archive ouverte UNIGE
http://archive-ouverte.unige.ch

Article

# Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography

BRANCIARD, Cyril, GISIN, Nicolas, SCARANI, Valerio

**Abstract**

The differential-phase-shift (DPS) and the coherent-one-way (COW) are among the most practical protocols for quantum cryptography, and are therefore the object of fast-paced experimental developments. The assessment of their security is also a challenge for theorists: the existing tools, that allow to prove security against the most general attacks, do not apply to these two protocols in any straightforward way. We present new upper bounds for their security in the limit of large distances (d≥50 km with typical values in optical fibers) by considering a large class of collective attacks, namely those in which the adversary attaches ancillary quantum systems to each pulse or to each pair of pulses. We introduce also two modified versions of the COW protocol, which may prove more robust than the original one.

Reference

BRANCIARD, Cyril, GISIN, Nicolas, SCARANI, Valerio. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New journal of physics*, 2008, vol. 10, no. 1, p. 013031

DOI : 10.1088/1367-2630/10/1/013031

Available at:
http://archive-ouverte.unige.ch/unige:36626

Disclaimer: layout of this document may differ from the published version.

UNIVERSITÉ DE GENÈVE

New Journal of Physics
The open-access journal for physics

# Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography

**Cyril Branciard**[1], **Nicolas Gisin**[1] **and Valerio Scarani**[2]

[1] Group of Applied Physics, University of Geneva, Geneva, Switzerland
[2] Centre for Quantum Technologies, National University of Singapore, Singapore
E-mail: Cyril.Branciard@physics.unige.ch

*New Journal of Physics* **10** (2008) 013031 (25pp)
Received 25 October 2007
Published 25 January 2008
Online at http://www.njp.org/
doi:10.1088/1367-2630/10/1/013031

**Abstract.** The differential-phase-shift (DPS) and the coherent-one-way (COW) are among the most practical protocols for quantum cryptography, and are therefore the object of fast-paced experimental developments. The assessment of their security is also a challenge for theorists: the existing tools, that allow to prove security against the most general attacks, do not apply to these two protocols in any straightforward way. We present new upper bounds for their security in the limit of large distances ($d \gtrsim 50$ km with typical values in optical fibers) by considering a large class of collective attacks, namely those in which the adversary attaches ancillary quantum systems to each pulse or to each pair of pulses. We introduce also two modified versions of the COW protocol, which may prove more robust than the original one.


© IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

## Contents

**1. Introduction** **2**
**2. Definitions and tools** **3**
2.1. The COW and DPS codings . . . 3
2.2. Three versions of COW . . . 4
2.3. Secret key rates . . . 4
**3. Collective beam-splitting attack ($Q = 0$ and $V = 1$)** **5**
**4. Collective attacks with $Q \geqslant 0$, $V \leqslant 1$** **7**
4.1. Original COW coding: two-pulse attacks . . . 7
4.2. COWm1 coding: two-pulse attacks . . . 9
4.3. COWm2 coding: one-pulse attacks . . . 11
4.4. DPS coding: two-pulse attacks . . . 12
4.5. Numerical optimization and comparison . . . 13
**5. Conclusion** **14**
**Acknowledgments** **15**
**Appendix A. Other possible variants of the COW protocol** **15**
**Appendix B. Optimization of 2PA on COW** **16**
**Appendix C. Optimization of 2PA on COWm1** **18**
**Appendix D. Optimization of 1PA on COWm2** **20**
**Appendix E. Optimization of 1PA and 2PA on DPS** **21**
**References** **25**

## 1. Introduction

Over recent years quantum cryptography has evolved from niche physics to a technology that could revolutionize the science of secrecy. The basic idea, as formulated by Bennett and Brassard in 1984 (BB84), was based on the use of individual qubits [1], quickly 'translated' to individual photons. Given the lack of convenient single photon sources, most experiments use instead weak laser pulses. However, it was then realized that such sources sometimes emit multiphoton pulses and are thus in danger of photon-number-splitting (PNS) attacks [2]. The cheap counter-measure to PNS attacks is to reduce further the intensity of the weak laser pulses, but this solution leads to secret bit rates that scale quadratically with the quantum channel transmission coefficient, $r \propto t^2$. Hwang [3] found an elegant way out of this drawback, suggesting using more than one intensity. This method, called decoy state implementation, allows one to achieve a linear secret key rate, as for the historical single-qubit protocols [4].

The BB84 protocol in all its implementations, several variations thereof—two-state [5], six-state [6], SARG04 [7], protocols using higher-dimensional systems [8], etc—and all the corresponding entanglement-based versions [9], share a common feature: they all send quantum symbols one by one. However, convenient telecom laser sources emit either a continuous train of pulses (mode-locked lasers), or a continuous wave (cw) that can be formatted by an intensity modulator into trains of pulses. This observation led to new protocols for efficient quantum key distribution (QKD) like the *differential-phase-shift* (DPS) [10, 11] and the *coherent-one-way* (COW) [12, 13] protocols. In both protocols a continuous train of weak laser pulses is sent from

the sender, Alice, to the receiver, Bob. In the DPS protocol the intensity of the pulses is constant, but the phase modulated. In the COW protocol, the phases of all pulses are constant, but their intensity modulated. The DPS and the COW protocols are so-called *distributed-phase-reference* protocols: the intervention of an adversary, Eve, is monitored by measuring the coherence between successive non-empty pulses. Both protocols are robust against PNS attacks, because these can be detected [13, 14]; security has also been studied against individual attacks [13, 15] and more recently against some form of intercept-resend attacks based on unambiguous state discrimination [16]–[18]. However, security against the most general attacks is still elusive: the tools that have been developed in the last decade to tackle this cannot be applied in any straightforward way, because both protocols move away from the symbol-per-symbol type of coding.

The purpose of this paper is to analyze the security of the COW and the DPS protocols against a large class of collective attacks in the long distance regime (i.e. when the transmission coefficient $t$ is small). This study leads also to defining variants of the COW protocol, which make it more robust while keeping its simplicity.

The paper is structured as follows. In section 2, we recall the COW and DPS protocols, as well as some notions of security bounds. In section 3, we present the bound for security against a beam-splitting attack (BSA) treated as a collective attack. In section 4, we study a family of attacks that generalize the BSA by introducing errors. The basic idea is that the adversary, Eve, attaches ancillary quantum systems to each pulse or to each pair of pulses. For these attacks, bounds for security are provided in the limits of large distances, typically $d \gtrsim 50\,\mathrm{km}$. These upper bounds on the secret key rates scale linearly with $t$.

## 2. Definitions and tools

The source, on Alice's side, produces weak coherent pulses. A non-empty pulse is written $|\alpha\rangle$, its mean photon number $\mu = |\alpha|^2$. The transmission coefficient of the quantum channel connecting Alice and Bob is $t$, the efficiency of Bob's photon counters is $\eta$; we neglect the effects of dark counts and dead times of the detectors. Accordingly, in the absence of Eve, when Alice sends $|\alpha\rangle$, Bob receives $|\sqrt{t}\alpha\rangle$ and has a probability $1 - \mathrm{e}^{-\mu t\eta} (\approx \mu t\eta$ in the limit $\mu t \ll 1)$ of detecting a photon.

### 2.1. The COW and DPS codings

In the COW protocol, each bit is coded in a sequence of one non-empty and one empty pulse: the bit value 0 is coded in the sequence $|\alpha\rangle|0\rangle$, the bit value 1 in the sequence $|0\rangle|\alpha\rangle$. These two states are not orthogonal because of the vacuum component, and can be unambiguously discriminated in an optimal way by just measuring the time of arrival. This is the very simple *data line*, in which the raw key is created. The quantum bit error rate (QBER) $Q$ is, as usual, the probability that Bob accepts the wrong value of the bit: in physical terms, this means that Bob has got a detection in a time slot in which Alice has sent an empty pulse. To estimate the loss of coherence in the channel (and thence Eve's information), a fraction of the light is sent into a *monitoring line*, consisting of an unbalanced interferometer. The phase between the two arms is chosen so that two consecutive non-empty pulses sent by Alice should always interfere constructively in one output port (and be detected with probability $p_{\mathrm{D}_0} > 0$) and destructively

in the other one ($p_{D_1} = 0$). The departure from this ideal situation is measured by the visibility

$$V = \frac{p_{D_0} - p_{D_1}}{p_{D_0} + p_{D_1}}$$

of the interference pattern observed for two consecutive non-empty pulses. Note that there is no *a priori* relation between $Q$ and $V$.

In the DPS protocol, Alice produces a sequence of coherent states of the same intensity $\ldots |e^{i\varphi_{k-1}}\alpha\rangle|e^{i\varphi_k}\alpha\rangle|e^{i\varphi_{k+1}}\alpha\rangle \ldots$, where each phase can be set at $\varphi = 0$ or $\varphi = \pi$. The bits are coded in the difference between two successive phases: $b_k = 0$ if $e^{i\varphi_k} = e^{i\varphi_{k+1}}$ and $b_k = 1$, otherwise. These two cases can be unambiguously discriminated using an unbalanced interferometer. The same interferometer provides the information about the lack of coherence in the channel, used to estimate Eve's information. Contrary to what happens for COW, the QBER $Q$ and the visibility $V$ of the interference pattern are tightly related in DPS through the relation $Q = \frac{1-V}{2}$.

### 2.2. Three versions of COW

In the *original version* of COW, the pairing of the pulses is known in advance; in addition to sending the two sequences that code for a bit value, Alice should also send *decoy sequences* $|\alpha\rangle|\alpha\rangle$ with probability $f$ in order to prevent a subtle form of PNS attacks. Such sequences do not code for a bit value: therefore, if they give rise to a detection in the data line, this event must be eliminated in sifting. Throughout this paper we will set $f \approx 0$: in fact, all the bounds for security that we are going to use are valid only in the asymptotic limit of infinitely long keys, in which case an arbitrarily small amount of events is sufficient to produce meaningful statistics.

Along with this original version, we introduce and study here *two modified versions* of COW, in which the pairing of the pulses is not known *a priori* by Bob, nor Eve. Alice and Bob's devices are the same as in the original version: Alice sends a train of empty or non-empty pulses; Bob measures the time of arrival on his data line and checks the coherence of successive non-empty pulses on his monitoring line. Only after the transmission does Alice announce the pairings publicly; the bit is accepted if Bob has got one and only one detection in the data line corresponding to that pair of pulses. Given this, the two versions differ in the possible choices of pulses to be paired.

In *COWm1*, Alice still pairs consecutive pulses: this makes it the closest analog to DPS. If she wants to use (almost) all the pulses, she will still send sequences $|\alpha\rangle|0\rangle$ or $|0\rangle|\alpha\rangle$, and sometimes introduce an unused pulse. In *COWm2*, Alice is allowed to pair any two pulses; obviously, all the pulses are used. There is no simple version of DPS that would be analog to COWm2, because in order to pair arbitrary pulses in DPS, Bob should arbitrarily change the unbalance in the interferometer[3].

Note that many other variants of COW can be imagined, as we mention in appendix A.

### 2.3. Secret key rates

We consider from now on that the two values 0 and 1 are equally probable both in Alice's and in Bob's list; since this can be obtained by public communication, there is no loss in

[3] Note that a modified version of DPS was proposed in [19], where Bob can choose between $N$ path differences in his interferometer. For a large $N$, this would be analogous to COWm2. However, Bob needs to modify his apparatus, which does not make it very practical when $N$ increases.

generality in this assumption. As said, the bound for security against the most general attack by an eavesdropper has been elusive to date for both COW and DPS. In this paper, we are concerned with specific attacks, which of course define only *upper bounds* for security (i.e. it is guaranteed that one cannot obtain larger rates). In the family of attacks that we consider, Eve interacts with the pulses one-by-one or two-by-two, always with the same strategy. She is allowed to keep her ancillae in a quantum memory, and to extract the largest possible information out of them after Alice and Bob have run the classical post-processing. Therefore, we will compute the bound for security against *collective attacks* (as in most QKD studies to date, we compute this bound for the asymptotic case of an infinitely long raw key).

