Security of differential phase shift QKD from relativistic principles

Martin Sandfuchs[1], Marcus Haberland[1,2], V. Vilasini[1], and Ramona Wolf[1]

[1]Institute for Theoretical Physics, ETH Zürich, Wolfgang-Pauli-Str. 27, 8093 Zürich, Switzerland
[2]Max Planck Institute for Gravitational Physics (Albert Einstein Institute), Am Mühlenberg 1, 14476 Potsdam, Germany

The design of quantum protocols for secure key generation poses many challenges: On the one hand, they need to be practical concerning experimental realisations. On the other hand, their theoretical description must be simple enough to allow for a security proof against all possible attacks. Often, these two requirements are in conflict with each other, and the differential phase shift (DPS) QKD protocol is an excellent example of this: It is designed to be implementable with current optical telecommunication technology, which, for this protocol, comes at the cost that many standard security proof techniques do not apply to it. In this work, we give the first full security proof of DPS QKD against general attacks, including finite-size effects. The proof combines techniques from quantum information theory, quantum optics, and relativity. We first give a security proof of a QKD protocol whose security stems from relativistic constraints. We then show that DPS QKD can be formulated as an instance of the relativistic protocol. In addition, we show that coherent attacks on the DPS protocol are, in fact, stronger than collective attacks.

1 Introduction

The art of encryption is as old as the concept of writing systems. For thousands of years, people have invented sophisticated cryptographic techniques to hide the content of messages for various purposes, such as secret communication between governments or militaries. However, a look back at history suggests that cryptography is caught in a vicious circle: Cryptanalysts have always been quick to find ways to break any supposedly secure encryption method, prompting cryptographers to invent even more sophisticated schemes to hide information, and so on. In today's society, secure communication is a highly relevant issue as a large amount of sensitive data is transmitted over the internet. Quantum key distribution (QKD) [BB84, Eke91] offers a possibility to break the vicious circle by providing information-theoretically secure encryption, which is based (almost) solely on the laws of physics. Nonetheless, caution is still advised in this case: even these protocols can only break the circle if they come with a complete security proof against all possible attacks.

While QKD, in principle, offers a way to achieve unbreakable encryption, it comes with a number of challenges, in particular when turning theoretical ideas into practical applications. A crucial issue in this transformation is that actual devices, such as quantum sources and measurements, rarely conform to their corresponding description in the theoretical protocol. For example, a typical information carrier in QKD protocols is single photons. However, perfect single photon sources and detectors do not exist in practice. Since the security proof only applies to the assumptions made in the protocol description, these deviations open up the possibility of side-channel attacks such as the photon number splitting (PNS) attack [BBB+92, BLMS00]. This attack exploits that in an implementation, information is typically encoded into weak coherent pulses instead of single

Martin Sandfuchs: martisan@phys.ethz.ch
Marcus Haberland: marcus.haberland@aei.mpg.de
V. Vilasini: vilasini@phys.ethz.ch
Ramona Wolf: rawolf@phys.ethz.ch

photons. These pulses have a small non-zero probability that more than one photon is emitted in one pulse, which allows the adversary to split off one of these photons without influencing the second one. Since this photon contains all information encoded in the pulse, the adversary can obtain information on the key without being detected.

A way to get around these kinds of problems is to design protocols whose theoretical description is closer to an experimentally feasible implementation, an approach that is followed by the differential phase shift (DPS) QKD protocol originally proposed in [IWY02]. Already on the level of the theoretical description, this protocol employs coherent states as information carriers instead of single photons, which allows for an implementation with readily available optical telecommunication equipment. However, as explained above, using weak coherent pulses opens up the possibility of the PNS attack. DPS QKD counteracts this attack by combining coherent states with encoding information in the relation between two consecutive rounds rather than into single rounds. This directly rules out attacks that extract information from individual pulses, which includes the PNS attack. However, designing a protocol with a focus on implementations comes at a cost: While the protocol is simpler concerning its experimental realisation, the security proof poses two significant challenges:

1. Using coherent states instead of single photons means we have to deal with states in an infinite-dimensional Fock space instead of a qubit (or some other finite-dimensional) Hilbert space. This renders any numerical method for calculating secure key rates infeasible if one tries to apply it directly to states in the Fock space.

2. The fact that information is encoded into the relation between two consecutive rounds rather than the individual rounds directly rules out some of the standard security proof techniques such as the quantum de Finetti theorem [Ren07, Ren08] and the postselection technique [CKR09]. This is because these techniques require the protocol rounds to be permutation invariant.

In light of these challenges, it is perhaps not surprising that a full security proof of DPS QKD has not been achieved yet. Instead, the security of DPS has been proven in various simplified scenarios. These efforts of proving the security of the DPS protocol generally fall into two categories: In the first, additional assumptions are made about the possible attacks that an eavesdropper can carry out. Consequently, these proofs only provide conditional (rather than unconditional) security of the protocol. One example in this category is a security proof that only applies to the class of individual attacks [WTY06]. In the second category, typically, a modified version of the protocol with a (block) IID[1] structure is analysed. Notable examples include the security proof of single photon DPS [WTY09] and security proofs for versions of DPS with phase-randomised blocks [TKK12, MSK+17]. In addition to the security proofs, some upper bounds on the performance of DPS QKD have been derived [CZLL07, CTM08, CTMG09].

In this work, we provide a security proof of DPS QKD against general attacks, which combines ideas from quantum information theory, quantum optics, and relativity. As such, it is the first full security proof of a protocol where information is encoded in between rounds instead of into individual rounds, which does not require making any adjustments to the protocol. The method we employ to achieve this task is a generalisation of the *entropy accumulation theorem* (EAT) [MFSR22, MR22], which allows us to derive secure key rates against general attacks taking into account finite-size effects. In contrast to methods such as the de Finetti theorem, it does not require the rounds of the protocol to be symmetric under permutation. It can hence be applied to protocols where information is encoded between two rounds. To account for the problem of the infinite-dimensional Fock space that describes the involved quantum states, we use a method called *squashing* [GLLP02, TT08, BML08, GBN+14]. The general idea here is to formulate a protocol on a low-dimensional Hilbert space that is analogous (with respect to its security) to the actual protocol. On the level of the low-dimensional space, we can then apply numerical techniques for calculating the secure key rate. The combination of the generalised EAT and the squashing map are almost sufficient to prove the security of DPS QKD. There is only one missing ingredient: To meet the requirements of the generalised EAT, we need to assume that the adversary has access to

[1] "IID" stands for "independent and identically distributed" and describes attacks where the eavesdropper applies the same strategy to each signal and, in particular, does not exploit correlations between signals.

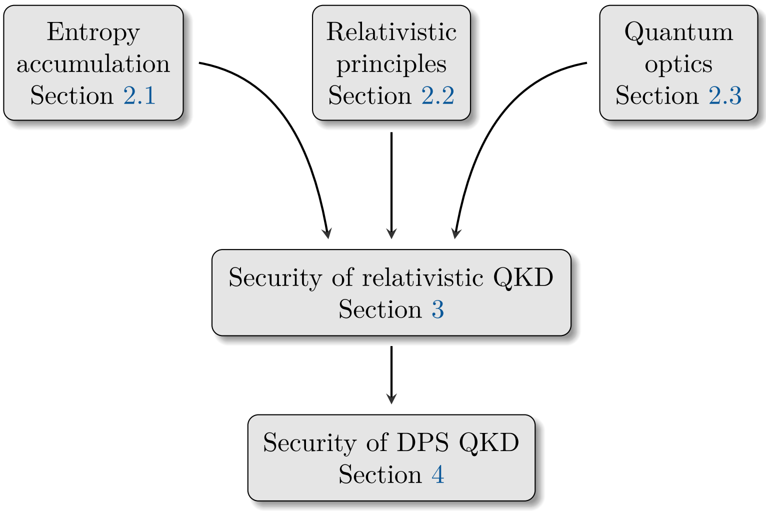


Figure 1: Overview of the ingredients of the security proofs presented in this work, together with their corresponding sections in the paper.

only one of the signals at a time. It can be argued that from a practical perspective, this is a very restrictive assumption since it requires a specific time interval between the signals, which reduces the possible secure key rate. However, we will show that it is, in fact, necessary to impose some assumption in this direction if one wants to use any security proof technique that reduces general attacks to IID attacks (such as the generalised EAT). This demonstrates that coherent attacks on the DPS protocol are generally stronger than collective ones (see Section 5).

The assumption that Eve can only access one of the systems simultaneously provides a natural connection to relativistic principles, particularly causality, since it implies that certain systems cannot signal to each other. This non-signalling constraint plays a vital role throughout our security proof, particularly in constructing the squashing map. The same type of constraint lies at the heart of the security of *relativistic QKD protocols* [RKKM14, KRKM18]. In these protocols, information is encoded in the relation between a signal and a reference state. To exploit that the adversary is constrained by the principles of relativity, the transmission timing in the protocol is designed such that the eavesdropper cannot access both states at the same time. Hence, her possibilities to attack the protocol are limited. This is very similar in spirit to how the DPS protocol works; in both kinds of protocols, information is encoded in the relation between two signals that are not simultaneously accessible to the adversary. In this work, we propose a new relativistic QKD protocol, give a general security proof of this protocol, and show how the security of DPS QKD follows as a special case of this proof. The structure and ingredients of the security proof are depicted in Figure 1.

In summary, in this paper, we give a security proof for DPS QKD and relativistic QKD against general attacks, including finite-size effects. This proof combines concepts from different areas, namely quantum information theory, quantum optics, and relativistic principles. To make it accessible for readers with different scientific backgrounds, we first introduce all necessary concepts from these areas in Section 2. With these concepts at hand, we can then introduce relativistic QKD protocols and prove their security in Section 3. In Section 4, we explain the DPS QKD protocol and show how to reduce its security to that of relativistic QKD protocols. Some aspects of these proofs deserve a more in-depth discussion, in particular the assumptions we use, which is provided in Section 5. In Section 6, we conclude by providing some perspective on how our techniques can be used or modified for security proofs of related protocols.

2 Preliminaries and techniques

In this section we cover the necessary background knowledge that is required to understand the security proofs. As hinted at in the introduction, there are three central ingredients: The entropy

Symbol	Definition
$\mathcal{S}(A)$	Density operators on the system A
$\mathcal{S}_{\leq}(A)$	Sub-normalised density operators on the system A
$\mathcal{I}_A$	The identity channel on system A
$\mathbb{P}_{\mathcal{X}}$	Probability distributions over the alphabet $\mathcal{X}$
$\|M\|_1$	Trace norm of M
M^*	The adjoint of M
A^n	Concatenation of the systems $A_1 \dots A_n$
$\log(x)$	The logarithm of x to base 2
$\oplus$	Addition modulo 2
$[n]$	The set $\{1, 2, \dots, n\}$
Ω^c	The complement of the set Ω

Table 1: Various symbols and their definitions

accumulation theorem, causality, and the squashing technique. In the following, we will cover these topics in that order. The notation and some basic definitions that are used throughout the section are listed in Table 1. The more technical definitions can be found in Appendix A.

2.1 Security of quantum key distribution

The security proof of any quantum key distribution protocol has to guarantee that the resulting key can be used in any application, for example in an encryption scheme. This is called *composable security* [MR11, PR22], and achieving it boils down to deriving a security definition that ensures the security statement holds in any context. In this section, we explain the composable security definition we use in this work that goes back to [Ren08], including notions of correctness, secrecy, and completeness, and discuss what a security proof must entail to meet it.

The general idea of the security definition is that we aim to quantify how far the actual key resource whose security we want to prove is from an ideal key resource. The goal of a QKD protocol is for two spatially distant parties (called Alice and Bob) to establish a shared secret key, hence the ideal key resource should fulfil two properties: (i) the resulting key has to be the same for Alice and Bob, and (ii) an adversary must not have any knowledge of it. A secure QKD protocol will either produce a key that fulfils these properties or abort. This is captured by the following definition:

Definition 2.1. Consider a QKD protocol which can either produce a key of length l or abort, and let $\rho_{K_A^l K_B^l E}$ be the final quantum state at the end of the protocol, where K_A^l and K_B^l are Alice's and Bob's version of the final key, respectively, and E is the quantum system that contains all knowledge available to an adversary Eve. The protocol is said to be $\varepsilon^{\mathrm{cor}}$-correct, $\varepsilon^{\mathrm{sec}}$-secret, and $\varepsilon^{\mathrm{comp}}$-complete if the following holds:

1. *Correctness:* For any implementation of the protocol and any behaviour of the adversary,

$$\Pr[K_A^l \neq K_B^l \wedge \mathrm{accept}] \leq \varepsilon^{\mathrm{cor}}. \tag{1}$$

2. *Secrecy:* For any implementation of the protocol and any behaviour of the adversary,

$$\frac{1}{2}\left\|(\rho_{\wedge\Omega})_{K_A^l E} - \tau_{K_A^l} \otimes (\rho_{\wedge\Omega})_E\right\|_1 \leq \varepsilon^{\mathrm{sec}}, \tag{2}$$

where $\rho_{\wedge\Omega}$ is the sub-normalized state after running the protocol conditioned on the event Ω of not aborting, and $\tau_{K_A^l} = \frac{1}{2^l}\sum_k |k\rangle\langle k|_{K_A^l}$ is the maximally mixed state on the system K_A^l (i.e., a uniformly random key for Alice).

