{2(1 - f)}} \leq e^{-\frac{\mu}{2}},$$

where $\mu = |\alpha|^2$ is the intensity of Alice’s signals. In this scenario, the parameters $p_c$ and $q_s$ have the form [48]

$$q_s = 1 - e^{-\mu},$$

$$p_c = (1 - f)(1 - e^{-\mu}).$$

By combining Eqs. (5)-(8), we find that

$$p(0|c) = p(1|c) = \frac{1}{2}, \quad \text{and} \quad p(2|c) = 0.$$

That is, Eve’s optimal USD measurement does not identify decoy signals. Or to put it in other words, in this situation Eve resends Bob blocks of signals that contain only key generation signals $|\varphi_i\rangle$, with $i = 0, 1$.

IV. MONITORING COINCIDENCES

In this section, we study a first possible countermeasure against the zero-error attack described above. Precisely, this countermeasure exploits the fact that Eve sends Bob coherent states of very high intensity $|\beta|^2$ (with $\beta \gg |\alpha|$) to maximise the gain $G_{\text{zero}}$. In doing so, she can assure that the signals that are correctly identified by her USD measurement will produce a “click” at Bob’s data...
line with basically unit probability. However, if $|\beta|^2$ is too large, these signals will produce coincidence detection events. These are events in which Bob observes a simultaneous detection “click” (within the time duration of an optical pulse emitted by Alice) both in the data and monitoring lines. Therefore, Alice and Bob could monitor such coincidence detection events to detect Eve’s zero-error attack. To put it in other words, to remain undetected, Eve should send weaker optical pulses to Bob, and thus $G_{\text{zero}}$ will decrease.

This countermeasure implicitly assumes the trusted device scenario, where Eve cannot modify the properties of Bob’s measurement device. This might be a reasonable assumption for many practical situations, and is the scenario that we consider below. If Eve could change, say, the detection efficiency of Bob’s detectors together with the transmittance $t_B$, then monitoring coincidence detection events would not translate into relevant restrictions on her capabilities. This is so because, in that case, even single-photon pulses sent by Eve could produce a “click” at Bob’s data line with essentially unit probability.

We shall define the coincidence gain of a zero-error attack, which we denote by $G_{\text{zero}}$, as the probability that Bob observes a coincidence detection event per signal sent by Alice. By following the same procedure used in [48] to derive Eq. (3), it is straightforward to show that $G_{\text{zero}}$ can be written as

$$G_{\text{zero}} = \frac{1 - p_c}{1 - p_c^{M_{\text{max}} + 1}} \left[ \sum_{k=2}^{M_{\text{max}}} p_c^k (1 - p_c) p_{\text{coin}}(k) \right] + p_c^{M_{\text{max}}} p_{\text{coin}}(M_{\text{max}}),$$

where $p_{\text{coin}}(k)$ represents the average number of coincidence detection events observed by Bob when Eve sends him a block containing $k$ correctly identified signals. This latter parameter can be expressed as

$$p_{\text{coin}}(k) = \sum_{j=0}^{2} p(j|c) p_{\text{coin}}(k|j),$$

where $p_{\text{coin}}(k|j)$ is the average number of coincidence detection events observed by Bob when Eve sends him a block containing $k$ correctly identified signals and the first signal of the block is in the state $|\varphi_j\rangle$.

If the condition given by Eq. (7) holds, which is the experimental parameter regime in which we are interested, then from Eq. (9)-(11) we have that

$$p_{\text{coin}}(k) = \frac{1}{2} \left[ p_{\text{coin}}(k|0) + p_{\text{coin}}(k|1) \right].$$

Similarly, from Eqs (4)-(9), we have that the parameter $p_{\text{click}}(k)$ required to calculate $G_{\text{zero}}$, can be written as

$$p_{\text{click}}(k) = \frac{1}{2} \left[ p_{\text{click}}(k|0) + p_{\text{click}}(k|1) \right].$$

**FIG. 3:** The non-vacuum optical pulses within a block of correctly identified signals that Eve resends to Bob are either surrounded by vacuum pulses (as shown in case (a) in the figure) or they have, at most, one adjacent non-vacuum pulse (as shown in case (b) in the figure). A grey (white) oval, drawn with a solid line, represents a non-vacuum (vacuum) optical pulse.

**A. Signals sent by Eve**

Due to the fact that Eve’s optimal USD measurement does not identify decoy signals when Eq. (7) holds, all blocks of signals that Eve resends to Bob satisfy the following property: The non-vacuum optical pulses within the block are either surrounded by vacuum pulses or they have, at most, one adjacent non-vacuum pulse. This is illustrated in Fig. 3.

The former case arises, for instance, when Eve’s correctly identified adjacent signals are in the same state $|\varphi_j\rangle$, with $j = 0, 1$. We shall call these non-vacuum optical pulses as individual, and we will denote their quantum state as $|\Phi_{\text{ind}}\rangle$. The latter case arises when Eve’s correctly identified adjacent signals are in the state $|\varphi_0\rangle|\varphi_1\rangle$. We shall call these non-vacuum optical pulses as double, and we will denote their joint quantum state as $|\Phi_{\text{double}}\rangle$.

We can always write the state $|\Phi_{\text{ind}}\rangle$ as

$$|\Phi_{\text{ind}}\rangle = \sum_{n=0}^{\infty} q_n |n\rangle,$$

where $\sum_{n=0}^{\infty} |q_n|^2 = 1$, and $|n\rangle$ is a Fock state with $n$ photons. That is, Eq. (14) simply expresses a general pure state $|\Phi_{\text{ind}}\rangle$ in the Fock basis.

In the case of double non-vacuum optical pulses, Eve must preserve the coherence between the two pulses. The
mode that preserves such coherence has the form [50]
\[ a_{12}^\dagger = \frac{a_1^\dagger + a_2^\dagger}{\sqrt{2}} \] (15)

where \( a_i^\dagger \), with \( i = 1, 2 \), denotes the creation operator of photons in the time instants associated to the two non-vacuum pulses. This means, in particular, that \( |\Phi^{\text{double}}\rangle \) can be expressed as
\[ |\Phi^{\text{double}}\rangle = \sum_{n=0}^\infty p_n |n\rangle, \] (16)

where \( \sum_{n=0}^\infty |p_n|^2 = 1 \) and \( |n\rangle = (a_1^\dagger a_2^\dagger)^n/\sqrt{n!} |0\rangle \) is a Fock state with \( n \) photons in total in the two non-vacuum pulses.

In the next section we calculate the parameters \( p_{\text{click}}(k|j) \) and \( p_{\text{coin}}(k|j) \), with \( j = 0, 1 \), that are needed to evaluate Eqs. (12)-(13).

B. Probabilities \( p_{\text{click}}(k|j) \) and \( p_{\text{coin}}(k|j) \)

For simplicity, in the calculations below, and also in other sections of this paper, we shall disregard the effect of the dark counts of Bob’s detectors.

1. Probabilities \( p_{\text{click}}(k|1) \) and \( p_{\text{coin}}(k|1) \)

This scenario is illustrated in Fig. 4. Since the first signal of the block is \( |\varphi_1\rangle \), and the first optical pulse of this signal is a vacuum pulse, the longest sub-block that starts and ends with vacuum pulses (if there is any) must include this signal \( |\varphi_1\rangle \). Now, there are two options, depending on the state of the signal located in the \( k \)th position of the block. If this signal is \( |\varphi_0\rangle \), which happens with probability \( p(0|c) = 1/2 \), then the block starts and ends with vacuum pulses, and Eve sends this block to Bob. We shall call this block as a sub-block of the type “01”. It is illustrated in Fig. 4 with a grey dashed rectangle. On the other hand, if the signal in the \( k \)th position of the block is \( |\varphi_1\rangle \), which happens with probability \( p(1|c) = 1/2 \), then the block ends with a non-vacuum optical pulse. Therefore, Eve replaces the signal \( |\varphi_1\rangle \) with a vacuum signal \( |\varphi_{\text{vac}}\rangle \). In doing so, she guarantees that the block now ends with a correctly identified vacuum pulse (which corresponds to the first optical vacuum pulse in \( |\varphi_1\rangle \)). We shall refer to this sub-block as being of the type “11”, and is illustrated in Fig. 4 also with a grey dashed rectangle.

We define the parameters \( N_{\text{ind}}^{\text{01}}(k) \) \( (N_{\text{01}}^{\text{double}}(k)) \) as the average number of individual \( (\text{double}) \) non-vacuum optical pulses (see Fig. 3) contained in a sub-block of signals of the type “01” that Eve obtains from a block with \( k \) correctly identified signals. Likewise, we define the analogous parameters \( N_{\text{ind}}^{\text{11}}(k) \) and \( N_{\text{11}}^{\text{double}}(k) \) for the sub-blocks of signals of the type “11”. These parameters are calculated in Appendix A, and their values are provided in Table I.

Putting all together, we find that the probability \( p_{\text{click}}(k|1) \) can be written as
\[ p_{\text{click}}(k|1) = p(0|c) [N_{\text{ind}}^{\text{01}}(k) P_{\text{click}} + N_{\text{01}}^{\text{double}}(k) P_{\text{click}}^{\text{double}}] + p(1|c) [N_{\text{ind}}^{\text{11}}(k) P_{\text{click}} + N_{\text{11}}^{\text{double}}(k) P_{\text{click}}^{\text{double}}] \]
\[ = \frac{1}{2} \left[ [N_{\text{ind}}^{\text{01}}(k) + N_{\text{ind}}^{\text{11}}(k)] P_{\text{click}}^{\text{double}} + [N_{\text{01}}^{\text{double}}(k) + N_{\text{11}}^{\text{double}}(k)] P_{\text{click}}^{\text{double}} \right], \]
(17)

where in the second equality we have used the fact that \( p(0|c) = p(1|c) = 1/2 \). The quantity \( P_{\text{click}}^{\text{double}} \) denotes the average number of “clicks” observed by Bob in his data line when Eve sends him an individual \( (\text{double}) \) non-vacuum optical pulse. These quantities can be cal-
and $p$ (drawn with a solid line) denote optical pulses. The signals in position of the block with a signal \( \phi \) containing two optical pulses, while small ovals (drawn with a solid line) denote optical pulses. The signals in the first \( k \) positions of the block correspond to the correctly identified signals, while the signal located in the \( k + 1 \)th position of the block is a vacuum signal \( |\varphi_{\text{vac}}\rangle = |0\rangle \langle 0| \). Eve replaces the signal \( |\varphi_{\text{0}}\rangle \) in the first position of the block with a signal \( |\varphi_{\text{vac}}\rangle \) to guarantee that the resulting sub-block starts with a correctly identified vacuum pulse. Now, there are two options, depending on the state of the signal located in the \( k \)th position. With probability \( p(0|c) = 1/2 \) (\( p(1|c) = 1/2 \)) this signal is \( |\varphi_{\text{0}}\rangle \) (|\varphi_{\text{1}}\rangle). If it is \( |\varphi_{\text{1}}\rangle \). Eve also replaces this signal with a vacuum signal \( |\varphi_{\text{vac}}\rangle \) to guarantee that the resulting sub-block ends with a correctly identified vacuum pulse. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.

2. Probabilities $p_{\text{click}}(k|0)$ and $p_{\text{coin}}(k|1)$

The procedure to obtain $p_{\text{click}}(k|0)$ and $p_{\text{coin}}(k|1)$ is completely analogous to that used to calculate $p_{\text{click}}(k|1)$ and $p_{\text{coin}}(k|1)$ in Sec. IV B 1, and, for simplicity, we omit the details here. This scenario is illustrated in Fig. 5. We find that

$$p_{\text{click}}(k|0) = \frac{1}{2} \left\{ N_{10}^\text{ind}(k) + N_{00}^\text{ind}(k) \right\} p_{\text{click}}^\text{ind} + \frac{1}{2} \left\{ N_{10}^\text{double}(k) + N_{00}^\text{double}(k) \right\} p_{\text{click}}^\text{double},$$

$$p_{\text{coin}}(k|0) = \frac{1}{2} \left\{ N_{10}^\text{ind}(k) + N_{00}^\text{ind}(k) \right\} p_{\text{coin}}^\text{ind} + \frac{1}{2} \left\{ N_{10}^\text{double}(k) + N_{00}^\text{double}(k) \right\} p_{\text{coin}}^\text{double},$$

where the parameters $N_{10}^\text{ind}(k)$ and $N_{00}^\text{ind}(k)$ ($N_{10}^\text{double}(k)$ and $N_{00}^\text{double}(k)$) refer to the sub-blocks of the type “00” (“10”) illustrated in Fig. 5. Their values are also provided in Table I.