For collective attacks, Devetak and Winter [20] have shown that Eve's information on Alice's bits is upper-bounded by the maximal capacity of a channel Alice–Eve, in which Alice would code her bit value $a$ in the state $\rho_{\mathrm{E}}^{\mathrm{A}=a}$. This quantity is called Holevo bound, and reads

$$\chi_{\mathrm{AE}} \equiv \chi\left(\rho_{\mathrm{E}}^{\mathrm{A}=0}, \rho_{\mathrm{E}}^{\mathrm{A}=1}\right) = S(\rho_{\mathrm{E}}) - \tfrac{1}{2}S(\rho_{\mathrm{E}}^{\mathrm{A}=0}) - \tfrac{1}{2}S(\rho_{\mathrm{E}}^{\mathrm{A}=1}), \tag{1}$$

where $\rho_{\mathrm{E}} = \frac{1}{2}\rho_{\mathrm{E}}^{\mathrm{A}=0} + \frac{1}{2}\rho_{\mathrm{E}}^{\mathrm{A}=1}$ is Eve's state and $S$ is the von Neumann entropy. A similar definition holds for Eve's information on Bob's bits. Concerning the Alice–Bob channel, the QBER is $\mathrm{Prob}(\mathrm{A} \neq \mathrm{B}) = Q$; in particular, for the conditional Shannon entropy it holds $\mathrm{H}(\mathrm{A}|\mathrm{B}) = \mathrm{H}(\mathrm{B}|\mathrm{A}) = h(Q)$ where $h$ is the binary entropy. The Devetak–Winter bound reads, for the secret key rate $r$:

$$r = r_{\mathrm{sift}}\left[1 - h(Q) - \min(\chi_{\mathrm{AE}}, \chi_{\mathrm{BE}})\right], \tag{2}$$

where $r_{\mathrm{sift}}$ is the sifting rate, i.e. the probability that Alice and Bob accept a bit; we suppose that the two protocols are run with the same repetition rate: the rates will be given 'per time slot' (or 'per pulse', independently of whether the pulse is empty or not). We work in the *trusted-device scenario*, in which one assumes that Eve cannot modify the efficiency of Bob's detectors. Note that the whole analysis can be readily adapted to the *untrusted-device scenario* by replacing everywhere first $\eta \to 1$, then $t \to t\eta$.

## 3. Collective beam-splitting attack ($Q = 0$ and $V = 1$)

The beam-splitting attack (BSA) translates the fact that all the light that is lost in the channel must be given to Eve. The attack consists of Eve simulating the losses $1 - t$ by putting a beam-splitter just outside Alice's laboratory, and then forwarding the remaining photons to Bob through a lossless line. Since it simulates exactly Bob's expected optical mode, the BSA introduces no errors (here, $Q = 0$ and $V = 1$) and is therefore impossible to detect[4].

For both COW and DPS, Alice prepares a sequence of coherent states $\otimes_k|\alpha_k\rangle$: each $\alpha_k$ is chosen in $\{+\alpha, 0\}$ for COW, in $\{+\alpha, -\alpha\}$ for DPS. Bob receives the state $\otimes_k|\alpha_k\sqrt{t}\rangle$: Bob's optical mode is not modified. Eve's state is $\otimes_k|\alpha_k\sqrt{1-t}\rangle$; let us introduce the notations $\alpha_{\mathrm{E}} = \alpha\sqrt{1-t}$, $\mu_{\mathrm{E}} = |\alpha_{\mathrm{E}}|^2$ and

$$\gamma_{\mathrm{E}} = \mathrm{e}^{-\mu_{\mathrm{E}}} = \mathrm{e}^{-\mu(1-t)}. \tag{3}$$

[4] Apart from BSA, other attacks exist that do not introduce errors in distributed-phase-reference protocols: for instance, PNS attacks over the whole key, preserving the coherence (these are hard to parametrize and have never been studied in detail). For COW, there also exist zero-error attacks based on unambiguous state discrimination [16].

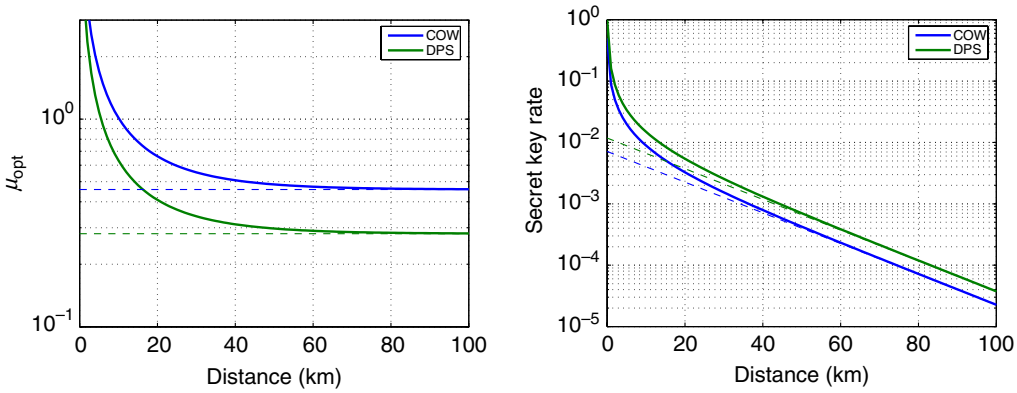


**Figure 1.** Optimal mean photon number $\mu$ and secret key rate as a function of the distance, for the BSA on the COW and DPS protocols. Detection efficiency: $\eta = 0.1$; losses: 0.25 dB km$^{-1}$; no dark counts.

When Bob announces a detection involving pulses $k-1$ and $k$, Eve shall extract the highest possible information out of her systems, measured by the Holevo quantity (1). The information available to Eve differs for the two protocols, because of the different coding of the bits.

In COW, the bit is 0 when $\alpha_{k-1} = \alpha$ , $\alpha_k = 0$ and is 1 when $\alpha_{k-1} = 0$ , $\alpha_k = \alpha$; so, writing $P_\psi$ the projector on $|\psi\rangle$, we have $\rho_{\mathrm{E}}^{\mathrm{A}=0} = \rho_{\mathrm{E}}^{\mathrm{B}=0} = P_{+\alpha_{\mathrm{E}},0}$ and $\rho_{\mathrm{E}}^{\mathrm{A}=1} = \rho_{\mathrm{E}}^{\mathrm{B}=1} = P_{0,+\alpha_{\mathrm{E}}}$; therefore, noticing that $|\langle +\alpha_{\mathrm{E}}, 0|0, +\alpha_{\mathrm{E}}\rangle| = \gamma_{\mathrm{E}}$, we obtain

$$\chi_{\mathrm{AE}} = \chi_{\mathrm{BE}} \equiv \chi_{\mathrm{E}}^{\mathrm{COW}}(\mu, t) = h\left(\frac{1-\gamma_{\mathrm{E}}}{2}\right). \tag{4}$$

Since in COW half of the pulses are empty, the secret key rate is given by

$$r_{\mathrm{COW}}(\mu, t) = \tfrac{1}{2}\left(1 - \mathrm{e}^{-\mu t \eta}\right)\left[1 - \chi_{\mathrm{E}}^{\mathrm{COW}}(\mu, t)\right]. \tag{5}$$

Since BSA is a pulse-by-pulse attack independent of the pairing, the analysis is unchanged for COWm1 and COWm2.

In DPS, the bit is 0 when $\alpha_{k-1} = \alpha_k$ and is 1 when $\alpha_{k-1} = -\alpha_k$. So, with similar notations as above, we have $\rho_{\mathrm{E}}^{\mathrm{A}=0} = \rho_{\mathrm{E}}^{\mathrm{B}=0} = \frac{1}{2}P_{+\alpha_{\mathrm{E}},+\alpha_{\mathrm{E}}} + \frac{1}{2}P_{-\alpha_{\mathrm{E}},-\alpha_{\mathrm{E}}}$ and $\rho_{\mathrm{E}}^{\mathrm{A}=1} = \rho_{\mathrm{E}}^{\mathrm{B}=1} = \frac{1}{2}P_{+\alpha_{\mathrm{E}},-\alpha_{\mathrm{E}}} + \frac{1}{2}P_{-\alpha_{\mathrm{E}},+\alpha_{\mathrm{E}}}$; therefore, noticing that $|\langle +\alpha_{\mathrm{E}}| - \alpha_{\mathrm{E}}\rangle| = \gamma_{\mathrm{E}}^2$, we obtain

$$\chi_{\mathrm{AE}} = \chi_{\mathrm{BE}} \equiv \chi_{\mathrm{E}}^{\mathrm{DPS}}(\mu, t) = 2\,h\left(\frac{1-\gamma_{\mathrm{E}}^2}{2}\right) - h\left(\frac{1-\gamma_{\mathrm{E}}^4}{2}\right), \tag{6}$$

and the resulting secret key rate is

$$r_{\mathrm{DPS}}(\mu, t) = \left(1 - \mathrm{e}^{-\mu t \eta}\right)\left[1 - \chi_{\mathrm{E}}^{\mathrm{DPS}}(\mu, t)\right]. \tag{7}$$

Both for COW and DPS, Alice and Bob should choose $\mu$ such that the secret key rate is maximized. We performed this one-parameter optimization numerically. Figure 1 shows the optimal choice for the intensity $\mu = \mu_{\mathrm{opt}}$ and the corresponding secret key rates for the COW and the DPS protocols.

One notices that the two protocols show similar behaviors against BSA. The optimal choice of $\mu$ is approximately twice as large for COW as it is for DPS; since in COW one pulse out of two is empty, the number of photons per bit is thus approximately the same. As for the secret key rates obtained for the respective $\mu_{\mathrm{opt}}$, they are very similar, within a factor of two. The question

of whether one protocol performs better than the other one, does not have a clear-cut answer: other practical issues should be taken into consideration. For instance, we did not consider for COW the fraction of the signal that should be sent through Bob's monitoring line, which will not contribute to the key. We did not consider the losses in Bob's interferometer either: in DPS, they will decrease the secret key rates, while in COW, they will not alter the key rates. A more complete analysis should therefore lead to different factors before the given key rates, and the factor of two that appears here between the two protocols is not meaningful in itself.

In the limit of large distances $\mu t \ll 1$ (typically, for $d \gtrsim 50\,\mathrm{km}$[5]), the secret key rates under a BSA become linear in $t\eta$ ($r = r_0 t\eta$), and the $\mu_{\mathrm{opt}}$ tend to a constant value (dashed lines on figure 1). Specifically: for COW, $\mu_{\mathrm{opt}} \to 0.4583$ and $r_0 \approx 0.0714$; for DPS, $\mu_{\mathrm{opt}} \to 0.2808$ and $r_0 \approx 0.1182$. Note that the attacks presented in the next section of this paper shall be studied only in this limit, due to their complexity, and will coincide with the asymptotic limits for BSA when $Q = 0$ and $V = 1$.

## 4. Collective attacks with $Q \geqslant 0$, $V \leqslant 1$

In both COW and DPS, bits are coded in the relation between two successive pulses. In the study of upper bounds, a natural class of attacks is therefore the one in which Eve attacks coherently pairs of successive pulses. These we call 'two-pulse attacks' (2PA). In general, they are defined by

$$[|\alpha_{k-1}\rangle|\alpha_k\rangle]_{\mathrm{A}(k-1,k)} \otimes |\mathcal{E}\rangle_{\mathrm{E}} \longrightarrow |\Psi[\alpha_{k-1}, \alpha_k]\rangle_{\mathrm{B}(k-1,k),\mathrm{E}} \tag{8}$$

with the only constraint that the transformation must be unitary. This class is clearly too large to be parametrized efficiently. However, in the limit of large distances $\mu t \ll 1$, multi-photon components on Bob's side are supposed to be negligible; and Bob will have to check, through the statistics of his detection rates (singles, double-clicks in two detectors, etc), that this is indeed the case. In view of this, we restrict our study to the case where, for any two-pulse signal sent by Alice, Bob's Hilbert space consists only of the three orthogonal states $|00\rangle$ (no photon), $|10\rangle$ (one photon at time $k-1$) and $|01\rangle$ (one photon at time $k$).

In this section, 2PA are studied on COW (4.1), on COWm1 (4.2) and on DPS (4.4). On COWm2, since there is no preferred pairing at all, we shall rather study 'one-pulse attacks', 1PA (4.3). The resulting upper bounds will be computed numerically and compared (4.5). Unless stated otherwise, pure and mixed quantum states are normalized (in the limit $\mu t \ll 1$) in all that follows.

### *4.1. Original COW coding: two-pulse attacks*

*4.1.1. Eve's attack.* In the original COW protocol, the pairing of the pulses sent by Alice is publicly known. When Eve attacks the pulses two-by-two, we suppose that she does it according to the same pairing. The three sequences that Alice can send (bit 0, bit 1 and decoy sequence)

[5] Of course, the distance cannot be too large: it has to be below the distance where dark counts become important; and for COW, also below the distance (∼100 km) at which other zero-error attacks become possible [16].

are modified by Eve's intervention as

$$
\begin{aligned}
|\sqrt{\mu}, 0\rangle_{\mathrm{A}}|\mathcal{E}\rangle &\longrightarrow |00\rangle_{\mathrm{B}}|v_{\mu 0}\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}\,|10\rangle_{\mathrm{B}}|p^{10}_{\mu 0}\rangle_{\mathrm{E}} + \sqrt{Q\mu t}\,|01\rangle_{\mathrm{B}}|p^{01}_{\mu 0}\rangle_{\mathrm{E}} \\
|0, \sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\rangle &\longrightarrow |00\rangle_{\mathrm{B}}|v_{0\mu}\rangle_{\mathrm{E}} + \sqrt{Q\mu t}\,|10\rangle_{\mathrm{B}}|p^{10}_{0\mu}\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}\,|01\rangle_{\mathrm{B}}|p^{01}_{0\mu}\rangle_{\mathrm{E}} \\
|\sqrt{\mu}, \sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\rangle &\longrightarrow |00\rangle_{\mathrm{B}}|v_{\mu\mu}\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}\,(|10\rangle_{\mathrm{B}}|p^{10}_{\mu\mu}\rangle_{\mathrm{E}} + |01\rangle_{\mathrm{B}}|p^{01}_{\mu\mu}\rangle_{\mathrm{E}}),
\end{aligned}
\tag{9}
$$

where $|v_{jk}\rangle_{\mathrm{E}}$ $(j, k \in \{0, \mu\})$ are the states that Eve attaches to the vacuum part of the signal, while $|p^{10}_{jk}\rangle_{\mathrm{E}}$ and $|p^{01}_{jk}\rangle_{\mathrm{E}}$ are the states that Eve attaches to the 1-photon part of the signal. While we have left Eve's states free (up to some constraints to be described soon), we have fixed the probability amplitude of each term. These amplitudes are motivated by the expected behavior of an imperfect intensity modulator on Alice's side, which would prepare pulses of intensity $(1-Q)\mu$ and $Q\mu$ instead of perfectly modulated intensities $\mu$ and 0. In this case, for each bit sequence sent by Alice we still have an average probability $\mu t$ that a photon arrives at Bob; in a fraction $1-Q$ of these cases, it arrives at the correct time, in the other cases it arrives at the wrong time, whence $Q$ is indeed the QBER. Again, Bob has to check that the multi-photon components are negligible.