3. *Completeness:* There exists an honest implementation of the protocol such that

$$\Pr[\mathrm{abort}] \leq \varepsilon^{\mathrm{comp}}. \tag{3}$$

Note that in the above definition, correctness and secrecy must be fulfilled for any behaviour of the adversary. These conditions ensure that Alice and Bob's probability of getting different or insecure keys without detecting it (i.e., without the protocol aborting) is low. They are often summarized to a single condition called *soundness*:

Definition 2.2. Consider a QKD protocol which can either produce a key of length l or abort, and let $\rho_{K^l_A K_K E}$ be the final quantum state at the end of the protocol, where K^l_A and K^l_B are Alice's and Bob's version of the final key, respectively, and E is the quantum system that contains all knowledge available to an adversary Eve. The protocol is said to be ε^{snd}-sound if

$$\frac{1}{2}\left\|(\rho_{\wedge\Omega})_{K^l_A K^l_B E} - \tau_{K^l_A K^l_B} \otimes (\rho_\wedge)_E\right\|_1 \leq \varepsilon^{\text{snd}}, \tag{4}$$

where $\rho_{\wedge\Omega}$ is the sub-normalized state after running the protocol conditioned on the event Ω of not aborting, and $\tau_{K^l_A K^l_B} = \frac{1}{2^l}\sum_k |kk\rangle\langle kk|_{K^l_A K^l_B}$ is the maximally mixed state on the system $K^l_A K^l_B$ (i.e., an identical pair of uniformly random keys for Alice and Bob).

It is straightforward to show that if a protocol is ε^{cor}-correct and ε^{sec}-secret, then it is ε^{snd}-sound with $\varepsilon^{\text{snd}} = \varepsilon^{\text{cor}} + \varepsilon^{\text{sec}}$ (see, for example, [PR22]). It is possible to either show correctness and secrecy separately or to show soundness directly. For the differential phase shift protocol, we choose to show soundness directly. In contrast to soundness, completeness is concerned only with the honest implementation, i.e., the case where the adversary is not trying to corrupt the execution of the protocol. For instance, a protocol that always aborts fulfils the first two conditions of the definition, but it is not a useful protocol. These kinds of protocols are excluded by imposing the completeness condition.

To prove that a QKD protocol fulfils the conditions in Definition 2.1, we typically employ two-universal hash functions and randomness extractors (see, for example, the protocol described in Section 4.1). Here, we give a rough sketch of what a security proof entails and briefly recall the definitions of the required primitives. In Appendices D to F, you can find a detailed security proof.

Completeness

To show completeness, one has to show that there exists an honest implementation of the protocol such that it aborts with low probability. This is usually straightforward to show as the honest behaviour typically has an IID structure. As long as we allow for enough tolerance in the parameter estimation step, one can choose the amount of resources used for the error correction step such that the probability of aborting is low (see Appendix D).

Correctness

Showing correctness means deriving a bound on the probability that the error-corrected strings are not equal but the protocol does not abort. In case the error-correction procedure includes a step where Bob checks whether his guess of Alice's string is correct, this is also straightforward to show. The checking step can be implemented using two-universal hash functions:

Definition 2.3 (Two-universal hash function)**.** Let $\mathcal{F}$ be a family of hash functions between sets $\mathcal{X}$ and $\mathcal{Z}$. We call $\mathcal{F}$ two-universal if for all $x, x' \in \mathcal{X}$ with $x \neq x'$ it holds that

$$\Pr_{f\in\mathcal{F}}[f(x) = f(x')] \leq \frac{1}{|\mathcal{Z}|}, \tag{5}$$

where $f \in \mathcal{F}$ is chosen uniformly at random.

Alice and Bob can hence choose a hash function $f \in \mathcal{F}$ and compare the outputs of Alice's key and Bob's guess of her key. If their bit strings are not equal, they will detect it with probability $1 - 1/|\mathcal{Z}|$, which means that by choosing the size of the output set $\mathcal{Z}$ one can ensure that this probability is high. This checking step is independent of the actual error correction procedure that is employed, hence it allows us to decouple the proof of correctness from all properties of the error correction step (except its output).

Secrecy

Showing secrecy is the most difficult part of the security proof, as one has to take into account any possible behaviour of the adversary. Secrecy is ensured in the last step of the protocol, privacy amplification. A possible procedure to implement this step is again based on two-universal hashing [Ren08]: As in the checking step after the error correction procedure, Alice and Bob choose a function from a family of two-universal hash functions and apply it to their respective strings. The following lemma (taken from [TL17]) then ensures that the resulting key fulfils the properties described in Definition 2.1:

Lemma 2.4 (Quantum leftover hashing). *Let $\rho_{f(X)FE} \in \mathcal{S}_{\leq}(ZFE)$ be the (sub-normalized) state after applying a function f, randomly chosen from a family of two-universal hash functions $\mathcal{F}$ from $\mathcal{X}$ to $\mathcal{Z}$, to the bit string X. Then, for every $\varepsilon > 0$ it holds that*

$$\frac{1}{2}\left\|\rho_{f(X)FE} - \tau_Z \otimes \rho_{FE}\right\|_1 \leq 2\varepsilon + 2^{-\frac{1}{2}(H^{\varepsilon}_{\min}(X|E)-l+2)}, \tag{6}$$

where $l = |\mathcal{Z}|$, τ_Z is the maximally mixed state on Z, and F is the register that holds the choice of the hash function.

Note that the smooth min-entropy $H^{\varepsilon}_{\min}(X|E)$ is evaluated on the state ρ_{XE}, i.e., the state of the system before applying the hash function. Lemma 2.4 then states that if there is a sufficient amount of initial smooth min-entropy, applying a random hash function results in a state that is almost product with the adversary's information. This means that to prove secrecy we need to find a sufficiently large lower bound on the smooth min-entropy which holds for general attacks of the adversary.

There are several techniques for finding such a bound. The typical strategy in a security proof is to find a bound that is valid if the adversary is limited to collective attacks, i.e., they apply the same attack in every round, and the individual rounds are uncorrelated. From this, a bound that is valid for general attacks can be inferred via techniques based on the quantum de Finetti theorem [Ren08, CKR09] or the entropy accumulation theorem (EAT) [DFR20, GLvH+22]. From the bound on the smooth min-entropy we can then obtain a lower bound on the *key rate*

$$r = \frac{l}{n}, \tag{7}$$

where l is the length of the final key, and n is the number of rounds via Lemma 2.4 (more details about this can be found in Appendix D.2). It is often easier to calculate this bound in the asymptotic case where the number of rounds n goes to infinity. However, for a full security proof and to obtain meaningful bounds for practical protocols, it is necessary to also include finite-size effects, which occur because the protocol consists only of a finite number of rounds.

The technique we employ in this work is the EAT in its recently developed generalised form [MFSR22, MR22]. Apart from guaranteeing security against general attacks it allows us to take into account finite-size effects. The EAT relates the smooth min-entropy of n rounds in the case of general attacks to the von Neumann entropy of a single round in the case of collective attacks, which, in general, is much easier to bound. The general setting in which we can apply the generalised EAT is depicted in Figure 2. Before we can state the theorem, we need to introduce some definitions that describe the setup to which it applies, in particular, the notion of EAT channels. For the technical definitions we refer to Appendix A.

Definition 2.5 (EAT channel). Let $\{\mathcal{M}_i \in \mathrm{CPTP}(R_{i-1}E_{i-1}, R_iE_iA_iC_i)\}_{i\in[n]}$ be a sequence of channels, where C_i are classical registers with common alphabet $\mathcal{C}$. We call the channels $\{\mathcal{M}_i\}_i$ *EAT channels* if they satisfy the following conditions:

1. There exists a channel $\mathcal{R}_i \in \mathrm{CPTP}(E_{i-1}, E_i)$ such that $\mathrm{tr}_{A_iR_iC_i} \circ \mathcal{M}_i = \mathcal{R}_i \circ \mathrm{tr}_{R_{i-1}}$.
2. Let $\mathcal{M}'_i = \mathrm{tr}_{C_i} \circ \mathcal{M}_i$. Then there exists $\mathcal{T} \in \mathrm{CPTP}(A^nE_n, C^nA^nE_n)$ of the form

$$\mathcal{T}(\omega_{A^nE_n}) = \sum_{y\in\mathcal{Y},z\in\mathcal{Z}} (\Pi^{(y)}_{A^n} \otimes \Pi^{(z)}_{E_n})\omega_{A^nE_n}(\Pi^{(y)}_{A^n} \otimes \Pi^{(z)}_{E_n}) \otimes |r(y,z)\rangle\langle r(y,z)|_{C^n}, \tag{8}$$

such that $\mathcal{M}_n \circ \ldots \circ \mathcal{M}_1 = \mathcal{T} \circ \mathcal{M}'_n \circ \ldots \circ \mathcal{M}'_1$. The operators $\{\Pi^{(y)}_{A^n}\}_y$ and $\{\Pi^{(z)}_{E_n}\}_z$ are mutually orthogonal projectors and $r : \mathcal{Y} \times \mathcal{Z} \to \mathcal{C}$ is a (deterministic) function.

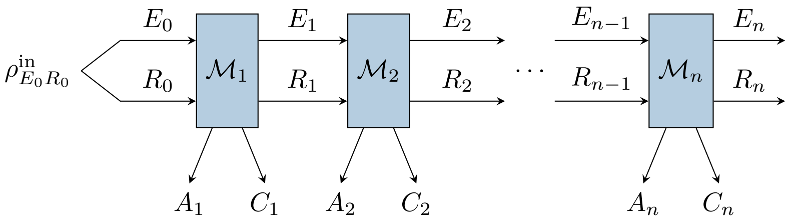


Figure 2: Setup of the generalised EAT with testing. In each round i the channels take quantum inputs E_{i-1} and R_{i-1} and produce classical outputs A_i and C_i. The registers C_i are used to restrict the set of allowed channels $\{\mathcal{M}_i\}_i$.

The first of these conditions states that the map $\mathcal{M}_i$ does not signal from R_{i-1} to E_i. This non-signalling constraint is required as part of the EAT and is distinct from the other non-signalling constraints that will arise in the analysis of the protocol. For a more detailed discussion of non-signalling maps we refer to Section 2.2. We note that the second condition above is always satisfied if C_i is computed from classical information in A^n and E_n. A diagram of the channels is shown in Figure 2.

Definition 2.6 (Min-tradeoff function)**.** Let $\{\mathcal{M}_i\}_i$ be a sequence of EAT channels. For $i \in [n]$ and $q \in \mathbb{P}_\mathcal{C}$ we define the set $\Sigma_i(q)$ of all states that are compatible with the statistics q under the map $\mathcal{M}_i$:

$$\Sigma_i(q) = \{\nu_{C_iA_iR_iE_i\tilde{E}_{i-1}} = \mathcal{M}_i(\omega_{R_{i-1}E_{i-1}\tilde{E}_{i-1}}) \mid \omega \in \mathcal{S}(R_{i-1}E_{i-1}\tilde{E}_{i-1}) \text{ and } \nu_{C_i} = q\}, \tag{9}$$

where ν_{C_i} represents the distribution over $\mathcal{C}$ given by $\Pr[c] = \langle c|\nu_{C_i}|c\rangle$ and $\tilde{E}_{i-1}$ is a system isomorphic to $R_{i-1}E_{i-1}$. An affine function $f : \mathbb{P}_\mathcal{C} \to \mathbb{R}$ is called a *min-tradeoff function* for $\{\mathcal{M}_i\}_i$ if it satisfies

$$f(q) \leq \inf_{\nu \in \Sigma_i(q)} H(A_i|E_i\tilde{E}_{i-1})_\nu \qquad \forall q \in \mathbb{P}_\mathcal{C}, i \in [n]. \tag{10}$$

The second-order corrections in the EAT will depend on some properties of the min-tradeoff function (see Definition 2.6), which are given in the following definition:

Definition 2.7 (Min, Max and Var)**.** Let $\{\mathcal{M}_i\}_i$ be a sequence of EAT channels and let $f : \mathbb{P}_\mathcal{C} \to \mathbb{R}$ be an affine function. We define

$$\begin{aligned} \mathrm{Max}(f) &= \max_{q \in \mathbb{P}_\mathcal{C}} f(q), \\ \mathrm{Min}_\Sigma(f) &= \min_{q:\Sigma(q)\neq\emptyset} f(q), \\ \mathrm{Var}(f) &= \max_{q:\Sigma(q)\neq\emptyset} \left\{ \sum_{c\in\mathcal{C}} q(c) f(\delta_c)^2 - \left(\sum_{c\in\mathcal{C}} q(c) f(\delta_c) \right)^2 \right\}, \end{aligned} \tag{11}$$

where $\Sigma(q) = \bigcup_i \Sigma_i(q)$ and δ_c is the distribution with deterministic output c.

