IOP Publishing    *Quantum Sci. Technol.* **10** (2025) 015001    https://doi.org/10.1088/2058-9565/ad8181

Quantum Science and Technology

OPEN ACCESS

RECEIVED
13 May 2024

REVISED
29 August 2024

ACCEPTED FOR PUBLICATION
30 September 2024

PUBLISHED
14 October 2024

PAPER

# Quantum key distribution with unbounded pulse correlations

Margarida Pereira[1,2,3,4,*], Guillermo Currás-Lorenzo[1,2,3,4], Akihiro Mizutani[1], Davide Rusca[2,3,4], Marcos Curty[2,3,4] and Kiyoshi Tamaki[1]

[1] Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan
[2] Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[3] Escuela de Ingenierá de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[4] atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain
[*] Author to whom any correspondence should be addressed.

**E-mail:** mpereira@vqcc.uvigo.es

**Keywords:** implementation security of QKD, side channels, QKD

## Abstract

Typical security proofs of quantum key distribution (QKD) require that the emitted signals are independent and identically distributed. In practice, however, this assumption is not met because intrinsic device flaws inevitably introduce correlations between the emitted signals. Although analyses addressing this issue have been recently proposed, they only consider a restrictive scenario in which the correlations have a finite and known maximum length that is much smaller than the total number of emitted signals. While it is expected that the magnitude of the correlations decreases as the pulse separation increases, the assumption that this magnitude is exactly zero after a certain point does not seem to have any physical justification. Concerningly, this means that the available analyses cannot guarantee the security of current QKD implementations. Here, we solve this pressing problem by developing a rigorous framework that, when combined with existing results, can guarantee security against pulse correlations of unbounded length. Our framework is rather general and could be applied to other situations for which the existing analyses consider a scenario that differs slightly from the actual one.

## 1. Introduction

Quantum key distribution (QKD) promises secure communications between two distant parties based on the laws of physics [1, 2]. However, conventional security proofs of QKD often rely on idealised assumptions, neglecting inevitable device imperfections. This gap between theoretical models and real-world implementations could be exploited by an eavesdropper, compromising the security claim of QKD [3]. Addressing this challenge has become a focal point in the field [4], with experimentalists striving to accurately characterise the magnitude of different device imperfections and refine hardware design to better match the theoretical models, and theorists developing new protocols and security proofs that accommodate various device imperfections.

One of the most important imperfections in practice, especially among high-speed QKD systems [5], are pulse correlations. These occur when the setting choices made in a given round are not only encoded into the signal emitted in that round, but also inadvertently into the signals emitted in subsequent rounds. This phenomenon, purely classical in nature, can arise, for instance, from memory effects in the modulation devices (such as phase and amplitude modulators). It constitutes a security risk because it could allow an eavesdropper to learn key information by investigating the leaked information in subsequent pulses, while causing no disturbance on the current one.

Accommodating this imperfection in security proofs of QKD was believed to be difficult, as many of them require that the emitted states are independent and identically distributed [1]. Recently, however, analyses addressing bit and basis correlations [6–9], intensity correlations [10–12] and phase-randomisation correlations [13] have been proposed. Using these analyses, one is able to effectively bound the amount of information leaked to a potential eavesdropper and apply sufficient privacy amplification to obtain a secure key.

These proofs, however, rely on the assumption that the correlations have a finite and known maximum length $l_c$, beyond which the pulses are completely uncorrelated. In other words, one needs to guarantee that the setting choice made in the $k$th round has absolutely no influence on the signal emitted in the $(k+l)$th round for $l > l_c$. While it is reasonable to expect that the magnitude of the correlations decreases rapidly as the pulse separation $l$ increases, the assumption that this magnitude will drop to exactly zero for any finite value of $l$ does not seem to be justified. Indeed, these correlations could even span the entire communication sequence, i.e. the setting choices made in the first round of the protocol could in principle influence the signals emitted in the very last round.

That being said, intuitively, there should exist a pulse separation threshold after which this influence is so small as to be almost negligible, in the sense that an eavesdropper could gain almost no information from it. This suggests that the key generated in this scenario should be almost as secure as the key that would have been generated in a scenario in which the magnitude of the correlations drops to exactly zero after the threshold. In this work, we confirm this intuition by proving that, even if the correlations technically have an unbounded length, one can apply the existing security analyses as if their length was bounded by the threshold, and then rigorously account for the neglected long-range correlations by slightly adjusting the security parameter of the final key. By doing so, we close a critical loophole in QKD's security, making it resilient against potential attacks exploiting this imperfection.

We remark that the simple formalism we introduce is rather general and versatile, as it can be applied to other situations for which the existing security proofs consider a scenario that differs slightly from the actual one. For this reason, the outline of this paper is as follows. First, in section 2, we describe a general QKD protocol. Then, in section 3 we present our formalism for a general scenario. After that, in section 4, we apply it to the case of unbounded bit and basis pulse correlations and explain how experimentalists can use this result in practice. Finally, in section 5, we discuss and summarise our findings.

## 2. Description of a general QKD protocol

For clarity and simplicity, our discussion focuses on prepare-and-measure (P&M) protocols, although our results are equally applicable to measurement-device-independent scenarios [14]. A general P&M protocol can be described as follows: (1) Alice makes a probabilistic selection of setting choices (such as bit and basis choices) and then sends, through a quantum channel, a sequence of quantum states on systems $S_1,\ldots,S_N =: \boldsymbol{S}$; (2) Eve performs the most general attack allowed by quantum mechanics, which, without loss of generality, can be described as the application of a unitary operator $U_{\boldsymbol{SE}}$ on $\boldsymbol{S}$ and on her ancillary system $\boldsymbol{E}$, and resends the output systems $\boldsymbol{B}$ to Bob; (3) Bob performs measurements on the received systems; (4) Alice and Bob apply post-processing (this is the classical phase of the protocol and it typically involves, e.g. basis announcements, sifting, error correction, error verification and privacy amplification) to obtain an $\epsilon_{\text{sec}}$-secure key pair, where

$$\frac{1}{2}\left|\left|\rho^{\text{final}}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal}}_{\boldsymbol{A'B'E'}}\right|\right|_1 \leqslant \epsilon_{\text{sec}}. \tag{1}$$

Here, $\rho^{\text{final}}_{\boldsymbol{A'B'E'}}$ is the final joint state of Alice, Bob and Eve at the end of the protocol, where $\boldsymbol{A'}$ and $\boldsymbol{B'}$ are Alice's and Bob's classical systems holding their respective keys $k_A$ and $k_B$, and $\boldsymbol{E'}$ is Eve's ancilliary output system after applying $U_{\boldsymbol{SE}}$. The state $\rho^{\text{ideal}}_{\boldsymbol{A'B'E'}}$ is their joint state in an ideal protocol in which Alice and Bob share an identical key that is completely random and uncorrelated with Eve's system. Intuitively, equation (1) means that if a protocol is $\epsilon_{\text{sec}}$-secure then the probability that Eve has any information about the key and/or that Alice's and Bob's keys are not identical is at most $\epsilon_{\text{sec}}$.