The relations between Eve's states are constrained by the requirement that the transformation must be unitary, and by the results of the parameter estimation (i.e. by the values of the visibilities). The requirement of unitarity reads (recall that we work in the limit $\mu t \ll 1$)

$$
\langle v_{0\mu}|v_{\mu 0}\rangle = \mathrm{e}^{-\mu}, \quad \langle v_{\mu\mu}|v_{\mu 0}\rangle = \langle v_{\mu\mu}|v_{0\mu}\rangle = \mathrm{e}^{-\mu/2}. \tag{10}
$$

The visibility in COW is measured only conditioned to the fact that Alice has sent two consecutive non-empty pulses. There are five such cases: the case of decoy sequences (two non-empty pulses in the same pair) and the four two-pair sequences $(x, y) = (0\mu, \mu 0), (\mu\mu, \mu 0), (0\mu, \mu\mu)$ and $(\mu\mu, \mu\mu)$. The corresponding visibilities after Eve's intervention are

$$
V_{\mu\mu} = \mathrm{Re}\big[\langle p^{01}_{\mu\mu}|p^{10}_{\mu\mu}\rangle\big], \tag{11}
$$

$$
V_{xy} = \mathrm{Re}\big[\langle v_x|p^{01}_{x}\rangle\langle p^{10}_{y}|v_y\rangle\big]. \tag{12}
$$

As an example, consider $V_{\mu\mu}$. When Alice sends a decoy sequence $|\sqrt{\mu}, \sqrt{\mu}\rangle$, a detection in the interferometer at the correct timing should reveal the coherence between $|10\rangle$ and $|01\rangle$. After Eve's intervention, the action of the interferometer (non-normalized) reads

$$
|10\rangle_{\mathrm{B}}|p^{10}_{\mu\mu}\rangle_{\mathrm{E}} + |01\rangle_{\mathrm{B}}|p^{01}_{\mu\mu}\rangle_{\mathrm{E}} \longrightarrow |D_0\rangle(|p^{10}_{\mu\mu}\rangle_{\mathrm{E}} + |p^{01}_{\mu\mu}\rangle_{\mathrm{E}}) + |D_1\rangle(|p^{10}_{\mu\mu}\rangle_{\mathrm{E}} - |p^{01}_{\mu\mu}\rangle_{\mathrm{E}}). \tag{13}
$$

The probability that the photon going to Bob is detected by detector $D_0$ (resp $D_1$) of the interferometer is proportional to $p_{0/1} \propto \| |p^{10}_{\mu\mu}\rangle_{\mathrm{E}} \pm |p^{01}_{\mu\mu}\rangle_{\mathrm{E}} \|^2 = 2 \pm 2\mathrm{Re}\langle p^{01}_{\mu\mu}|p^{10}_{\mu\mu}\rangle \propto 1 \pm V_{\mu\mu}$, whence (11). The visibilities $V_{xy}$ are computed in a similar way, considering that the interference across the pairing is due to the coherence between $|01\rangle|00\rangle$ and $|00\rangle|10\rangle$. In the present study, we suppose that Alice and Bob check that all these visibilities are the same:

$$
V_{\mu\mu} = V_{0\mu,\mu 0} = V_{\mu\mu,\mu 0} = V_{0\mu,\mu\mu} = V_{\mu\mu,\mu\mu} \equiv V. \tag{14}
$$

*4.1.2. Eve's information.* The task is to compute the information that Eve obtains when she performs the attack (9). For each bit detected by Bob, if Eve is interested in Alice's bit, her information is the Holevo quantity $\chi_{\rm AE}$ computed for $\rho_{\rm E}^{\rm A=0} = (1-Q)|p_{\mu 0}^{10}\rangle\langle p_{\mu 0}^{10}| + Q|p_{\mu 0}^{01}\rangle\langle p_{\mu 0}^{01}|$ and $\rho_{\rm E}^{\rm A=1} = (1-Q)|p_{0\mu}^{01}\rangle\langle p_{0\mu}^{01}| + Q|p_{0\mu}^{10}\rangle\langle p_{0\mu}^{10}|$; if Eve is interested in Bob's bit, her information is the Holevo quantity $\chi_{\rm BE}$ computed for $\rho_{\rm E}^{\rm B=0} = (1-Q)|p_{\mu 0}^{10}\rangle\langle p_{\mu 0}^{10}| + Q|p_{0\mu}^{10}\rangle\langle p_{0\mu}^{10}|$ and $\rho_{\rm E}^{\rm B=1} = (1-Q)|p_{0\mu}^{01}\rangle\langle p_{0\mu}^{01}| + Q|p_{\mu 0}^{01}\rangle\langle p_{\mu 0}^{01}|$. These are formal expressions, whose value has to be optimized under the constraints (10) and (14). Now, none of the constraints (10)–(12) on Eve's states involves $|p_{0\mu}^{10}\rangle$ and $|p_{\mu 0}^{01}\rangle$. Eve can, therefore choose these two states freely, and the best choice is obviously to take them orthogonal to one another and to all her other states, in order to distinguish those cases perfectly. In this case, $\chi_{\rm AE} = \chi_{\rm BE} = Q + (1-Q)\chi(P_{p_{\mu 0}^{10}}, P_{p_{\mu 0}^{01}})$, that we write explicitly as

$$\chi_{\rm COW} = Q + (1-Q)\, h\left(\frac{1+|\langle p_{\mu 0}^{10}|p_{0\mu}^{01}\rangle|}{2}\right). \tag{15}$$

In particular, Eve has all the information on Alice's and Bob's bit when she introduces an error.

So finally, the Devetak–Winter bound for 2PA on COW in the limit $\mu t \ll 1$ reads

$$r_{\rm COW}(Q,V) = r_0 t\eta \quad \text{with} \quad r_0 = \tfrac{1}{2}\mu\left[1 - h(Q) - \chi_{\rm COW}\right]. \tag{16}$$

Note that $r_0$ does not depend on $t\eta$: the long-distance upper bound that we obtain is linear in $t$.

### 4.2. COWm1 coding: two-pulse attacks

*4.2.1. Eve's attack.* We now consider the first modified version of the COW protocol (COWm1). In this version, the coding still implies pairs of consecutive pulses, but the pairing is decided by Alice and Bob *a posteriori*. Thus, during the exchange of quantum signals, Eve does not know which pulses she should attack together: half of the times, her 2PA will therefore be applied on pulses that are not going to be paired to form a bit. In particular, now all four sequences of two consecutive pulses are possible: the transformation (9) must be complemented with a fourth line

$$|0,0\rangle_{\rm A}|\mathcal{E}\rangle \quad \longrightarrow \quad |00\rangle_{\rm B}|v_{00}\rangle_{\rm E} + \sqrt{Q\mu t}\,(|10\rangle_{\rm B}|p_{00}^{10}\rangle_{\rm E} + |01\rangle_{\rm B}|p_{00}^{01}\rangle_{\rm E}), \tag{17}$$

where the choice of probability amplitude is dictated by the same considerations as above. The requirement of unitarity consists of (10) and of the three additional constraints

$$\langle v_{00}|v_{\mu\mu}\rangle = {\rm e}^{-\mu}, \quad \langle v_{00}|v_{\mu 0}\rangle = \langle v_{00}|v_{0\mu}\rangle = {\rm e}^{-\mu/2}. \tag{18}$$

The computation of the loss of visibility is identical to the case of the original COW, leading to (11) and (12); as for that case, we shall impose (14). Note that the states $|p_{0\mu}^{10}\rangle$, $|p_{\mu 0}^{01}\rangle$, $|p_{00}^{10}\rangle$, $|p_{00}^{01}\rangle$ do not enter in any of the constraints, and can therefore be chosen orthogonal to each other and to all other states.

*4.2.2. Eve's information.* When it comes to computing Eve's information, two cases have to be treated separately:

*Case 1.* The two pulses that code a bit have been attacked together by Eve. In this case, the computation of Eve's information is the same for the original COW protocol (4.1), so $\chi_{\rm AE}^{(2)} = \chi_{\rm BE}^{(2)}$ is given by (15).

*Case 2.* The two pulses that code a bit have not been attacked together by Eve. To study this case, we must consider four pulses. Writing $j, k, j', k' \in \{0, 1\}$ and neglecting as usual the two-photon terms, the transformation reads

$$|j\sqrt{\mu}, k\sqrt{\mu}\rangle_{\mathrm{A}}|j'\sqrt{\mu}, k'\sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\mathcal{E}'\rangle \longrightarrow \sqrt{(k+(-1)^k Q)\mu t}|0100\rangle_{\mathrm{B}}|p^{01}_{j\mu,k\mu}, v_{j'\mu,k'\mu}\rangle_{\mathrm{E}} + \sqrt{(j'+(-1)^{j'} Q)\mu t}|0010\rangle_{\mathrm{B}}|v_{j\mu,k\mu}, p^{10}_{j'\mu,k'\mu}\rangle_{\mathrm{E}} + \cdots. \tag{19}$$

The terms that we left out do not contribute, for we focus on the case where Bob detects a photon in one of the two middle time-slots and pairs precisely those slots. Moreover, *a posteriori* it is decided that pulses $j'$ and $k$ form a bit $a$, i.e. Alice must have used $j' = 1 - k = a$. Depending on the sequence sent by Alice and on the bit detected by Bob, Eve's (unnormalized) state is thus

$$\rho_{\mathrm{E}_4}^{\mathrm{A}=\{jk,j'k'\},\mathrm{B}=0} = (k+(-1)^k Q)|p^{01}_{j\mu,k\mu}, v_{j'\mu,k'\mu}\rangle\langle p^{01}_{j\mu,k\mu}, v_{j'\mu,k'\mu}|, \tag{20}$$

$$\rho_{\mathrm{E}_4}^{\mathrm{A}=\{jk,j'k'\},\mathrm{B}=1} = (j'+(-1)^{j'} Q)|v_{j\mu,k\mu}, p^{10}_{j'\mu,k'\mu}\rangle\langle v_{j\mu,k\mu}, p^{10}_{j'\mu,k'\mu}|. \tag{21}$$

Eve's (now normalized) states conditioned on Alice's or on Bob's bit become

$$\rho_{\mathrm{E}_4}^{\mathrm{A}=a} = \frac{1}{4}\sum_{j,k',b} \rho_{\mathrm{E}_4}^{\mathrm{A}=\{j\bar{a},ak'\},\mathrm{B}=b} \equiv (1-Q)\rho_{\mathrm{E}_4}^{a,b=a} + Q\rho_{\mathrm{E}_4}^{a,b=\bar{a}}, \tag{22}$$

$$\rho_{\mathrm{E}_4}^{\mathrm{B}=b} = \frac{1}{4}\sum_{j,k',a} \rho_{\mathrm{E}_4}^{\mathrm{A}=\{j\bar{a},ak'\},\mathrm{B}=b} \equiv (1-Q)\rho_{\mathrm{E}_4}^{a=b,b} + Q\rho_{\mathrm{E}_4}^{a=\bar{b},b}, \tag{23}$$

where $\bar{a} = 1 - a$ and $\bar{b} = 1 - b$, and where

$$\rho_{\mathrm{E}_4}^{0,0} = \frac{1}{4}\sum_{j,k'} |p^{01}_{j\mu,\mu}, v_{0,k'\mu}\rangle\langle p^{01}_{j\mu,\mu}, v_{0,k'\mu}|, \quad \rho_{\mathrm{E}_4}^{0,1} = \frac{1}{4}\sum_{j,k'} |v_{j\mu,\mu}, p^{10}_{0,k'\mu}\rangle\langle v_{j\mu,\mu}, p^{10}_{0,k'\mu}|, \tag{24}$$

$$\rho_{\mathrm{E}_4}^{1,1} = \frac{1}{4}\sum_{j,k'} |v_{j\mu,0}, p^{10}_{\mu,k'\mu}\rangle\langle v_{j\mu,0}, p^{10}_{\mu,k'\mu}|, \quad \rho_{\mathrm{E}_4}^{1,0} = \frac{1}{4}\sum_{j,k'} |p^{01}_{j\mu,0}, v_{\mu,k'\mu}\rangle\langle p^{01}_{j\mu,0}, v_{\mu,k'\mu}|. \tag{25}$$

As it happened for COW, $\rho_{\mathrm{E}_4}^{1,0}$ and $\rho_{\mathrm{E}_4}^{0,1}$ are orthogonal to one another and to the other two mixtures; therefore $\chi_{\mathrm{AE}}^{(4)} = \chi_{\mathrm{BE}}^{(4)} = Q + (1-Q)\chi(\rho_{\mathrm{E}_4}^{0,0}, \rho_{\mathrm{E}_4}^{1,1})$.