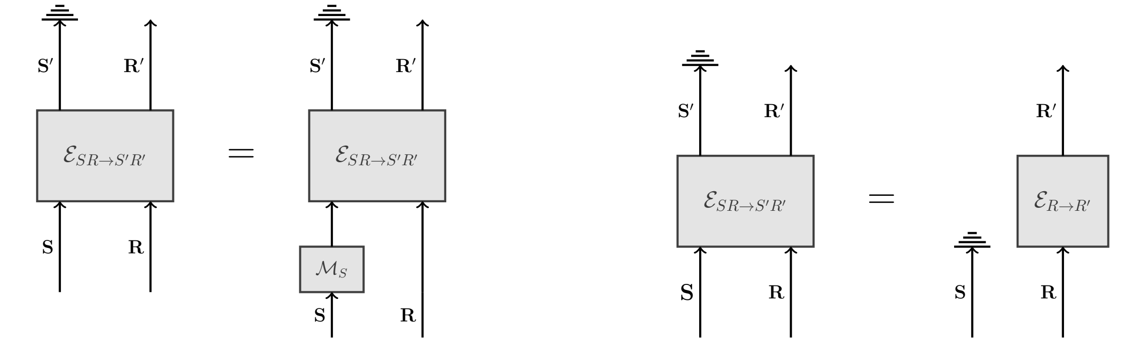
Definition 2.8. Let $\mathcal{C}$ be some finite alphabet and let $C^n \in \mathcal{C}^n$ for some $n \in \mathbb{N}$. Then $\mathrm{freq}(C^n) \in \mathbb{P}_\mathcal{C}$ is defined as the probability distribution given by:

$$\mathrm{freq}(C^n)(c) = \frac{|\{i|C_i = c\}|}{n} \qquad \forall c \in \mathcal{C}. \tag{12}$$

With this in hand we are now able to state the theorem:

Theorem 2.9 (Generalised EAT [MFSR22])**.** *Let $\{\mathcal{M}_i\}_i$ be a sequence of EAT channels and let f be a min-tradeoff function for those channels. Furthermore, let $\Omega \subseteq \mathcal{C}^n$ and $\rho_{A^nC^nR_nE_n} = \mathcal{M}_n \circ \ldots \circ \mathcal{M}_1(\omega_{R_0E_0})$ be the output state for some initial state $\omega_{R_0E_0} \in \mathcal{S}(R_0E_0)$. Then for all $\alpha \in (1, 3/2)$ and $\varepsilon > 0$,*

$$H^\varepsilon_{\min}(A^n|E_n)_{\rho_{|\Omega}} \geq nt - n\frac{\alpha-1}{2-\alpha}\frac{\ln(2)}{2}V^2 - \frac{g(\varepsilon) + \alpha\log\left(\frac{1}{\rho[\Omega]}\right)}{\alpha-1} - n\left(\frac{\alpha-1}{2-\alpha}\right)^2 K(\alpha), \tag{13}$$



(a) Diagrammatic representation of (15). The above equality must hold for all local maps $\mathcal{M}_S$ on S.

(b) Diagrammatic representation of (16). There must exist a quantum CPTP map $\mathcal{E}_{R\to R'}$ such that the above equality holds.

Figure 3: Diagrammatic representation of two equivalent definitions of non-signalling in a quantum map. The ground symbol ⏚ denotes the trace operation.

where $\rho[\Omega]$ is the probability of observing the event Ω, and

$$
\begin{aligned}
t &= \min_{c^n \in \Omega} f(\mathrm{freq}(c^n)),\\
g(\varepsilon) &= \log \frac{1}{1-\sqrt{1-\varepsilon^2}},\\
V &= \log(2d_A^2+1) + \sqrt{2+\mathrm{Var}(f)},\\
K(\alpha) &= \frac{(2-\alpha)^3}{6(3-2\alpha)^3 \ln 2} 2^{\frac{\alpha-1}{2-\alpha}(2\log d_A + \mathrm{Max}(f) - \mathrm{Min}_\Sigma(f))} \ln^3\left(2^{2\log d_A + \mathrm{Max}(f) - \mathrm{Min}_\Sigma(f)} + e^2\right),
\end{aligned}
\tag{14}
$$

with $d_A = \max_i \dim(A_i)$.

Proof. See [MFSR22]. □

2.2 Relativistic principles and causality

Relativistic principles of causation prohibit signalling outside the future light-cone. In order to incorporate such principles into quantum protocols in a space-time, we must consider how non-signalling conditions can be formulated at the level of quantum operations. Consider a quantum operation (a completely positive and trace preserving linear map) $\mathcal{E}_{SR\to S'R'} : \mathcal{S}(SR) \to \mathcal{S}(S'R')$, where S, R, S' and R' are quantum systems of arbitrary (possibly infinite) dimensions. Suppose the input quantum system S and the output system R' are associated with space-like separated locations. We would then desire that S does not signal to R'. Operationally speaking, the choice of a local operation $\mathcal{M}_S : \mathcal{S}(S) \to \mathcal{S}(S)$ performed on the input S of $\mathcal{E}_{SR\to S'R'}$ must never be detectable when accessing the system R' alone. This is captured by the following definition:

Definition 2.10. We say that S does not signal to R' in a linear CPTP map $\mathcal{E}_{SR\to S'R'} : \mathcal{S}(SR) \to \mathcal{S}(S'R')$ if and only if for all local operations $\mathcal{M}_S : \mathcal{S}(S) \to \mathcal{S}(S)$ on S, the following holds

$$\mathrm{tr}_{S'} \circ \mathcal{E}_{SR\to S'R'} = \mathrm{tr}_{S'} \circ \mathcal{E}_{SR\to S'R'} \circ \left(\mathcal{M}_S \otimes \mathcal{I}_R\right). \tag{15}$$

Another natural way to define signalling would be to require that once we trace out S' and only observe the output at R', then we can also trace out the input at S and only use the input at R. That is, there exists a quantum channel $\mathcal{E}_{R\to R'} : \mathcal{S}(R) \to \mathcal{S}(R')$ such that

$$\mathrm{tr}_{S'} \circ \mathcal{E}_{SR\to S'R'} = \mathrm{tr}_S \otimes \mathcal{E}_{R\to R'}. \tag{16}$$

In fact, it turns out that the two definitions of signalling, (15) and (16) are equivalent [OVB22].[2]

[2]While this result is stated only for unitary $\mathcal{E}_{SR\to S'R'}$ in [OVB22], their proof applies to arbitrary quantum CPTP maps.

The following lemma provides another equivalent condition to non-signalling in the CPTP map $\mathcal{E}_{SR\to S'R'}$, in terms of its Choi state $\mathcal{C}(\mathcal{E}_{SR\to S'R'}) \in \mathcal{S}(\bar{S}\bar{R}S'R')$, in the case where S, R, S' and R' are finite dimensional quantum systems. The Choi state of a CP map on finite dimensional systems is defined as follows.

$$\mathcal{C}(\mathcal{E}_{SR\to S'R'}) := (\mathcal{I}_{\bar{S}\bar{R}} \otimes \mathcal{E}_{SR\to S'R'})|\Phi\rangle\langle\Phi|_{\bar{S}\bar{R}SR}, \tag{17}$$

where $\bar{S}$ and $\bar{R}$ have isomorphic state spaces to the systems S and R, respectively, and $|\Phi\rangle_{\bar{S}\bar{R}SR} = \frac{1}{\sqrt{d_S d_R}} \sum_{ij} |ijij\rangle_{\bar{S}\bar{R}SR}$ is the normalised maximally entangled state on the bi-partition $\bar{S}\bar{R}$ and SR with respect to a chosen basis $\{|i\rangle\}_i$ of the isomorphic systems S and $\bar{S}$, and the basis $\{|j\rangle\}$ of the isomorphic systems R and $\bar{R}$. While a Choi representation for the infinite dimensional case can be defined, it does not correspond to a state, but to a sesquilinear positive-definite form [Hol11]. In this paper, we will only require the finite-dimensional Choi representation which is captured by the Choi state of a CP map. Note however that the definitions of signalling defined above also apply to the infinite dimensional case.

Lemma 2.11. *S does not signal to R' in a linear CPTP map $\mathcal{E}_{SR\to S'R'} : \mathcal{S}(SR) \to \mathcal{S}(S'R')$ on finite-dimensional quantum systems S, R, S' and R' if and only if*

$$\mathrm{tr}_{S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})] = \frac{\mathbb{1}_{\bar{S}}}{d_{\bar{S}}} \otimes \mathrm{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})], \tag{18}$$

where $\mathcal{C}(\mathcal{E}_{SR\to S'R'})$ is the Choi state of the map $\mathcal{E}_{SR\to S'R'}$, given by (17).

Proof. See Appendix B. □

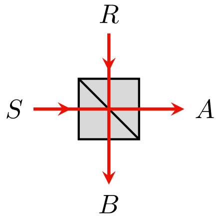
The above form of the non-signalling condition in terms of the Choi state (18) derives its usefulness from the fact that it no longer involves any quantifiers, in contrast to (15) and (16). Furthermore, it is a linear constraint on the Choi state. Both these features are beneficial for conveniently encoding relativistic constraints within the numerical procedure of our QKD security proofs, as we will see in Appendix E.

It is important to note that while relativistic principles associated with a spacetime may motivate us to impose certain non-signalling conditions (e.g., between S and R' when they are spacelike separated), these conditions are independent of the spacetime locations of the systems involved and rely on the information-theoretic structure of the associated CPTP map. Thus, such no-signalling conditions may be of interest even in scenarios where S and R' are timelike separated, but where we wish to restrict the information flow from S to R'.

2.3 Quantum optics

In this section, we turn to more practical considerations when studying photonic implementations of QKD protocols. In particular, we introduce the necessary background knowledge required to formulate the photonic implementations of our protocols. Our protocol will make use of the two most common devices in quantum optics, namely the beam splitter (BS) and the threshold detector. Therefore, in the following, we introduce the mathematical language required to describe the operation of these two devices.

The first of these components is the beam splitter. A 50/50 BS can be described using the following transformation of creation operators:



$$\begin{aligned} a_A^\dagger &= \frac{1}{\sqrt{2}}\left(a_S^\dagger + a_R^\dagger\right), \\ a_B^\dagger &= \frac{1}{\sqrt{2}}\left(a_S^\dagger - a_R^\dagger\right), \end{aligned} \tag{19}$$

where the modes are as shown in the picture. These operators create states with photons in a given mode (S, R, A or B). This allows us to view the above transformations as a transformation acting on states by writing

$$\begin{aligned}|N,0\rangle_{AB} &= \frac{1}{\sqrt{N!}}\left(a_A^\dagger\right)^N|0,0\rangle = \frac{1}{\sqrt{2^N N!}}\left(a_S^\dagger + a_R^\dagger\right)^N|0,0\rangle,\\ |0,N\rangle_{AB} &= \frac{1}{\sqrt{N!}}\left(a_B^\dagger\right)^N|0,0\rangle = \frac{1}{\sqrt{2^N N!}}\left(a_S^\dagger - a_R^\dagger\right)^N|0,0\rangle.\end{aligned} \tag{20}$$

Of particular importance is the action of a BS on a coherent state:

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{21}$$

The parameter $\alpha \in \mathbb{C}$ quantifies the amplitude of a laser pulse, as the state has an average photon number $\langle n\rangle_{|\alpha\rangle} = |\alpha|^2$. Under the action of the BS, coherent states are mapped to coherent states, more precisely

$$|\alpha\rangle_S|\beta\rangle_R \mapsto |(\alpha+\beta)/\sqrt{2}\rangle_A \otimes |(\alpha-\beta)/\sqrt{2}\rangle_B. \tag{22}$$

Furthermore, the probability of detecting no photon when measuring a coherent state $|\alpha\rangle$ is given by

$$\Pr[n=0|\alpha] = |\langle 0|\alpha\rangle|^2 = e^{-|\alpha|^2}. \tag{23}$$

When a coherent state $|\alpha\rangle$ travels through a lossy beam line with transmittance $\eta \in [0,1]$, it is mapped to the state $|\sqrt{\eta}\alpha\rangle$.