The objective of a security analysis is proving equation (1). To achieve this, it is often useful to assume an equivalent scenario (typically called a source-replacement scheme) in which Alice generates a global entangled state $|\Psi\rangle_{\boldsymbol{AS}}$ and then performs measurements on the ancillary systems $\boldsymbol{A} := A_1,\ldots,A_N$ to learn her setting choices. Also, it is helpful to consider that Alice delays her measurements until after Eve's attack. In this case, we have the following modified steps: $(1')$ Alice prepares $|\Psi\rangle_{\boldsymbol{AS}}$ and sends systems $\boldsymbol{S}$ through the quantum channel while keeping systems $\boldsymbol{A}$ in her lab; $(3')$ Alice and Bob perform measurements on their local systems $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively. We can denote Alice's and Bob's actions in steps $(3')$ and (4) as a trace-preserving completely positive (TPCP) map $\mathcal{E}_{\boldsymbol{AB}}$ such that $\mathcal{E}_{\boldsymbol{AB}}(\hat{P}[U_{\boldsymbol{SE}}|\Psi\rangle_{\boldsymbol{AS}}|0\rangle_{\boldsymbol{E}}]) = \rho^{\text{final}}_{\boldsymbol{A'B'E'}}$, where $\hat{P}[\cdot] = |\cdot\rangle\langle\cdot|$. And if we define a TPCP map $\mathcal{O}_{\epsilon_{\text{sec}}}$ that also includes Eve's action in step (2), then we have that $\rho^{\text{final}}_{\boldsymbol{A'B'E'}} = \mathcal{O}_{\epsilon_{\text{sec}}}\left(|\Psi\rangle\langle\Psi|_{\boldsymbol{AS}}\right)$. See figure 1 for a pictorial representation of this operation.

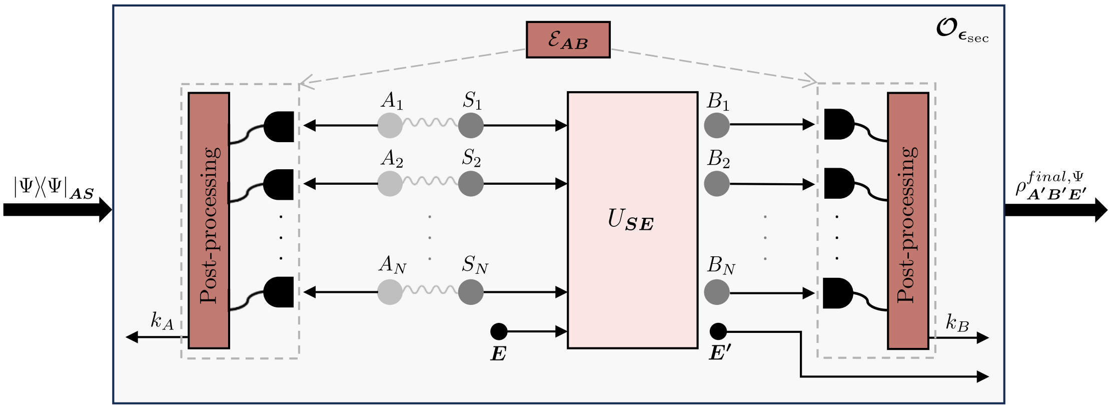

**Figure 1.** Pictorial description of the quantum operation $\mathcal{O}_{\epsilon_{\rm sec}}$, which contains Alice's, Bob's and Eve's operations on a QKD protocol with a source-replacement scheme. First, Alice prepares the entangled state $|\Psi\rangle_{AS}$ and sends systems $S = S_1, S_2, \ldots, S_N$ through the quantum channel while keeping systems $A = A_1, A_2, \ldots, A_N$ in her lab. Note that we only explicitly depict three rounds of the protocol, namely the 1st, 2nd and $N$th rounds, and the rest are represented by the vertical ellipses. After that, Eve performs a coherent attack, which can be described by a unitary operator $U_{SE}$ acting on $S$ and Eve's ancilla system $E$, and resends the output systems $B = B_1, B_2, \ldots, B_N$ to Bob. Then, Alice and Bob perform the operation $\mathcal{E}_{AB}$, that is, they measure their respective systems and apply post-processing to obtain an $\epsilon_{\rm sec}$-secure key pair $k_A, k_B$. The final joint state at the end of the protocol, or in other words, after applying the quantum operation $\mathcal{O}_{\epsilon_{\rm sec}}$, is $\rho^{\rm final,\Psi}_{A'B'E'}$.

## 3. Main result

In QKD protocols, the security of the final key pair depends on the precise characteristics of the quantum states prepared by Alice. While theoretical security proofs often assume idealized conditions, practical implementations may deviate slightly from these assumptions. Consider a scenario where we have a security proof for a QKD protocol under slightly idealized conditions for Alice's state preparation, which, as explained in the previous section, can be mathematically represented by the generation of a global entangled state $|\Psi\rangle_{AS}$. In reality, Alice's state preparation may differ from this idealized scenario, and we can represent the actual scenario by considering a different global entangled state $|\Phi\rangle_{AS}$ that is close to, but not identical to, $|\Psi\rangle_{AS}$. Our Theorem, presented below, quantifies the impact of this deviation on the security of the protocol by using two main tools: the triangle inequality and the non-increasing property of the trace distance under quantum operations. In particular, it shows that if we can bound the trace distance between $|\Psi\rangle_{AS}$ and $|\Phi\rangle_{AS}$ by some value $d$, we can extend the original security proof for the idealized scenario to the actual scenario by simply increasing the security parameter of the final key by $2d$. Crucially, it allows us to do so without affecting the protocol's performance or introducing any additional assumptions. The extended proof maintains the same expected secret-key generation rate and inherits all the properties of the original proof, including its assumptions, the type of source considered (e.g. single-photon or coherent-light), its ability to handle side channels (if applicable), and its compatibility with techniques like the decoy-state method (if applicable). Finally, we remark that to apply our proof and determine $d$ it is necessary certain experimental characterization (see section 4 for more details).