C. Parameters $P_{\text{click}}^\text{ind}$, $P_{\text{click}}^\text{double}$, $P_{\text{coin}}^\text{ind}$ and $P_{\text{coin}}^\text{double}$

It can be shown (see Appendix B) that when the state $|\Phi^\text{ind}\rangle$ given by Eq. (14) enters Bob’s receiver surrounded by vacuum pulses, the parameters $P_{\text{click}}^\text{ind}$ and $P_{\text{coin}}^\text{ind}$ have

$$P_{\text{click}}(k|0) = \frac{1}{2} \left\{ N_{10}^\text{ind}(k) + N_{00}^\text{ind}(k) \right\} p_{\text{click}}^\text{ind} + \frac{1}{2} \left\{ N_{10}^\text{double}(k) + N_{00}^\text{double}(k) \right\} p_{\text{click}}^\text{double},$$

$$P_{\text{coin}}(k|0) = \frac{1}{2} \left\{ N_{10}^\text{ind}(k) + N_{00}^\text{ind}(k) \right\} p_{\text{coin}}^\text{ind} + \frac{1}{2} \left\{ N_{10}^\text{double}(k) + N_{00}^\text{double}(k) \right\} p_{\text{coin}}^\text{double}.$$
the form
\[ P_{\text{click}}^\text{ind} = 1 - \sum_{n=0}^{\infty} |q_n|^2 \left( 1 - t_B \eta_{\text{det}} \right)^n, \]
\[ P_{\text{coin}}^\text{ind} = 1 - \sum_{n=0}^{\infty} |p_n|^2 \left\{ \left[ 1 - (1 - t_B) \eta_{\text{det}} \right]^n + (1 - \eta_{\text{det}} t_B)^n - \left[ 1 - (1 + t_B) \eta_{\text{det}} \right]^n \right\}. \] (20)

Similarly, when the state \( \Phi^\text{double} \) given by Eq. (16) enters Bob’s receiver surrounded by vacuum pulses, the parameters \( P_{\text{click}}^\text{double} \) and \( P_{\text{coin}}^\text{double} \) have the form
\[ P_{\text{click}}^\text{double} = 2 \left[ 1 - \sum_{n=0}^{\infty} |p_n|^2 \left( 1 - \frac{t_B \eta_{\text{det}}}{2} \right)^n \right], \]
\[ P_{\text{coin}}^\text{double} = 2 + \sum_{n=0}^{\infty} |p_n|^2 \left\{ \left[ 1 - \frac{\eta_{\text{det}}}{2} \right]^n - 2 \left[ 1 - \frac{t_B \eta_{\text{det}}}{2} \right]^n \right\} + \left[ 1 - \frac{(1 + t_B) \eta_{\text{det}}}{4} \right]^n - \left[ 1 - \frac{(1 - t_B) \eta_{\text{det}}}{2} \right]^n - \left[ 1 - \frac{(1 - t_B) \eta_{\text{det}}}{4} \right]^n \right\}. \] (21)

The calculations are provided in Appendix C.

D. Parameters \( p_{\text{click}}(k) \) and \( p_{\text{coin}}(k) \)

By combining Eqs. (12)-(13)-(17)-(18)-(19), and substituting the values of the parameters \( N_{ij}^\text{ind}(k) \) and \( N_{ij}^\text{double}(k) \), with \( i, j = 0, 1 \), given by Table I, we obtain that \( p_{\tau}(k) \), with \( \tau \in \{ \text{click}, \text{coin} \} \), can be expressed as
\[ p_{\tau}(k) = \frac{k - 1}{2} \left\{ P_{\tau}^\text{ind} + P_{\tau}^\text{double} \right\}, \] (22)
for \( k \geq 2 \). If we further insert in this equation (see Appendix D) the values of \( P_{\tau}^\text{ind} \) and \( P_{\tau}^\text{double} \) given by Eqs. (20)-(21), we find that \( p_{\tau}(k) \) has the form given by Eq. (21).

E. Evaluation

To evaluate the effectiveness of this countermeasure, we optimize numerically the probability distributions \( |q_n|^2 \) and \( |p_n|^2 \) corresponding to the signal states sent by Eve, such that, for each achievable value of the gain \( G_{\text{zero}} \), they provide the minimum value of the coincidence detection rate \( G_{\text{zero}}^\text{coin} \).

For simplicity, in the simulations below, we consider that Eve’s signals contain at most five photons (i.e., \( q_n = p_n = 0 \) for \( n > 5 \)), which is the regime that is relevant for the experimental values considered, which are provided in Table II. They correspond to those COW-QKD implementations reported in [32] in which Alice uses the highest and the lowest intensity value \( \mu = |\alpha|^2 \) for her signals. Moreover, we fix the parameter \( M_{\text{max}} = 10 \) and, as already mentioned, we disregard the effect of the dark counts of Bob’s detectors.

The results are illustrated in Fig. 6. The dashed blue line (dash-dotted green line) shows the minimum value of \( G_{\text{zero}}^\text{log} \) in logarithmic scale achievable by Eve as a function of \( G_{\text{zero}} \) for the experimental parameters corresponding to \( \mu = 0.06 \) (\( \mu = 0.1 \)) in Table II. When one increases the probability that Eve sends Bob higher photon number states, the values of \( G_{\text{zero}} \) and \( G_{\text{zero}}^\text{coin} \) increase, and eventually \( G_{\text{zero}}^\text{coin} \) matches the results obtained in [48], though this is not shown in the figure. The solid magenta line corresponds to the expected coincidence detection rate as a function of the gain in the absence of Eve for a typical channel model. These expected values are calculated in Appendix E. Precisely, the expected coincidence detection rate, which we denote by \( G_{\text{coin}} \), is given by Eq. (E9), while the expected gain, which we denote by \( G \), is given by Eq. (E3). In reality, in Fig. 6 there are two magenta lines, corresponding to the two sets of experimental parameters provided in Table II. However, both lines essentially overlap each other and cannot be distinguished with the resolution of the figure.

To remain undetected, Eve must guarantee that \( G_{\text{zero}}^\text{coin} = G_{\text{coin}} \). This reduces the maximum value of \( G_{\text{zero}} \) for which Eve’s attack is successful, as shown in Fig. 6. The values of \( G_{\text{zero}} \) that satisfy this latter condition are provided in Table III. According to these results, by monitoring coincidences Alice and Bob can approximately double the maximum achievable distance, which we denote by \( L_{\text{zero}} \), when compared to [48]. That is, \( L_{\text{zero}} \) corresponds to the transmission distance that provides a gain at Bob’s side equal to \( G_{\text{zero}} \) in the absence of Eve’s attack, for the channel model considered in Appendix E and the experimental parameters provided in Table II.

While this is a positive result, the robustness of COW-QKD against channel loss still remains quite limited even if coincidence detection events are monitored, specially when compared to protocols like decoy-state QKD [11–13, 23–26]. Indeed, the resulting values of \( G_{\text{zero}} \) are very close to those that could be obtained if Eve mainly sends

| \( \mu \) | Att. [dB] | Distance (km) | \( \alpha_{\text{channel}} \) | \( \eta_{\text{det}} \) | \( f \) | \( t_B \) |
|-----|--------|-------------|----------------|--------|-----|-----|
| 0.06 | 16.9   | 104         | 0.1625         | 0.22   | 0.155 | 0.9 |
| 0.1  | 34.1   | 203         | 0.1680         | 0.27   | 0.155 | 0.9 |

TABLE II: Experimental parameters corresponding to those COW-QKD demonstrations reported in [32] that use the highest and the lowest intensity value \( \mu = |\alpha|^2 \) for Alice’s signals. The parameter “Att.” in the table refers to the attenuation due only to channel loss, the distance refers to the fibre length, \( \alpha_{\text{channel}} \) represents the loss coefficient of the channel, \( \eta_{\text{det}} \) is the efficiency of Bob’s detectors, \( f \) denotes the probability that Alice emits a decoy signal \( |\varphi_2| \), and \( t_B \) is the transmittance of Bob’s beam splitter.
Att. \[\text{dB}\]

\[\begin{array}{|c|c|c|c|}
\hline
\text{This work } & \log_{10}(G_{\text{zero}}) & \text{Att. } & L_{\text{zero}} \text{(km)} \\
\text{Attack in [48] } & \text{[dB]} & \text{[dB]} & \text{[km]} \\
\hline
\text{This work } & -3.44 & \approx 15.8 & \approx 97 \\
\text{Attack in [48] } & -2.62 & \approx 7.6 & \approx 47 \\
\text{This work } & -2.92 & \approx 13.7 & \approx 81 \\
\text{Attack in [48] } & -2.19 & \approx 6.4 & \approx 38 \\
\hline
\end{array}\]

**TABLE III:** Values of \(G_{\text{zero}}\) that satisfy \(G_{\text{zero}}^\text{coin} = G_{\text{coin}}\). The parameter “Att.” \((L_{\text{zero}})\) refers to the channel loss (distance) associated to \(G_{\text{zero}}\) if one considers the channel model described in Appendix E and the experimental parameters provided in Table II. For comparison, this table also includes the maximum values of \(G_{\text{zero}}\) obtained in [48] when one does not impose any restriction on \(G_{\text{zero}}^\text{coin}\).

single-photon pulses to Bob (i.e., when \(|g_1|^2 = |p_1|^2 = 1\)). As we will see in the next two sections, the other two countermeasures considered turn out to be significantly more effective to protect COW-QKD against zero-error attacks. Moreover, in their analysis we assume the conservative untrusted device scenario.

**V. MONITORING DETECTION RATES**

Here, we consider another possible countermeasure against the zero-error attack presented in Sec. III. It exploits the fact that when Eq. (7) holds, which happens in most implementations of COW-QKD that satisfy \(f < 0.5\) and \(\mu < 0.5\), Eve’s optimal USD measurement does not identify decoy signals. Therefore, these signals are never forwarded to Bob. This means that Alice and Bob could monitor the detection rates of the emitted signals to detect a zero-error attack. Indeed, this approach has been considered in [50] against a restricted class of this type of attack.

To remain undetected, Eve will have to modify her attack to reproduce the expected detection rates of the signals. Importantly, this implies the following. First, she will have to use a sub-optimal USD measurement capable of identifying decoy signals. And, second, she will have to post-process the blocks of correctly identified signals by using a sub-optimal strategy. This is so because the post-processing strategy in [48] favours the transmission of key generation signals. Indeed, to keep all the visibilities observed by Bob equal to one, the blocks of signals that Eve resends him cannot include decoy signals in their edges. For instance, in the extreme case of blocks of length \(k = 2\) (i.e., blocks that contain precisely two correctly identified signals), which, on the other hand, have the highest probability to occur, none of the signals within the block can be a decoy signal. Thus, to match the expected detection rate of these signals, Eve will have to discard some blocks depending on their length.

Precisely, we define the gain of the decoy signals in a zero-error attack, which we shall denote by \(G_{\text{zero}}^\text{decoy}\), as the probability that Bob observes a detection “click” in his data due to these signals. By using exactly the same procedure employed to obtain Eqs. (3)-(10), it is straightforward to show that \(G_{\text{zero}}^\text{decoy}\) is given by

\[
G_{\text{zero}}^\text{decoy} = \frac{1 - p_{c,\zeta}}{1 - p_{c,\zeta}^{M_{\text{max}}+1}} \left[ \sum_{k=2}^{M_{\text{max}}} \gamma k p_{c,\zeta}^k (1 - p_{c,\zeta}) p_{\text{click}}(k) \right]
\]

\[
+ \gamma M_{\text{max}} p_{c,\zeta}^{M_{\text{max}}} p_{\text{click}}^{M_{\text{max}}}(M_{\text{max}}).
\]

Here, \(p_{c,\zeta}\) denotes the probability that Eve’s USD measurement provides a conclusive outcome. This quantity now depends on a parameter \(\zeta \in [f, 1]\), which allows Eve to adjust the probability to correctly identify a decoy signal, between zero (when \(\zeta = f\) [56]) and its maximum allowed value (when \(\zeta = 1\)). For further details see Appendix F. The probability \(p_{\text{click}}(k)\), on the other hand, represents the average number of “clicks” observed by Bob in his data line due to a decoy signal when Eve sends him a block containing \(k\) correctly identified signals. This quantity is given by

\[
p_{\text{click}}(k) = \sum_{j=0}^{2} p(j|c) p_{\text{click}}(k|j),
\]

where \(p_{\text{click}}(k|j)\) is the average number of “clicks” observed by Bob in his data line due to a decoy signal when
Eve sends him a block containing \( k \) correctly identified signals and the first signal of the block is \( |\varphi_1\rangle \).

We note that in Eq. (23), we have also included certain parameters \( \gamma_k \in [0, 1] \), with \( k = 2, \ldots, M_{\text{max}} \). They denote the probability that Eve actually resends Bob a block that contains \( k \) correctly identified signals. This means that, in this scenario, the gain \( G_{\text{zero}} \) now reads

\[
G_{\text{zero}} = \frac{1 - p_{c, \zeta}}{1 - p_{\text{max}, \zeta}} \left[ \sum_{k=2}^{M_{\text{max}} - 1} \gamma_k p_{c, \zeta}^k (1 - p_{c, \zeta}) p_{\text{click}}(k) \right] + \gamma_{M_{\text{max}}} p_{c, \zeta}^{M_{\text{max}}} p_{\text{click}}(M_{\text{max}}),
\]

where the parameter \( p_{\text{click}}(k) \) is given by Eq. (6).

We shall denote the expected values of the analogous parameters in the absence of Eve for a typical channel model as \( G_{\text{decoy}} \) and \( G \). That is, \( G_{\text{decoy}} \) (\( G \)) is the expected detection rate of the decoy signals (expected gain). These two quantities are calculated in Appendices G and E, respectively. This means that for \( G_{\text{zero}} = G \), Eve must guarantee that \( G_{\text{zero}} = G_{\text{decoy}} \).

Importantly, since the expected gain of the key generation signals is equal for both of them, and this property is preserved by the zero-error attack, this condition is sufficient to assure that the detection rates of all the signals sent by Alice match their expected values.

In the next section, we compute \( p_{\text{click}}^{\text{decoy}}(k|j) \), with \( j = 0, 1, 2 \). Eve’s USD measurement, including the value of the parameter \( p_{c, \zeta} \), is described in Appendix F.