The second component of consideration is the threshold detector. There are four different measurement outcomes: only the first detector clicks, only the second detector clicks, both detectors click, or neither detector clicks. These four events are described by the following POVM:

$$\begin{aligned}\tilde{M}^{(0)} &= \sum_{N=1}^{\infty}|N,0\rangle\langle N,0|_{AB},\\ \tilde{M}^{(1)} &= \sum_{N=1}^{\infty}|0,N\rangle\langle 0,N|_{AB},\\ \tilde{M}^{(\mathrm{dc})} &= \sum_{N=2}^{\infty}\sum_{n=1}^{N-1}|N-n,n\rangle\langle N-n,n|_{AB},\\ \tilde{M}^{(\perp)} &= |0,0\rangle\langle 0,0| = \mathbb{1} - \tilde{M}^{(0)} - \tilde{M}^{(1)} - \tilde{M}^{(\mathrm{dc})}.\end{aligned} \tag{24}$$

We will be interested in the scenario where a pair of threshold detectors is placed behind a BS. Therefore, the states in the above expressions should be understood as photonic states in the respective mode after the BS (compare with (20)). In our protocols we will post-process the measurement outcomes by randomly assigning the double-click outcomes to the outcome 0 or 1. We describe this via the post-processed POVM:

$$\begin{aligned}M^{(0)} &= \tilde{M}^{(0)} + \frac{1}{2}\tilde{M}^{(\mathrm{dc})},\\ M^{(1)} &= \tilde{M}^{(1)} + \frac{1}{2}\tilde{M}^{(\mathrm{dc})},\\ M^{(\perp)} &= \tilde{M}^{(\perp)}.\end{aligned} \tag{25}$$

Studying photonic implementations directly is infeasible due to the infinite dimension of the Fock space. This issue can be addressed using a theoretical tool known as squashing maps [GLLP02, TT08, BML08, GBN+14]:

Definition 2.12 (Squashing map)**.** Let A and A' be two quantum systems. Let $\{M_A^{(x)}\}_x$ and $\{N_{A'}^{(x)}\}_x$ be two POVMs for the systems A and A', respectively. A CPTP map $\Lambda : \mathcal{S}(A) \to \mathcal{S}(A')$ is called a *squashing map from* $\{M_A^{(x)}\}_x$ *to* $\{N_{A'}^{(x)}\}_x$ if for all x and all $\rho_A \in \mathcal{S}(A)$,

$$\mathrm{tr}\left[M_A^{(x)}\rho_A\right] = \mathrm{tr}\left[N_{A'}^{(x)}\Lambda(\rho_A)\right]. \tag{26}$$

A squashing map is an essential tool in our security proof because it allows us to reduce the analysis of photonic QKD implementations to qubit-based implementations, which are much simpler to analyse. The argument goes as follows: Since the measurement statistics are preserved by the squashing map, introducing an artificial squashing map before Bob's detectors does not change the post-measurement state. We can now see this squashing map as part of Eve's attack channel. Hence, any attack on the large system implies an equally strong attack on the reduced system. Thus, the key rate of the qubit protocol is a lower bound on the key rate of the original protocol. Finding a squashing map for the given detectors is usually good enough for security proofs. Unfortunately, this is not sufficient in our case because we have a non-signalling constraint on Eve's attack, which needs to be preserved by the squashing map. Therefore, we want a squashing map that is non-signalling. This is achieved by the following theorem:

Theorem 2.13. *Let S and R be two Fock spaces and let S' and R' be two qubit systems. The target POVM is*

$$\begin{aligned} N_{S'R'}^{(0)} &= |\phi^+\rangle\langle\phi^+| + \frac{1}{2}|11\rangle\langle 11|, \\ N_{S'R'}^{(1)} &= |\phi^-\rangle\langle\phi^-| + \frac{1}{2}|11\rangle\langle 11|, \\ N_{S'R'}^{(\perp)} &= |00\rangle\langle 00|, \end{aligned} \tag{27}$$

where $|\phi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ are Bell states. Note that the POVM above is simply the restriction of the POVM defined in (25) to the one-photon subspaces. Let $N \in \mathbb{N}_{>0}$, $0 \leq k \leq N$ and $0 \leq l \leq N$, where k is an odd and l is an even number in $\mathbb{N}$. Define the Kraus operators

$$K^{(0)} = |00\rangle_{S'R'}\langle 0,0|_{SR}, \tag{28}$$

$$K_{k,l}^{(N)} = \frac{\sqrt{2}}{\sqrt{2^N}}\left(\sqrt{\binom{N}{l}}|01\rangle_{S'R'}\langle N-k,k|_{SR} + \sqrt{\binom{N}{k}}|10\rangle_{S'R'}\langle N-l,l|_{SR}\right). \tag{29}$$

Then the map

$$\Lambda(\rho_{SR}) = K^{(0)}\rho_{SR}\left(K^{(0)}\right)^* + \sum_{N=1}^{\infty}\sum_{k,l}^{N} K_{k,l}^{(N)}\rho_{SR}\left(K_{k,l}^{(N)}\right)^* \tag{30}$$

is a squashing map from the POVM given in (25) to the POVM given in (27), which is non-signalling from S to R'.

Proof. See Appendix C. □

3 Security of relativistic QKD

As a first step towards proving the security of DPS QKD, we introduce a novel relativistic QKD protocol, based on ideas from [RKKM14, KRKM18]. This serves two purposes: As we will show in Section 4, the security of DPS QKD is inherited from the security of the relativistic QKD protocol. The reason is that both protocols share the same measurement operators and similar relativistic constraints, even if their experimental setups differ. Secondly, the relativistic QKD protocol we introduce in this section may be of independent interest since it comes with a complete security proof against general attacks.

The setup of the relativistic QKD protocol is as follows: Broadly speaking, Alice and Bob share a Mach-Zehnder interferometer with two delay lines as shown in Figure 4. A single round of the protocol contains the following steps: At the time $t_A^{(i)}$ Alice prepares two states, a weak coherent *reference* pulse $|\alpha\rangle_R$ that she immediately sends to Bob, and a weak coherent *signal* state that she delays by a time Δt before sending it to Bob. Alice encodes her uniformly random raw key bit $V_i \in \{0,1\}$ in the phase of the signal state, i.e., she sends $|(-1)^{V_i}\alpha\rangle_S$ to Bob. The delay Δt is chosen such that the following condition holds:

Condition 3.1. *Eve does not signal from the signal state to the reference state.*

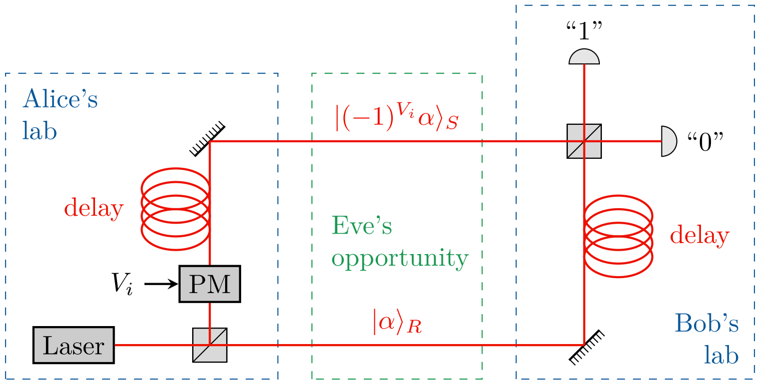


Figure 4: The experimental setup of our novel relativistic QKD protocol, which boils down to a shared Mach-Zehnder interferometer between Alice and Bob. In each round of the protocol, Alice chooses a uniformly random bit $V_i \in \{0,1\}$. She then sends a weak coherent state through a BS, creating a reference state and a signal state. The reference state $|\alpha\rangle_R$ is sent to Bob immediately. Additionally, Alice uses a phase modulator (PM) to apply a phase $(-1)^{V_i}$ to the signal state $|\alpha\rangle_S$, producing the state $|(-1)^{V_i}\alpha\rangle_S$. This state is delayed by a time Δt before Alice sends it to Bob (depicted via a delay line). Bob correspondingly first receives the reference state and delays it by the same amount Δt. Upon receiving the signal state, he measures the relative phase between the reference and signal state using a BS on his side.

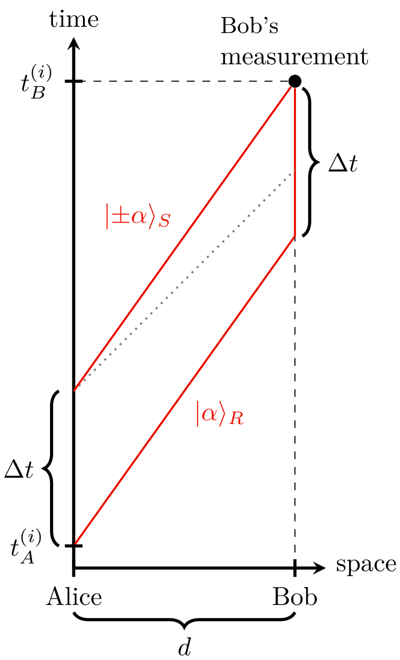


Figure 5: A spacetime diagram depicting how Condition 3.1 can be enforced. Alice's lab is depicted as the left world line, and Bob's lab is separated by a distance d. The (red) world lines of the (not necessarily light-like) reference state $|\alpha\rangle_R$ and the signal state $|\pm\alpha\rangle_S$ are separated by the time shift Δt. The dotted line depicts the future light cone of Alice revealing information about the signal state. For large enough Δt, Eve therefore can't influence the reference based on this information before it enters Bob's lab.

Figure 5 shows how Condition 3.1 can be enforced in an experimental setup via the delay of the signal by Δt, which is implemented in Figure 4 via the delay lines. In Section 5.1, we further elaborate on how to enforce this condition by choosing an appropriate value for Δt. In line with the concepts introduced in Section 2.2, we interpret this condition as a non-signalling constraint on Eve's possible attacks.

After the delay, Alice sends the modulated signal pulse $|(-1)^{V_i}\alpha\rangle_S$ to Bob. He correspondingly first receives the reference state, which he delays by the same amount Δt. At time t_B, he receives the signal state and interferes both states through his own BS. Using (22), this transformation can be written as

$$\begin{aligned} |(-1)^0\alpha\rangle_S|\alpha\rangle_R &\mapsto |+\sqrt{2}\alpha\rangle_A \otimes |0\rangle_B, \\ |(-1)^1\alpha\rangle_S|\alpha\rangle_R &\mapsto |0\rangle_A \otimes |-\sqrt{2}\alpha\rangle_B. \end{aligned} \tag{31}$$

We see that, depending on the phase of the signal state, only one of Bob's detectors will click. This then allows Bob to recover Alice's raw key bit V_i. Bob's measurement can be seen as optimal unambiguous state discrimination between $|\pm\alpha\rangle_S$. Bob also records the time t_B at which his detector clicked.

If both detectors click due to the presence of noise or the interaction of an adversary, Bob randomly reassigns the measurement outcome to either 0 or 1. This leaves him with the measurement operators as defined in (25), where single detector-click outcomes 0 or 1 correspond to his guess for Alice's raw key bit V_i, and the inconclusive outcome $\perp$ represents that no detector has clicked.

Afterwards, Alice communicates the time $t_A^{(i)}$ at which she dispatched the reference state over an authenticated classical channel to Bob. If Bob determines the time of interference $t_B^{(i)}$ to be above a threshold given explicitly by $t_A^{(i)} + 2\Delta t + d/c$, he aborts the protocol[3]. Through this abort condition, Alice and Bob know that Condition 3.1 is satisfied if the protocol didn't abort.

To be able to apply the generalised EAT in the security proof of the relativistic QKD protocol, it is necessary that the assumptions of the theorem are fulfilled. In particular, we have to enforce a sequential form of our protocol which is formalized through the following additional condition:

Condition 3.2. *Eve does not signal from round $i+1$ to round i.*

This condition is easily satisfied by requiring that Alice starts the $i+1$-th round at a time $t_A^{(i+1)} = t_A^{(i)} + 2\Delta t$ by the same argument we used to ensure that Condition 3.1 is fulfilled (see Section 5.1). Conceptually, Alice should therefore send a (reference or signal) pulse every Δt, as agreed upon by Alice and Bob beforehand.