**Theorem.** *If a QKD protocol whose prepared entangled state is $|\Psi\rangle_{AS}$ has been proven to be $\epsilon_{sec}$-secure, then the same protocol but whose prepared entangled state is instead $|\Phi\rangle_{AS}$ is $(\epsilon_{sec} + 2d)$-secure, where d denotes the trace distance between $|\Psi\rangle_{AS}$ and $|\Phi\rangle_{AS}$.*

*Proof.* The goal is to upper bound $\frac{1}{2}\left|\left|\rho^{\rm final,\Phi}_{A'B'E'} - \rho^{\rm ideal,\Phi}_{A'B'E'}\right|\right|_1$, which is the trace distance between the final state in the actual scenario and in a fictitious scenario in which the users share an ideal key (see discussion after equation (1)). Here, the superscript $\Phi$ indicates the prepared entangled state,

$$\rho^{\rm final,\Phi}_{A'B'E'} = \sum_{K\geqslant 0} p_\Phi\left(K\right) \sum_{k_A,k_B=0}^{2^K-1} p_\Phi\left(k_A,k_B|K\right) |k_A,k_B\rangle\langle k_A,k_B|_{A'B'} \otimes \rho^{\rm final,\Phi}_{E'|K}\left(k_A,k_B\right) =: \sum_{K\geqslant 0} p_\Phi\left(K\right) \rho^{\rm final,\Phi}_{A'B'E'|K}, \tag{2}$$

and

$$\rho^{\rm ideal,\Phi}_{A'B'E'} = \sum_{K\geqslant 0} p_\Phi\left(K\right) \frac{1}{2^K} \sum_{k=0}^{2^K-1} |k,k\rangle\langle k,k|_{A'B'} \otimes {\rm Tr}_{A'B'}\left[\rho^{\rm final,\Phi}_{A'B'E'|K}\right]. \tag{3}$$

Also, $p_\Phi(K)$ is the probability distribution of obtaining a final key of length $K$ and $p_\Phi(k_A, k_B|K)$ is the probability that Alice and Bob get the keys $k_A$ and $k_B$ given $K$. Note that in equations (2) and (3), the information about the length of $K$ is implicitly included in systems $\boldsymbol{A'B'}$, and that we are assuming a variable $K$ with $K = 0$ corresponding to the case in which the protocol aborts.

To achieve our goal, we introduce the analogous states $\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}$ and $\rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}}$, that are defined by simply replacing $\Phi$ with $\Psi$ in equations (2) and (3), respectively. Note that $\rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}$ and $\rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}}$ are not equal because the reduced state on Eve's system $\boldsymbol{E'}$ depends on whether Alice prepares $|\Phi\rangle_{\boldsymbol{AS}}$ or $|\Psi\rangle_{\boldsymbol{AS}}$. Then, by using the triangle inequality consecutively we have that

$$\begin{aligned}\frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}||_1 &\leqslant \frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}||_1 + \frac{1}{2}||\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}||_1 \\ &\leqslant \frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}||_1 + \frac{1}{2}||\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}}||_1 + \frac{1}{2}||\rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}||_1.\end{aligned} \tag{4}$$

Next, we bound each term in the last inequality of equation (4) separately, where we will use the non-increasing property of the trace distance under quantum operations:

**1st term:** as discussed in section 2, when Alice prepares the entangled state $|\Psi\rangle_{\boldsymbol{AS}}$, the joint state of Alice, Bob and Eve at the end of the protocol can be expressed as

$$\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}} = \mathcal{O}_{\epsilon_{\text{sec}}}\left(|\Psi\rangle\langle\Psi|_{\boldsymbol{AS}}\right). \tag{5}$$

Note that this protocol is $\epsilon_{\text{sec}}$-secure for *any* fixed unitary operator $U_{\boldsymbol{SE}}$, since the existing security proof did not impose any restrictions on Eve's operation, and therefore, $U_{\boldsymbol{SE}}$ can be the operator that would have been the most advantageous to Eve if Alice had prepared the state $|\Phi\rangle_{\boldsymbol{AS}}$ instead. If we now substitute the prepared entangled state $|\Psi\rangle_{\boldsymbol{AS}}$ by $|\Phi\rangle_{\boldsymbol{AS}}$, their final joint state is instead

$$\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} = \mathcal{O}_{\epsilon_{\text{sec}}}\left(|\Phi\rangle\langle\Phi|_{\boldsymbol{AS}}\right). \tag{6}$$

Then, by substituting equations (5) and (6) in the first term of equation (4), we have that

$$\frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}||_1 = T\left(\mathcal{O}_{\epsilon_{\text{sec}}}\left(|\Phi\rangle\langle\Phi|_{\boldsymbol{AS}}\right), \mathcal{O}_{\epsilon_{\text{sec}}}\left(|\Psi\rangle\langle\Psi|_{\boldsymbol{AS}}\right)\right) \leqslant T\left(|\Phi\rangle\langle\Phi|_{\boldsymbol{AS}}, |\Psi\rangle\langle\Psi|_{\boldsymbol{AS}}\right) =: d, \tag{7}$$

where we have used the fact that the trace distance $T(|\cdot\rangle\langle\cdot|, |\cdot\rangle\langle\cdot|)$ is non-increasing by quantum operations.

**2nd term:** since the QKD protocol is assumed to be $\epsilon_{\text{sec}}$-secure when Alice prepares the entangled state $|\Psi\rangle_{\boldsymbol{AS}}$, by definition, the second term in equation (4) is bounded by $\epsilon_{\text{sec}}$ (see equation (1)).

**3rd term:** the ideal states $\rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}$ and $\rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}}$ can be directly obtained from their respective actual states $\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}}$ and $\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}$ by simply replacing the actual keys $k_A$ and $k_B$ with the ideal key pair. By defining this TPCP map as $\Gamma$ (see appendix A for more details), we have that the third term in equation (4) becomes

$$\frac{1}{2}||\rho^{\text{ideal},\Psi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}||_1 = \frac{1}{2}||\Gamma\left(\rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}\right) - \Gamma\left(\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}}\right)||_1 \leqslant \frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{final},\Psi}_{\boldsymbol{A'B'E'}}||_1 \leqslant d, \tag{8}$$

where in the last inequality we have used equation (7).