### A. Parameters \( p_{\text{click}}^{\text{decoy}}(k|j) \)

In the calculations below, we assume that the signals resent by Eve have sufficient intensity to produce a detection “click” at Bob’s side with basically unit probability. For instance, Eve can resend Bob coherent states of very high intensity.

#### 1. Parameter \( p_{\text{click}}^{\text{decoy}}(k|1) \)

This scenario is illustrated in Fig. 7. Since the first optical pulse of \( |\varphi_1\rangle \) is a vacuum pulse, the longest sub-block that starts and ends with correctly identified vacuum pulses (if there is any) includes \( |\varphi_1\rangle \).

With probability \( p(0|c) \) the signal in the \( k \)-th position of the block is \( |\varphi_0\rangle \). This means that Eve resends Bob all the \( k \) signals in the block, as it starts and ends with correctly identified vacuum pulses. The decoy signals can only be located from position 2 to position \( k - 1 \) within the block. Therefore, Bob will observe on average \((k - 2)p(2|c)\) “clicks” from decoy signals.

Similarly, if the \( k \)-th signal of the block is \( |\varphi_1\rangle \), which happens with probability \( p(1|c) \), Eve replaces that signal with \( |\varphi_{\text{vac}}\rangle \) (not shown in the figure) and she resends Bob the first \( k - 1 \) conclusive signals in the block because such sub-block has correctly identified vacuum pulses on its edges. Again, decoy signals can only be located from position 2 to position \( k - 1 \) within the block, and, thus, Bob will observe on average \((k - 2)p(2|c)\) “clicks” from these signals.

Finally, with probability \( p(2|c) \) the \( k \)-th signal of the block is \( |\varphi_2\rangle \). Since this signal does not include a vacuum pulse, she replaces it with \( |\varphi_{\text{vac}}\rangle \) (not shown in the figure). Then, Bob will observe \( p_{\text{click}}^{\text{decoy}}(k|1) \) “clicks”, because now Eve’s block starts with \( |\varphi_1\rangle \) and contains \( k - 2 \) correctly identified signals \( |\varphi_j\rangle \), with \( j = 0, \ldots, 3 \).

Putting all together, we obtain the following recursive...
relation for $p_{\text{click}}^{\text{decoy}}(k|1)$,
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k|1) &= \left[ p(0|c)(k - 2) + p(1|c)(k - 2) \\
  &\quad+ p_{\text{click}}^{\text{decoy}}(k - 1|1) \right] p(2|c). \tag{26}
\end{align*}

By taking into account that $\sum_{i=0}^{2} p(i|c) = 1$, $p(0|c) = p(1|c)$, and the fact that $p_{\text{click}}^{\text{decoy}}(1|1) = 0$, from Eq. (26)
we find that
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k|1) &= \frac{p(2|c)}{1 - p(2|c)} \left[ (1 - p(2|c))k + p(2|c) - 2 \\
  &\quad+ p(2|c)k - 1 \right], \tag{27}
\end{align*}
for $k \geq 2$.

2. Parameter $p_{\text{click}}^{\text{decoy}}(k|0)$

This case is illustrated in Fig. 8. The analysis is essentially equal to that of the previous section, and we omit the details here for simplicity. It can be shown that $p_{\text{click}}^{\text{decoy}}(k|0)$ satisfies
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k|0) &= p_{\text{click}}^{\text{decoy}}(k|1). \tag{28}
\end{align*}

3. Parameter $p_{\text{click}}^{\text{decoy}}(k|2)$

When the first signal of a block is $|\varphi_2\rangle$, Eve replaces this signal with $|\varphi_{\text{vac}}\rangle$ because $|\varphi_2\rangle$ does not contain a vacuum pulse. Now the new block has $k - 1$ correctly identified signals $|\varphi_i\rangle$, with $i = 0, 1, 2$. This means that
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k|2) &= p_{\text{click}}^{\text{decoy}}(k - 1). \tag{29}
\end{align*}

B. Parameters $p_{\text{click}}^{\text{decoy}}(k)$

By combining Eqs. (24)-(27)-(28)-(29), we obtain that the parameter $p_{\text{click}}^{\text{decoy}}(k)$ can be written as
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k) &= \left[ (1 - p(2|c))k + p(2|c) - 2 + p_{\text{click}}^{\text{decoy}}(k - 1) \right] \\
  &\quad\times p(2|c) + p(2|c)k. \tag{30}
\end{align*}

This recursive relation can be solved by taking into account that $p_{\text{click}}^{\text{decoy}}(1) = 0$. In particular, we find that
\begin{align*}
  p_{\text{click}}^{\text{decoy}}(k) &= \frac{p(2|c)}{1 - p(2|c)} \left[ (1 - p(2|c))k - 2 \\
  &\quad+ \left[ (1 - p(2|c))k + 2p(2|c) \right] p(2|c)k - 1 \right], \tag{31}
\end{align*}
for $k \geq 2$.

C. Evaluation

To evaluate the effectiveness of this countermeasure, we optimize numerically the probabilities $\gamma_k \in [0, 1]$, with $k = 2, \ldots, M_{\text{max}}$, and the parameter $\zeta \in [0, 1]$. $\gamma_k$ characterizes the probability that Eve resends Bob a block that contains $k$ correctly identified signals, while $\zeta$ refers to the probability to correctly identify a decoy signal.

The conclusive probability $p_{\text{click}}$ of Eve’s USD measurement depends on the value of $\zeta$ (see Appendix F). In the simulations below, we set $M_{\text{max}} = 10$, and disregard the effect of the dark counts of Bob’s detectors.

The results are illustrated in Fig. 9. The dashed blue line (dash-dotted green line) represent signals, while small ovals (drawn with a solid line) represent optical pulses within a signal. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.
Eve, as a function of $G_{\text{zero}}$ for the experimental parameters corresponding to $\mu = 0.06$ $(\mu = 0.1)$ in Table II. We note that the scenario considered in [48] corresponds to $\zeta = f$ (which provides $G_{\text{decoy}} = 0$). The solid magenta line shows the expected detection rate $G_{\text{decoy}}/G$ of the decoy signals as a function of the expected gain $G = G_{\text{zero}}$ for a typical channel model. In fact, in Fig. 9 there are two magenta lines, one for each of the two sets of experimental parameters provided in Table II. However, these two lines cannot be distinguished with the resolution of the figure.

As shown in Fig. 9, by monitoring the detection rates, Alice and Bob can dramatically decrease the value of $G_{\text{zero}}$, and thus increase the maximum achievable distance $L_{\text{zero}}$. This is so because now Eve must guarantee that $G_{\text{decoy}} = G_{\text{decoy}}$ for a certain $G = G_{\text{zero}}$. To obtain $L_{\text{zero}}$, we use the channel model described in Appendix E. The values of $G_{\text{zero}}$ (and the corresponding $L_{\text{zero}}$) that satisfy this latter condition are provided in Table IV. By comparing these results with those in Table III, we find that $L_{\text{zero}}$ is now more than eight times larger than the case where no detection rates are monitored, which is remarkable.

To conclude this section, we evaluate the simple upper bound on the secret key rate of COW-QKD derived in [47]. It reads

$$K < (1-f)\eta_{\text{channel}}\mu_{\text{max}}(f) \equiv R_{\text{app}},$$

where $\eta_{\text{channel}}$ refers to the channel transmittance, and $\mu_{\text{max}}(f)$ is the maximum allowed intensity for Alice’s signals such that Eve’s zero-error attack is not possible, i.e., the expected gain in the absence of Eve is greater than $G_{\text{zero}}$. We note that in Eq. (47) we implicitly assume the optimistic scenario in which the efficiency of Bob’s detectors is $\eta_{\text{det}} = 1$. For further details, we refer the reader to [47]. The results are illustrated in Fig. 10. Remarkably, now the upper bound on the secret key rate scales close to $O(\eta_{\text{channel}}^{4/3})$ with the channel transmittance (instead of quadratically, as is the case in the original COW scheme [47]).

### VI. FOUR-STATE COW-QKD

In this section, we study a third possible countermeasure against zero-error attacks. The idea is to increase the number of signals sent by Alice to reduce the probability that Eve can unambiguously identify them. Precisely, we shall consider the situation in which Alice sends

| $\mu$ | $\log_{10}(G_{\text{zero}})$ | Att. [dB] | $L_{\text{zero}}$ [km] |
|-------|-----------------|----------|-----------------|
| 0.06  | -8.16           | 62.9     | 387             |
| 0.1   | -7.27           | 57.1     | 340             |

**TABLE IV**: Values of $G = G_{\text{zero}}$ for which $G_{\text{decoy}} = G_{\text{decoy}}$. The meaning of the different parameters coincides with that provided in Table III.
Bob an additional decoy signal $|\varphi_3\rangle = |0\rangle |0\rangle$ [59]. This solution has been evaluated in [50] against a restricted class of zero-error attacks.

Alice now prepares her signals with probabilities

$$p_{|\varphi_0\rangle} = p_{|\varphi_1\rangle} = \frac{1 - f}{2},$$
$$p_{|\varphi_2\rangle} = f_d,$$
$$p_{|\varphi_3\rangle} = f - f_d = f_v,$$
$$p_{|\varphi_3\rangle} = f - f_d = f_v,$$

with $f, f_d \in (0, 1)$ and $f > f_d$.

To calculate the gain $G_{\text{zero}}$ given by Eq. (3), we need to determine the parameters $p_c$ and $p_{\text{click}}(k)$. The conclusive probability $p_c$ corresponding to the optimal USD measurement is obtained in Appendix H. Below, we calculate $p_{\text{click}}(k)$.

### A. Probabilities $p_{\text{click}}(k)$

In this scenario, the probabilities $p(j|c)$ are given by

$$p(0|c) = p(1|c) = \frac{(1 - f_d - f_v)q_v}{2p_c},$$
$$p(2|c) = \frac{f_d q_d}{p_c},$$
$$p(3|c) = \frac{f_v q_v}{p_c},$$

where the terms $q_v$, $q^d_v$, and $q^v_v$ are defined in Table VII in Appendix H. They correspond to the probabilities that Eve’s optimal USD measurement provides a conclusive result when measuring the key generation signals $|\varphi_0\rangle$ or $|\varphi_1\rangle$, and the decoy signals $|\varphi_2\rangle$ and $|\varphi_3\rangle$, respectively.

To calculate $p_{\text{click}}(k)$, we consider four different cases, depending on the result obtained by Eve for the first signal of a block that contains $k$ consecutive conclusive measurement results, and a vacuum signal $|\varphi_{\text{vac}}\rangle = |0\rangle |0\rangle$ in its $k+1$th position. In particular, from Eq. (4) we have that

$$p_{\text{click}}(k) = \sum_{j=0}^{3} p(j|c)p_{\text{click}}(k|j).$$

Below we compute $p_{\text{click}}(k|j)$. Like in Sec. V, we shall consider that Eve resends Bob coherent pulses of very high intensity such that he obtains a detection “click” with basically unit probability.

#### 1. Parameter $p_{\text{click}}(k|1)$

This scenario is depicted in Fig. 11, which also shows the number of “clicks” that Bob observes in his data line for each of the four sub-cases considered in that figure. Since the first optical pulse of $|\varphi_1\rangle$ is a vacuum pulse, the longest sub-block that starts and ends with correctly identified vacuum pulses (if there is any) includes $|\varphi_1\rangle$.

![FIG. 11: Illustration of the four sub-cases that we consider to evaluate $p_{\text{click}}(k|1)$. With probability $p(0|c)$ the signal in the $k$-th position of the block is $|\varphi_0\rangle$. In this case, Eve resends Bob all the $k$ conclusive signals, as the block starts and ends with correctly identified vacuum pulses. The number of “clicks” at Bob’s data line is then $2 + (k - 2)p_{\text{click}}(c)$, where $p_{\text{click}}(c)$ is defined in the text. The other three sub-cases are analogous and are described in the text. In the figure, large oval (drawn with a dashed line) represent optical pulses within a signal. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.](image-url)
line. In Eq. (36), we use $\sum_{j=0}^{3} p(j|c) = 1$ together with the fact that, as already mentioned, Eve’s resent signals satisfy $p_{\text{click}|c} = 1$ for all $j = 0, 1, 2$, and $p_{\text{click}|c} = 0$. Here, note that double “clicks” in the data line within a signal duration are randomly assigned by Bob to single “clicks”.

With probability $p(0|c)$ the signal in the $k$-th position of the block is $|\varphi_0\rangle$. In this case, Eve resends Bob all the $k$ conclusive signals in the block, as it starts and ends with correctly identified vacuum pulses. Bob will observe two detection “clicks” from the signals located in the first and in the $k$-th position of the block, while for each of the other $k-2$ signals located in the middle between them, Bob will observe on average $p_{\text{click}|c}$ “clicks”. That is, the average number of “clicks” is $2 + (k-2)p_{\text{click}|c}$.

On the other hand, if the $k$-th signal of the block is $|\varphi_1\rangle$, which happens with probability $p(1|c)$, then Eve resends Bob the first $k-1$ conclusive signals in the block because such sub-block has correctly identified vacuum pulses on its edges. Also, she replaces the $k$-th signal with $|\varphi_{\text{vac}}\rangle$ (not shown in Fig. 11). Therefore, Bob will observe one “click” from the first signal of the block, and $p_{\text{click}|c}$ “clicks” for each of the $k-2$ signals in positions 2, …, $k-1$. That is, the average number of “clicks” is $1 + (k-2)p_{\text{click}|c}$.