3.1 Protocol

Next, we formalise the protocol as described above and include the classical post-processing steps after repeating $n \in \mathbb{N}$ rounds of the protocol.

For a fraction $\gamma \in (0, 1)$ of the rounds, Bob publicly announces his measurement outcome B_i, which allows Alice to compute statistics in order to upper-bound Eve's knowledge. We refer to these rounds as *test rounds*. These statistics take values in the alphabet $\mathcal{C} = \{\text{corr}, \text{err}, \perp, \varnothing\}$. The first three correspond to Bob determining the value for Alice's raw key bit V_i correctly, incorrectly, or not at all, respectively. The value $\varnothing$ denotes that the round was not a test round and hence no statistics has been collected. Correspondingly, we define the evaluation function $\text{EV} : \{0, 1, \perp\} \times \{0, 1, \perp, \varnothing\} \to \mathcal{C}$ with inputs from Alice's raw key bit A and Bob's measurement outcome J as

$$\text{EV}(A, J) = \begin{cases} \text{corr}, & \text{if } J \in \{0, 1\} \text{ and } A = J \\ \text{err}, & \text{if } J \in \{0, 1\} \text{ and } A \neq J \\ \perp, & \text{if } J = \perp \\ \varnothing, & \text{if } J = \varnothing. \end{cases} \tag{32}$$

With these definitions we are now able to formally state the relativistic QKD protocol with Δt chosen such that Conditions 3.1 and 3.2 are satisfied as described in Section 5.1. The structure of this protocol (summarised in Protocol 1) is then the same one as the general prepare-and-measure protocol in [MR22].

3.2 Sketch of security proof

Here, we present a brief sketch of the security proof of the relativistic QKD protocol. The interested reader can find the details of the proof in Appendices D and E. The main steps of the security proof can be summarised as follows:

1. Cast the soundness condition into a form that matches the conditions of the leftover hashing lemma (Lemma 2.4). This lemma ensures that the trace-distance between the ideal state and the state that describes the actual protocol can be upper-bounded, given a lower bound on the smooth min-entropy.

2. Ensure that all requirements for applying the generalised EAT are fulfilled: via appropriate entropic chain rules, we can to bring the smooth min-entropy into the form that appears in the generalised EAT, and Condition 3.2 ensures the existence of well-defined EAT channels $\mathcal{M}_i$.

[3]It may appear drastic to abort the whole protocol if the timing of a single round was off. This, however, only allows Eve to abort the protocol at her will, which is a possibility she has in any QKD protocol. For instance, she could block the quantum transmission line such that none of Alice's states arrive at Bob's lab. In practice, one should only count detector clicks up to $t_B^{(i),\max} = t_A^{(i)} + 2\Delta t + d/c$ to realize Condition 3.1.

3. To get a bound on $H^{\varepsilon}_{\min}$ out of the generalised EAT we need a min-tradeoff function. This requires lower-bounding Eve's uncertainty about the raw key, i.e., finding a lower-bound on $H(A|EIJ)$.

   3.1 Use Condition 3.1 and Theorem 2.13 to squash the relativistic protocol into a qubit protocol that still satisfies Condition 3.1 (as Eve could have applied the squashing map herself). The measurement operators of the squashed protocol are then given by (27).

   3.2 The numerical optimization requires us to minimize the conditional entropy over all possible attacks of Eve that are non-signalling (compare Definition 2.10). This can be conveniently included in the optimization constraints by optimizing over Choi states and applying Lemma 2.11.

Protocol 1: Relativistic QKD

The protocol is defined in terms of the following parameters, which are chosen before the protocol begins:

$\alpha \in \mathbb{C}$:	amplitude of the laser light
$n \in \mathbb{N}$:	number of protocol rounds
$\gamma \in (0,1)$:	testing frequency
$\mathrm{leak}_{\mathrm{EC}}$:	maximum length of error correction
$\varepsilon_{\mathrm{EC}}$:	error tolerance during error correction
$f : \mathbb{P}_{\mathcal{C}} \to \mathbb{R}$:	collective attack bound
H_{exp}:	minimum expected single-round entropy
$l \in \mathbb{N}$:	length of the final secret key

---

1. **Quantum Phase:** For $i \in [n]$:

   1.1 Alice chooses a bit $V_i \in \{0,1\}$ uniformly at random, prepares a reference state $|\alpha\rangle_R$ and a signal state $|(-1)^{V_i}\alpha\rangle_S$ and sends them to Bob such that Condition 3.1 is enforced.

   1.2 Bob receives a joint state ρ_{SR} and performs a measurement given by the POVM $\{M^{(b)}_{SR}\}_b$ of (25). He records his measurement outcome in the register $B_i \in \{0,1,\perp\}$.

   1.3 If $B_i = \perp$ then Bob transmits $I_i = \perp$ to Alice and $I_i = \top$ otherwise.

   1.4 Bob chooses $T_i \in \{0,1\}$ randomly with $\Pr[T_i = 1] = \gamma$. If $T_i = 1$ Bob transmits $J_i = B_i$ to Alice, otherwise he transmits $J_i = \varnothing$.

   1.5 Alice waits to enforce Condition 3.2.

2. **Sifting:** For all $i \in [n]$ Alice sets $A_i = V_i$ if $I_i \neq \perp$ and $A_i = \perp$ otherwise.

3. **Error correction:**

   3.1 Alice and Bob use their outputs A^n and B^n to perform error correction by communicating at most $\mathrm{leak}_{\mathrm{EC}}$ number of bits. Bob stores his guess for Alice's key in $\tilde{A}^n$.

   3.2 Alice chooses a hash function $h \in \mathcal{F}$ uniformly at random from a family of two-universal hash functions of length $\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil$ and applies it to her raw key. She sends the output $h(A^n)$ and her choice of hash function to Bob.

   3.3 Bob applies the same hash function to his guess $\tilde{A}^n$. If the two hashes disagree, Alice and Bob abort the protocol.

4. **Parameter estimation:** For all $i \in [n]$ Alice computes $C_i = \mathrm{EV}(A_i, J_i)$. If $f(\mathrm{freq}(C^n)) \leq H_{\mathrm{exp}}$ they abort the protocol.

5. **Privacy amplification:** Alice and Bob perform privacy amplification on A^n and $\tilde{A}^n$ to obtain raw keys K^l_A and K^l_B.

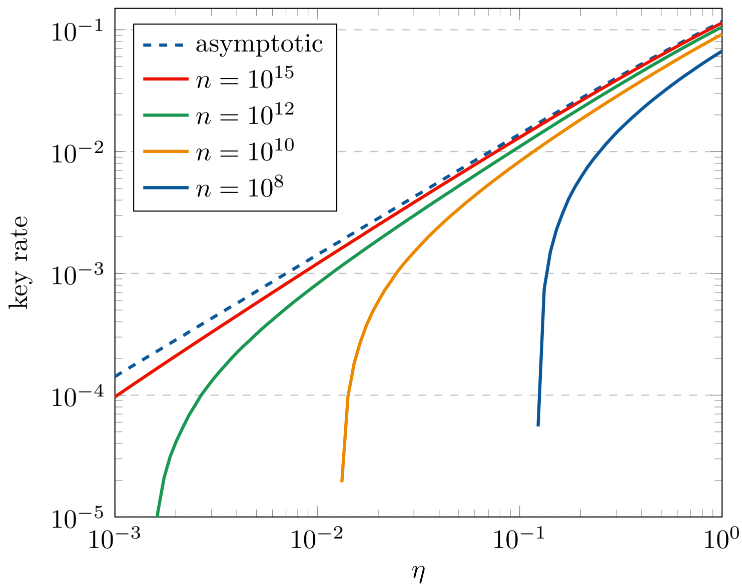


Figure 6: The key rates for a finite number of rounds n as given in the legend in dependence of different transmittances $\eta \in [0, 1]$ of the lossy beam line without considering QBER and for optimal α. Note that asymptotically one can distil a secret key for arbitrarily low transmittances.

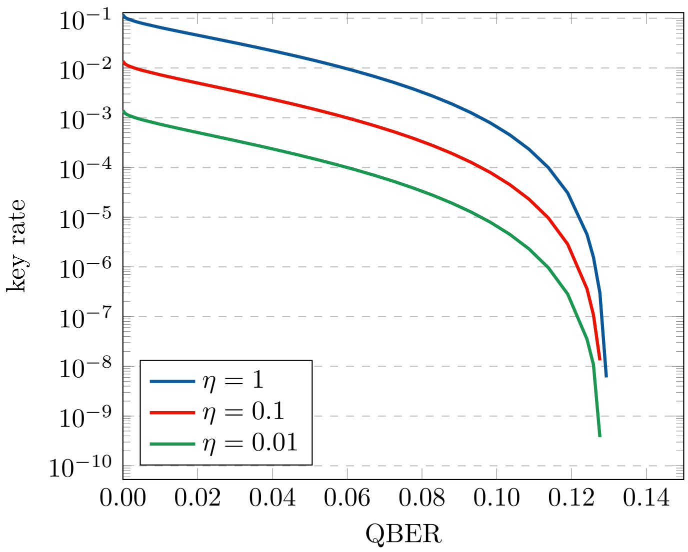


Figure 7: Asymptotic key rate in the limit $n \to \infty$ for different QBERs and transmittances. We choose α to optimize the key rates. Note that a secret key can be distilled up to a threshold $\mathrm{QBER} \approx 13\%$ independent of transmittance.

3.3 Results

Via the strategy sketched in Section 3.2. one can compute asymptotic and finite-size key rates of the relativistic QKD protocol under general adversarial attacks that resemble noise. Recall that the key rate is defined as $r = l/n$, where l is the length of the key and n is the number of rounds. Note that there are two laser pulses (reference and signal) per round. The key rate in time is then at most $r/(2\Delta t)$, based on the timing of our protocol.

To further study the behaviour of our protocol under noise, we consider channel losses through a lossy channel with transmittance $\eta \in [0, 1]$ and a general quantum-bit error rate $\mathrm{QBER} \in [0, 1]$

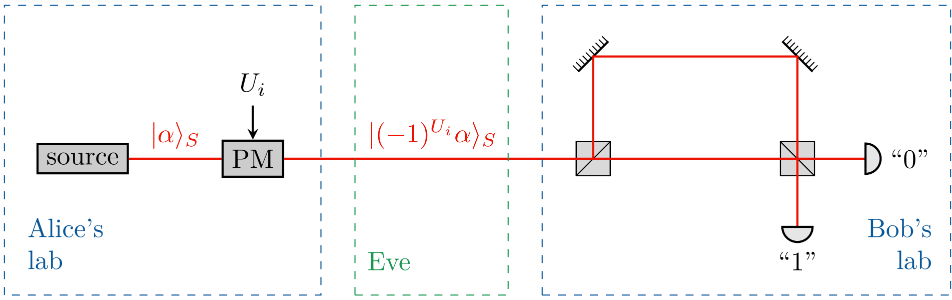


Figure 8: The experimental setup of the DPS QKD protocol. In each round, Alice picks a uniformly random bit U_i and uses a phase modulator (PM) to apply a random phase $(-1)^{U_i}$ to a coherent state $|\alpha\rangle$, producing the state $|(-1)^{U_i}\alpha\rangle$ which she sends to Bob. Bob then measures the relative phases between subsequent states using a Mach-Zehnder interferometer. Alice's raw key bit is given by the relative phase $V_i = U_i \oplus U_{i-1}$.

on the sifted key[4].

Based on (23), (25), (31) and (32) one finds the statistics for an honest implementation of the protocol with noise to be

$$\begin{aligned} \Pr[\perp|\alpha,\eta,\mathrm{QBER}] &= e^{-2\eta|\alpha|^2}, \\ \Pr[\mathrm{err}|\alpha,\eta,\mathrm{QBER}] &= \left(1-e^{-2\eta|\alpha|^2}\right)\cdot \mathrm{QBER}, \\ \Pr[\mathrm{corr}|\alpha,\eta,\mathrm{QBER}] &= \left(1-e^{-2\eta|\alpha|^2}\right)\cdot (1-\mathrm{QBER}), \end{aligned} \tag{33}$$

which we use as the observed statistics under Eve's attack. The respective key rates can be computed numerically (see Appendix E) and are depicted in Figures 6 and 7.