Finally, by substituting equations (7) and (8) into equation (4) and using the fact that the protocol in which Alice prepares $|\Psi\rangle_{\boldsymbol{AS}}$ is $\epsilon_{\text{sec}}$-secure by definition, we obtain the following bound

$$\frac{1}{2}||\rho^{\text{final},\Phi}_{\boldsymbol{A'B'E'}} - \rho^{\text{ideal},\Phi}_{\boldsymbol{A'B'E'}}||_1 \leqslant \epsilon_{\text{sec}} + 2d, \tag{9}$$

as required.

## 4. Application of the theorem to unbounded pulse correlations

In this section, we show how our Theorem can be applied to extend a security proof addressing finite-length correlations to incorporate correlations of unbounded length. For concreteness, we focus on bit-and-basis correlations, which have been addressed by the security proofs in [6–9] for the finite-length scenario. In particular, let us consider a practical scenario in which Alice employs an imperfect source that introduces bit and basis correlations between the emitted pulses. In this case, the state of the $k$th pulse depends not only on

Alice's $k$th setting choice $j_k$, but also on her previous setting choices $j_{k-1}, j_{k-2}, \ldots, j_1$. We can quantify the strength of the correlation between pulses separated by $l$ rounds, denoted by $\epsilon_l$, by considering the maximum variation that the state on the $k$th round can undergo when the $(k-l)$th setting choice is altered, that is,

$$\left| \langle \psi_{j_k|j_{k-1},\ldots,j_{k-l+1},\tilde{j}_{k-l},j_{k-l-1},\ldots,j_1} | \psi_{j_k|j_{k-1},\ldots,j_{k-l+1},j_{k-l},j_{k-l-1},\ldots,j_1} \rangle \right|^2 \geqslant 1 - \epsilon_l. \tag{10}$$

The existing security proofs addressing this imperfection [6–9] require the assumption that a bound on $\epsilon_l$ is known and that the correlations have a finite length, i.e. that there is a certain length $l_c$ such that $\epsilon_l = 0$ for all $l > l_c$. The latter condition is needed because these proofs divide the protocol rounds in $l_c + 1$ groups and prove the security of each group separately, which can only be done if $l_c$ is bounded. Unfortunately, however, while it seems natural that the strength of the correlations should decrease rapidly as the pulse separation $l$ increases, it is unreasonable to assume that it will decrease to exactly zero at any point.

That being said, there must exist a certain pulse separation $l$ after which the strength of the correlations is so small that it is essentially negligible. Let us denote this value of $l$ as the effective maximum correlation length $l_e$. Using the Theorem in the previous section, we can make this intuition explicit. First of all, we define the following source replacement scheme for the protocol:

$$|\Psi_\infty\rangle_{\boldsymbol{AS}} = \sum_{j_1} \sqrt{p_{j_1}} \mathrm{e}^{\mathrm{i}\theta_{j_1}} |j_1\rangle_{A_1} |\psi_{j_1}\rangle_{S_1} \sum_{j_2} \sqrt{p_{j_2}} \mathrm{e}^{\mathrm{i}\theta_{j_1,j_2}} |j_2\rangle_{A_2} |\psi_{j_2|j_1}\rangle_{S_2} \cdots \sum_{j_N} \sqrt{p_{j_N}} \mathrm{e}^{\mathrm{i}\theta_{j_1,\ldots,j_N}} |j_N\rangle_{A_N} |\psi_{j_N|j_{N-1},\ldots,j_1}\rangle_{S_N}, \tag{11}$$

where $\{|j_k\rangle_{A_k}\}_{j_k}$ is an orthonormal basis for the system $A_k$ and the terms $\mathrm{e}^{\mathrm{i}\theta_{j_1,\ldots,j_k}}$ are complex phases that have no effect on Alice's measurements on systems $\boldsymbol{A}$. The motivation to include these phases will be understood soon. Also, we introduce the following state

$$|\Psi_{l_e}\rangle_{\boldsymbol{AS}} = \sum_{j_1} \sqrt{p_{j_1}} |j_1\rangle_{A_1} |\psi_{j_1}\rangle_{S_1} \sum_{j_2} \sqrt{p_{j_2}} |j_2\rangle_{A_2} |\psi_{j_2|j_1}\rangle_{S_2} \cdots \sum_{j_N} \sqrt{p_{j_N}} |j_N\rangle_{A_N} |\psi_{j_N|j_{N-1},\ldots,j_{N-l_e}}\rangle_{S_N}, \tag{12}$$

where we have defined

$$|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}\rangle_{S_k} := |\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\rangle_{S_k}, \tag{13}$$

with $j,j,j,\ldots,j$ being any fixed sequence of setting choices for all rounds before the round $k - l_e$. Equation (12) represents a source replacement scheme for a fictitious scenario in which the correlations of Alice's source have a maximum bounded length of $l_e$. By applying the analyses in [6–9], one can obtain a security proof for this fictitious scenario that results in an $\epsilon_{\mathrm{sec}}$-secure key. Then, provided that one can obtain the bound

$$T\left(|\Psi_\infty\rangle\langle\Psi_\infty|_{\boldsymbol{AS}}, |\Psi_{l_e}\rangle\langle\Psi_{l_e}|_{\boldsymbol{AS}}\right) \leqslant d, \tag{14}$$

our Theorem ensures that, if we apply this security proof to the actual protocol, the final key is guaranteed to be $(\epsilon_{\mathrm{sec}} + 2d)$-secure. In what follows, we first show how to bound this trace distance and then explain how to use this result in practice.

### 4.1. Bounding the trace distance

**Proposition.** *The trace distance between* $|\Psi_\infty\rangle_{\boldsymbol{AS}}$ *and* $|\Psi_{l_e}\rangle_{\boldsymbol{AS}}$ *is bounded by*

$$T\left(|\Psi_\infty\rangle\langle\Psi_\infty|_{\boldsymbol{AS}}, |\Psi_{l_e}\rangle\langle\Psi_{l_e}|_{\boldsymbol{AS}}\right) \leqslant \sqrt{N\delta_{l_e}} =: d, \tag{15}$$

*where* $N$ *is the number of emitted signals and* $\sqrt{\delta_{l_e}} = \sum_{l=l_e+1}^{N} \sqrt{\epsilon_l}$.