Likewise, with probability $p(2|c)$ the $k$-th signal of the block is $|\varphi_2\rangle$. Then, Eve replaces that signal with $|\varphi_{\text{vac}}\rangle$ (not shown in Fig. 11) because it does not include a vacuum pulse. This means that Bob will observe $p_{\text{click}}(k-1|1)$ “clicks”, since now Eve’s block starts with $|\varphi_1\rangle$ and includes $k-2$ correctly identified signals $|\varphi_j\rangle$, with $j = 0, \ldots, 3$.

Finally, if the $k$-th signal of the block is $|\varphi_3\rangle$, which happens with probability $p(3|c)$, the situation is analogous to that in which that signal is $|\varphi_1\rangle$. That is, Eve resends Bob the first $k-1$ conclusive signals in the block because such sub-block has correctly identified vacuum pulses on its edges. Bob will observe on average $1 + (k-2)p_{\text{click}|c}$ “clicks” in this case.

Putting all together, we find the following recursive relation for $p_{\text{click}}(k|1)$,

$$
p_{\text{click}}(k|1) = p(0|c)[2 + (k-2)p_{\text{click}|c}] + p(1|c) \\
\times \left[1 + (k-2)p_{\text{click}|c}\right] + p(2|c)p_{\text{click}}(k-1|1) \\
+ p(3|c)[1 + (k-2)p_{\text{click}|c}].
$$

(37)

After some algebra, and taking into account that $p_{\text{click}}(1|1) = 0$, we obtain from Eq. (37) that

$$
p_{\text{click}}(k|1) = 
\frac{1}{p(2|c)[p(2|c) - 1]} \left\{ \left[1 - p(0|c) - 2p(2|c)\right] \\
\times \left[1 + (k-2)p_{\text{click}|c}\right] + p(2|c)[1 - p(0|c) + p(2|c)] \\
+ [2 + (k-1)p(2|c) - k] p_{\text{click}|c}\right\}.
$$

(38)

FIG. 12: Illustration of the four sub-cases that we consider to evaluate $p_{\text{click}}(k|0)$. With probability $p(0|c)$ the $k$-th signal of the block is $|\varphi_0\rangle$. In this case, Eve resends Bob the $k-1$ conclusive signals from position 2 to position $k$, while the first signal is replaced with $|\varphi_{\text{vac}}\rangle$ (not shown in the figure). The number of “clicks” at Bob’s side is then $1 + (k-2)p_{\text{click}|c}$. The other three sub-cases are analogous and are described in the text. In the figure, large ovals (drawn with a dashed line) represent signals, while small ovals (drawn with a solid line) represent optical pulses within a signal. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.

2. Parameter $p_{\text{click}}(k|0)$

This case is very similar to the previous one, and is illustrated in Fig. 12. With probability $p(0|c)$, the $k$-th signal of the block is $|\varphi_0\rangle$. Then, Eve resends Bob the $k-1$ conclusive signals from positions 2 to $k$, and she replaces the first signal with $|\varphi_{\text{vac}}\rangle$ (not shown in the figure). Bob will observe one “click” from the $k$-th signal, and $p_{\text{click}|c}$ “clicks” for each of the other $k-2$ signals. That is, the average number of “clicks” is $1 + (k-2)p_{\text{click}|c}$. 
the first and the happens with probability \( p \). If the signal with \( |\varphi_1\rangle \) (not shown in the figure) is \( |\varphi_0\rangle \), Eve replaces that signal with \( |\varphi_0\rangle \) (not shown in the figure) because it does not include a vacuum pulse. This means that Bob will observe \( p_{\text{click}}(k - 1|0) \) “clicks”, since now Eve’s block starts with \( |\varphi_0\rangle \) and includes \((k - 2)\) correctly identified signals \( |\varphi_j\rangle \), with \( j = 0, \ldots, 3 \).

Finally, if the \( k \)-th signal of the block is \( |\varphi_3\rangle \), which happens with probability \( p(3|c) \), the situation is analogous to that in which that signal is \( |\varphi_1\rangle \). Eve replaces the first and the \( k \)th signals with \( |\varphi_\text{vac}\rangle \) (not shown in the figure), and resends Bob the \((k - 2)\) conclusive signals from positions 2 to \( k - 1 \), as such sub-block has correctly identified vacuum pulses on its edges. This means that Bob will observe on average \((k - 2)p_{\text{click}c} \) “clicks”.

Putting all together, we obtain the following recursive relation for \( p_{\text{click}}(k|0) \),

\[
p_{\text{click}}(k|0) = p(0|c)[1 + (k - 2)p_{\text{click}c} + p(1|c)(k - 2)]
\times p_{\text{click}c} + p(2|c)p_{\text{click}}(k - 1|0) + p(3|c)
\times (k - 2)p_{\text{click}c}
\]  

Since \( p_{\text{click}}(1|0) = 0 \), from Eq. (39) it can be shown that \( p_{\text{click}}(k|0) \) satisfies

\[
p_{\text{click}}(k|0) = \frac{1}{p(2|c)[p(2|c) - 1]} \left\{ \begin{array}{l}
\left[ p(0|c) - p_{\text{click}c} \right] \\
\times p(2|c)^k - p(2|c)[p(0|c) + [(1 - k)p(2|c) + k - 2]p_{\text{click}c}] \end{array} \right\}.
\]  

3. Parameter \( p_{\text{click}}(k|2) \)

If the first signal of a block is \( |\varphi_2\rangle \), Eve always replaces it with \( |\varphi_\text{vac}\rangle \), as \( |\varphi_2\rangle \) does not contain a vacuum pulse.

The remaining sub-block has now \( k - 1 \) conclusive results, each of which can be a signal \( |\varphi_j\rangle \) with \( j = 0, \ldots, 3 \). That is, \( p_{\text{click}}(k|2) \) is given by the average number of “clicks” of such sub-block,

\[
p_{\text{click}}(k|2) = p_{\text{click}}(k - 1).
\]  

4. Parameter \( p_{\text{click}}(k|3) \)

This case is essentially equal to that of \( p_{\text{click}}(k|0) \), because when a block starts with a signal \( |\varphi_0\rangle \), Eve always replaces that signal with \( |\varphi_\text{vac}\rangle \). We find, therefore, that

\[
p_{\text{click}}(k|3) = p_{\text{click}}(k|0)
\]  

5. Parameter \( p_{\text{click}}(k) \)

By combining Eqs. (35)-(38)-(40)-(41)-(42), we obtain the following recursive relation for \( p_{\text{click}}(k) \),

\[
p_{\text{click}}(k) = 2p(0|c)\left[1 - p(2|c)^{k-1}\right] + \left[k - 2 + (1 - k)p(2|c)\right]p_{\text{click}c}
+ \frac{p(2|c)}{p(2|c) - 1}p_{\text{click}c} - (k - 2)p_{\text{click}c}\]
\]  

To solve this equation for any \( k > 2 \), we need to calculate the starting point of the recursion, \( p_{\text{click}}(2) \). For this, we consider the sixteen cases depicted in Fig. 13 with their \( a \text{ priori} \) probabilities. We obtain

\[
p_{\text{click}}(2) = p(0|c)^2 + 2p(0|c)p(1|c) + p(1|c)^2
+ p(3|c)p(1|c) + p(0|c)p(3|c)
= 2p(0|c)[1 - p(2|c)],
\]  

where in the second equality we use \( p(0|c) = p(1|c) \) and \( \sum_{j=0}^{3} p(j|c) = 1 \).

By combining Eqs. (43)-(44), we find that \( p_{\text{click}}(k) \) satisfies

\[
p_{\text{click}}(k) = \frac{1}{p(2|c)[p(2|c) - 1]}
\left\{ -2p(0|c)p(2|c) + p(2|c)^k \right\}
\times 2p(2|c)[p(0|c) - p_{\text{click}c}]
+ \left[ 2 + k \left( p(2|c) - 1 \right) \right] p(2|c)p_{\text{click}c}
\]  

for any \( k \geq 2 \).

B. Evaluation

To evaluate the effectiveness of this countermeasure against zero-error attacks, we compute \( G_{\text{zero}} \) for the ex-
Together with the number of “clicks” that Bob will observe in his data line. For example, in the first case, with probability \( p(0|c)p(0|c) \) the signals in the block are \( |\varphi_{\text{vac}}\rangle|\varphi_{0}\rangle|\varphi_{0}\rangle \). This means that Eve can extract a sub-block surrounded by vacuum pulses by simply replacing the first signal of the block with \( |\varphi_{\text{vac}}\rangle \) (not shown in the figure). The number of “clicks” at Bob’s data line is then one. The other cases are analogous. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.

![Illustration of the sixteen possible cases for a block with \( k = 2 \) consecutive conclusive measurement results.](image)

**FIG. 13:** Illustration of the sixteen possible cases for a block with \( k = 2 \) consecutive conclusive measurement results, together with the number of “clicks” that Bob will observe in his data line. For example, in the first case, with probability \( p(0|c)p(0|c) \) the signals in the block are \( |\varphi_{\text{vac}}\rangle|\varphi_{0}\rangle|\varphi_{0}\rangle \). This means that Eve can extract a sub-block surrounded by vacuum pulses by simply replacing the first signal of the block with \( |\varphi_{\text{vac}}\rangle \) (not shown in the figure). The number of “clicks” at Bob’s data line is then one. The other cases are analogous. The sub-blocks of signals that Eve resends to Bob are illustrated with grey dashed rectangles.

| \( \mu \) | \( \log_{10}(G_{\text{zero}}) \) | Att. [dB] | \( L_{\text{zero}} \) (km) |
|---|---|---|---|
| 0.06 | -5.66 | \( \approx 37.5 \) | \( \approx 231 \) |
| 0.1 | -4.79 | \( \approx 31.9 \) | \( \approx 190 \) |

**TABLE V:** \( G_{\text{zero}} \) for the experimental parameters provided in Table II. For illustration purposes, we replace \( f = 0.155 \) with \( f_{d} = 0.1 \) and \( f_{v} = 0.055 \). The parameter “Att.” (\( L_{\text{zero}} \)) refers to the channel loss (distance) associated to \( G_{\text{zero}} \) if one considers the channel model described in Appendix E.

Experimental parameters provided in Table II. For this, we use Eqs. (3)-(45), together with the value of \( p_{c} \) that corresponds to the optimal USD measurement calculated in Appendix H. Like in the previous measurements, we fix \( M_{\text{max}} = 10 \) and, for simplicity, we disregard the effect of the dark counts of Bob’s detectors. The results are illustrated in Table V. They indicate that the resulting \( G_{\text{zero}} \) for the four-state COW-QKD protocol is significantly much smaller than that reported in [48] for the original scheme (see Table III).

Table V includes the maximum tolerable channel loss, and the maximum achievable distance \( L_{\text{zero}} \). To obtain \( L_{\text{zero}} \), we use the channel model described in Appendix E, but now adapted to the four-state protocol. It can be shown that the expected value of the gain \( G \) at Bob’s data line in the absence of Eve’s attack is now given by

\[
G = (1 - f_{d} - f_{v}) \left[ 1 - e^{-\mu \eta_{\text{sys}}} \right] + f_{d} \left[ 1 - e^{-2\mu \eta_{\text{sys}}} \right],
\]

where \( \eta_{\text{sys}} \) is the overall system’s transmittance (see Appendix E). The parameter \( L_{\text{zero}} \) corresponds to the distance for which \( G = G_{\text{zero}} \).

Fig. 14 shows the upper bound on the secret key rate of COW-QKD derived in [47]. In this scenario it has the form

\[
K < (1 - f_{d} - f_{v}) \eta_{\text{channel}} \mu_{\max}(f) \equiv R_{\text{upp}}.
\]

The meaning of the different parameters has been given in Sec. V.C. Again, like in Sec. V, we obtain that now this upper bound scales close to \( O(\eta_{\text{channel}}^{4/3}) \) with the channel transmittance, which contrasts with the quadratic scaling reported in [47] for the original COW scheme.

**VII. CONCLUSION**

In this paper, we have evaluated the effectiveness of three possible countermeasures for COW-QKD to foil zero-error attacks, in which the eavesdropper measures out all the emitted signals, and we have derived asymptotic upper security bounds for them.
The first two countermeasures require that Alice and Bob monitor additional detection statistics. Precisely, we have considered the cases where they monitor the number of coincidences, and the detection rates of Alice’s signals at Bob’s data line. We have shown that the former countermeasure might allow them to approximately double the maximum achievable distance when compared to the original COW-QKD protocol, while the latter countermeasure improves the resulting performance even further, as now the upper security bounds on the secret key rate scale close to linear with the channel transmittance. This strongly contrasts with the quadratic scaling provided for the original scheme. Also, we have shown that a similar improvement could be obtained by increasing the number of transmitted signals, by adding, for instance, say a decoy vacuum signal.

These countermeasures might be used to boost the performance of COW-QKD, though, for this, it would be necessary to derive lower security bounds that can confirm their merits.

VIII. ACKNOWLEDGEMENTS

The authors wish to thank the company ID Quantique for very useful discussions, and for suggesting the consideration of this project. This work was funded by ID Quantique, the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), and the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21.
we consider the

16
can be calculated similarly, and we omit the details

η
detection efficiency. Since in Sec.