The amplitude α of the laser light is chosen to optimize the asymptotic key rates for a given amount of noise. Typical values are $\alpha \approx 0.45$. We emphasize that there are many places in the finite-size analysis where the bound on the key rate could possibly be tightened. The finite-size plots should therefore be viewed only for illustrational purposes. We have chosen a soundness parameter of $\varepsilon^{\mathrm{snd}} = 4\cdot 10^{-12}$ and a completeness parameter of $\varepsilon^{\mathrm{comp}} = 10^{-2}$.

An interesting observation is the linear scaling of the asymptotic key rate for the entire parameter range. As a consequence, the asymptotic key rate remains positive for arbitrary amounts of losses. This is important for applications between parties at large distances (i.e., for low transmittances) who aim to establish a secret key. We also highlight that the threshold QBER up to which the protocol stays secure is given by QBER $\approx 13\%$ and stays there even for $\eta < 1$ (compare Figure 7).

4 Security of DPS QKD

In the DPS protocol Alice encodes her raw key in the relative phase between subsequent coherent pulses. Bob then uses a Mach-Zehnder interferometer to measure the relative phase of these pulses to reconstruct Alice's key. This setup is sketched in Figure 8. The main motivation for the DPS protocol is that it is both experimentally simple to implement while being resistant against the photon number splitting attack [BBB+92, BLMS00]. The reason for this is that the PNS attack requires Eve to measure the total photon number. This measurement is undetectable by a polarization measurement but does influence the phase coherence (a coherent state is transformed into a mixed state). In this section we present the key steps in proving security of the DPS protocol. The full technical details can be found in Appendices D to F.

Historically, the security of QKD protocols against general attacks (including finite-size effects) was proven using de Finetti type arguments [Ren07, Ren08] or the post-selection technique [CKR09]. These techniques however require that the protocol of study be permutation invariant. Unfortunately, this is not given for the DPS protocol (permuting the rounds completely changes

[4] A more in-depth analysis could include effects like detector dark counts.

Bob's raw key bits and does not merely permute them). Thankfully, the EAT does not have this limitation since it applies to any situation where a sequence of channels are applied to some initial state. In fact, a generalised version of the EAT [MFSR22] has recently been used to prove security of QKD protocols [MR22]. However, the generalised EAT comes with its own restrictions: In order to apply the generalised EAT we need a well-defined sequence of channels. This then leads us to the following condition:

Condition 4.1. *Eve does not signal from round $i+1$ to round i.*

A discussion of this condition can be found in Section 5.1. For the DPS QKD protocol the above condition can be thought of as encompassing both Condition 3.1 and Condition 3.2 of the relativistic protocol.

4.1 Protocol

Protocol 2 provides a formal description of the steps of the DPS QKD protocol sketched in Figure 8. This serves two purposes: firstly, it ensures that the steps of the protocol are clearly laid out. Secondly, it introduces all the registers which will be referenced in the full security proof (see Appendices D and F).

4.2 Reduction to the relativistic protocol

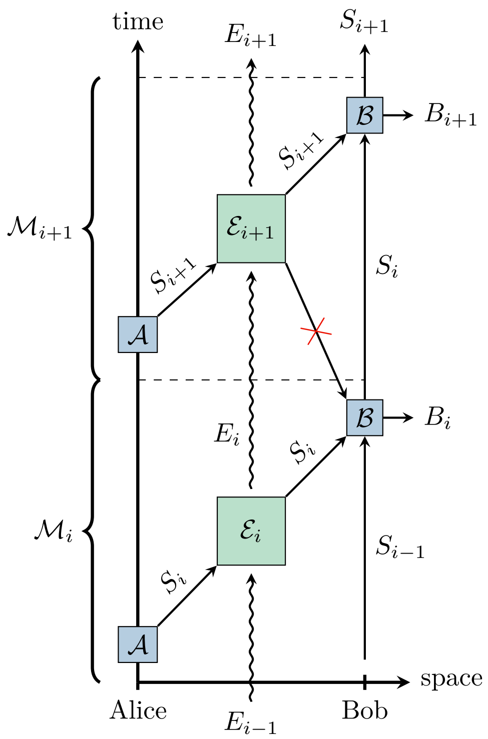


Figure 9: Two rounds of Eve's attack. Alice sends a signal state S_i which gets interrupted by Eve. Eve applies $\mathcal{E}_i$ to this signal state and her previous side information. Bob measures the signal state together with S_{i-1} to produce his key raw bit B_i. Eve's attack cannot signal from S_{i+1} to S_i.

The main idea behind the security proof is to view the DPS QKD protocol as an instance of the relativistic protocol introduced in Section 3. As a consequence we can then recycle the results of the relativistic protocol to prove the security of the DPS QKD protocol. For this we assume that Bob again monitors the measurement times and that Alice and Bob abort if the observed timing suggests that there could be any signalling between neighbouring rounds, i.e., they experimentally enforce Condition 4.1 (see also Section 5.1).

To see the equivalence between the two protocols we model Eve's attack using a sequence of CPTP maps that take as inputs Alice's signal states on S_i and some prior (possibly quantum) side-information E_{i-1} and produces a new state on S_i and some new side-information E_i (see Figure 9). The collective attack bound is then given by $H(A_i|E_iI^iJ^i\tilde{E}_{i-1})$ (the system $\tilde{E}_{i-1}$ is as defined in Definition 2.6). The equivalence between the two protocols becomes clear in Figure 9 on the left: in every round Alice sends a new signal state which gets interrupted by Eve. Due to the sequential condition, Eve cannot hold on to the signal state S_i for too long. In particular, she cannot signal from round $i+1$ back to round i. In Figure 9 this is given due to the fact that it is impossible to signal backwards in time, however, for our purposes a simple space-like separation is sufficient. This non-signalling constraint then allows us to define the channels $\mathcal{M}_i$ for the DPS QKD protocol. Next, we note that in round i Eve may possess a copy of U_{i-1} (formally as part of $\tilde{E}_{i-1}$) and hence $H(A_i|E_iI^iJ^i\tilde{E}_{i-1}) = H(U_i|E_iI^iJ^i\tilde{E}_{i-1})$.

Looking at the situation with the new raw key register, we see that indeed the DPS protocol corresponds to the relativistic protocol with the identification $U_i \leftrightarrow A_i$ (due to symmetry between $|\pm\alpha\rangle$, the value of U_{i-1} does not matter). We also note that we do not assume that Eve has no phase reference, different to some prior work [WTY06]. This is justified by the observation that Eve could always sacrifice a small fraction of rounds at the start of the protocol to learn the phase of Alice's laser to arbitrary precision. Lastly, we note that there are some subtleties when applying the generalised EAT regarding the assignment of the memory system (the upper arm in Bob's Mach-Zehnder interferometer). For a more detailed discussion of this issue we refer to Appendix F.

Protocol 2: Differential phase shift QKD

The protocol is defined in terms of the following parameters, which are chosen before the protocol begins:

$\alpha \in \mathbb{C}$:	amplitude of the laser light
$n \in \mathbb{N}$:	number of protocol rounds
$\gamma \in \mathbb{R}$:	testing frequency
leak_{EC}:	maximum length of error correction
ε_{EC}:	error tolerance during error correction
$f : \mathbb{P}_{\mathcal{C}} \to \mathbb{R}$:	a valid min-tradeoff function
$H_{\text{exp}} \in \mathbb{R}$:	minimum expected single-round entropy
$l \in \mathbb{N}$:	length of the final secret key

---

1. **Initialization:** Alice chooses a bit $U_0 \in \{0, 1\}$ uniformly at random and sends the state $|(-1)^{U_0}\alpha\rangle_S$ to Bob.
2. **Measurement:** For $i \in [n]$:
   - 2.1 Alice chooses a bit $U_i \in \{0, 1\}$ uniformly at random.
   - 2.2 Alice prepares the state $|(-1)^{U_i}\alpha\rangle_S$ and sends it to Bob.
   - 2.3 Alice computes her raw key bit $V_i = U_i \oplus U_{i-1}$.
   - 2.4 Bob receives a state ρ_S and sends it through a Mach-Zehnder interferometer (see Figure 8).
   - 2.5 Bob applies the POVM $\{M_{SR}^{(b)}\}_b$ to the output of the interferometer and records the outcome in the register $B_i \in \{0, 1, \perp\}$.
   - 2.6 If $B_i = \perp$ then Bob transmits $I_i = \perp$ and $I_i = \top$ otherwise.
   - 2.7 Bob chooses $T_i \in \{0, 1\}$ randomly with $\Pr[T_i = 1] = \gamma$. If $T_i = 1$ then Bob transmits $J_i = B_i$ and $J_i = \varnothing$ otherwise.
   - 2.8 Alice waits to enforce Condition 4.1.
3. **Sifting:** For all $i \in [n]$ Alice sets $A_i = V_i$ if $I_i = \top$ and $A_i = \perp$ otherwise.
4. **Error correction:**
   - 4.1 Alice and Bob use their outputs A^n and B^n to perform error correction by communicating at most leak_{EC} number of bits. Bob stores his guess for Alice's key in $\tilde{A}^n$.
   - 4.2 Alice chooses a hash function $h \in \mathcal{F}$ uniformly at random from a family of two-universal hash functions of length $\lceil \log(1/\varepsilon_{\text{EC}}) \rceil$ and applies it to her raw key. She sends the output $h(A^n)$ and her choice of hash function to Bob.
   - 4.3 Bob applies the same hash function to his guess $\tilde{A}^n$. If the two hashes disagree, Alice and Bob abort the protocol.
5. **Parameter estimation:** For all $i \in [n]$ Alice computes $C_i = \text{EV}(A_i, J_i)$. If $f(\text{freq}(C^n)) < H_{\text{exp}}$ they abort the protocol.
6. **Privacy amplification:** Alice and Bob perform privacy amplification on A^n and $\tilde{A}^n$ to obtain raw keys K_A^l and K_B^l.

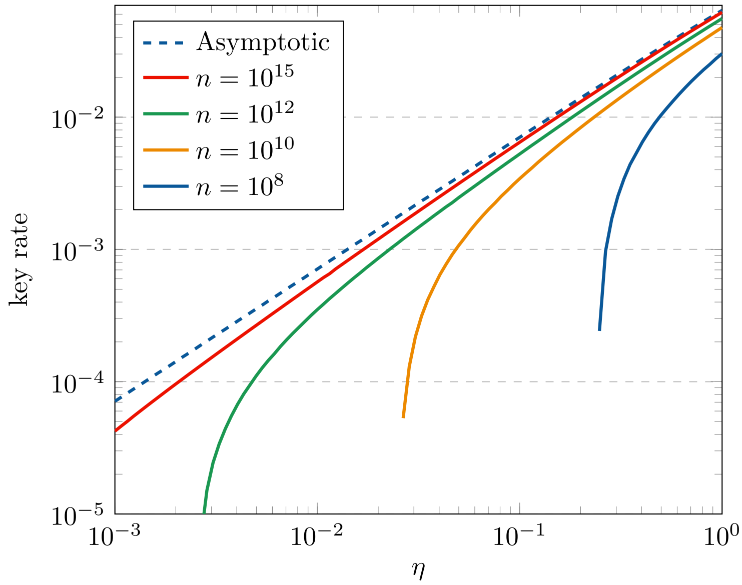


Figure 10: Key rates of the DPS QKD protocol as a function of the transmittance $\eta \in [0, 1]$ for different numbers of rounds n. Loss is the only type of noise that is considered here.

4.3 Results

We now present the results of the security analysis of the DPS QKD protocol. We limit ourselves to loss as the only source of noise in our protocol. Furthermore, we choose a soundness parameter of $\varepsilon^{\mathrm{snd}} = 4 \cdot 10^{-12}$ and a completeness parameter of $\varepsilon^{\mathrm{comp}} = 10^{-2}$. The amplitude α of the laser light is chosen such that it optimizes the asymptotic key rates. Typical values are $\alpha \approx 0.45$. We emphasize that there are many places in the finite-size analysis where the bound on the key rate could be tightened. The finite-size plots in Figure 10 should therefore be viewed only for illustrational purposes.

Similarly to the relativistic protocol we observe a linear scaling of the key rate for the entire parameter range of efficiencies. When compared with the relativistic protocol (Section 3), we observe a modest increase in the asymptotic key rate (for a fair comparison we need to half the key rates of the relativistic protocol since it uses two light pulses per key bit). Other than that, the protocol behaves in the same way as the relativistic protocol. This is expected since, after all, the security proof exploits the equivalence of the two protocols.

5 Discussion

There are a some aspects of the security proofs of the two protocols that deserve special attention. First, we would like to discuss how to satisfy Conditions 3.1 and 3.2 for the relativistic QKD protocol. We will then discuss the impact and enforceability of Condition 4.1 for the DPS QKD protocol. In the third part of the discussion, we relate our work to a known attack on DPS QKD. In particular, we will make good on the promise made in the introduction by showing that it is impossible to reduce the security analysis of DPS QKD to IID attacks without making additional assumptions.