*Proof.* For pure states, the trace distance can be expressed exactly in terms of their inner product as

$$T\left(|\Psi_\infty\rangle\langle\Psi_\infty|_{\boldsymbol{AS}}, |\Psi_{l_e}\rangle\langle\Psi_{l_e}|_{\boldsymbol{AS}}\right) = \sqrt{1 - |\langle\Psi_{l_e}|\Psi_\infty\rangle_{\boldsymbol{AS}}|^2}. \tag{16}$$

Therefore, a bound on the trace distance between $|\Psi_\infty\rangle_{\boldsymbol{AS}}$ and $|\Psi_{l_e}\rangle_{\boldsymbol{AS}}$ can be derived by bounding $|\langle\Psi_{l_e}|\Psi_\infty\rangle_{\boldsymbol{AS}}|$. Using equations (12) and (11), we have that

$$
\begin{aligned}
|\langle\Psi_{l_e}|\Psi_\infty\rangle_{\boldsymbol{AS}}| &= \left|\sum_{j_1} p_{j_1}\mathrm{e}^{\mathrm{i}\theta_{j_1}}\,\langle\psi_{j_1}|\psi_{j_1}\rangle_{S_1}\dots\sum_{j_N} p_{j_N}\mathrm{e}^{\mathrm{i}\theta_{j_1,\dots,j_N}}\,\langle\psi_{j_N|j_{N-1},\dots,j_{N-l_e}}|\psi_{j_N|j_{N-1},\dots,j_1}\rangle_{S_N}\right| \\
&= \left|\sum_{j_1} p_{j_1}|\langle\psi_{j_1}|\psi_{j_1}\rangle_{S_1}|\dots\sum_{j_N} p_{j_N}|\langle\psi_{j_N|j_{N-1},\dots,j_{N-l_e}}|\psi_{j_N|j_{N-1},\dots,j_1}\rangle_{S_N}|\right| \\
&= \sum_{j_1,\dots,j_N} p_{j_1}\dots p_{j_N}|\langle\psi_{j_1}|\psi_{j_1}\rangle_{S_1}|\dots|\langle\psi_{j_N|j_{N-1},\dots,j_{N-l_e}}|\psi_{j_N|j_{N-1},\dots,j_1}\rangle_{S_N}| \\
&= \sum_{j_1,\dots,j_N} p_{j_1}\dots p_{j_N}\prod_{k=l_e+2}^{N}|\langle\psi_{j_k|j_{k-1},\dots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\dots,j_1}\rangle_{S_k}|,
\end{aligned}
\tag{17}
$$

where, without loss of generality, we have exploited the freedom to introduce and choose the phases in equation (11) such that all inner products are real and positive, i.e. $\theta_{j_1,\dots,j_k} = -\arg(\langle\psi_{j_k|j_{k-1},\dots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\dots,j_1}\rangle_{S_k})$. Also, in the first equality of equation (17) we have used $\langle j_k|j_k'\rangle_{A_k} = \delta_{j_k,j_k'}$ and in the last equality we have used the fact that the first $l_e+1$ inner products equal one.

Now, the terms $|\langle\psi_{j_k|j_{k-1},\dots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\dots,j_1}\rangle_{S_k}|$ in equation (17) can be bounded using equation (10) and the relationship between trace distance and fidelity. In appendix B, we show that

$$
|\langle\psi_{j_k|j_{k-1},\dots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\dots,j_1}\rangle_{S_k}| \geqslant \sqrt{1-\delta_{l_e}},
\tag{18}
$$

where $\sqrt{\delta_{l_e}} = \sum_{l=l_e+1}^{N}\sqrt{\epsilon_l}$. Then, substituting equation (18) in equation (17), we obtain

$$
|\langle\Psi_{l_e}|\Psi_\infty\rangle_{\boldsymbol{AS}}| \geqslant \sum_{j_1,\dots,j_N} p_{j_1}\dots p_{j_N}\prod_{k=l_e+2}^{N}\sqrt{1-\delta_{l_e}} = \prod_{k=l_e+2}^{N}\sqrt{1-\delta_{l_e}} = (1-\delta_{l_e})^{\frac{N-l_e-2}{2}},
\tag{19}
$$

since the probabilities sum to one. Finally, by substituting equation (19) in equation (16) and using Bernoulli's inequality, we find that

$$
T\left(|\Psi_\infty\rangle\langle\Psi_\infty|_{\boldsymbol{AS}}, |\Psi_{l_e}\rangle\langle\Psi_{l_e}|_{\boldsymbol{AS}}\right) \leqslant \sqrt{(N-l_e-2)\,\delta_{l_e}} \leqslant \sqrt{N\delta_{l_e}} =: d,
\tag{20}
$$

as required.

### 4.2. Specific pulse correlations model

As a particular example to illustrate the application of our formalism, we consider a model in which the correlation strength $\epsilon_l$ decreases exponentially[5] with the correlation length $l$. Specifically, we assume that

$$
\epsilon_l = \epsilon_1\mathrm{e}^{-C(l-1)},
\tag{21}
$$

where $\epsilon_1$ represents the magnitude of nearest-neighbor pulse correlations, and $C$ is a constant determining the rate at which the correlation strength decays as the separation between pulses increases. We remark, however, that our formalism can be applied to any decay model, and that our derivations below could be adapted accordingly.

The first step to apply the Theorem is determining $\delta_{l_e}$. Using equation (21), we have that $\sqrt{\delta_{l_e}}$ can be expressed as

$$
\sqrt{\delta_{l_e}} = \sum_{l=l_e+1}^{N}\sqrt{\epsilon_l} \leqslant \sum_{l=l_e+1}^{\infty}\sqrt{\epsilon_l} = \sum_{l=l_e+1}^{\infty}\sqrt{\epsilon_1\mathrm{e}^{-C(l-1)}} = \frac{\sqrt{\epsilon_1\mathrm{e}^{-Cl_e}}}{1-\sqrt{\mathrm{e}^{-C}}},
\tag{22}
$$

where we have substituted equation (21) in equation (B5). Note that, in equation (22), we have upper bounded $\sum_{l=l_e+1}^{N}\sqrt{\epsilon_l}$ by an infinite sum, since for an exponential decay model this sum converges and results in a simpler expression. For decay models in which this infinite sum does not converge, one could

[5] In an independent research project [15] aimed at investigating pulse correlations in QKD modulation devices, some of our co-authors have obtained preliminary evidence suggesting that the limited bandwidth of modulation devices is a primary cause of pulse correlations, and that the magnitude of these correlations can indeed be bounded by a function that decays exponentially as the pulse separation increases, which aligns with our model in equation (21). Interestingly, recent work has shown that these bandwidth limitations also introduce an encoding side channel [16], underscoring the importance of addressing the security vulnerabilities introduced by this imperfection.