On average, each of these two cases happens with probability $\frac{1}{2}$, so $\chi_{\mathrm{AE}} = \chi_{\mathrm{BE}}$ is given by

$$\chi_{\mathrm{COWm1}} = Q + \frac{1-Q}{2}\left\{h\left(\frac{1+|\langle p^{10}_{\mu 0}|p^{01}_{0\mu}\rangle|}{2}\right) + \chi\left(\rho_{\mathrm{E}_4}^{0,0}, \rho_{\mathrm{E}_4}^{1,1}\right)\right\}. \tag{26}$$

The Devetak–Winter bound for 2PA on COWm1 in the limit $\mu t \ll 1$ reads

$$r_{\mathrm{COWm1}}(Q, V) = r_0 t\eta \quad \text{with} \quad r_0 = \tfrac{1}{2}\mu\,[1 - h(Q) - \chi_{\mathrm{COWm1}}]. \tag{27}$$

### 4.3. COWm2 coding: one-pulse attacks

*4.3.1. Eve's attack.* Let's now consider the second modified version of the COW protocol (COWm2). In this version, Alice and Bob check the coherence on successive pulses, but pair arbitrary pulses in order to define key bits. In this case, there is no longer any natural definition of 2PA: almost always, Eve's pairing shall not correspond to the pairing that defines a bit. Therefore, we obtain the upper bound on COWm2 considering 1PA: we suppose that Eve attaches a probe to each pulse sent by Alice, and performs the transformation

$$\begin{aligned} |0\rangle_{\mathrm{A}}|\mathcal{E}\rangle &\longrightarrow |0\rangle_{\mathrm{B}}|v_0\rangle_{\mathrm{E}} + \sqrt{Q\mu t}|1\rangle_{\mathrm{B}}|p_0\rangle_{\mathrm{E}} \\ |\sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\rangle &\longrightarrow |0\rangle_{\mathrm{B}}|v_\mu\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}|1\rangle_{\mathrm{B}}|p_\mu\rangle_{\mathrm{E}}, \end{aligned} \tag{28}$$

where $|v_{0/\mu}\rangle_{\mathrm{E}}$ are the states that Eve attaches to the vacuum part of the signal, while $|p_{0/\mu}\rangle_{\mathrm{E}}$ are the states that Eve attaches to the 1-photon part of the signal. The probability amplitudes are fixed according to the same physical considerations done for COW and COWm1. The requirement of unitarity reads

$$\langle v_0|v_\mu\rangle = \mathrm{e}^{-\mu/2}. \tag{29}$$

The loss of visibility introduced by Eve's intervention is computed along the same lines as in 4.1. Suppose Alice sends a sequence $|\sqrt{\mu}, \sqrt{\mu}\rangle$: in the limit $\mu t \ll 1$, where we neglect the 2-photon terms, Eve's intervention leads to $|00\rangle_{\mathrm{B}}|v_\mu, v_\mu\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}[|10\rangle_{\mathrm{B}}|p_\mu, v_\mu\rangle_{\mathrm{E}} + |01\rangle_{\mathrm{B}}|v_\mu, p_\mu\rangle_{\mathrm{E}}]$ whence

$$V = \mathrm{Re}\big[\langle v_\mu, p_\mu|p_\mu, v_\mu\rangle\big] = |\langle v_\mu|p_\mu\rangle|^2. \tag{30}$$

None of these constraints involves $|p_0\rangle$, that can therefore be chosen orthogonal to all other states of Eve.

*4.3.2. Eve's information.* On any pair of pulses that define a bit, Eve's intervention has the product structure

$$\begin{aligned} |\sqrt{\mu}, 0\rangle_{\mathrm{A}}|\mathcal{E}\mathcal{E}'\rangle &\longrightarrow |00\rangle_{\mathrm{B}}|v_\mu, v_0\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}|10\rangle_{\mathrm{B}}|p_\mu, v_0\rangle_{\mathrm{E}} + \sqrt{Q\mu t}|01\rangle_{\mathrm{B}}|v_\mu, p_0\rangle_{\mathrm{E}}, \\ |0, \sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\mathcal{E}'\rangle &\longrightarrow |00\rangle_{\mathrm{B}}|v_0, v_\mu\rangle_{\mathrm{E}} + \sqrt{Q\mu t}|10\rangle_{\mathrm{B}}|p_0, v_\mu\rangle_{\mathrm{E}} + \sqrt{(1-Q)\mu t}|01\rangle_{\mathrm{B}}|v_0, p_\mu\rangle_{\mathrm{E}}. \end{aligned} \tag{31}$$

For each bit detected by Bob, if Eve is interested in Alice's bit, her information is the Holevo quantity $\chi_{\mathrm{AE}}$ computed for $\rho_{\mathrm{E}}^{\mathrm{A}=0} = (1-Q)|p_\mu, v_0\rangle\langle p_\mu, v_0| + Q|v_\mu, p_0\rangle\langle v_\mu, p_0|$ and $\rho_{\mathrm{E}}^{\mathrm{A}=1} = (1-Q)|v_0, p_\mu\rangle\langle v_0, p_\mu| + Q|p_0, v_\mu\rangle\langle p_0, v_\mu|$; if Eve is interested in Bob's bit, her information is the Holevo quantity $\chi_{\mathrm{BE}}$ computed for $\rho_{\mathrm{E}}^{\mathrm{B}=0} = (1-Q)|p_\mu, v_0\rangle\langle p_\mu, v_0| + Q|p_0, v_\mu\rangle\langle p_0, v_\mu|$ and $\rho_{\mathrm{E}}^{\mathrm{B}=1} = (1-Q)|v_0, p_\mu\rangle\langle v_0, p_\mu| + Q|v_\mu, p_0\rangle\langle v_\mu, p_0|$. Since $|v_\mu, p_0\rangle$ and $|p_0, v_\mu\rangle$ are orthogonal to one another and to the other states $|p_\mu, v_0\rangle$ and $|v_0, p_\mu\rangle$, we have $\chi_{\mathrm{AE}} = \chi_{\mathrm{BE}}$ given by

$$\chi_{\mathrm{COWm2}} = Q + (1-Q)h\left(\frac{1+|\langle v_0|p_\mu\rangle|^2}{2}\right). \tag{32}$$

So finally, the Devetak–Winter bound for 1PA on COWm2 in the limit $\mu t \ll 1$ reads

$$r_{\mathrm{COWm2}}(Q, V) = r_0 t\eta \quad \text{with} \quad r_0 = \tfrac{1}{2}\mu\,[1 - h(Q) - \chi_{\mathrm{COWm2}}]. \tag{33}$$

### 4.4. DPS coding: two-pulse attacks

We turn now to the DPS protocol and derive an upper bound for security considering 2PA. The formalism is analog to the one described for the COWm1 protocol in section 4.2, so we go fast through many details. The main differences are of course those related to the protocol: the different coding of bits, and the link between $Q$ and $V$.

*4.4.1. Eve's attack.* We suppose that Eve attaches her probe to two successive pulses sent by Alice. Four two-pulse sequences are possible: with $\sigma, \omega \in \{+, -\}$, Eve's intervention reads

$$|\sigma\sqrt{\mu}, \omega\sqrt{\mu}\rangle_{\mathrm{A}}|\mathcal{E}\rangle \longrightarrow |00\rangle_{\mathrm{B}}|v_{\sigma\omega}\rangle_{\mathrm{E}} + \sqrt{\mu t}(\sigma|10\rangle_{\mathrm{B}}|p^{10}_{\sigma\omega}\rangle_{\mathrm{E}} + \omega|01\rangle_{\mathrm{B}}|p^{01}_{\sigma\omega}\rangle_{\mathrm{E}}), \tag{34}$$

where $|v_{\sigma\omega}\rangle_{\mathrm{E}}$ are the states that Eve attaches to the vacuum part of the signal, while $|p^{10}_{\sigma\omega}\rangle_{\mathrm{E}}$ and $|p^{01}_{\sigma\omega}\rangle_{\mathrm{E}}$ are the states that Eve attaches to the 1-photon part of the signal (as before, Bob shall check that the multi-photon components are negligible). The transformation leads to the expected detection rate $\mu t\eta$ for each pulse. The constraint of unitarity reads

$$\langle v_{++}|v_{--}\rangle = \langle v_{+-}|v_{-+}\rangle = \mathrm{e}^{-4\mu}, \tag{35}$$

$$\langle v_{++}|v_{+-}\rangle = \langle v_{++}|v_{-+}\rangle = \langle v_{--}|v_{+-}\rangle = \langle v_{--}|v_{-+}\rangle = \mathrm{e}^{-2\mu}. \tag{36}$$

The visibilities can now be computed for all possible sequences, since there are no empty pulses. Formally, the expressions depend on which sequence of pulses was sent, and on whether the two pulses that interfere belong to a same or to different sequences according to the pairing chosen by Eve. The resulting visibilities are

$$V_{\sigma\omega} = \mathrm{Re}\left[\langle p^{01}_{\sigma\omega}|p^{10}_{\sigma\omega}\rangle\right], \tag{37}$$

$$V_{\sigma\omega,\sigma'\omega'} = \mathrm{Re}\left[\langle v_{\sigma\omega}|p^{01}_{\sigma\omega}\rangle\langle p^{10}_{\sigma'\omega'}|v_{\sigma'\omega'}\rangle\right]. \tag{38}$$

Again, Alice and Bob shall check that all these visibilities are equal: for all $\sigma, \omega, \sigma', \omega' \in \{+, -\}$,

$$V_{\sigma\omega} = V_{\sigma\omega,\sigma'\omega'} \equiv V. \tag{39}$$

*4.4.2. Eve's information.* As happened for COWm1, when it comes to computing Eve's information, two cases have to be treated separately:

*Case 1.* The two pulses that contribute to the detected event have been attacked together by Eve. The evolution in Bob's interferometer is $\sigma|10\rangle_{\mathrm{B}}|p^{10}_{\sigma\omega}\rangle_{\mathrm{E}} + \omega|01\rangle_{\mathrm{B}}|p^{01}_{\sigma\omega}\rangle_{\mathrm{E}} \longrightarrow \sum_b |D_b\rangle|\psi_{\sigma,\omega,b}\rangle_{\mathrm{E}}$ with $|\psi_{\sigma,\omega,b}\rangle = \sigma|p^{10}_{\sigma\omega}\rangle + (-1)^b\omega|p^{01}_{\sigma\omega}\rangle$ (non-normalized). Writing $\rho_{\mathrm{E}_2}^{\mathrm{A}=\{\sigma\omega\},\mathrm{B}=b} = |\psi_{\sigma,\omega,b}\rangle\langle\psi_{\sigma,\omega,b}|$, Eve's normalized states conditioned on Alice's bit are $\rho_{\mathrm{E}_2}^{\mathrm{A}=0} = \frac{1}{8}\sum_{\sigma,b}\rho_{\mathrm{E}_2}^{\mathrm{A}=\{\sigma\sigma\},\mathrm{B}=b}$ and $\rho_{\mathrm{E}_2}^{\mathrm{A}=1} = \frac{1}{8}\sum_{\sigma,b}\rho_{\mathrm{E}_2}^{\mathrm{A}=\{\sigma\bar{\sigma}\},\mathrm{B}=b}$ (where $\bar{\sigma} = -\sigma$ ); Eve's normalized states conditioned on Bob's bit are $\rho_{\mathrm{E}_2}^{\mathrm{B}=b} = \frac{1}{8}\sum_{\sigma,\omega}\rho_{\mathrm{E}_2}^{\mathrm{A}=\{\sigma\omega\},\mathrm{B}=b}$. Eve's information for this case 1 is then

$$\chi^{(2)}_{\mathrm{AE}} = \chi\left(\rho_{E_2}^{\mathrm{A}=0}, \rho_{\mathrm{E}_2}^{\mathrm{A}=1}\right), \quad \chi^{(2)}_{\mathrm{BE}} = \chi\left(\rho_{\mathrm{E}_2}^{\mathrm{B}=0}, \rho_{\mathrm{E}_2}^{\mathrm{B}=1}\right). \tag{40}$$