5.1 Sequential conditions

Here we discuss some implications of Conditions 3.1, 3.2 and 4.1. First, we note that, in practice, this condition can be imposed by Alice and Bob if Bob monitors the arrival time of the quantum systems (or equivalently his detection times). For there to be no signalling between the signal and the reference we require that the arrival of the reference in Bob's lab is outside the future light cone of Alice sending the signal state (grey dotted line in Figure 5). From Figure 5 it follows that for the two signals to be spacelike separated we require that

$$t_A^{(i)} + \Delta t + \frac{d}{c} > t_B^{(i)} - \Delta t \iff t_B^{(i)} - t_A^{(i)} < 2\Delta t + \frac{d}{c}. \tag{34}$$

If we assume that Alice and Bob are connected by a fibre of refractive index n and length d, we require that $t_B^{(i)} \geq t_A^{(i)} + nd/c + \Delta t$. Inserting this into (34) provides a lower bound on the time delay Δt that is required for the protocol to not abort:

$$\Delta t > (n-1)\frac{d}{c}. \tag{35}$$

One way to think about these conditions is that (34) is required for the soundness of the protocol, whereas (35) is required for completeness (note that (34) does not make any assumptions about the refractive index of the fibre). To enforce Condition 3.2 we choose $t_A^{(i+1)} = t_A^{(i)} + 2\Delta t$. Combining this with (34) we get that $t_A^{(i+1)} + d/c = t_A^{(i)} + 2\Delta t + d/c > t_B^{(i)}$, which says that the reference from round $i+1$ cannot signal to round i.

Enforcing these conditions requires Alice and Bob to share a pair of synchronized clocks. This is a reasonable request, as synchronized clocks are already needed in the DPS protocol so that Bob knows which of his detections corresponds to which of Alice's key bits. Enforcing the sequential condition, however, imposes a minimal time delay between signals. This has two consequences: firstly, it limits the repetition rate of protocol rounds. Secondly, this might introduce additional noise (due to the longer arm in Bob's interferometer) and requires better phase coherence of Alice's laser. The first problem can be fixed if Bob measures the relative phase between more temporally distant pulses instead of performing interferometry on neighbouring pulses. Effectively, this corresponds to running many copies of the DPS QKD protocol in parallel. Lastly, we note that this non-signalling assumption is also implicitly made when considering many restricted sets of attacks such as individual attacks [WTY06] or collective attacks (for which the security of DPS QKD has not been established before this paper). Therefore, the security statement presented in this paper is stronger than that of prior work.

5.2 Comparison with upper bounds

Next, we discuss the relation of our work to the upper bounds on DPS derived in [CTM08]. In this work, the authors discovered an attack where Eve performs an intercept-resend attack but only resends the pulses if she gets a sufficient number of consecutive conclusive outcomes. This allows Eve to exploit losses to reduce the detectable effects (i.e., the QBER) of her attack. This attack constitutes an entanglement-breaking channel, and as a result, the authors found a parameter regime in which DPS QKD is insecure. Note, however, that this attack violates Condition 4.1; hence, we do not necessarily expect that this upper bound holds for our security claim. In fact, using our methods, we can derive a parameter regime for which the DPS QKD protocol is secure, as shown in Figure 11. We observe that there exists a region where the two regimes overlap, i.e., the security claims disagree. This shows that the attack in [CTM08] is stronger than any collective attack since those are covered by our security proof. Furthermore, the converse also holds: any attempt to reduce the security of DPS QKD to collective attacks necessarily requires additional assumptions (since in such a reduction, you need to exclude the type of attack reported in [CTM08]).

6 Conclusion and outlook

In this work, we proved the security of DPS QKD against general attacks by exploiting relativistic constraints. In particular, we use relativity to enforce a non-signalling constraint on the eavesdropper, i.e., the eavesdropper can only signal from previous to future rounds but not in the other direction. This strategy then allows us to reduce the DPS QKD protocol to a relativistic protocol. We then applied methods from quantum information theory, relativity, and quantum optics to prove the security of this relativistic protocol. The particular methods of interest are the

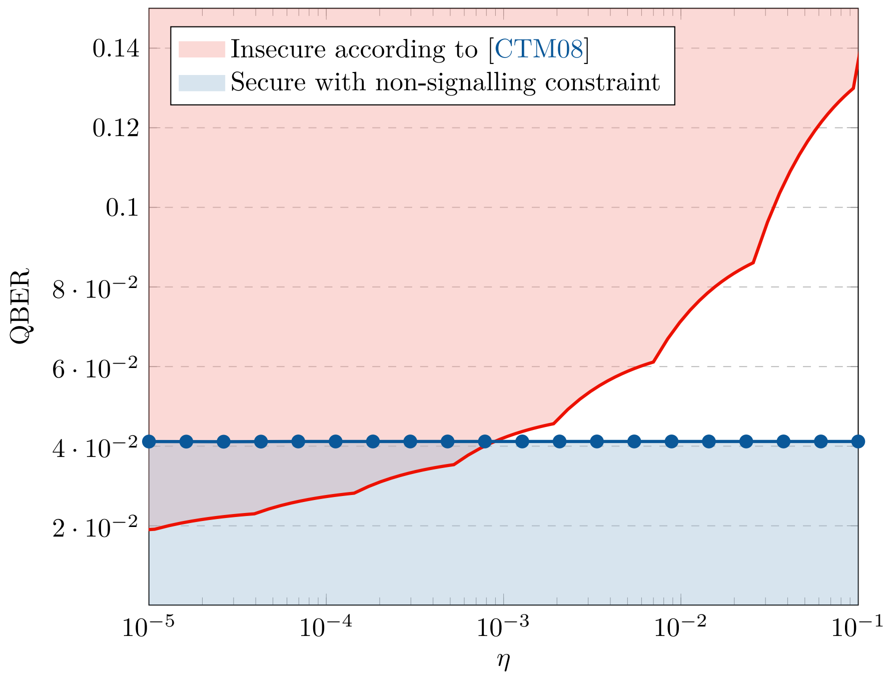


Figure 11: Comparison between noise thresholds derived in [CTM08] and the ones derived in this paper. The red region is insecure according to [CTM08], whereas the blue region is secure according to our security proof. There is a non-empty overlap of the two regions. Both curves were computed at $\alpha = 0.4$ with zero detector dead time.

generalised entropy accumulation theorem (discussed in Section 2.1), a formal way of treating non-signalling (discussed in Section 2.2), and the squashing technique (discussed in Section 2.3). We observed linear scaling of the secret key rate as a function of the detection efficiency, which is the best we can hope for [TGW14, PLOB17]. This observation and the practicality of implementing DPS QKD make the protocol attractive for real-world implementations. Naturally, one may ask whether it would be possible to prove the security of the DPS QKD protocol against general attacks without the non-signalling constraint. By comparing our results with upper-bounds for DPS QKD derived in [CTM08], we observed that our security statement can violate these bounds (which do not satisfy the non-signalling condition). Since any collective attack fulfils the non-signalling property, it follows that it is impossible to reduce the security analysis of the DPS QKD protocol to collective attacks without additional assumptions. Since many proof techniques proceed by reducing security against general attacks to the security against collective attacks, they cannot be applied to DPS QKD without making additional assumptions (such as the non-signalling assumption). Furthermore, even if one were to prove the security of DPS without the non-signalling assumption, this would incur a loss of secret key rate and hence could limit the practicality of the protocol.

A natural question to ask is whether similar techniques could be applied to other distributed phase reference protocols such as the coherent one-way protocol [SBG⁺05]. Here, we note that the trick of exploiting the non-signalling condition to cast the protocol into a relativistic protocol works quite generally. The main challenge when trying to apply the techniques to other protocols lies in finding a squashing map which is itself non-signalling. In general, this is a difficult problem which we leave for future work.

The security analysis presented in this paper could be improved in many places. Firstly, we assume here that both detectors have equal efficiency, which is required to be able to push all losses from the detectors into the channel. This allows us to consider ideal detectors when applying the squashing technique. Recently, the scenario with unequal detection efficiencies has been studied in [ZCW⁺21]. However, it is not obvious how their technique could be applied to our protocols, since we require the "squashed" protocol to retain the relativistic constraint on Eve's attack. Similar problems arise when trying to apply different dimension reduction techniques such as the one presented in [UvHLL21] to our protocols. Furthermore, the same caveats of typical QKD security analyses apply to this paper: If the implementation does not match with the theoretical model of the devices, the protocol could become insecure. One example of such a limitation are imperfections in the source, which we do not consider here. Lastly, there are some places where the security analysis could be tightened. To carry out the security proof of DPS QKD, we need to give Eve more power than she has in practice (see Appendix F), which is required to put the protocol into a form that allows for the application of the generalised EAT. This requirement, however, seems rather artificial; hence, we can hope that it is possible to avoid it. Unfortunately, it seems that reducing Eve's area of influence would also prohibit one from finding (an obvious) squashing map for the DPS QKD protocol.

Finally, there are several other directions that can be considered for the relativistic QKD protocol. Compared to other protocols, the relativistic QKD protocol has quite a low threshold QBER. To remedy this, one could try to allow Alice to choose different bases to encodce her key bit. This is motivated by the fact that the BB84 and six-state protocols can tolerate a higher QBER than the B92 protocol and so we might hope to observe similar effects here. Similarly, there could be opportunities for improved key rates by considering a phase-randomized version of the relativistic protocol. This is motivated by the observation that some other protocols benefit from phase randomization [LP07].

Code availability

The code and data necessary to reproduce the results of this paper are available at https://gitlab.phys.ethz.ch/martisan/dps-key-rates.

Acknowledgements

We thank Tony Metger, Renato Renner, and Ernest Tan for helpful comments and discussions. This work was supported by the Air Force Office of Scientific Research (AFOSR), grant No. FA9550-19-1-0202, the QuantERA project eDICT, the National Centre of Competence in Research SwissMAP, and the Quantum Center at ETH Zurich. VV is supported by an ETH Postdoctoral Fellowship and acknowledges financial support from the Swiss National Science Foundation (SNSF) Grant Number 200021_188541.

References

[AHN+22] Mateus Araújo, Marcus Huber, Miguel Navascués, Matej Pivoluska, and Armin Tavakoli. Quantum key distribution rates from semidefinite programming, 2022. arXiv:2211.05725.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India*, pages 175–179, 1984. arXiv:2003.06557.

[BBB+92] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992, 10.1007/bf00191318.

[BLMS00] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85:1330–1333, 2000, 10.1103/PhysRevLett.85.1330. arXiv:quant-ph/9911054.

[BML08] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Physical Review Letters*, 101(9), 2008, 10.1103/physrevlett.101.093601. arXiv:0804.3082.

[CKR09] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2), 2009, 10.1103/physrevlett.102.020504. arXiv:0809.3019.

[CTM08] Marcos Curty, Kiyoshi Tamaki, and Tobias Moroder. Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks. *Physical Review A*, 77(5), 2008, 10.1103/physreva.77.052321. arXiv:0803.1473.

[CTMG09] Marcos Curty, Kiyoshi Tamaki, Tobias Moroder, and Hipólito Gómez-Sousa. Upper bounds for the security of differential-phase-shift quantum key distribution with weak coherent states. In *AIP Conference Proceedings*. AIP, 2009, arXiv:0806.0858. 10.1063/1.3131346.

[CZLL07] Marcos Curty, Lucy Liuxuan Zhang, Hoi-Kwong Lo, and Norbert Lütkenhaus. Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. *Quantum Info. Comput.*, 7(7):665–688, 2007. arXiv:quant-ph/0609094.

[DF19] Frederic Dupuis and Omar Fawzi. Entropy accumulation with improved second-order term. *IEEE Transactions on Information Theory*, 65(11):7596–7612, 2019, 10.1109/tit.2019.2929564. arXiv:1805.11652.

[DFR20] Frédéric Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. *Communications in Mathematical Physics*, 379(3):867–913, 2020, 10.1007/s00220-020-03839-5. arXiv:1607.01796.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991, 10.1103/physrevlett.67.661.

[GBN+14] Oleg Gittsovich, Normand J. Beaudry, Varun Narasimhachar, Ruben Romero Alvarez, Tobias Moroder, and Norbert Lütkenhaus. Squashing model for detectors and applications to quantum-key-distribution protocols. *Physical Review A*, 89(1), 2014, 10.1103/physreva.89.012325. arXiv:1310.5059.

[GLLP02] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information & Computation*, 4(5):325–360, 2002. arXiv:quant-ph/0212066.