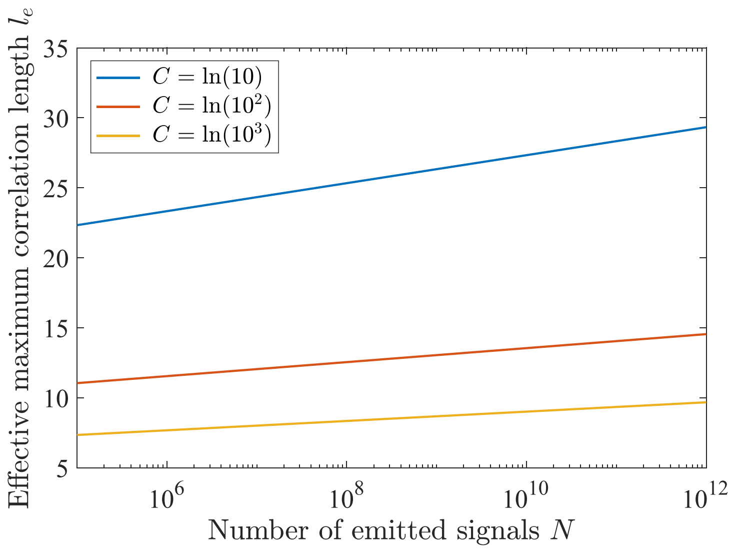

**Figure 2.** Value of the effective maximum correlation length $l_e$ that one should set to achieve $d = 10^{-10}$ [17] as a function of the number of emitted signals $N$. For the simulations, we have assumed that $\epsilon_1 = 10^{-3}$ [5].

simply evaluate the finite sum to obtain $\sqrt{\delta_{l_e}}$. Then, by substituting equation (22) in equation (20), $d$ can be re-defined as

$$d = \frac{\sqrt{N\epsilon_1 \mathrm{e}^{-Cl_e}}}{1 - \sqrt{\mathrm{e}^{-C}}}. \tag{23}$$

To have a good security guarantee, we want that $d$ is of the same order of magnitude as $\epsilon_{\mathrm{sec}}$. To achieve this for a particular value of $N$, we need to appropriately choose the effective maximum correlation length $l_e$, which our security proof is based on. For this, it is useful to express $l_e$ as a function of $d$ and $N$ as

$$l_e = \frac{1}{C} \ln\left(\frac{N\epsilon_1}{d^2\left(1 - \sqrt{\mathrm{e}^{-C}}\right)^2}\right). \tag{24}$$

Therefore, in practice, to prove the security of a QKD protocol with a fixed $N$ whose pulses are all correlated one should do the following: (1) infer from a source-characterisation experiment the value of the parameters $\epsilon_l$ (if they follow the expression given by equation (21), this reduces to determining the parameters $C$ and $\epsilon_1$); (2) decide the desired value of $d$ and calculate the effective maximum correlation length $l_e$ (in the case of an exponential decrease, this can be done using equation (24)); (3) apply one of the security analyses in [6–9] assuming that the true maximum correlation length $l_c$ equals $l_e$; and (4) increase the security parameter $\epsilon_{\mathrm{sec}}$ claimed by the applied analysis by $2d$.

As a particular example, in figure 2, we plot the required value of $l_e$ as a function of $N$ using equation (24). Since to the best of our knowledge there are no experimental works quantifying $C$, in our simulations we consider a range of values for this parameter. Moreover, we assume that $\epsilon_1 = 10^{-3}$ [5], and given that $10^{-10}$ is a typical value for $\epsilon_{\mathrm{sec}}$ [17], we assume that $d = 10^{-10}$.

The results in figure 2 show that as $N$ increases, $l_e$ also increases. This is expected because a larger $N$ means that potentially more pulses could be correlated with one another, and therefore one would need to set a higher $l_e$ to achieve the same level of security. While increasing $N$ is known to reduce finite key effects, our work shows that it also leads to a higher $l_e$, thereby presenting a compromise due to the additional time required for post-processing. Moreover, in figure 2, one can see that the parameter $C$, which quantifies how fast the magnitude of the correlations drops with distance, has a high impact on the required $l_e$. Again, this is expected because if $C$ drops very fast then the correlations between far-away pulses will be very faint, allowing us to achieve the desired level of security with a smaller value of $l_e$.

## 5. Discussion and conclusion

QKD implementations often suffer from correlations among the emitted signals. Recent works have addressed this imperfection [6–13], but only under the assumption that the correlations have a bounded length. Since this is not expected to be met in practice, these analyses cannot guarantee the security of practical QKD systems. In this work, we have solved this critical vulnerability by providing a general framework to prove the security of QKD in real-life scenarios in which the length of the correlations may be unbounded.

Our approach involves the consideration of an effective maximum correlation length $l_e$, which should be chosen such that the magnitude of the residual correlations between pulses separated by more than $l_e$ rounds is so small as to be almost negligible. Here, by 'almost negligible', we mean that the global entangled state prepared in the actual protocol cannot be distinguished from the global entangled state that would have been prepared in a protocol for which the magnitude of these residual correlations is exactly zero, except with a tiny failure probability $d$. More specifically, we have shown that, under this condition, one can simply apply the existing security proofs [6–11, 13] as if the true maximum correlation length was indeed $l_e$, and then account for the residual correlations beyond this limit by simply increasing the security parameter of the final key by $2d$. Importantly, our formalism can extend these security proofs to incorporate unbounded correlations while requiring no additional assumptions beyond those made in the original security proofs, and without affecting the expected secret-key generation rate.