IV

that all detectors at Bob’s side have the same detection

efficiency by placing a beamsplitter (BS) of

transmittance \( \eta_{\text{det}} \) placed right before Bob’s receiver. In
doing so, we can now assume that all of his detectors
have perfect detection efficiency. This fictitious beamsplitter cannot be controlled by Eve. We further
assume that Eve sends Bob a non-vacuum optical pulse
in the state \( |\Phi^{\text{ind}}\rangle \) in the mode \( a_1 \) (where the subindex
“1” indicates the time instant), surrounded by vacuum
pulses in the modes \( a_0 \) and \( a_2 \). The non-vacuum optical
pulse is illustrated in the figure with a grey oval. To
determine \( P_{\text{click}}^{\text{ind}} \) and \( P_{\text{coin}}^{\text{ind}} \), we are interested in the state
of the signal in the modes \( b_2, b_1, c_2, c_1, d_2 \) and \( d_1 \).

In the figure, the states \( |0\rangle \) represent vacuum pulses.

The other parameters \( N_{ij}^{\text{ind}}(k) \) and \( N_{ij}^{\text{double}}(k) \) in Table I can be calculated similarly, and we omit the details
here for simplicity.

Appendix B: Calculation of \( P_{\text{click}}^{\text{ind}} \) and \( P_{\text{coin}}^{\text{ind}} \)

This corresponds to the scenario where Eve sends Bob an
individual non-vacuum optical pulse in a state \( |\Phi^{\text{ind}}\rangle \)
given by Eq. (14) surrounded by vacuum pulses.

For simplicity, in the calculations below, we assume that
all detectors at Bob’s side have the same detection
efficiency \( \eta_{\text{det}} \). This means that we can model the effect
of their finite detection efficiency by placing a beamsplitter
of transmittance \( \eta_{\text{det}} \) right before Bob’s receiver, and
then we assume that all his detectors have now perfect
detection efficiency. Since in Sec. IV we consider the
trusted device scenario, this fictitious beamsplitter cannot
be controlled by Eve. Moreover, we consider that Eve
sends the signals to Bob with a transmitter located
very close to his receiver, and thus they are not affected
by channel loss. This situation is illustrated in Fig. 16.

According to Eq. (14), the input state in modes \( a_i \),
where the subindex \( i = 0, 1, 2 \), represents the time in-
stant, is given by

\[
|\Psi\rangle_{a_2 a_1 a_0} = |0\rangle_{a_2} \left( \sum_{n=0}^{\infty} q_n |n\rangle_{a_1} \right) |0\rangle_{a_0}. \tag{B1}
\]

When this state enters the linear optics circuit illustrated in Fig. 16, it can be shown that the output state at the
optical modes \( b_2, b_1, c_2, c_1, d_2 \) and \( e \) depicted in that figure can be written as

\[
|\Phi\rangle_{b_2 b_1 c_2 c_1 d_2 e} = \langle \phi |_{b_1 c_2 d_1 e} |0\rangle_{b_2 c_1 d_2}, \tag{B2}
\]

where the state \( |\phi \rangle_{b_1 c_2 d_1 e} \) has the form

\[
|\phi\rangle_{b_1 c_2 d_1 e} = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sum_{m=0}^{l} \left( \begin{array}{c} n \\ k \\ l \\ m \end{array} \right) q_n \sqrt{n!} \times \sqrt{1 - \eta_{\text{det}}}^{n-k} \eta_{\text{det}}^{k-l} \sqrt{t_B}^{k-l} \sqrt{1 - t_B}^{l-k} \times \sqrt{(n-k)!} \sqrt{(k-l)!} \sqrt{(l-m)!} \times \langle k-l |_{b_1} | l-m |_{c_2} \rangle \langle m |_{d_1} | n-k \rangle_e. \tag{B3}
\]

Here, \( |k-l \rangle_{b_1} \) is the Fock state with \( k - l \) photons in the
mode \( b_1 \), and the other states are defined similarly. In the output modes \( b_0, c_3 \) and \( d_0 \) illustrated in Fig. 16 there are vacuum states. These states are not relevant
for the discussion and calculations below, as we are only
interested in the detection events that may occur in the
time instances “1” and “2.”

To calculate \( P_{\text{click}}^{\text{ind}} \) and \( P_{\text{coin}}^{\text{ind}} \), we first trace out mode
\( e \) from the state \( |\phi\rangle_{b_1 c_2 d_1 e} |0\rangle_{b_2 c_1 d_2} \) and consider instead
the state \( \rho_{b_2 b_1 c_2 c_1 d_2} = Tr_e (|\phi\rangle_{b_1 c_2 d_1 e} \langle \phi |_{b_1 c_2 d_1 e} ) \otimes |0\rangle\langle 0 |_{b_2 c_1 d_2}. \) Moreover, since Bob’s measurement operators on the
modes \( b_2, b_1, c_2, c_1, d_2 \) and \( d_1 \) are diagonal in the Fock
basis (due to the use of single-photon detectors), we can
further simplify the calculations by replacing \( \rho_{b_2 b_1 c_2 c_1 d_2} \) with a state \( \tilde{\rho}_{b_2 b_1 c_2 c_1 d_2} \) that is diagonal in the Fock
basis, and whose diagonal elements coincide with those of
\( \rho_{b_2 b_1 c_2 c_1 d_2} \). That is, it follows that the measurement
statistics provided by \( \tilde{\rho}_{b_2 b_1 c_2 c_1 d_2} \) match those of
\( \rho_{b_2 b_1 c_2 c_1 d_2} \) when both states are measured with Fock
diagonal measurement operators. The state \( \tilde{\rho}_{b_2 b_1 c_2 c_1 d_2} \) has the form

\[
\tilde{\rho}_{b_2 b_1 c_2 c_1 d_2} = \tilde{\rho}_{b_1 c_2 d_1} \otimes |0\rangle\langle 0 |_{b_2 c_1 d_2}, \tag{B4}
\]

with \( \tilde{\rho}_{b_1 c_2 d_1} \) having the form

\[
\tilde{\rho}_{b_1 c_2 d_1} = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} \sum_{m=0}^{l} \left( \begin{array}{c} n \\ k \\ l \\ m \end{array} \right) q_n \times (1 - \eta_{\text{det}})^{n-k} \eta_{\text{det}}^{k-l} \times \langle k-l |_{b_1} | l-m |_{c_2} \rangle \langle m |_{d_1} | n-k \rangle, \tag{B5}
\]

The state \( \tilde{\rho}_{b_2 b_1 c_2 c_1 d_2} \) can only produce a “click” in
Bob’s data line in the time instant “1” because in mode
there are vacuum states that are not relevant in mode 1. Since there is vacuum in mode 1, the probability to have a "click" in this mode directly. This means that the state $|0\rangle$ represent vacuum pulses.

$b_2$ there is a vacuum state. This means that $P_{\text{click}}$ can be expressed as

$$P_{\text{click}} = 1 - \langle 0 | \text{Tr}_{c_2 d_1} (\hat{\rho}_{b_1 c_2 d_1}) | 0 \rangle_{b_1} .$$  \hspace{1cm} (B6)

By using Eqs. (B5)-(B6) we obtain Eq. (20).

For the same reason, a coincidence detection event is only possible in the time instant “1”. Since there is vacuum in mode $c_1$, the probability that at least one of the two detectors $D_{M1}$ and $D_{M2} “\text{click}”$ at Bob’s monitoring line, is equal to the probability to have a “click” in $d_1$ if we would had measured this mode directly. This means that $P_{\text{coin}}$ can be written as

$$P_{\text{coin}} = \text{Tr} (\hat{\rho}_{b_1 c_2 d_1} M_{b_1 c_2 d_1}) ,$$  \hspace{1cm} (B7)

where the operator $M_{b_1 c_2 d_1}$ has the form

$$M_{b_1 c_2 d_1} = (\mathbb{1}_{b_1} - |0\rangle_{b_1} \langle 0|_{b_1}) \otimes \mathbb{1}_{c_2} \otimes (\mathbb{1}_{d_1} - |0\rangle_{d_1} \langle 0|_{d_1}) .$$  \hspace{1cm} (B8)

The input state $|0\rangle$ in Fig. 17, we use the same linear optics circuit employed in Fig. 16, which we reproduce in this figure as well. However, now Eve sends Bob two adjacent non-vacuum optical pulses in a joint state $|\Phi^{\text{double}}\rangle$, surrounded by vacuum pulses. The two non-vacuum optical pulses are illustrated in the figure with two grey ovals. To determine $P_{\text{click}}$ and $P_{\text{coin}}$, we are interested in the state of the optical modes $b_2$, $b_1$, $c_2$, $c_1$, $d_2$ and $d_1$. In the figure, the states $|0\rangle$ represent vacuum pulses.

In Fig. 17: To calculate the probabilities $P_{\text{click}}$ and $P_{\text{coin}}$, we use the same linear optics circuit employed in Fig. 16, which we reproduce in this figure as well. However, now Eve sends Bob two adjacent non-vacuum optical pulses in a joint state $|\Phi^{\text{double}}\rangle$, surrounded by vacuum pulses. The two non-vacuum optical pulses are illustrated in the figure with two grey ovals. To determine $P_{\text{click}}$ and $P_{\text{coin}}$, we are interested in the state of the optical modes $b_2$, $b_1$, $c_2$, $c_1$, $d_2$ and $d_1$. In the figure, the states $|0\rangle$ represent vacuum pulses.

In this equation, we have defined the creation operator $e_i = (e_{i1} + e_{i2})/\sqrt{2}$.

with $\mathbb{1}$ denoting the identity operator. That is, $M_{b_1 c_2 d_1}$ corresponds to a simultaneous detection “click” in the modes $b_1$ and $d_1$. By using Eqs. (B5)-(B7)-(B8), we obtain Eq. (20).

**Appendix C: Calculation of $P_{\text{click}}$ and $P_{\text{coin}}$**

This corresponds to the scenario where Eve sends Bob a double non-vacuum optical pulse in a state $|\Phi^{\text{double}}\rangle$ given by Eq. (16).

Like in Appendix B, we consider that Bob’s detectors have detection efficiency $\eta_{\text{det}}$, and Eve’s signals are not affected by channel loss as she could send them to Bob with a transmitter located very close to him. This situation is illustrated in Fig. 17.

According to Eq. (16), the input state in modes $a_i$, where the subindex $i = 0, 1, 2, 3$, represents the time instant, is given by

$$|\Psi\rangle_{a_3 a_2 a_1 a_0} = |0\rangle_{a_3} \sum_{n=0}^{\infty} \frac{\eta_{\text{det}}^n}{\sqrt{n!}} \left( \frac{a_0^+ \eta_{\text{det}}}{\sqrt{2}} \right)^n |0\rangle_{a_2} |0\rangle_{a_1} |0\rangle_{a_0} ,$$  \hspace{1cm} (C1)

where $a_0^+ \eta_{\text{det}}$ denotes the creation operator associated to photons in mode $a$ at the time instant “1” (“2”).

When this state enters the linear optics circuit illustrated in Fig. 17, it can be shown that the output state at the optical modes $b_2$, $b_1$, $c_2$, $c_1$, $d_3$, $d_2$, $d_1$ and $e$ depicted in that figure is of the form

$$|\phi\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e} = |\phi\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e} \otimes |0\rangle_{c_2} ,$$  \hspace{1cm} (C2)

where the state $|\phi\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e}$ is given by

$$|\phi\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e} = \sum_{n=0}^{\infty} \frac{\eta_{\text{det}}^n}{\sqrt{n!}} |n\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e} ,$$  \hspace{1cm} (C3)

and the state $|n\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e}$, which has in total $n$ photons, has the form

$$|n\rangle_{b_2 b_1 c_2 c_1 d_3 d_2 d_1 e} = \frac{1}{\sqrt{n!}} \frac{\eta_{\text{det}}^n}{\sqrt{2}} \left( \sqrt{2(1 - \eta_{\text{det}})} e_0^+ \sqrt{\eta_{\text{det}} t_B} (b_2^+ + b_1^+) + \sqrt{\eta_{\text{det}}(1 - t_B)} \left( -c_3^+ + c_1^+ + d_3^+ + 2d_2^+ + d_1^+ \right) \right)^n$$  \hspace{1cm} (C4)

In the output modes $b_3$, $b_0$, $c_4$, $c_0$, $d_4$ and $d_0$ illustrated in Fig. 17 there are vacuum states that are not relevant.
for the calculations below, as we are only interested in the
detection events that may occur in the time instances “1”
and “2”. Also, we note that the fact that there is vacuum
in mode $c_2$ confirms that the state $|\Psi\rangle_{a_3a_2a_1a_0}$
sent by Eve
preserves the mode of COW-QKD.