*Case 2.* The two pulses that contribute to the detected event have not been attacked together by Eve. Then, we have to study the four-pulse sequence, in which the bit has been produced by the interference of pulses number two and three. The evolution in Bob's interferometer is $\omega|0100\rangle_{\mathrm{B}}|p^{01}_{\sigma\omega}, v_{\sigma'\omega'}\rangle_{\mathrm{E}} + \sigma'|0010\rangle_{\mathrm{B}}|v_{\sigma\omega}, p^{10}_{\sigma'\omega'}\rangle_{\mathrm{E}} \longrightarrow \sum_b |D_b\rangle|\psi_{\sigma,\omega,\sigma',\omega',b}\rangle_{\mathrm{E}}$ with $|\psi_{\sigma,\omega,\sigma',\omega',b}\rangle = \omega|p^{01}_{\sigma\omega}\rangle|v_{\sigma'\omega'}\rangle + (-1)^b\sigma'|v_{\sigma\omega}\rangle|p^{10}_{\sigma'\omega'}\rangle$ (non-normalized). Writing $\rho_{\mathrm{E}_4}^{\mathrm{A}=\{\sigma\omega,\sigma'\omega'\},\mathrm{B}=b} = |\psi_{\sigma,\omega,\sigma',\omega',b}\rangle\langle\psi_{\sigma,\omega,\sigma',\omega',b}|$, Eve's normalized states conditioned on Alice's bit are $\rho_{\mathrm{E}_4}^{\mathrm{A}=0} = \frac{1}{32}\sum_{\sigma,\omega,\omega',b}\rho_{\mathrm{E}_4}^{\mathrm{A}=\{\sigma\omega,\omega\omega'\},\mathrm{B}=b}$ and $\rho_{\mathrm{E}_4}^{\mathrm{A}=1} = \frac{1}{32}\sum_{\sigma,\omega,\omega',b}\rho_{\mathrm{E}_4}^{\mathrm{A}=\{\sigma\omega,\bar{\omega}\omega'\},\mathrm{B}=b}$ (where $\bar{\omega} = -\omega$); Eve's normalized states conditioned on Bob's bit are $\rho_{\mathrm{E}_4}^{\mathrm{B}=b} = \frac{1}{32}\sum_{\sigma,\omega,\sigma',\omega'}\rho_{\mathrm{E}_4}^{\mathrm{A}=\{\sigma\omega,\sigma'\omega'\},\mathrm{B}=b}$. Eve's information for this case 2 is then

$$\chi^{(4)}_{\mathrm{AE}} = \chi\left(\rho_{\mathrm{E}_4}^{\mathrm{A}=0}, \rho_{\mathrm{E}_4}^{\mathrm{A}=1}\right), \quad \chi^{(4)}_{\mathrm{BE}} = \chi\left(\rho_{\mathrm{E}_4}^{\mathrm{B}=0}, \rho_{\mathrm{E}_4}^{\mathrm{B}=1}\right). \tag{41}$$

Each of the two cases happens with probability $\frac{1}{2}$. Therefore, Eve's average information is

$$\chi_{\mathrm{AE}} = \frac{\chi^{(2)}_{\mathrm{AE}} + \chi^{(4)}_{\mathrm{AE}}}{2}, \quad \chi_{\mathrm{BE}} = \frac{\chi^{(2)}_{\mathrm{BE}} + \chi^{(4)}_{\mathrm{BE}}}{2}. \tag{42}$$

For the versions of COW, some of Eve's states could be immediately chosen as being orthogonal to all the other ones; there is no such simplification here. The Devetak–Winter bound for 2PA on DPS in the limit $\mu t \ll 1$ reads

$$r_{\mathrm{DPS}}(Q, V) = r_0 t\eta \quad \text{with} \quad r_0 = \mu\left[1 - h\left(\frac{1-V}{2}\right) - \min(\chi_{\mathrm{AE}}, \chi_{\mathrm{BE}})\right]. \tag{43}$$

### *4.5. Numerical optimization and comparison*

In the previous subsections, we have derived upper bounds for the secret key rate of COW (16), COWm1 (27), COWm2 (33) and DPS (43) in the limit $\mu t \ll 1$ of large distances. In this limit, all these bounds scale linearly with losses: $r = r_0 t\eta$, where only the constant factor $r_0$ depends on the protocol. Incidentally, we remind that for COWm1 and COWm2 we have supposed that Alice makes the pairings; if Bob makes them, the rates given above for these protocols should be divided by 2.

At this point, we want to evaluate these bounds. This involves a double optimization: first, for a fixed value of $\mu$, one has to find the strategy that maximizes Eve's information; then, one has to find the value of $\mu$ that maximizes $r$—in our case, $r_0$. The details on how the optimizations over Eve's strategies were performed, are given in appendices B–E. For COW and COWm2, these optimizations could be performed analytically, and we give the analytical expressions for Eve's optimal states. For COWm1, the optimization was performed numerically, but we could find an analytical expression for Eve's states, in which there remain only three parameters to optimize. For DPS, only numerical optimizations could be performed. The second optimization (over $\mu$) could only be done numerically in all cases.

The results of the optimizations are shown in figure 2 for the four protocols, as a function of $V$, and in the case $Q = 0$ for all versions of COW. The effect of the QBER in the COW protocols is shown in figures B.1, C.1 and D.1.

As expected, when $V = 1$ and $Q = 0$, the attacks under study coincide for all protocols with the asymptotic limits for BSA. As was the case for BSA, one notices similar behaviors for the COW and the DPS protocols, at least for high visibilities: the secret key rates (or the factors $r_0$) are again very similar, within a factor of two. Again, we cannot conclude that one

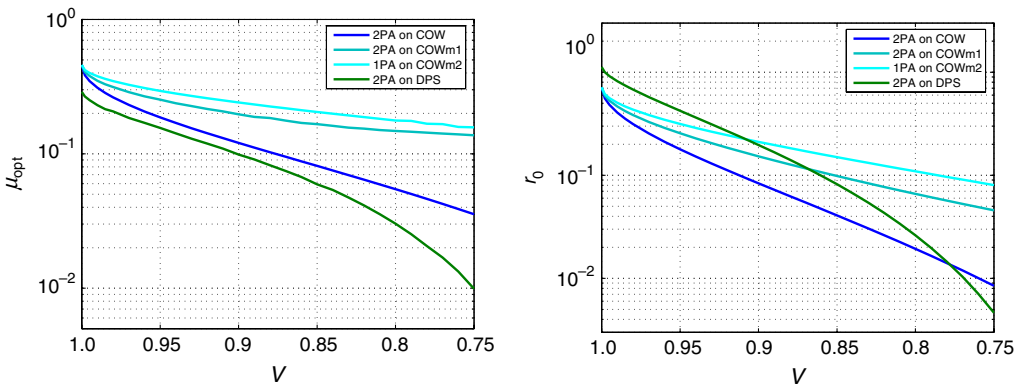


**Figure 2.** $\mu_{opt}$ and $r_0$ as a function of the visibility $V$, for 2PA on the COW, COWm1 and DPS protocols, and for 1PA on COWm2. For all versions of COW, we show here the curve for $Q = 0$.

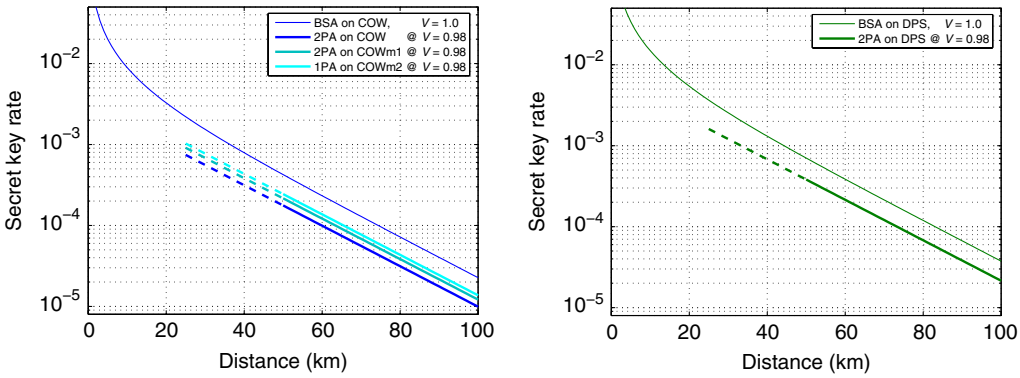


**Figure 3.** Secret key rates as a function of the distance, for 2PA or 1PA on each protocol (for $V = 0.98$), compared to BSA. Same parameters as in figure 1. Recall that the bounds obtained for 2PA and 1PA are valid only in the limit of large distances.

protocol performs better than the other one. The choice of which protocol to run should be motivated by various practical reasons that we did not consider here. Still, and as expected, the modified versions of COW provide better bounds than the original COW: Eve's attack is less efficient when Eve does not know how Alice and Bob will choose the pairing of the pulses.

Finally, in order to get the secret key rates for a given distance, one just has to multiply the factor $r_0$ by $t\eta$. We show as an example in figure 3 the rates that we get for each protocol in the case of $V = 0.98$ (and still $Q = 0$ for COW and its variations), compared to BSA.

## 5. Conclusion

We have provided new upper bounds for the security of the COW (the original and two modified versions) and the DPS protocols, in the limit of large distances. In all cases, the secret key rate goes as $r \approx r_0 t\eta$ and therefore scales linearly with the transmission $t$ of the channel; also, all the values of $r_0$ are similar, within a factor of two for high visibilities. Hence, at least given

our present-day knowledge, the choice between any of these protocols should be dictated by practical reasons rather than by security concerns.

The two modified versions COWm1 and COWm2, introduced in a very natural way in the context of this paper, may also prove very useful in the future to find the bound for security against the most general attack by the eavesdropper. Indeed, intuition suggests that the random *a posteriori* choice of the pairing may provide the symmetry argument, which would allow to use the exponential De Finetti theorem [21].

## Acknowledgments

We acknowledge financial support from the European Project SECOQC and from the Swiss NCCR 'Quantum Photonics'. We are grateful to Antonio Acín, Norbert Lütkenhaus, Renato Renner and Christoph Simon for stimulating discussions.

## Appendix A. Other possible variants of the COW protocol

In the main text, we introduced two modified versions of COW. More generally, many other variants can be defined, as we briefly mention in this appendix. We give examples of such variants, that could be useful for future studies.

There are two main motivations for looking at possible variants: one is to find a more efficient or more robust protocol (in the present case for instance, COWm1 and COWm2 were found to be more robust against the attacks under study); the other one is to find a protocol for which it should be easier to prove the security (for instance, a protocol with more symmetries, or where the signals that code for different bits would be more independent).

In all the following variants, Alice and Bob use the same devices as in the original COW protocol: Alice sends a certain fraction $q$ of weak coherent pulses $|\sqrt{\mu}\rangle$ (with an overall phase relationship) and a fraction $1-q$ of empty pulses $|0\rangle$; Bob measures the time of arrival on his data line and checks the coherence of successive non-empty pulses on his monitoring line. The only differences lie in the way the classical information is encoded, or in how the key reconciliation is performed.

We do not provide here a security analysis for the following variants; nonetheless, in order to give a rough idea of how the various versions should perform, we estimate the sifting rate $r_s$ and the ideal mutual information per sifted pulse $I_{AB}$ between Alice and Bob in the limit of large distances ($\mu t \ll 1$), in the absence of an eavesdropper and without dark counts. The ideal key rate would then be $r = r_s I_{AB}$.

The simplest possible coding is that the logical bit value 1 is coded as a non-empty pulse $|\sqrt{\mu}\rangle$ and the bit 0 as an empty pulse $|0\rangle$. In such a simple coding, the raw key is as long as the entire train of pulses: $r_s = 1$ (as for instance in continuous variable QKD ([22] and references therein). However, even in the absence of an adversary and of dark counts, the error rate is large: Bob is very likely to fail to detect a non-empty pulse, and the quantum channel acts as a Z-channel, where the bit 0 is always detected correctly, while the bit 1 has a high probability $e^{-\mu t\eta}$ to be detected as a 0. Straightforward application of Shannon channel capacity shows that in the ideal case, $I_{AB} = h(q\mu t\eta) - qh(\mu t\eta) \approx -q\log_2 q\mu t\eta$. For the optimal choice of $q = e^{-1}$ one finds: $r \approx \frac{e^{-1}}{\ln 2}\mu t\eta \approx 0.53\,\mu t\eta$.

In practice, the main drawback of this basic protocol is the large error rate. In fact, while $I_{AB}$ can in principle be extracted by error correction (which we have supposed everywhere in this paper), real codes do not reach this bound and become very inefficient if the error rate is large. In other words, it is better to try and have fewer, better correlated signals, than to keep a lot of poorly correlated ones. One possibility to reduce this error rate is to include a sifting step: Bob would announce his $q\mu t\eta$ fraction of time slots where he got a click on his data line, along with another fraction $f_0$ where he had no click. In this case, the sifting rate reduces to $r_s = q\mu t\eta + f_0$, but the fraction of errors to be corrected is also reduced. Depending on the practical efficiency of the error correction, one can try to optimize $f_0$.

When dealing with such a Z-channel, a way to symmetrize the errors is to code the logical bits into two physical symbols: '0'; $\rightarrow \mu 0$, '1' $\rightarrow 0\mu$. In this prospect, the original coding of COW appears very naturally. Contrary to the previous version, there are no more errors due to the losses (Bob only keeps the cases where he had one detection), and in the absence of dark counts and of Eve $I_{AB} = 1$, and $r = r_s$.