To show how one can apply our formalism, we have focused on the scenario in which the emitted signals suffer from bit and basis correlations, which was considered in [6–9]. For this, we have assumed that the magnitude of the correlations decreases exponentially with their length, and used it to determine the appropriate value of $l_e$ as a function of the total number of transmitted rounds $N$, the desired failure probability $d$, and the exponential decay constants. We remark, however, that our framework can also be applied to extend existing security proofs addressing intensity correlations [10, 11] and phase-randomisation correlations [13] to the case in which these correlations have an unbounded length. Moreover, it could readily incorporate other small imperfections into existing security proofs, such as quantum correlations[6] and discrete phase randomisation [18, 19]. Therefore, our work not only solves a crucial problem but also constitutes an important step towards securing QKD implementations in practical scenarios.

## Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

## Acknowledgments

We thank Ainhoa Agulleiro, Fadri Grünenfelder, Ana Blázquez and Xoel Sixto for valuable discussions. This work was supported by Cisco Systems Inc. the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through the Grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the 'Planes Complementarios de I+D+I con las Comunidades Autónomas' in Quantum Communication, the European Union's Horizon Europe Framework Programme under the Marie Sklodowska-Curie Grant No. 101072637 (Project QSI) and the project 'Quantum Security Networks Partnership' (QSNP, Grant Agreement No. 101114043). M P and G C-L acknowledge support from JSPS Postdoctoral Fellowships for Research in Japan. A M is partially supported by JSPS KAKENHI Grant Number JP24K16977. K T acknowledges support from JSPS KAKENHI Grant Number 23H01096.

[6] In section 4, we have focused on *classical* pulse correlations, where the classical setting choices in one round influence the quantum states emitted in subsequent rounds. In principle, *quantum* correlations—where emitted pulses are entangled across rounds—are also possible. Although the magnitude of such quantum correlations would be expected to be minimal due to the fragility of entanglement, their mere presence could invalidate the assumptions of existing security proofs. However, the formalism introduced in section 3 also offers a solution to this problem. That is, we can apply our Theorem by defining $|\Phi\rangle_{AS}$ as the source-replacement scheme for the actual scenario with quantum correlations, and $|\Psi\rangle_{AS}$ as the scheme for an idealized scenario without such correlations. This allows us to extend existing security proofs to incorporate sources suffering from a small amount of quantum correlations by simply increasing the security parameter, without altering the protocol's performance or introducing additional assumptions.

## Author contributions

K T conceptualised the work. M P, G C-L, K T and A M developed the main result with contributions from M C. M P performed the simulations. D R provided the correlations model. M P wrote most of the manuscript, with inputs from G C-L and A M, and all authors contributed towards improving it.

## Appendix A. Constructing Γ

The construction of Γ is as follows. First note that the final state can be expressed as

$$\begin{aligned}\rho^{\text{final}}_{\boldsymbol{A'B'E'}} &= \sum_{K\geqslant 0} p(K) \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,|k_A,k_B\rangle\langle k_A,k_B|_{\boldsymbol{A'B'}}\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B)\\ &= \mathrm{Tr}_K \sum_{K\geqslant 0} p(K)\,|K\rangle\langle K|_K \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,|k_A,k_B\rangle\langle k_A,k_B|_{\boldsymbol{A'B'}}\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B)\,. \end{aligned} \tag{A1}$$

Then, by taking the trace over $\boldsymbol{A'B'}$ we obtain

$$\mathrm{Tr}_K \sum_{K\geqslant 0} p(K)\,|K\rangle\langle K|_K \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B)\,, \tag{A2}$$

and after adding the state $|0\rangle_{\boldsymbol{A'B'}}$ we arrive to

$$\mathrm{Tr}_K \sum_{K\geqslant 0} p(K)\,|K\rangle\langle K|_K\,|0\rangle\langle 0|_{\boldsymbol{A'B'}} \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B)\,. \tag{A3}$$

Finally, we swap the state of $\boldsymbol{A'B'}$ with the ideal key state $\tau_K := 1/2^K \sum_{k=0}^{2^K-1} |k,k\rangle\langle k,k|_{\boldsymbol{A'B'}}$ by controlling system $K$, leading to

$$\begin{aligned}&\mathrm{Tr}_K \sum_{K\geqslant 0} p(K)\,|K\rangle\langle K|_K\,\tau_K \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B)\\ &\quad= \sum_{K\geqslant 0} p(K)\,\frac{1}{2^K}\sum_{k=0}^{2^K-1} |k,k\rangle\langle k,k|_{\boldsymbol{A'B'}} \sum_{k_A,k_B=0}^{2^K-1} p(k_A,k_B|K)\,\rho^{\text{final}}_{\mathbf{E'}|K}(k_A,k_B) = \rho^{\text{ideal}}_{\boldsymbol{A'B'E'}}\,. \end{aligned} \tag{A4}$$

The transformation from equations (A1) to (A4), which we call Γ, is a TPCP map that takes the actual state $\rho^{\text{final}}_{\boldsymbol{A'B'E'}}$ into its respective ideal state $\rho^{\text{ideal}}_{\boldsymbol{A'B'E'}}$.

## Appendix B. Bounding $|\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\ldots,j_1}\rangle_{S_k}|$

In this appendix, we derive a bound on the inner product $|\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}|\psi_{j_k|j_{k-1},\ldots,j_1}\rangle_{S_k}|$ in equation (17). Note that, using the definition of $|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}\rangle_{S_k}$ in equation (13), we have that

$$\left|\left\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}\middle|\psi_{j_k|j_{k-1},\ldots,j_1}\right\rangle_{S_k}\right| = \left|\left\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\middle|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right|, \tag{B1}$$

which corresponds to the fidelity between two hypothetical states emitted in the $k$th round that differ in *all* setting choices from the first to the $(k-l_e-1)$th one. Now, to bound equation (B1), we use our knowledge of the fidelity between the states when changing only *one* setting choice at a time, i.e. equation (10). To relate these two quantities, we will first convert this fidelity to trace distance, then use the trace distance triangle inequality consecutively, and finally convert back to fidelity.