As discussed in Appendix B, Bob’s measurement
operators are diagonal in the Fock basis. This means
that they cannot distinguish the state $|\bar{\phi}\rangle_{b_2c_1c_3d_3d_2d_1}$
given by Eq. (C3) from a state $\rho_{b_2b_1c_3d_3d_2d_1}$
given by

$$\rho_{b_2b_1c_3d_3d_2d_1} = \sum_{n=0}^{\infty} |p_n|^2 \langle \bar{n}|_{b_2b_1c_3d_3d_2d_1} \rangle.$$  \hspace{1cm} (C5)

After tracing out the systems $c_3$, $d_3$ and $e$ from

$$|k\rangle_{b_2b_1c_3d_3d_2d_1} = \frac{\sqrt{2}}{\sqrt{k!(3+t_B)^k}} \sum_{l=0}^{k} \sum_{m=0}^{k-l} \sum_{c=0}^{l-m} \binom{k}{l} \binom{k-l}{m} \binom{l}{l-m} \binom{t_B^{m+c}}{l-m} \frac{\sqrt{t_B^{m+c}}}{\sqrt{4^{l-m}}} \sqrt{m!p!(l-m-p)!} \times \langle k | \langle b_2 | | d_2 | (k-l-o) | d_2 | (l-m-p) | d_1 \rangle.$$  \hspace{1cm} (C7)

This state has still non-zero off-diagonal terms in the
Fock basis. So, to simplify the calculations below, we
use again the fact that Bob’s measurement operators are
diagonal in the Fock basis. This means that we can con-

$$\langle k | \langle k |_{b_2b_1c_3d_3d_2d_1} = \frac{2^k}{k!(3+t_B)^k} \sum_{l=0}^{k} \sum_{m=0}^{k-l} \sum_{c=0}^{l-m} \binom{k}{l} \binom{k-l}{m} \binom{l}{l-m} \binom{t_B^{m+c}}{l-m} \frac{\sqrt{t_B^{m+c}}}{\sqrt{4^{l-m}}} \sqrt{m!p!(l-m-p)!} \times \langle k | \langle b_2 | | d_2 | (k-l-o) | d_2 | (l-m-p) | d_1 \rangle.$$  \hspace{1cm} (C8)

That is, it follows that the measurement statistics
provided by $|k\rangle_{b_2b_1c_3d_3d_2d_1}$ match those of $|\bar{k}\rangle_{b_2b_1c_3d_3d_2d_1}$
when both states are measured with Fock diagonal
measurement operators.

Therefore, to obtain $P_{\text{double}}$ and $P_{\text{coin}}$, we use the following state

$$\rho_{b_2b_1c_2c_1d_2d_1} = \sum_{n=0}^{\infty} \frac{|p_n|^2}{4^n} \sum_{k=0}^{n} \binom{n}{k} \left[ 4 - (3+t_B)\eta_{det} \right]^{n-k} \times \langle k | \langle b_2 | (3+t_B)\eta_{det} k | \langle b_2 | | d_2 | (k-l-o) | d_2 | (l-m-p) | d_1 \rangle.$$  \hspace{1cm} (C9)

The probability that Bob observes a single “click” in
his data line can then be calculated as

$$P_{\text{single-click}} = \text{Tr} \left( \rho_{b_2b_1c_2c_1d_2d_1} M_{b_2b_1c_2c_1d_2d_1} \right).$$  \hspace{1cm} (C10)

\[ \begin{align*}
\rho_{b_2b_1c_2c_1d_2d_1} & = \text{Tr}_{d_3e} \left( \rho_{b_2b_1c_3d_3d_2d_1} \otimes |0\rangle \langle 0 |_{c_2} \right) \\
& = \sum_{n=0}^{\infty} \frac{|p_n|^2}{4^n} \sum_{k=0}^{n} \binom{n}{k} \left[ 4 - (3+t_B)\eta_{det} \right]^{n-k} \times \left[ (3+t_B)\eta_{det} k \right] |k\rangle \langle k|_{b_2b_1c_2c_1d_2d_1} \otimes |0\rangle \langle 0 |_{c_2},
\end{align*} \]

where the state $|k\rangle_{b_2b_1c_2c_1d_2d_1}$, which has $k$ photons in total,
has the form

\[ \begin{align*}
M_{b_2b_1c_2c_1d_2d_1} & = \left( \mathds{1}_{b_2} - |0\rangle \langle 0 |_{b_2} \otimes |0\rangle \langle 0 |_{b_1} \otimes \mathds{1}_{c_2c_1d_2d_1} \\
& + |0\rangle \langle 0 |_{b_2} \otimes (\mathds{1}_{b_1} - |0\rangle \langle 0 |_{b_1} \otimes \mathds{1}_{c_2c_1d_2d_1} \right) \\
& \text{Tr}_{d_3e} \left( \rho_{b_2b_1c_3d_3d_2d_1} \otimes |0\rangle \langle 0 |_{c_2} \right) \\
& = \sum_{n=0}^{\infty} \frac{|p_n|^2}{4^n} \left[ \left( \frac{t_B\eta_{det}}{2} \right)^n - (1 - t_B\eta_{det})^n \right].
\end{align*} \]
Likewise, we have that the probability that Bob observes two detection “clicks” in his data line, one in $b_1$ and one in $b_2$, has the form

$$P_{\text{double-click}} = \text{Tr} \left( \hat{\rho}_{b_2 b_1 c_2 c_1 d_2 d_1} M_{\text{double-click}} \right), \quad (C13)$$

where the operator $M_{\text{double-click}}$ is given by

$$M_{\text{double-click}} = (\mathbb{1}_{b_2} - |0\rangle \langle 0|_{b_2}) \otimes (\mathbb{1}_{b_1} - |0\rangle \langle 0|_{b_1}) \otimes \mathbb{1}_{c_2 c_1 d_2 d_1}. \quad (C14)$$

By combining Eqs. (C9)-(C13)-(C14), we obtain

$$P_{\text{double-click}} = 1 - \sum_{n=0}^{\infty} |p_n|^2 \left[ 2 \left( 1 - \frac{t_B \eta_{\text{det}}}{2} \right)^n \right. - \left. (1 - t_B \eta_{\text{det}})^n \right]. \quad (C15)$$

The average number of “clicks” in Bob’s data line can be written as

$$P_{\text{click}} = P_{\text{single-click}} + 2P_{\text{double-click}}. \quad (C16)$$

The factor two that multiplies $P_{\text{double-click}}$ arises because the two non-vacuum optical pulses sent by Eve correspond to two different signals sent by Alice. That is, in this case Bob do not assign double “clicks” to single “click” events. By combining Eqs. (C12)-(C15)-(C16), we obtain Eq. (21).

The parameter $P_{\text{coin}}$ can also be expressed as the sum of two terms

$$P_{\text{double}} = P_{\text{single-coin}} + 2P_{\text{double-coin}}, \quad (C17)$$

where $P_{\text{single-coin}}$ ($P_{\text{double-coin}}$) denotes the probability to observe a coincidence detection event only in one of the time instants “1” or “2” (in both time instants).

The probability $P_{\text{single-coin}}$ is given by

$$P_{\text{single-coin}} = P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2} + P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2} + P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2} + P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2}, \quad (C18)$$

where $P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2}$ denotes the probability that Bob observes a “click” in the modes $b_1$, $c_1$ and/or $d_1$, and no “click” in the modes $b_2$, $c_2$ and $d_2$. That is, this is the probability that Bob observes a coincidence detection event in the time instant “1” and no “click” in the time instant “2”. This probability can be expressed as

$$P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2} = \text{Tr} \left( \hat{\rho}_{b_2 b_1 c_2 c_1 d_2 d_1} M_{b_1, c_1 d_1, b_2, c_2 d_2} \right), \quad (C19)$$

where the state $\hat{\rho}_{b_2 b_1 c_2 c_1 d_2 d_1}$ is given by Eq. (C9), and the operator $M_{b_1, c_1 d_1, b_2, c_2 d_2}$ has the form

$$M_{b_1, c_1 d_1, b_2, c_2 d_2} = |0\rangle \langle 0|_{b_2} \otimes (\mathbb{1}_{b_1} - |0\rangle \langle 0|_{b_1}) \otimes (\mathbb{1}_{c_1 d_1} - |0\rangle \langle 0|_{c_1 d_1}) \otimes |0\rangle \langle 0|_{c_2 d_2}, \quad (C20)$$

By combining Eqs. (C9)-(C19)-(C20), we obtain

$$P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2} = \sum_{n=0}^{\infty} |p_n|^2 \left\{ 1 - \frac{\eta_{\text{det}}}{2} \right\}^n - \left[ 1 - \frac{(3 - t_B)\eta_{\text{det}}}{4} \right]^n - \left[ 1 - \frac{(1 + t_B)\eta_{\text{det}}}{2} \right]^n + \left[ 1 - \frac{(3 + t_B)\eta_{\text{det}}}{4} \right]^n \right\}, \quad (C21)$$

The other probabilities that appear in Eq. (C18) are defined similarly, and can be obtained by following an analogous procedure to that used to calculate $P_{\text{click}}^{b_1, c_1 d_1, b_2, c_2 d_2}$. For simplicity, we omit the details here.

The results are shown in Table VI. By inserting the values of these probabilities in Eq. (C18), we find that $P_{\text{single-coin}}$ can be expressed as

$$P_{\text{single-coin}} = \sum_{n=0}^{\infty} |p_n|^2 \left\{ -3 \left[ 1 - \frac{\eta_{\text{det}}}{2} \right]^n + 4 \left[ 1 - \frac{(3 - t_B)\eta_{\text{det}}}{4} \right]^n + 2 \left[ 1 - \frac{(1 + t_B)\eta_{\text{det}}}{2} \right]^n - 2 \left[ 1 - \frac{(3 + t_B)\eta_{\text{det}}}{4} \right]^n \right\}$$

$$- 3 \left\{ 1 - \frac{(1 + t_B)\eta_{\text{det}}}{2} \right\}^n + 2 \left\{ 1 - \frac{(1 + 3t_B)\eta_{\text{det}}}{4} \right\}^n + 1 \left\{ 1 - \frac{(1 - t_B)\eta_{\text{det}}}{2} \right\}^n - 2 \left\{ 1 - \frac{3(1 - t_B)\eta_{\text{det}}}{4} \right\}^n \right\}, \quad (C22)$$
\[ p_{\text{click}}^{b_1,c_1,d_1,b_2,c_2,d_2} = \sum_{n=0}^{\infty} |p_n|^2 \left\{ \left[ 1 - \frac{1 - t_B \eta_{\text{det}}}{2} \right]^n - 2 \left[ 1 - \frac{3 - t_B \eta_{\text{det}}}{4} \right]^n + 2 \left[ 1 - \frac{3 - t_B \eta_{\text{det}}}{4} \right]^n - \left[ 1 - \frac{1 + t_B \eta_{\text{det}}}{2} \right]^n \right\} \]

\[ p_{\text{double-coin}} = \sum_{n=0}^{\infty} |p_n|^2 \left\{ \left[ 1 - \frac{t_B \eta_{\text{det}}}{2} \right]^n - 1 - \frac{3 - t_B \eta_{\text{det}}}{4} \right\} \]

TABLE VI: Values of the probabilities that appear in Eq. (C18).

On the other hand, we have that the parameter \( P_{\text{double-coin}} \) is given by the probability \( p_{\text{click}}^{b_1,c_1,d_1,b_2,c_2,d_2} \). This means that it can be written as

\[ P_{\text{double-coin}} = \text{Tr} \left( \hat{p}_{b_2} \hat{b}_c \hat{c}_d \hat{d}_4 M_{b_1,c_1,d_1,b_2,c_2,d_2} \right), \]

where the operator \( M_{b_1,c_1,d_1,b_2,c_2,d_2} \) has the form

\[
M_{b_1,c_1,d_1,b_2,c_2,d_2} = \left( \mathbb{1}_{b_2} - |0\rangle \langle 0|_{b_2} \right) \otimes \left( \mathbb{1}_{c_1} - |0\rangle \langle 0|_{c_1} \right) \\
\otimes \left( \mathbb{1}_{c_2} - |0\rangle \langle 0|_{c_2} \right).
\]

That is, this operator corresponds to having a “click” in the modes \( b_2, c_2 \) and/or \( d_2, b_1, \) and \( c_1 \) and/or \( d_1 \). By combining Eqs. (C9)-(C23)-(C24), we obtain

\[ P_{\text{double-coin}} = 1 + \sum_{n=0}^{\infty} |p_n|^2 \left\{ \left[ 1 - \frac{t_B \eta_{\text{det}}}{2} \right]^n - \left[ 1 - \frac{3 - t_B \eta_{\text{det}}}{4} \right]^n + \left[ 1 - \frac{3 - t_B \eta_{\text{det}}}{4} \right]^n - \left[ 1 - \frac{1 + t_B \eta_{\text{det}}}{2} \right]^n \right\} \]

Finally, from Eqs. (C17)-(C22)-(C25), we obtain that \( P_{\text{double-coin}} \) is given by Eq. (21).

Appendix D: Parameters \( p_{\text{click}}(k) \) and \( p_{\text{coin}}(k) \)

In this Appendix, we provide the value for \( p_\tau(k) \), with \( \tau \in \{\text{click, coin}\} \), that we obtain after combining Eqs. (20)-(21)-(22),
\[
p_{\text{click}}(k) = (k-1) \left\{ 1 - \frac{1}{2} \sum_{n=0}^{\infty} \left[ |q_n|^2 \left( 1 - t_B \eta_{\text{det}} \right)^n + |p_n|^2 \left( 1 - \frac{t_B \eta_{\text{det}}}{2} \right)^n \right] \right\},
\]
\[
p_{\text{coin}}(k) = (k-1) \left\{ 1 - \frac{1}{2} \sum_{n=0}^{\infty} \left[ |q_n|^2 \left\{ \left[ 1 - (1 - t_B \eta_{\text{det}})^n \right] + (1 - \eta_{\text{det}} t_B)^n \right\} - \left[ 1 - (1 + t_B \eta_{\text{det}})^n \right] \right] \right\}
\]
\[
- \frac{|p_n|^2}{2} \left\{ \left[ 1 - \eta_{\text{det}} \right]^n - 2 \left[ 1 - \frac{t_B \eta_{\text{det}}}{2} \right]^n \right\} + \left[ 1 - \frac{(1 + t_B \eta_{\text{det}})}{4} \right]^n - \left[ 1 - \frac{(1 - t_B \eta_{\text{det}})}{2} \right]^n \right\} \right\},
\]
for \( k \geq 2 \).