In the original version of COW, the pairs of pulses defining each classical bit are predefined. Alice sends pairs $\mu 0$ or $0\mu$, along with some decoy sequences $\mu\mu$ (and possibly also sequences 00). When the fraction of decoy sequences is negligible, the sifting rate is $r_s = \frac{1}{2}\mu t\eta$.

A first possible variant of this original COW corresponds to COWm1, where Alice still sends sequences $\mu 0$ or $0\mu$, but sometimes she introduces an unused pulse, so that the bit separations are not known in advance by Eve. Again, if the fraction of unused pulses is negligible, the sifting rate is $r_s = \frac{1}{2}\mu t\eta$.

Another variant would be that Alice sends a completely random train of pulses $|0\rangle$ and $|\sqrt{\mu}\rangle$. She then pairs consecutive pulses *a posteriori*. Here we lose a factor $\frac{1}{2}$ in the sifting rate ($r_s = \frac{1}{4}\mu t\eta$) because of the sequences 00 and $\mu\mu$ that Alice sometimes pairs together, but the security might be easier to analyze.

In the previous two variants, one can also imagine that the pairs are not necessarily composed of successive pulses (such as in COWm2 for instance). This might be more robust against Eve's attacks, but this necessitates a large amount of information to be sent from Alice to Bob for the key reconciliation.

Also, one can imagine that it is Bob who chooses the pairing: when he gets a detection, he announces two time-slots (successive or not), and Alice checks that they correspond to a sequence $\mu 0$ or $0\mu$. Since Bob has approximately a probability $\frac{1}{2}$ to announce two time-slots that correspond to a sequence $\mu\mu$ instead, the sifting rate in this case is $r_s \approx \frac{1}{4}\mu t\eta$.

Finally, one can imagine that Alice and Bob use other (longer) sequences of pulses $|\sqrt{\mu}\rangle$ and $|0\rangle$ to encode their classical bits (or dits). All previous variations, whether the way the pulses are grouped is defined *a priori* or *a posteriori*, by Alice or by Bob, whether they group successive pulses or not, also apply to this more general variant.

## Appendix B. Optimization of 2PA on COW

We have to maximize $\chi_{COW}$ (15), i.e. to minimize $|\langle p_{0\mu}^{01}|p_{\mu 0}^{10}\rangle|$, submitted to the constraints

$$\langle v_{0\mu}|v_{\mu 0}\rangle = \mathrm{e}^{-\mu} \equiv \gamma, \quad \langle v_{\mu\mu}|v_{\mu 0}\rangle = \langle v_{\mu\mu}|v_{0\mu}\rangle = \mathrm{e}^{-\mu/2}, \tag{B.1}$$

$$\mathrm{Re}\big[\langle p_{\mu\mu}^{01}|p_{\mu\mu}^{10}\rangle\big] = \mathrm{Re}\big[\langle v_x|p_x^{01}\rangle\langle p_y^{10}|v_y\rangle\big] = V, \tag{B.2}$$

for the four two-pair sequences $(x, y) = (0\mu, \mu 0), (\mu\mu, \mu 0), (0\mu, \mu\mu)$ and $(\mu\mu, \mu\mu)$. We notice that the states $|p^{10}_{\mu 0}\rangle$ and $|p^{01}_{0\mu}\rangle$, whose overlap fully defines Eve's information, are related to the states $|v_{\mu 0}\rangle$ and $|v_{0\mu}\rangle$ through (B.2), specifically

$$\mathrm{Re}\big[\langle v_{0\mu}|p^{01}_{0\mu}\rangle\langle p^{10}_{\mu 0}|v_{\mu 0}\rangle\big] = V. \tag{B.3}$$

So, we focus at first only on finding four states $|v_{\mu 0}\rangle$, $|v_{0\mu}\rangle$, $|p^{10}_{\mu 0}\rangle$ and $|p^{01}_{0\mu}\rangle$ that satisfy (B.3) and such that $|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle|$ is minimal. Later, we shall check that we can find states $|v_{\mu\mu}\rangle$, $|p^{10}_{\mu\mu}\rangle$, and $|p^{01}_{\mu\mu}\rangle$ in order to satisfy all the constraints (recall that the states $|p^{01}_{\mu 0}\rangle$ and $|p^{10}_{0\mu}\rangle$ are chosen to be orthogonal to all other states).

### *B.1. Parametrization of Eve's states*

First, let's choose the first two basis vectors such that the states $|v_{\mu 0}\rangle$ and $|v_{0\mu}\rangle$ read

$$|v_{\mu 0}\rangle = \begin{pmatrix} \sqrt{\frac{1+\gamma}{2}} \\ \sqrt{\frac{1-\gamma}{2}} \end{pmatrix}, \quad |v_{0\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1+\gamma}{2}} \\ -\sqrt{\frac{1-\gamma}{2}} \end{pmatrix}. \tag{B.4}$$

Let's also define $|v^{\perp}_{j}\rangle$ as the orthogonal state to $|v_j\rangle$, in the same two-dimensional (2D) subspace:

$$|v^{\perp}_{\mu 0}\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{2}} \\ -\sqrt{\frac{1+\gamma}{2}} \end{pmatrix}, \quad |v^{\perp}_{0\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{2}} \\ \sqrt{\frac{1+\gamma}{2}} \end{pmatrix}. \tag{B.5}$$

We must have (B.3). Now, if $\langle v_{0\mu}|p^{01}_{0\mu}\rangle\langle p^{10}_{\mu 0}|v_{\mu 0}\rangle \notin \mathbb{R}$, then Eve could just add a global phase to $|p^{10}_{\mu 0}\rangle$ for instance, and increase $V$ without changing her information. This implies that Eve's maximal information compatible with $V$ is obtained when the above quantity is real. Then we can write, for some factor $\lambda \in [V, 1/V]$ and some phase $\tilde{\phi} \in \mathbb{R}$: $\langle v_{\mu 0}|p^{10}_{\mu 0}\rangle = \sqrt{\lambda V}\mathrm{e}^{\mathrm{i}\tilde{\phi}}$ and $\langle v_{0\mu}|p^{01}_{0\mu}\rangle = \sqrt{V/\lambda}\mathrm{e}^{\mathrm{i}\tilde{\phi}}$. But since the phase $\tilde{\phi}$ does not play any role in Eve's information (which depends only on $|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle|$), we can without loss of generality set it to 0. In conclusion, $|p^{10}_{\mu 0}\rangle$ and $|p^{01}_{0\mu}\rangle$ are of the form

$$|p^{10}_{\mu 0}\rangle = \sqrt{\lambda V}|v_{\mu 0}\rangle - \sqrt{1-\lambda V}\cos\theta_0 \mathrm{e}^{\mathrm{i}\phi_0}|v^{\perp}_{\mu 0}\rangle + \sqrt{1-\lambda V}\sin\theta_0|w_0\rangle, \tag{B.6}$$

$$|p^{01}_{0\mu}\rangle = \sqrt{V/\lambda}|v_{0\mu}\rangle - \sqrt{1-V/\lambda}\cos\theta_1 \mathrm{e}^{\mathrm{i}\phi_1}|v^{\perp}_{0\mu}\rangle + \sqrt{1-V/\lambda}\sin\theta_1|w_1\rangle, \tag{B.7}$$

where $|w_0\rangle$ and $|w_1\rangle$ are any states orthogonal to both $|v_{\mu 0}\rangle$ and $|v_{0\mu}\rangle$ and $\theta_0$, $\theta_1$, $\phi_0$ and $\phi_1$ are free parameters.

### *B.2. Results of the optimization*

For $\gamma > 2\sqrt{V(1-V)}$ (i.e. $\mu$ small enough) and $V > 1/2$, it can be proved analytically[6] that the minimum of $|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle|$ is

$$|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle| = (2V-1)\gamma - 2\sqrt{V(1-V)}\sqrt{1-\gamma^2}, \tag{B.8}$$

[6] Here are the main steps of the proof: first, one can easily show that $\theta_0, \theta_1 \in [0, \pi/2]$, $\phi_0 = \phi_1 = 0$ and $\langle w_0|w_1\rangle = -1$ are optimal; once this is fixed, one can show that for any given $\lambda$, the minimum of $|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle|$ over $\theta_0$ and $\theta_1$ is obtained for $\theta_0 = \theta_1 = 0$; finally, one can prove that $\lambda = 1$ is optimal.

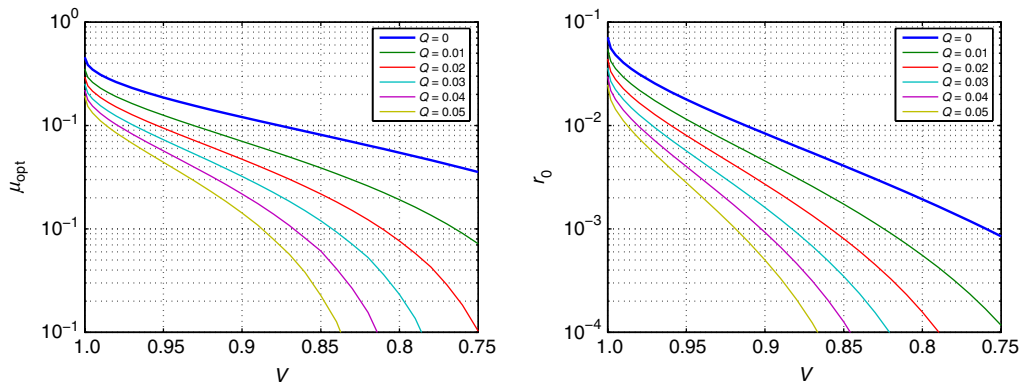


**Figure B.1.** COW, original version: $\mu_{\rm opt}$ and $r_0$ for 2PA, for different values of $Q$.

obtained for $\lambda = 1, \theta_0 = \theta_1 = \phi_0 = \phi_1 = 0$, in which case $|p^{10}_{\mu 0}\rangle = \sqrt{V}|v_{\mu 0}\rangle - \sqrt{1-V}|v^{\perp}_{\mu 0}\rangle$, $|p^{01}_{0\mu}\rangle = \sqrt{V}|v_{0\mu}\rangle - \sqrt{1-V}|v^{\perp}_{0\mu}\rangle$. Having maximized Eve's information, one can run the one-parameter optimization over the pulse intensity $\mu$. The optimal choice $\mu_{\rm opt}$ and the corresponding value of $r_0$ are plotted in figure B.1, as a function of $V$ and for different values of $Q$.

We still have to check that we can find states $|v_{\mu\mu}\rangle$, $|p^{10}_{\mu\mu}\rangle$ and $|p^{01}_{\mu\mu}\rangle$ that satisfy all the constraints. This is indeed the case. For instance, we complete the previous basis with a third orthogonal vector and choose

$$|v_{\mu\mu}\rangle = \begin{pmatrix} \sqrt{\frac{2\gamma}{1+\gamma}} \\ 0 \\ \sqrt{\frac{1-\gamma}{1+\gamma}} \end{pmatrix}, \quad |p^{10}_{\mu\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1+V}{2}}c \\ \sqrt{\frac{1-V}{2}} \\ \sqrt{\frac{1+V}{2}}s \end{pmatrix}, \quad |p^{01}_{\mu\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1+V}{2}}c \\ -\sqrt{\frac{1-V}{2}} \\ \sqrt{\frac{1+V}{2}}s \end{pmatrix}, \tag{B.9}$$

with $c = \sqrt{\frac{2V}{1+V}}\sqrt{\frac{2\gamma}{1+\gamma}} + \sqrt{\frac{1-V}{1+V}}\sqrt{\frac{1-\gamma}{1+\gamma}}$ and $s = \sqrt{\frac{2V}{1+V}}\sqrt{\frac{1-\gamma}{1+\gamma}} - \sqrt{\frac{1-V}{1+V}}\sqrt{\frac{2\gamma}{1+\gamma}}$. The fact that the minimum of $|\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle|$ can be reached without using the constraints that involve the sequence $(\mu, \mu)$ means that the presence of decoy sequences does not increase the security of COW against 2PA.

Note finally that if $\gamma \leqslant 2\sqrt{V(1-V)}$ or if $V \leqslant 1/2$, Eve can choose her states $|p^{10}_{\mu 0}\rangle$ and $|p^{01}_{0\mu}\rangle$ (for instance $\lambda = 1, \cos\theta_0 = \frac{\gamma V}{(1-V)\gamma + 2\sqrt{V(1-V)}\sqrt{1-\gamma^2}}, \theta_1 = \phi_0 = \phi_1 = 0$) such that $\langle p^{01}_{0\mu}|p^{10}_{\mu 0}\rangle = 0$, in which case Eve can perfectly discriminate the two states: she has the full information on Alice and Bob's bit. Therefore, $\gamma > 2\sqrt{V(1-V)}$ and $V > 1/2$ are necessary conditions for Alice and Bob to establish a secret key.