First, using the relationship between trace distance and fidelity, we have that

$$\begin{aligned}&\left|\left\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\middle|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right|\\ &\quad= \sqrt{1-T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)^2}\,. \end{aligned} \tag{B2}$$

Then, we bound the trace distance term in equation (B2) as

$$\begin{aligned}
&T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)\\
&\quad\leqslant T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right)\right)\\
&\qquad+T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)\\
&\quad\leqslant T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right)\right)\\
&\qquad+T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j,\ldots,j}\right\rangle_{S_k}\right)\right)\\
&\qquad+T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)\\
&\quad\leqslant T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right)\right)\\
&\qquad+T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j,\ldots,j}\right\rangle_{S_k}\right)\right)\\
&\qquad+T\left(\hat{P}(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j,\ldots,j}\right\rangle_{S_k}),\hat{P}(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j}\right\rangle_{S_k})\right)+\ldots\\
&\qquad+T\left(\hat{P}(\left|\psi_{j_k|j_{k-1},\ldots,j}\right\rangle_{S_k}),\hat{P}(\left|\psi_{j_k|j_{k-1},\ldots,j_1}\right\rangle_{S_k})\right),
\end{aligned}\tag{B3}$$

where we have applied the triangle inequality consecutively. Note that, in the RHS of equation (B3), we have a sum of $k-l_e-1$ trace distance terms, each involving two states that differ in exactly one setting choice. The first term differs in the $(k-l_e-1)$th setting choice, the second term differs in the $(k-l_e-2)$th setting choice, and so on. Applying again the relationship between the trace distance and fidelity for each of these terms, we obtain

$$\begin{aligned}
&T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)\\
&\leqslant\sqrt{1-\left|\left\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\middle|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j,j,\ldots,j}\right\rangle_{S_k}\right|^2}+\ldots+\sqrt{1-\left|\left\langle\psi_{j_k|j_{k-1},\ldots,j}\middle|\psi_{j_k|j_{k-1},\ldots,j_1}\right\rangle_{S_k}\right|^2}.
\end{aligned}\tag{B4}$$

Note that using equation (10) we can upper bound each of the terms on the RHS of equation (B4) such that

$$\begin{aligned}
&T\left(\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j,j,j,\ldots,j}\right\rangle_{S_k}\right),\hat{P}\left(\left|\psi_{j_k|j_{k-1},\ldots,j_{k-l_e},j_{k-l_e-1},j_{k-l_e-2},j_{k-l_e-3},\ldots,j_1}\right\rangle_{S_k}\right)\right)\\
&\leqslant\sqrt{\epsilon_{l_e+1}}+\ldots+\sqrt{\epsilon_{l_e+k-1}}=\sum_{n=1}^{k-1}\sqrt{\epsilon_{l_e+n}}\leqslant\sum_{n=1}^{N-l_e}\sqrt{\epsilon_{l_e+n}}=\sum_{l=l_e+1}^{N}\sqrt{\epsilon_l}=:\sqrt{\delta_{l_e}}.
\end{aligned}\tag{B5}$$

Substituting equation (B5) into equation (B2), we finally arrive at

$$\left|\left\langle\psi_{j_k|j_{k-1},\ldots,j_{k-l_e}}\middle|\psi_{j_k|j_{k-1},\ldots,j_1}\right\rangle_{S_k}\right|\geqslant\sqrt{1-\delta_{l_e}}.\tag{B6}$$

## ORCID iDs

Margarida Pereira https://orcid.org/0000-0002-7429-6292
Guillermo Currás-Lorenzo https://orcid.org/0000-0003-2096-0036
Akihiro Mizutani https://orcid.org/0009-0008-5161-253X
Davide Rusca https://orcid.org/0000-0002-3319-6893
Marcos Curty https://orcid.org/0000-0002-0330-6828
Kiyoshi Tamaki https://orcid.org/0000-0002-6446-5769

## References

[1] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[2] Pirandola S *et al* 2020 Advances in quantum cryptography *Adv. Opt. Photon.* **12** 1012
[3] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution *Nat. Photon.* **8** 595
[4] Zapatero V, Navarrete A and Curty M 2023 Implementation security in quantum key distribution *Adv. Quantum Technol.* **7** 2300380
[5] Grünenfelder F, Boaron A, Rusca D, Martin A and Zbinden H 2020 Performance and security of 5 GHz repetition rate polarization-based quantum key distribution *Appl. Phys. Lett.* **117** 144003
[6] Pereira M, Kato G, Mizutani A, Curty M and Tamaki K 2020 Quantum key distribution with correlated sources *Sci. Adv.* **6** eaaz4487

[7] Mizutani A and Kato G 2021 Security of round-robin differential-phase-shift quantum-key-distribution protocol with correlated light sources *Phys. Rev.* A **104** 062611

[8] Pereira M, Currás-Lorenzo G, Navarrete A, Mizutani A, Kato G, Curty M and Tamaki K 2023 Modified BB84 quantum key distribution protocol robust to source imperfections *Phys. Rev. Res.* **5** 023065

[9] Currás-Lorenzo G, Pereira M, Kato G, Curty M and Tamaki K 2023 A security framework for quantum key distribution implementations (arXiv:2305.05930)

[10] Zapatero V, Navarrete A, Tamaki K and Curty M 2021 Security of quantum key distribution with intensity correlations *Quantum* **5** 602

[11] Sixto X, Zapatero V and Curty M 2022 Security of decoy-state quantum key distribution with correlated intensity fluctuations *Phys. Rev. Appl.* **18** 044069

[12] Yoshino K-i, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Takeoka M, Sasaki M, Tajima A, Koashi M and Tomita A 2018 Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses *npj Quantum Inf.* **4** 1

[13] Currás-Lorenzo G, Nahar S, Lütkenhaus N, Tamaki K and Curty M 2023 Security of quantum key distribution with imperfect phase randomisation *Quantum Sci. Technol.* **9** 015025

[14] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503

[15] Agulleiro A, Grünenfelder F, Pereira M, Currás-Lorenzo G, Zbinden H, Curty M and Rusca D 2024 Modelling and characterization of pulse correlations for quantum key distribution (in preparation)

[16] Gnanapandithan A, Qian L and Lo H-K 2024Security flaws from time-varying active encoding in high-speed measurement-device-independent quantum key distribution (arXiv: 2404.14216)

[17] Navarrete A and Curty M 2022 Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks *Quantum Sci. Technol.* **7** 035021

[18] Cao Z, Zhang Z, Lo H-K and Ma X 2015 Discrete-phase-randomized coherent state source and its application in quantum key distribution *New J. Phys.* **17** 053014

[19] Jin X-H, Yin Z-Q, Wang S, Chen W, Guo G-C and Han Z-F 2024 Finite Key Analysis for Discrete Phase Randomized BB84 Protocol *Quantum Inf. Process.* **23** 312