**Appendix E: Expected Gain and coincidence detection rate**

In this Appendix, we calculate the expected gain and coincidence detection rate at Bob’s side in the absence of Eve’s attack. We denote these two expected values by \( G \) and \( G_{\text{coin}} \), respectively. For this, we use a simple channel model.

Precisely, we consider a lossy quantum channel, and we disregard any misalignment effect both in the channel and in Alice’s and Bob’s apparatuses. Also, as already mentioned, we neglect the effect of the dark count probability of Bob’s detectors. In particular, let \( \eta_{\text{channel}} = 10^{-\alpha_{\text{channel}}L/10} \) denote the transmittance of the quantum channel, where \( \alpha_{\text{channel}} \) (L) represents the loss coefficient (length) of the channel measured in dB/km (km). Also, we define \( \eta_{\text{sys}} = \eta_{\text{channel}} \eta_{\text{det}} \), where \( \eta_{\text{det}} \) is the detection efficiency of Bob’s detectors, which we assume is equal for all of them.

Let us first calculate the gain \( G \). We need to consider three cases, depending on the actual signal sent by Alice. If Alice sends Bob the signal \( |\varphi_0\rangle \), he receives in his data line the state \( |0\rangle \sqrt{\eta_{\text{sys}} B \alpha} \). This means that he can only observe a “click” in that line in the first time instant, which happens with probability

\[
P_{\text{click},|\varphi_0\rangle} = 1 - \left| \langle 0 | \sqrt{\eta_{\text{sys}} B \alpha} \right|^2 = 1 - e^{-\eta_{\text{sys}} t_B \mu},
\]

where \( \mu = |\alpha|^2 \). Likewise, it is straightforward to show that the probability that Bob observes a “click” in his data line when Alice sends him the signal \( |\varphi_1\rangle \) satisfies

\[
P_{\text{click},|\varphi_1\rangle} = P_{\text{click},|\varphi_0\rangle}.
\]

On the other hand, if Alice sends Bob the signal \( |\varphi_2\rangle \), we have that Bob receives in his data line the signal \( \sqrt{\eta_{\text{sys}} B \alpha} \sqrt{\eta_{\text{sys}} B \alpha} \) and, therefore, he observes a “click” with probability

\[
P_{\text{click},|\varphi_2\rangle} = 1 - \left| \langle 0 | \sqrt{\eta_{\text{sys}} B \alpha} \right|^4 = 1 - e^{-2\eta_{\text{sys}} t_B \mu}.
\]

In Eq. (E2) we have taken into account that whenever Bob observes in his data line two detection “clicks” within the same signal, he randomly assigns a single “click” event to it.

Putting all together, we have that \( G \) can be written as

\[
G = \sum_{j=0}^{2} p_{j|\varphi_j\rangle} P_{\text{click},|\varphi_j\rangle}
= 1 - (1 - f)e^{-\eta_{\text{sys}} t_B \mu} - f e^{-2\eta_{\text{sys}} t_B \mu},
\]

where the probabilities \( p_{j|\varphi_j\rangle} \), with \( j = 0, 1, 2 \), are given by Eq. (1). We note that the parameter \( L_{\text{zero}} \) considered in the main text corresponds to the value of \( L \) such that \( G = G_{\text{zero}} \).

To obtain \( G_{\text{coin}} \), we need to evaluate six cases, which depend on the actual signal state sent by Alice and on the previous optical pulse that she sent to Bob. The probability that the previous optical pulse sent by Alice is in a state \( |0\rangle \) (\( |\alpha\rangle \)), which we shall denote by \( p_{|0\rangle} (p_{|\alpha\rangle}) \), is equal to \( p_{|\varphi_j\rangle} (1 - p_{|\varphi_j\rangle}) \). According to Eq. (1), this means that

\[
p_{|0\rangle} = \frac{1 - f}{2}, \quad \text{and} \quad p_{|\alpha\rangle} = \frac{1 + f}{2}.
\]

Let us consider first the scenario where Alice sends Bob the signal \( |\varphi_0\rangle \) preceded by the optical pulse \( |0\rangle \), which happens with probability \( p_{|0\rangle} P_{|\varphi_0\rangle} = (1 - f)^2/4 \). This scenario is illustrated in Fig. 18. That is, here Alice sends him the following three optical pulses \( |0\rangle \oplus |\alpha\rangle \oplus |0\rangle \oplus |\alpha\rangle \), where we have introduced the subscripts \( a \) to explicitly indicate the input mode \( a \) and the time instants \( i \). We shall denote by \( P_{\text{coin},|\varphi_0\rangle|0\rangle} \) the average number of coincident detection events observed by Bob (in the relevant instants “1” and “2”) in this scenario. This parameter can be written as

\[
P_{\text{coin},|\varphi_0\rangle|0\rangle} = P_{\text{coin},|\varphi_0\rangle|0\rangle,1} + P_{\text{coin},|\varphi_0\rangle|0\rangle,2} + 2 P_{\text{coin},|\varphi_0\rangle|0\rangle,\text{double}},
\]

where \( P_{\text{coin},|\varphi_0\rangle|0\rangle,j} \), with \( j = 1, 2 \), represents the probability that Bob observes a coincidence detection event only in the time instant “\( j \)” and no coincidence detection event in the time instant “\( 1 + [(j - 1) \oplus 1] \)”,
\(P_{\text{coin},|\varphi_1\rangle|0\rangle,\text{double}}\) denotes the probability that Bob observes a coincidence detection event both in the time instants “1” and/or “2”.

As shown in Fig. 18, there is vacuum in the data line in the time instant “2” (i.e., in the mode \(b_2\)). This means that no coincidence detection event is possible in that time instant, i.e.,

\[
P_{\text{coin},|\varphi_0\rangle|0\rangle,2} = P_{\text{coin},|\varphi_0\rangle|0\rangle,\text{double}} = 0. \tag{E6}
\]

On the other hand, in the time instant “1” there is a coherent state \(|\sqrt{\eta_{\text{sys}}t_B/\alpha}\rangle_{i_1}\) in the data line, and a vacuum state \(|0\rangle_{c_1}\) and a coherent state \(|\sqrt{\eta_{\text{sys}}(1-t_B)/2\alpha}\rangle_{d_1}\) in the two arms of the monitoring line’s interferometer. This means that \(P_{\text{coin},|\varphi_0\rangle|0\rangle,1}\) is given by

\[
P_{\text{coin},|\varphi_0\rangle|0\rangle,1} = \left[1 - |\langle 0| \sqrt{\eta_{\text{sys}}t_B/\alpha} \rangle|^2\right] \times \left[1 - |\langle 0| \sqrt{\eta_{\text{sys}}(1-t_B)/2\alpha} \rangle|^2\right] = (1 - e^{-\eta_{\text{sys}}t_B\mu}) (1 - e^{-\eta_{\text{sys}}(1-t_B)\mu/2}). \tag{E7}
\]

By combining Eqs. (E5)-(E6) we obtain that \(P_{\text{coin},|\varphi_0\rangle|0\rangle}\) is also given by Eq. (E7).

The other five cases can be analyzed similarly and we omit the details here for simplicity. We find that

\[
P_{\text{coin},|\varphi_0\rangle|\alpha\rangle} = \frac{1}{2} P_{\text{coin},|\varphi_2\rangle|\alpha\rangle} = \left(1 - e^{-\eta_{\text{sys}}t_B\mu}\right) \times \left(1 - e^{-\eta_{\text{sys}}(1-t_B)\mu}\right), \tag{E8}
\]

\[
P_{\text{coin},|\varphi_1\rangle|0\rangle} = P_{\text{coin},|\varphi_1\rangle|\alpha\rangle} = \left(1 - e^{-\eta_{\text{sys}}t_B\mu}\right) \times \left(1 - e^{-\eta_{\text{sys}}(1-t_B)\mu/2}\right), \tag{E9}
\]

\[
P_{\text{coin},|\varphi_2\rangle|0\rangle} = \left(1 - e^{-\eta_{\text{sys}}t_B\mu}\right) \left[1 - e^{-\eta_{\text{sys}}(1-t_B)\mu/2}\right] + \left(1 - e^{-\eta_{\text{sys}}(1-t_B)\mu}\right). \tag{E10}
\]

Finally, if we include the a priori probabilities associated to the different six cases, we have that

\[
G_{\text{coin}} = \sum_{j=0}^{2} \sum_{i \in \{0,\alpha\}} P_{\varphi_j} P_{\eta_j} P_{\text{coin},|\varphi_j\rangle|l\rangle} = \frac{1 - e^{-\eta_{\text{sys}}t_B\mu}}{4} \times \left\{(1 - f)(3 + f) \left[1 - e^{-\eta_{\text{sys}}(1-t_B)\mu/2}\right] + (1 + 6f + f^2) \left[1 - e^{-\eta_{\text{sys}}(1-t_B)\mu}\right]\right\}. \tag{E11}
\]

Appendix F: Monitoring detection rates: Eve’s USD measurement

In this Appendix, we consider Eve’s USD measurement when Alice and Bob monitor the detection rates of the signals. This measurement has four possible outcomes. Three of them identify each of the signals \(|\varphi_i\rangle\), with \(i = 0, 1, 2\), while the fourth outcome denotes an inconclusive result.

Precisely, we shall consider a USD measurement that maximizes the following quantity,

\[
(1 - \zeta)q_{s,\zeta} + \zeta q_{s,\zeta}^d, \tag{F1}
\]

for a certain \(\zeta \in [f, 1]\). Here, \(q_{s,\zeta}\) (\(q_{s,\zeta}^d\)) represents the conditional probability that the result is conclusive when the input signal to the measurement is a key generation (decay) signal. In Eq. (F1), we use the fact that, for the optimal USD measurement, \(q_{s,\zeta}\) is equal for both key generation signals, as they have the same \textit{a priori} probability.

If \(\zeta = f\), we recover the solution provided by the optimal USD measurement in [48], i.e., the one that maximizes the probability to deliver a conclusive result. The case \(\zeta = 1\) corresponds to the USD measurement that provides the highest possible value for \(q_{s,\zeta}^d\), which we denote by \(q_{s,\zeta}^d_{\text{max}}\). When \(f < \zeta < 1\), we are in an intermediate scenario where \(q_{s,\zeta}^d < q_{s,\zeta}^d_{\text{max}}\), with \(q_{s,\zeta}^d\) referring to the optimal solution in [48]. That is, with the parameter \(\zeta\) we can tune the probability to correctly identify a decay signal up to its maximum allowed value. The drawback of using \(\zeta \neq f\) is that the overall probability to obtain a conclusive result (see Eq. (F5) below) decreases when compared to its maximum possible value.
From [48], it follows directly that the optimal values for \( q_{E,\zeta} \) and \( q_{d,E,\zeta} \) as a function of \( \zeta, \mu \) and the parameter \( \xi = \zeta/[2(1-\zeta)] \), are given by
\[
q_{E,\zeta} = 1 - \exp(-\mu) \quad \text{and} \quad q_{d,E,\zeta} = 0, \quad (F2)
\]
if \( \sqrt{\xi} \leq \exp(-\mu/2) \). On the other hand, we have
\[
q_{E,\zeta} = 1 + \exp(-\mu) - \exp(-\mu/2)/\sqrt{2\zeta/[1-\zeta]} ,
q_{d,E,\zeta} = 1 - \sqrt{\xi^{-1}} \exp(-\mu/2), \quad (F3)
\]
if \( \sqrt{\xi} > \exp(-\mu/2) \) and \( \cosh(\mu/2) > \sqrt{\xi} \). Finally, if \( \sqrt{\xi} > \exp(-\mu/2) \) and \( \cosh(\mu/2) < \sqrt{\xi} \), we obtain
\[
q_{E,\zeta} = 0 \quad \text{and} \quad q_{d,E,\zeta} = \tanh(\mu/2). \quad (F4)
\]
Given \( q_{E,\zeta} \) and \( q_{d,E,\zeta} \), the probability \( p_{E,\zeta} \) that Eve obtains a conclusive result with her USD measurement is then given by
\[
p_{E,\zeta} = (1 - f)q_{E,\zeta} + f q_{d,E,\zeta}. \quad (F5)
\]

**Appendix G: Expected Gain \( G_{\text{decoy}} \)**

Here, we calculate the expected gain of the decoy signals \( |\varphi_2\rangle \) at Bob’s data line in the absence of Eve’s attack. For this, we use the simple channel model introduced in Appendix E.

In particular, from Eqs. (1)-(E2)-(E3) we have that
\[
G_{\text{decoy}} = p_{|\varphi_2\rangle} \langle P_{\text{click}} \rangle = f \left( 1 - e^{-2\eta_{\text{sys}}t_{\text{sec}}} \right). \quad (G1)
\]

**Appendix H: Optimal USD measurement**

In this Appendix, we calculate Eve’s optimal USD measurement to discriminate the four signal states, \( |\varphi_i\rangle \) with \( i = 0, \ldots, 3 \), sent by Alice in the four-state COW-QKD protocol considered in Sec. VI.

This measurement is described by a positive-operator-valued measure (POVM) with five elements \( E_i \geq 0 \), with \( i = 0, \ldots, 4 \), that satisfy \( \sum_{i=0}^4 E_i = 1 \), with \( 1 \) being the identity operator. \( E_i \) identifies the signal \( |\varphi_i\rangle \), with \( i = 0, \ldots, 3 \), while \( E_4 \) corresponds to an inconclusive result.