## Appendix C. Optimization of 2PA on COWm1

We have to maximize $\chi_{\rm COWm1}$ (26) submitted to the constraints (B.1), (B.2) and

$$\langle v_{00}|v_{\mu\mu}\rangle = {\rm e}^{-\mu} \equiv \gamma, \quad \langle v_{00}|v_{\mu 0}\rangle = \langle v_{00}|v_{0\mu}\rangle = {\rm e}^{-\mu/2}. \tag{C.1}$$

### C.1. Parametrization of Eve's states

We write the states $|v_{jk}\rangle$ as

$$|v_{\mu 0}\rangle = \begin{pmatrix} \sqrt{\frac{1+\gamma}{2}} \\ \sqrt{\frac{1-\gamma}{2}} \\ 0 \\ 0 \end{pmatrix}, \quad |v_{0\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1+\gamma}{2}} \\ -\sqrt{\frac{1-\gamma}{2}} \\ 0 \\ 0 \end{pmatrix},$$

$$|v_{00}\rangle = \begin{pmatrix} \sqrt{\frac{2\gamma}{1+\gamma}} \\ 0 \\ \sqrt{\frac{1-\gamma}{1+\gamma}} \\ 0 \end{pmatrix}, \quad |v_{\mu\mu}\rangle = \begin{pmatrix} \sqrt{\frac{2\gamma}{1+\gamma}} \\ 0 \\ -\gamma\sqrt{\frac{1-\gamma}{1+\gamma}} \\ 1-\gamma \end{pmatrix}. \tag{C.2}$$

These states satisfy the constraints (B.1) and (C.1). We still have four states to consider, $|p^{10}_{\mu 0}\rangle$, $|p^{01}_{0\mu}\rangle$, $|p^{10}_{\mu\mu}\rangle$ and $|p^{01}_{\mu\mu}\rangle$ (recall that the states $|p^{01}_{\mu 0}\rangle$, $|p^{10}_{0\mu}\rangle$, $|p^{10}_{\mu\mu}\rangle$ and $|p^{01}_{\mu\mu}\rangle$ have already been chosen orthogonal to all other states). Therefore, Eve's states under consideration live in general in an 8D space. We have performed the numerical optimization over the most general choice of the four $|p\rangle$ states that satisfied the constraints (B.2).

### C.2. Results of the optimization

The best attack we found can be realized by 4D states and depends only on three free parameters ($\theta_0$, $\theta_1$ and $\phi$), that are still to be optimized. Let's introduce the following vectors:

$$|v^{\perp}_{\mu 0}\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{2}} \\ -\sqrt{\frac{1+\gamma}{2}} \\ 0 \\ 0 \end{pmatrix}, \quad |v^{\perp}_{0\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{2}} \\ \sqrt{\frac{1+\gamma}{2}} \\ 0 \\ 0 \end{pmatrix}, \quad |v^{\perp,1}_{\mu\mu}\rangle = \begin{pmatrix} 0 \\ 0 \\ \sqrt{1-\gamma^2} \\ \gamma \end{pmatrix},$$

$$|v^{\perp,2}_{\mu\mu}\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{1+\gamma}} \\ 0 \\ \gamma\sqrt{\frac{2\gamma}{1+\gamma}} \\ -\sqrt{2\gamma}\sqrt{1-\gamma} \end{pmatrix}, \tag{C.3}$$

$$|w_2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |w_3\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |w_4\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{C.4}$$

Our best attack is then defined by

$$|p^{10}_{\mu 0}\rangle = \sqrt{V}|v_{\mu 0}\rangle - \sqrt{1-V}|w_{\mu 0}\rangle, \quad |p^{01}_{0\mu}\rangle = \sqrt{V}|v_{0\mu}\rangle - \sqrt{1-V}|w_{0\mu}\rangle, \tag{C.5}$$

$$|p^{10}_{\mu\mu}\rangle = \sqrt{V}|v_{\mu\mu}\rangle - \sqrt{1-V}|w^{10}_{\mu\mu}\rangle, \quad |p^{01}_{\mu\mu}\rangle = \sqrt{V}|v_{\mu\mu}\rangle - \sqrt{1-V}|w^{01}_{\mu\mu}\rangle, \tag{C.6}$$

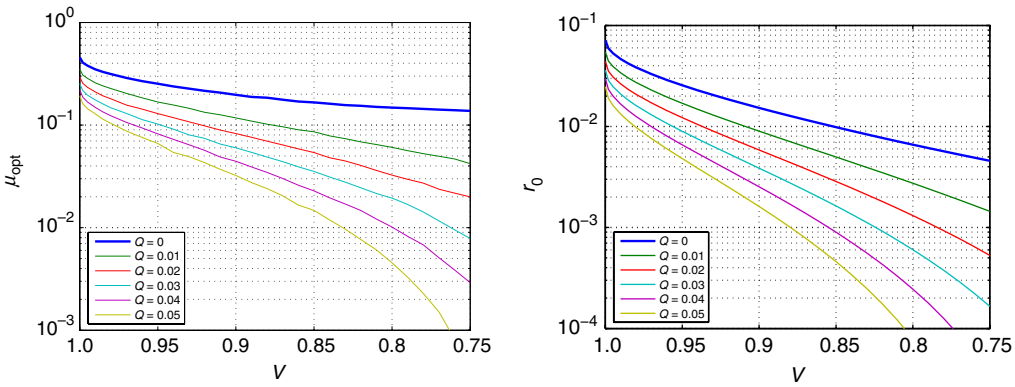


**Figure C.1.** COWm1: $\mu_{\rm opt}$ and $r_0$ for 2PA, for different values of $Q$.

where

$$|w_{\mu 0}\rangle = \cos\theta_0\,|v_{\mu 0}^{\perp}\rangle + \sin\theta_0\cos\theta_1\,|w_3\rangle + \sin\theta_0\sin\theta_1\,|w_4\rangle, \tag{C.7}$$

$$|w_{0\mu}\rangle = \cos\theta_0\,|v_{0\mu}^{\perp}\rangle + \sin\theta_0\cos\theta_1\,|w_3\rangle + \sin\theta_0\sin\theta_1\,|w_4\rangle, \tag{C.8}$$

$$|w_{\mu\mu}^{10}\rangle = \frac{1}{\sqrt{2}}(\cos\phi\,|v_{\mu\mu}^{\perp,1}\rangle + \sin\phi\,|v_{\mu\mu}^{\perp,2}\rangle) - \frac{1}{\sqrt{2}}\,|w_2\rangle, \tag{C.9}$$

$$|w_{\mu\mu}^{01}\rangle = \frac{1}{\sqrt{2}}(\cos\phi\,|v_{\mu\mu}^{\perp,1}\rangle + \sin\phi\,|v_{\mu\mu}^{\perp,2}\rangle) + \frac{1}{\sqrt{2}}\,|w_2\rangle. \tag{C.10}$$

Note that these states satisfy a more constraining version of (B.2): $\langle p_{\mu\mu}^{01}|p_{\mu\mu}^{10}\rangle = V$, $\langle v_{0\mu}|p_{0\mu}^{01}\rangle = \langle v_{\mu\mu}|p_{\mu\mu}^{01}\rangle = \langle p_{\mu 0}^{10}|v_{\mu 0}\rangle = \langle p_{\mu\mu}^{10}|v_{\mu\mu}\rangle = \sqrt{V}$. Finally, the optimization over the three remaining parameters $\theta_0$, $\theta_1$ and $\phi$ was performed numerically.

Having maximized Eve's information, one can run the one-parameter optimization over the pulse intensity $\mu$. The optimal choice $\mu_{\rm opt}$ and the corresponding value of $r_0$ are plotted in figure C.1.

## Appendix D. Optimization of 1PA on COWm2

We have to maximize $\chi_{\rm COWm2}$ (32), i.e. to minimize $|\langle v_0|p_\mu\rangle|$, submitted to the constraints

$$\langle v_0|v_\mu\rangle = \mathrm{e}^{-\mu/2}, \tag{D.1}$$

$$|\langle v_\mu|p_\mu\rangle|^2 = V. \tag{D.2}$$

The state $|p_0\rangle$ was already chosen to be orthogonal to the three other states; we have therefore to work in a 3D Hilbert space. Without loss of generality, we choose the following parametrization, which ensures automatically that the constraints are satisfied:

$$|v_\mu\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |v_0\rangle = \begin{pmatrix} \mathrm{e}^{-\mu/2} \\ \sqrt{1-\mathrm{e}^{-\mu}} \\ 0 \end{pmatrix}, \quad |p_\mu\rangle = \mathrm{e}^{\mathrm{i}\tilde{\phi}} \begin{pmatrix} \sqrt{V} \\ -\sqrt{1-V}\cos\theta\,\mathrm{e}^{i\phi} \\ \sqrt{1-V}\sin\theta \end{pmatrix}, \tag{D.3}$$

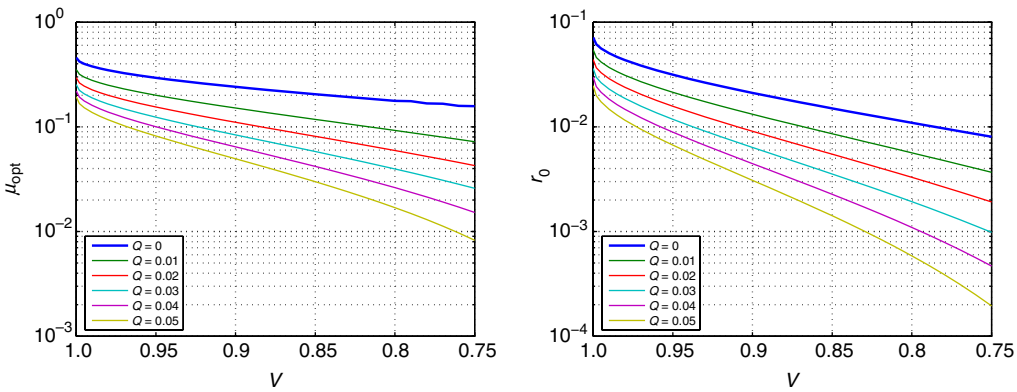


**Figure D.1.** COWm2: $\mu_{\rm opt}$ and $r_0$ for 1PA, for different values of $Q$.

actually the phase $\tilde{\phi}$ does not play any role, and we set it to be 0. So, for a given $V$ and a given $\mu$, Eve's states are parametrized by $\theta$ and $\phi$.

For $\mathrm{e}^{-\mu} \leqslant 1 - V$, Eve can choose $\phi = 0$ and $\cos\theta = \sqrt{\frac{\mathrm{e}^{-\mu}}{1-\mathrm{e}^{-\mu}}\frac{V}{1-V}}$, which gives $\langle v_0|p_\mu\rangle = 0$: in this case, Eve has full information on Alice and Bob's bit. A necessary condition for Alice and Bob to have secret bits is therefore to choose $\mu$ such that $\mathrm{e}^{-\mu} > 1 - V$. In this case, one can easily show that the minimum overlap is

$$|\langle v_0|p_\mu\rangle| = \mathrm{e}^{-\mu/2}\sqrt{V} - \sqrt{1-\mathrm{e}^{-\mu}}\sqrt{1-V}, \tag{D.4}$$

obtained by setting $\theta = \phi = 0$.

Having maximized Eve's information, one can run the one-parameter optimization over the pulse intensity $\mu$. The optimal choice $\mu_{\rm opt}$ and the corresponding value of $r_0$ are plotted in figure D.1.

## Appendix E. Optimization of 1PA and 2PA on DPS

As mentioned in the main text, the optimization of Eve's information for a 2PA on DPS is more complicated than the one for COW, because we could not find any evident simplification and had therefore to start from the general formal expressions. For this reason, we find it useful to sketch first the study of 1PA on DPS—if only to show that our optimization on the 2PA yields indeed a more strict bound.

### *E.1. Optimization of 1PA on DPS*

*E.1.1. Eve's attack and information.* We have not studied 1PA on DPS in the main text, but the pattern is the same as for all other attacks, so we just list the main points. Eve's attack is defined by (with $\sigma \in \{+, -\}$)

$$|\sigma\sqrt{\mu}\rangle_{\rm A}|\mathcal{E}\rangle \longrightarrow |0\rangle_{\rm B}|v_\sigma\rangle_{\rm E} + \sigma\sqrt{\mu t}|1\rangle_{\rm B}|p_\sigma\rangle_{\rm E} \tag{E.1}$$

so the unitarity condition and the visibility constraints read

$$\langle v_+|v_-\rangle = \mathrm{e}^{-2\mu} \equiv \gamma, \tag{E.2}$$

$$\forall \sigma, \omega \in \{+, -\}, \quad \mathrm{Re}\big[\langle v_\sigma | p_\sigma \rangle \langle p_\omega | v_\omega \rangle\big] = V. \tag{E.3}$$

This last condition implies $\langle v_+ | p_+ \rangle = \langle v_- | p_- \rangle = \sqrt{V} \mathrm{e}^{\mathrm{i}\tilde{\phi}}$, for some $\tilde{\phi}$ which won't play any role, and which we set to 0; so we have

$$\langle v_+ | p_+ \rangle = \langle v_- | p_- \rangle = \sqrt{V}. \tag{E.4}$$

Note how all the states participate in the constraints, contrary to what is the case in all versions of COW.