That is, we have that \( p_{|\varphi_i\rangle} = \langle \varphi_i | E_j | \varphi_i \rangle = 0 \) \( \forall i \neq j \) with \( i, j = 0, \ldots, 3 \), with \( p_{|\varphi_i\rangle} \) being the conditional probability of obtaining a result associated to the operator \( E_j \) when measuring the state \( |\varphi_i\rangle \). Moreover, since the signals \( |\varphi_0\rangle \) and \( |\varphi_1\rangle \) are sent with the same a priori probability, we impose \( p_{|\varphi_0\rangle} = p_{|\varphi_1\rangle} \). This is illustrated in Table VII.

This means that the probability that Eve obtains a conclusive measurement result when she measures Alice’s signals one by one with the USD measurement described above is given by
\[
p_{E} = \sum_{i=0}^3 p_{|\varphi_i\rangle} p_{|\varphi_i\rangle} = (1 - f_d - f_v) q_s + f_d q_{d,s} + f_v q_{d,v}, \quad (H1)
\]

**Table VII:** Conditional probabilities associated to Eve’s optimal USD measurement. \( E_4 \) corresponds to an inconclusive result. Here, we use the following notation:
\[
p_{|\varphi_0\rangle} = p_{|\varphi_1\rangle} = q_s, p_{|\varphi_2\rangle} = q_{d,s}, p_{|\varphi_3\rangle} = q_{d,v}\]
\[
\text{while the probability to obtain an inconclusive result is } p_{\text{inc}} = 1 - p_{E}.
\]

Next, we explain how to solve the SDP given by Eq. (H2) numerically.

1. **Solving the SDP numerically**

For this, we first rewrite Eq. (H2) in a more convenient way. Precisely, we express Alice’s signals \( |\varphi_i\rangle \) in some orthonormal basis \( \{ |b_j\rangle \}_{j=0,\ldots,3} \) of a four-dimensional Hilbert space \( \mathcal{H}_4 \),
\[
|\varphi_0\rangle = |b_0\rangle, \quad |\varphi_1\rangle = e^{-|\alpha|^2/2} |b_0\rangle + \sqrt{1 - e^{-2|\alpha|^2}} |b_1\rangle, \quad |\varphi_2\rangle = e^{-|\alpha|^2/2} |b_0\rangle + e^{-|\alpha|^2} \frac{1 - e^{-|\alpha|^2}}{\sqrt{1 - e^{-2|\alpha|^2}}} |b_1\rangle + \frac{1 - e^{-|\alpha|^2}}{\sqrt{1 - e^{-2|\alpha|^2}}} |b_2\rangle, \quad |\varphi_3\rangle = e^{-|\alpha|^2/2} |b_0\rangle + e^{-|\alpha|^2} \frac{1 - e^{-|\alpha|^2}}{\sqrt{1 - e^{-2|\alpha|^2}}} |b_1\rangle - e^{-|\alpha|^2} \frac{1 - e^{-|\alpha|^2}}{\sqrt{1 - e^{-2|\alpha|^2}}} |b_2\rangle + \left( 1 - e^{-|\alpha|^2} \right) |b_3\rangle.
\]

This implies that we can restrict ourselves to operators \( E_j \) that act on \( \mathcal{H}_4 \).

Next, we rewrite the states \( \rho_i = |\varphi_i\rangle \langle \varphi_i | \) and the operators \( E_j \) in terms of the generalized Gell-Mann matrices.
in $\mathcal{H}_n$. In general, say in $\mathcal{H}_n$, these matrices are $n \times n$ matrices $\sigma_k$, with $k = 0, \ldots, n^2 - 1$, that satisfy: $\sigma_0 = I_n$ is the identity operator in $\mathcal{H}_n$, and the remaining $\sigma_k$ are traceless Hermitian matrices fulfilling

$$
\text{Tr}(\sigma_k) = n\delta_{k0},
$$
$$
\text{Tr}(\sigma_k \sigma_l) = n\delta_{kl},
$$
(H4)

where $\delta_{kl}$ represents the Kronecker delta.

The matrices $\sigma_k$ can be obtained by using three different types of matrices. First, we take $C_n^2 = n!/2[(n-2)!]$ symmetric matrices with all its elements equal to zero except the $p$th row $q$th column element and the $q$th row $p$th column element that are equal to $\sqrt{n/2}$, with $1 \leq p < q \leq n$. Then, we take $C_n^2$ antisymmetric matrices with all its elements equal to zero except the $p$th row $q$th column element that is equal to $-i\sqrt{n/2}$ and the $q$th row $p$th column element that is equal to $i\sqrt{n/2}$, with $1 \leq p < q \leq n$. Finally, we take $n - 1$ diagonal matrices, which, for convenience, we denote by $\Delta^{(d)}$, with $1 \leq d \leq n - 1$, that satisfy

$$
\Delta^{(1)} = \sqrt{\frac{n}{2C_n^2}} \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
0 & -1 & 0 & \cdots & 0 \\
0 & 0 & -1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & -1
\end{pmatrix},
$$

$$
\Delta^{(2)} = \sqrt{\frac{n}{2C_n^2}} \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & -1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & -1
\end{pmatrix},
$$

$$
\Delta^{(n-1)} = \sqrt{\frac{n}{2C_n^2}} \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & -1
\end{pmatrix}.
$$
(H5)

In doing so, we indeed obtain $C_n^2 + C_n^2 + (n-1) = n^2 - 1$ matrices $\sigma_k$, with $k = 1, \ldots, n^2 - 1$, that satisfy Eq. (H4).

By using these matrices, we can rewrite $\rho_i$ and $E_j$ as follows

$$
\rho_i = \sum_{k=0}^{n^2-1} \varphi_{ik} \sigma_k,
$$
$$
E_j = \sum_{k=0}^{n^2-1} e_{jk} \sigma_k,
$$
(H6)

for certain known real coefficients $\varphi_{ik}$, and for certain unknown real coefficients $e_{jk}$.

For simplicity, we omit here the explicit values of the coefficients $\varphi_{ik}$. They can be obtained directly from Eq. (H3) by using the fact that

$$
\varphi_{ik} = \frac{1}{n} \text{Tr}(\rho_i \sigma_k).
$$
(H7)

This means, in particular, that the conditional probabilities $p_{ij}$ can now be expressed as

$$
p_{ij} = \text{Tr}(E_j \rho_i) = \sum_{k=0}^{n^2-1} \varphi_{ik} e_{jk},
$$
(H8)

where we have used Eqs. (H4)-(H6).

Putting all together, and taking into account that $n = 4$, we find that the SDP given by Eq. (H2) can be written as

$$
\text{maximize} \quad 4 \sum_{k=0}^{15} \left[ (1 - f_d - f_{\text{vac}}) \varphi_{0k} e_{0k} + f_d \varphi_{2k} e_{2k} + f_{\text{vac}} \varphi_{3k} e_{3k} \right]
$$

s. t. \quad \sum_{k=0}^{15} \sum_{j=0}^{4} e_{jk} \sigma_k - \sigma_0 = 0,

$$
\sum_{k=0}^{15} e_{jk} \sigma_k \geq 0 \quad \forall j = 0, \ldots, 4,
$$

$$
\sum_{k=0}^{15} \varphi_{ik} e_{jk} = 0 \quad \forall i, j = 0, \ldots, 3, \text{ with } i \neq j,
$$

$$
\sum_{k=0}^{15} (\varphi_{0k} e_{0k} - \varphi_{1k} e_{1k}) = 0,
$$
(H9)

where the unknown parameters are, as already mentioned, the coefficients $e_{jk}$. In this format, the SDP can be readily solved numerically to obtain the conditional probabilities $q_s$, $q_{\text{inc}}$, $q_s^{\text{d}}$, $q_{\text{inc}}^{\text{d}}$, $q_s^{\text{r}}$, and $q_{\text{inc}}^{\text{r}}$ given by Table VII and, thus, also obtain the conclusive probability $p_c$ given by Eq. (H1). For this, we use the solver Mosek [57] and the input tool YALMIP [58].

[1] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics 8, 595 (2014).
[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92, 025002 (2020).
[3] S. Pirandola et al., Advances in Quantum Cryptography, Adv. Opt. Photon. 12, 1012-1236 (2020).
[4] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, J. Am. Inst. Electr. Eng. 45, 109 (1926).
[5] C. H. Bennett, and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, (IEEE Press, Bangalore, India New York, 1984), p. 175.

[6] A. K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, 661 (1991).

[7] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68, 3121 (1992).

[8] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, Phys. Rev. Lett. 89, 037902 (2002).

[9] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature 509, 475 (2014).

[10] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, Towards practical and fast Quantum Cryptography, preprint arXiv:quant-ph/0411022 (2004).

[11] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. 91, 057901 (2003).

[12] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. 94, 230504 (2005).

[13] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. 94, 230503 (2005).

[14] M. Koashi, Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse, Phys. Rev. Lett. 93, 120501 (2004).

[15] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwan-tudawe, Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse, Phys. Rev. A 80, 032302 (2009).

[16] X. Ma, C.-H. F. Fung, and H.-K. Lo, Quantum key distribution with entangled photon sources, Phys. Rev. A 76, 012307 (2007).

[17] D. Mayers, and A. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science, (IEEE Computer Society, Los Alamitos, California, 1998), p. 503.

[18] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. 98, 230501 (2007).

[19] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 108, 130503 (2012).

[20] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature 557, 400 (2018).

[21] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A 98, 062323 (2018).

[22] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. 5, 64 (2019).

[23] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Experimental Quantum Key Distribution with Decoy States, Phys. Rev. Lett. 96, 070502 (2006).

[24] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding, Phys. Rev. Lett. 98, 010505 (2007).

[25] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber, Phys. Rev. Lett. 98, 010503 (2007).

[26] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, Opt. Express 16, 18790 (2008).

[27] A. Poppe et al., Practical quantum key distribution with polarization entangled photons, Opt. Express 12, 3865-3871 (2004).

[28] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorinser, E. Querasser, T. Matys, H. Hübel, and A. Zeilinger, A fully automated entanglement-based quantum cryptography system for telecom fiber networks, New J. Phys. 11, 045013 (2009).

[29] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, Nat. Photonics 1, 343 (2007).

[30] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. 87, 194108 (2005).

[31] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres, New J. Phys. 11, 075003 (2009).

[32] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, Nat. Photonics 9, 163 (2015).

[33] A. Rubenok, J. A. Slater, P. Chan, I. Lucia-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. 111, 130501 (2013).

[34] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A 88, 052303 (2013).

[35] Y. Liu et al., Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. 111, 130502 (2013).

[36] A. Boaron et al., Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. 121, 190502 (2018).

[37] D. Stucki, M. Legrè, F. Buntschu, B. Claussen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, and P. Monbaron, Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. 13, 123001 (2011).

[38] M. Sasaki et al., Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express 19, 10387 (2011).

[39] J. Qi, Quantum communications leap out of the lab, Nature 508, 441 (2014).

[40] J. Dynes et al., Cambridge quantum network, npj Quantum Information 5, 1 (2019).

[41] M. Pittaluga et al., 600 km repeater-like quantum communications with dual-band stabilisation, preprint arXiv:2012.15099 (2020).

[42] S.-K. Liao et al., Satellite-to-ground quantum key distribution, Nature 549, 43 (2017).

[43] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kita-
mura, M. Sasaki, and M. Toyoshima, Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nat. Photon. 11, 502 (2017).

[44] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. 5, 5235 (2014).

[45] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. 8, 15043 (2017).

[46] ID Quantique, Geneva, Switzerland, http://www.idquantique.com.

[47] J. González-Payo, R. Trényi, W. Wang, and M. Curty, Upper Security Bounds for Coherent-One-Way Quantum Key Distribution, Phys. Rev. Lett. 125, 260510 (2020).

[48] R. Trényi, and M. Curty, Zero-error attack against coherent-one-way quantum key distribution, preprint arXiv:2101.07192 (2021).

[49] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, Security of Distributed-Phase-Reference Quantum Key Distribution, Phys. Rev. Lett. 109, 260501 (2012).

[50] C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography, Quant. Inf. Comput. 7, 639 (2007).

[51] D. A. Kronberg, A. S. Nikolaeva, Y. V. Kurochkin, and A. K. Fedorov, Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol, Phys. Rev. A 101, 032334 (2020).

[52] A. Chefles, Unambiguous discrimination between linearly independent quantum states, Phys. Lett. A 239, 339 (1998).

[53] A. Chefles, and S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states, Phys. Lett. A 250, 223 (1998).

[54] Y. C. Eldar, A semidefinite programming approach to optimal unambiguous discrimination of quantum states, IEEE Trans. Inform. Theory 49, 446 (2003).

[55] M. Curty, M. Lewenstein, and Norbert Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, Phys. Rev. Lett. 92, 217903 (2004).

[56] This corresponds to the case where Eq. (7) holds, which is the parameter regime we are interested in, as this condition is satisfied by the experimental implementations of COW-QKD.

[57] MOSEK ApS, Copenhagen, Denmark, https://www.mosek.com.

[58] J. Löfberg, in Proceedings of the CACSD Conference (Taipei, Taiwan, 2004), pp. 284-289, available from https://yalmip.github.io.

[59] Obviously, $|\varphi_3\rangle = |\varphi_{\text{vac}}\rangle$. However, we prefer to use two different notations for the same signal because it allows us to distinguish the cases where Alice sent the state $|\varphi_3\rangle$ and Eve correctly identified this state (in which case we use $|\varphi_3\rangle$), from those instances where Eve obtained an inconclusive result with her measurement and she replaced the original signal sent by Alice with two vacuum optical pulses (in which case we use $|\varphi_{\text{vac}}\rangle$).