To compute Eve's information, we start from Eve's conditioned states $\rho_{\mathrm{E}}^{\mathrm{A}=\{\sigma\omega\},\mathrm{B}=b} = |\psi_{\sigma,\omega,b}\rangle\langle\psi_{\sigma,\omega,b}|$ with $|\psi_{\sigma,\omega,b}\rangle = \sigma|p_\sigma, v_\omega\rangle + (-1)^b \omega |v_\sigma, p_\omega\rangle$ and the mixtures $\rho_{\mathrm{E}}^{a,b} = \frac{1}{8}\sum_\sigma \rho_{\mathrm{E}}^{\mathrm{A}=\{\sigma\sigma(a)\},\mathrm{B}=b}$ where $\sigma(a) = (-1)^a \sigma$. Note that these states are not normalized; rather, $\mathrm{Tr}(\rho_{\mathrm{E}}^{a,b})$ is equal to $\frac{1+V}{2} = 1 - Q$ if $a = b$, and to $\frac{1-V}{2} = Q$ if $a \neq b$. Finally, $\rho_{\mathrm{E}}^{\mathrm{A}=a} = \sum_b \rho_{\mathrm{E}}^{a,b}$ and $\rho_{\mathrm{E}}^{\mathrm{B}=b} = \sum_b \rho_{\mathrm{E}}^{a,b}$ (now normalized). Eve's information is given by $\chi_{\mathrm{AE}} = \chi(\rho_{\mathrm{E}}^{\mathrm{A}=0}, \rho_{\mathrm{E}}^{\mathrm{A}=1})$, and similarly for $\chi_{\mathrm{BE}}$.

*E.1.2. Parametrization of Eve's states.* Eve's states can be chosen in a 4D Hilbert space. First, let's choose a basis with the first two vectors in the subspace spanned by $\{|v_+\rangle, |v_-\rangle\}$, and in which $|v_+\rangle$ and $|v_-\rangle$ read

$$|v_\sigma\rangle = \begin{pmatrix} \sqrt{\frac{1+\gamma}{2}} \\ \sigma\sqrt{\frac{1-\gamma}{2}} \\ 0 \\ 0 \end{pmatrix} \tag{E.5}$$

so that (E.2) is satisfied. Let's also define $|v_\sigma^\perp\rangle$ as the orthogonal state to $|v_\sigma\rangle$, in the subspace spanned by $\{|v_+\rangle, |v_-\rangle\}$:

$$|v_\sigma^\perp\rangle = \begin{pmatrix} \sqrt{\frac{1-\gamma}{2}} \\ -\sigma\sqrt{\frac{1+\gamma}{2}} \\ 0 \\ 0 \end{pmatrix}. \tag{E.6}$$

The constraint (E.4) on the visibility implies that $|p_\sigma\rangle$ can be written as $|p_\sigma\rangle = \sqrt{V}|v_\sigma\rangle - \sqrt{1-V}|w_\sigma\rangle$, where $|w_\sigma\rangle$ is any (4-D) state orthogonal to $|v_\sigma\rangle$; this can be further decomposed as $|w_\sigma\rangle = \cos\theta_\sigma \mathrm{e}^{\mathrm{i}\phi_\sigma}|v_\sigma^\perp\rangle + \sin\theta_\sigma |w'_\sigma\rangle$ for some states $|w'_\sigma\rangle$ orthogonal to both $|v_+\rangle$ and $|v_-\rangle$. Finally, we choose the last two vectors of the basis such that $|w'_+\rangle$ and $|w'_-\rangle$ read

$$|w'_+\rangle = \begin{pmatrix} 0 \\ 0 \\ \cos(\theta/2)\mathrm{e}^{\mathrm{i}\phi/2} \\ \sin(\theta/2)\mathrm{e}^{\mathrm{i}\phi/2} \end{pmatrix}, \quad |w'_-\rangle = \begin{pmatrix} 0 \\ 0 \\ \cos(\theta/2)\mathrm{e}^{-\mathrm{i}\phi/2} \\ -\sin(\theta/2)\mathrm{e}^{-\mathrm{i}\phi/2} \end{pmatrix}. \tag{E.7}$$

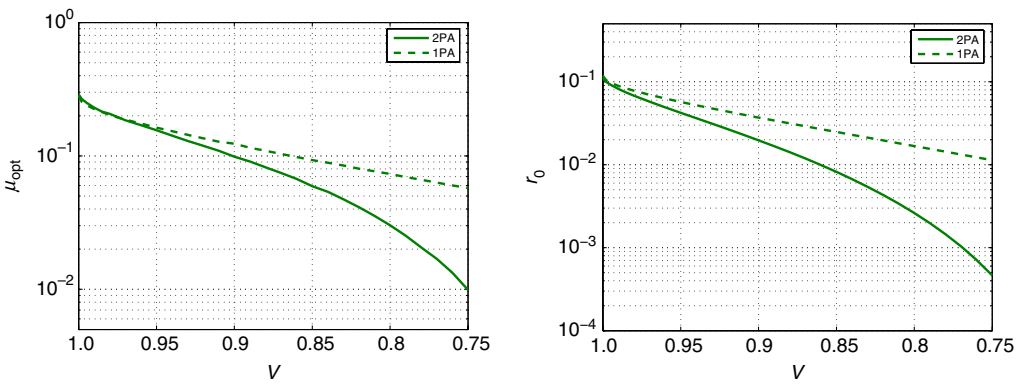


**Figure E.1.** $\mu_{\text{opt}}$ and $r_0$ for 1PA and 2PA on DPS.

In summary, for a given $V$ and a given $\mu$, we are left without loss of generality with the six free parameters $\theta_+$, $\theta_-$, $\theta$, $\phi_+$, $\phi_-$ and $\phi$ that define

$$|p_\sigma\rangle = \sqrt{V}|v_\sigma\rangle - \sqrt{1-V}\cos\theta_\sigma \mathrm{e}^{\mathrm{i}\phi_\sigma}|v_\sigma^\perp\rangle - \sqrt{1-V}\sin\theta_\sigma|w'_\sigma\rangle. \tag{E.8}$$

*E.1.3. Results of the optimization.* The optimization over the six free parameters was performed numerically. We find that Eve's optimal states have real coefficients (the parameters $\phi_\pm$, $\phi$ can be chosen to be 0), and also that $\theta_+ = -\theta_-$. Once we fix this, there remains only two free parameters to optimize.

Having maximized Eve's information, one can run the one-parameter optimization over the pulse intensity $\mu$. The optimal choice $\mu_{\text{opt}}$ and the corresponding value of $r_0$ are plotted in figure E.1, along with the results for 2PA. In the case $V = 1$, this attack reduces to the BSA; in all other cases, the optimal 1PA is manifestly less powerful than the best 2PA we have found.

Note that after optimization, we find $\chi_{\text{AE}} \leqslant \chi_{\text{BE}}$: Eve knows less about Alice's bit than about Bob's.

### *E.2. Optimization of 2PA on DPS*

We now consider the 2PA on DPS, and we have to optimize $\chi_{\text{AE}}$ and $\chi_{\text{BE}}$ as given in (42), submitted to the constraints

$$\langle v_{\sigma\omega}|v_{\sigma\bar{\omega}}\rangle = \langle v_{\sigma\omega}|v_{\bar{\sigma}\omega}\rangle = \mathrm{e}^{-2\mu} \equiv \gamma, \quad \langle v_{\sigma\omega}|v_{\bar{\sigma}\bar{\omega}}\rangle = \mathrm{e}^{-4\mu} = \gamma^2, \tag{E.9}$$

$$\mathrm{Re}\big[\langle p^{01}_{\sigma\omega}|p^{10}_{\sigma\omega}\rangle\big] = \mathrm{Re}\big[\langle v_{\sigma\omega}|p^{01}_{\sigma\omega}\rangle\langle p^{10}_{\sigma'\omega'}|v_{\sigma'\omega'}\rangle\big] = V, \tag{E.10}$$

for all $\sigma, \omega, \sigma', \omega' \in \{+, -\}$. We see that all the twelve states of Eve appear in the expressions of the constraints.

*E.2.1. Parametrization of Eve's states.* Without any loss of generality, we choose the following symmetric parametrization for Eve's four states $|v_{\sigma\omega}\rangle$:

$$|v_{++}\rangle = \begin{pmatrix} \frac{1+\gamma}{2} \\ \frac{1-\gamma}{2} \\ \sqrt{\frac{1-\gamma^2}{2}} \\ 0 \end{pmatrix}, \quad |v_{--}\rangle = \begin{pmatrix} \frac{1+\gamma}{2} \\ \frac{1-\gamma}{2} \\ -\sqrt{\frac{1-\gamma^2}{2}} \\ 0 \end{pmatrix}, \quad |v_{+-}\rangle = \begin{pmatrix} \frac{1+\gamma}{2} \\ -\frac{1-\gamma}{2} \\ 0 \\ \sqrt{\frac{1-\gamma^2}{2}} \end{pmatrix},$$

$$|v_{-+}\rangle = \begin{pmatrix} \frac{1+\gamma}{2} \\ -\frac{1-\gamma}{2} \\ 0 \\ -\sqrt{\frac{1-\gamma^2}{2}} \end{pmatrix}, \tag{E.11}$$

so that (E.9) is satisfied. At this point, we would have to optimize over Eve's most general states $|p^{10}_{\sigma\omega}\rangle$ and $|p^{01}_{\sigma\omega}\rangle$ that satisfied the constraints (E.10). In general, these eight states live in a 12D space, and the number of free parameters is quite large.

In order to have a more tractable problem, we make some assumptions (admittedly, we lose generality here). First, we look for states that satisfy a more constraining version of (E.10), namely

$$\langle p^{01}_{\sigma\omega}|p^{10}_{\sigma\omega}\rangle = V\,, \quad \langle v_{\sigma\omega}|p^{01}_{\sigma\omega}\rangle = \langle v_{\sigma\omega}|p^{10}_{\sigma\omega}\rangle = \sqrt{V}, \tag{E.12}$$

for all $\sigma, \omega$. Then, we can write

$$|p^{01}_{\sigma\omega}\rangle = \sqrt{V}|v_{\sigma\omega}\rangle - \sqrt{1-V}|w^{01}_{\sigma\omega}\rangle, \tag{E.13}$$

$$|p^{10}_{\sigma\omega}\rangle = \sqrt{V}|v_{\sigma\omega}\rangle - \sqrt{1-V}|w^{10}_{\sigma\omega}\rangle \tag{E.14}$$

with $\langle v_{\sigma\omega}|w^{01}_{\sigma\omega}\rangle = \langle v_{\sigma\omega}|w^{10}_{\sigma\omega}\rangle = 0$ and $\langle w^{01}_{\sigma\omega}|w^{10}_{\sigma\omega}\rangle = 0$. Note that this may not be a true restriction: actually, for all the cases treated above, an analog choice was found to be optimal. A more serious restriction comes now: we suppose that the eight states $|w^{10}_{\sigma\omega}\rangle$ and $|w^{01}_{\sigma\omega}\rangle$ live in a 6D space and are parametrized only by real coefficients. At this stage, we run the numerical optimization.

*E.2.2. Results of the optimization.* After having maximized Eve's information, one can run the one-parameter optimization over the pulse intensity $\mu$. The optimal choice $\mu_{\text{opt}}$ and the corresponding value of $r_0$ are plotted in figure E.1, along with the results for 1PA. In the case $V = 1$, this attack reduces again to the BSA.

We did not run the optimization aver all possible states, but we believe that our results are very close to the optimal bounds we could get for 2PA on DPS. Anyway, even though we might have missed the true maximum of Eve's information, the attack we found and the curves that are plotted still provide valid upper bounds, more strict than the bounds given by 1PA on DPS.

Note finally that as for 1PA, we find after optimization $\chi_{\text{AE}} \leqslant \chi_{\text{BE}}$: Eve knows less about Alice's bit than about Bob's.

## References


[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (New York: IEEE) pp 175–9

[2] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

[3] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901

[4] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[6] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238

[7] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[8] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902

[9] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
Bennett C H, Brassard G and Mermin N D 2002 *Phys. Rev. Lett.* **68** 557

[10] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev.* A **68** 022317

[11] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photon.* **1** 343

[12] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004 *Preprint* quant-ph/0411022

[13] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108

[14] Inoue K and Honjo T 2005 *Phys. Rev.* A **71** 042305

[15] Waks E, Takesue H and Yamamoto Y 2006 *Phys. Rev.* A **73** 012344

[16] Branciard C, Gisin N, Lütkenhaus N and Scarani V 2007 *Quantum Inf. Comput.* **7** 639

[17] Curty M, Zhang L L, Lo H-K and Lütkenhaus N 2007 *Quantum Inf. Comput.* **7** 665

[18] Tsurumaru T 2007 *Phys. Rev.* A **75** 062319

[19] Honjo T and Inoue K 2006 *Opt. Lett.* **31** 522

[20] Devetak I and Winter A 2005 *Proc. R. Soc. Lond.* A **461** 207

[21] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH, Zurich (*Preprint* quant-ph/0512258)
Renner R 2007 *Nat. Phys.* **3** 645

[22] Cerf N and Grangier P 2007 *J. Opt. Soc. Am.* B **24** 324