[GLvH+22] Ian George, Jie Lin, Thomas van Himbeeck, Kun Fang, and Norbert Lütkenhaus. Finite-key analysis of quantum key distribution with characterized devices using entropy accumulation. 2022. arXiv:2203.06554.

[Hol11] A. S. Holevo. The Choi–Jamiolkowski forms of quantum gaussian channels. *Journal of Mathematical Physics*, 52(4):042202, apr 2011, 10.1063/1.3581879.

[IWY02] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential phase shift quantum key distribution. *Physical Review Letters*, 89(3):037902, 2002, 10.1103/physrevlett.89.037902.

[KRKM18] K. S. Kravtsov, I. V. Radchenko, S. P. Kulik, and S. N. Molotkov. Relativistic quantum key distribution system with one-way quantum communication. *Scientific Reports*, 8(1), 2018, 10.1038/s41598-018-24533-6. arXiv:1801.02896.

[LP07] Hoi-Kwong Lo and John Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Information & Computation*, 7(5):431–458, 2007. arXiv:quant-ph/0610203.

[MFSR22] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. Generalised entropy accumulation. 2022. arXiv:2203.04989.

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In *The Second Symposium on Innovations in Computer Science, ICS 2011*, pages 1–21. Tsinghua University Press, 2011. `https://crypto.ethz.ch/publications/MauRen11.html`.

[MR22] Tony Metger and Renato Renner. Security of quantum key distribution from generalised entropy accumulation. 2022. arXiv:2203.04993.

[MSK+17] Akihiro Mizutani, Toshihiko Sasaki, Go Kato, Yuki Takeuchi, and Kiyoshi Tamaki. Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity. *Quantum Science and Technology*, 3(1):014003, 2017, 10.1088/2058-9565/aa8705. arXiv:1705.00171.

[OVB22] Nick Ormrod, Augustin Vanrietvelde, and Jonathan Barrett. Causal structure in the presence of sectorial constraints, with application to the quantum switch, 2022. arXiv:2204.10273.

[PLOB17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1), 2017, 10.1038/ncomms15043. arXiv:1510.08863.

[PR22] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, 2022, 10.1103/revmodphys.94.025008. arXiv:2102.00021.

[Ren07] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007, 10.1038/nphys684. arXiv:quant-ph/0703069.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127, 2008, 10.1142/s0219749908003256. arXiv:quant-ph/0512258.

[RKKM14] Igor V. Radchenko, Konstantin S. Kravtsov, Sergei P. Kulik, and Sergei N. Molotkov. Relativistic quantum cryptography. *Laser Physics Letters*, 11(6):065203, 2014, 10.1088/1612-2011/11/6/065203. arXiv:1403.3122.

[RR12] Joseph M. Renes and Renato Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58(3):1985–1991, 2012, 10.1109/TIT.2011.2177589. arXiv:1008.0452.

[SBG+05] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005, 10.1063/1.2126792. arXiv:quant-ph/0506097.

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5(1), 2014, 10.1038/ncomms6235. arXiv:1504.06390.

[TKK12] Kiyoshi Tamaki, Masato Koashi, and Go Kato. Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization, 2012. arXiv:1208.1995.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017, 10.22331/q-2017-07-14-14. arXiv:1506.08458.

[Tom16] Marco Tomamichel. Quantum information processing with finite resources. *SpringerBriefs in Mathematical Physics*, 2016, 10.1007/978-3-319-21891-5. arXiv:1504.00233.

[TSB+20] Ernest Y.-Z. Tan, Pavel Sekatski, Jean-Daniel Bancal, René Schwonnek, Renato Renner, Nicolas Sangouard, and Charles C.-W. Lim. Improved DIQKD protocols with finite-size analysis, 2020. arXiv:2012.08714.

[TT08] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Physical Review A*, 78:032302, 2008, 10.1103/PhysRevA.78.032302.

[UvHLL21] Twesh Upadhyaya, Thomas van Himbeeck, Jie Lin, and Norbert Lütkenhaus. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. *Physical Review X Quantum*, 2(2):020325, 2021, 10.1103/prxquantum.2.020325. arXiv:2101.05799.

[WTY06] Edo Waks, Hiroki Takesue, and Yoshihisa Yamamoto. Security of differential-phase-shift quantum key distribution against individual attacks. *Physical Review A*, 73(1), 2006, 10.1103/physreva.73.012344. arXiv:quant-ph/0508112.

[WTY09] Kai Wen, Kiyoshi Tamaki, and Yoshihisa Yamamoto. Unconditional security of single-photon differential phase shift quantum key distribution. *Physical Review Letters*, 103(17), 2009, 10.1103/physrevlett.103.170503. arXiv:0806.2684.

[ZCW+21] Yanbao Zhang, Patrick J. Coles, Adam Winick, Jie Lin, and Norbert Lütkenhaus. Security proof of practical quantum key distribution with detection-efficiency mismatch. *Physical Review Research*, 3:013076, 2021, 10.1103/PhysRevResearch.3.013076. arXiv:2004.04383.

Appendices

A Technical definitions

Definition A.1. Let $\rho_{XA} \in \mathcal{S}(XA)$ be a classical-quantum state, i.e., ρ_{XA} can be written in the form

$$\rho_{XA} = \sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_X \otimes \rho_A^{[x]}, \tag{36}$$

where $\mathcal{X}$ is some alphabet, $p(x)$ is a probability distribution over $\mathcal{X}$ and $\rho_A^{[x]} \in \mathcal{S}(A)$. For an event $\Omega \subseteq \mathcal{X}$ we define the following states: The subnormalised state $(\rho_{\wedge\Omega})_{XA}$ conditioned on Ω,

$$(\rho_{\wedge\Omega})_{XA} = \sum_{x\in\Omega} p(x)|x\rangle\langle x|_X \otimes \rho_A^{[x]}, \tag{37}$$

and the normalised state $(\rho_{|\Omega})_{XA}$ conditioned on Ω,

$$(\rho_{|\Omega})_{XA} = \frac{(\rho_{\wedge\Omega})_{XA}}{\rho[\Omega]}, \quad \text{where } \rho[\Omega] = \mathrm{tr}[(\rho_{\wedge\Omega})_{XA}] = \sum_{x\in\Omega} p(x). \tag{38}$$

Definition A.2. (von Neumann entropy) Let A and B be two quantum systems and $\rho_A \in \mathcal{S}(A)$ be a state. The *entropy* of ρ_A is defined as

$$H(A)_\rho = -\,\mathrm{tr}[\rho_A \log \rho_A]. \tag{39}$$

For a state $\rho_{AB} \in \mathcal{S}(AB)$ we define the *conditional entropy* as

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho, \tag{40}$$

where $H(B)_\rho$ is the entropy evaluated on $\rho_B = \mathrm{tr}_A\,\rho_{AB}$.

Definition A.3. (Generalised fidelity) Let $\rho_A, \sigma_A \in \mathcal{S}_\leq(A)$ be two subnormalised states. Define the *fidelity* by

$$F(\rho_A, \sigma_A) = \left(\mathrm{tr}\,|\sqrt{\rho_A}\sqrt{\sigma_A}| + \sqrt{(1-\mathrm{tr}\,\rho_A)(1-\mathrm{tr}\,\sigma_A)}\right)^2.$$

Definition A.4. (Purified distance) Let $\rho_A, \sigma_A \in \mathcal{S}_\leq(A)$, define the *purified distance* as

$$P(\rho_A, \sigma_A) = \sqrt{1 - F(\rho_A, \sigma_A)}.$$

Definition A.5. (ε-ball) Let $\varepsilon > 0$ and $\rho_A \in \mathcal{S}_\leq(A)$, we define the *$\varepsilon$-ball around ρ_A* as

$$\mathcal{B}^\varepsilon(\rho_A) = \{\sigma_A \in \mathcal{S}_\leq(A) \mid P(\rho_A, \sigma_A) < \varepsilon\}, \tag{41}$$

where $P(\rho_A, \sigma_A)$ denotes the purified distance (Definition A.4).

Definition A.6. (Smooth min and max-entropies) Let $\varepsilon > 0$ and $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$ be a quantum state, then the *smooth min-entropy* is defined as

$$H^{\varepsilon}_{\min}(A|B)_{\rho} = -\log \inf_{\tilde{\rho}_{AB}} \inf_{\sigma_B} \left\| \tilde{\rho}_{AB}^{1/2} \sigma_B^{-1/2} \right\|_{\infty}^{2}, \tag{42}$$

where the optimizations are over all $\tilde{\rho}_{AB} \in B^{\varepsilon}(\rho_{AB})$ and $\sigma_B \in \mathcal{S}(B)$. Similarly we define the *smooth max-entropy* as

$$H^{\varepsilon}_{\max}(A|B)_{\rho} = \log \inf_{\tilde{\rho}_{AB}} \sup_{\sigma_B} \left\| \tilde{\rho}_{AB}^{1/2} \sigma_B^{1/2} \right\|_{1}^{2}, \tag{43}$$

where $\tilde{\rho}_{AB}$ and σ_B are as before.

B Proof of Lemma 2.11

To establish the equivalence between Definition 2.10 of signalling and the condition on the Choi state given in (18), the intermediate condition given by (16) will be useful. As this condition is shown to be equivalent to Definition 2.10 in [OVB22], establishing the equivalence between (16) and (18) would conclude the proof. We repeat (16) below for convenience, it states that S does not signal to R' in the CPTP map $\mathcal{E}_{SR\to S'R'}$ if there exists a CPTP map $\mathcal{E}_{R\to R'}$ such that

$$\operatorname{tr}_{S'} \circ \mathcal{E}_{SR\to S'R'} = \operatorname{tr}_S \otimes \mathcal{E}_{R\to R'}. \tag{44}$$

We use the above equation to establish the necessary direction, a diagrammatic version of the proof of this part is given in Figure 12.

$$\begin{aligned}
\operatorname{tr}_{S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})] &= \operatorname{tr}_{S'}[(\mathbb{1}_{\bar{S}\bar{R}} \otimes \mathcal{E}_{SR\to S'R'})|\Phi\rangle\langle\Phi|_{\bar{S}\bar{R}SR}] \\
&= (\mathbb{1}_{\bar{S}\bar{R}} \otimes \operatorname{tr}_{S'} \circ \mathcal{E}_{SR\to S'R'})|\Phi\rangle\langle\Phi|_{\bar{S}\bar{R}SR} \\
&= (\mathbb{1}_{\bar{S}\bar{R}} \otimes \operatorname{tr}_S \otimes \mathcal{E}_{R\to R'})|\Phi\rangle\langle\Phi|_{\bar{S}\bar{R}SR} \\
&= \operatorname{tr}_S[|\Phi\rangle\langle\Phi|_{\bar{S}S}] \otimes (\mathbb{1}_R \otimes \mathcal{E}_{R\to R'})|\Phi\rangle\langle\Phi|_{\bar{R}R} \\
&= \frac{\mathbb{1}_{\bar{S}}}{d_{\bar{S}}} \otimes (\mathbb{1}_R \otimes \mathcal{E}_{R\to R'})|\Phi\rangle\langle\Phi|_{\bar{R}R} \\
&= \frac{\mathbb{1}_{\bar{S}}}{d_{\bar{S}}} \otimes \operatorname{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})].
\end{aligned} \tag{45}$$

In going from the third to the fourth step in the above, we have used the fact that $|\Phi\rangle_{\bar{S}\bar{R}SR} = \sum_{i,j} |ijij\rangle_{\bar{S}\bar{R}S'R'} \equiv \sum_i |ii\rangle_{\bar{S}S} \otimes \sum_j |jj\rangle_{\bar{R}R} = |\Phi\rangle_{\bar{S}S} \otimes |\Phi\rangle_{\bar{R}R}$.
For the sufficiency part, we use the gate teleportation version of the inverse Choi isomophism, given as follows, keeping in mind that $\mathcal{C}(\mathcal{E}_{SR\to S'R'}) \in \mathcal{S}(\bar{S}\bar{R}S'R')$.

$$\mathcal{E}_{SR\to S'R'}(\rho_{SR}) = \langle\Phi|_{\bar{S}\bar{R}SR}\big(\rho_{SR} \otimes \mathcal{C}(\mathcal{E}_{SR\to S'R'})\big)|\Phi\rangle_{\bar{S}\bar{R}SR}. \tag{46}$$

Then, employing (18), we have the following. A diagrammatic version of the proof of the sufficiency part is given in Figure 13.

$$\begin{aligned}
\operatorname{tr}_{S'}[\mathcal{E}_{SR\to S'R'}(\rho_{SR})] &= \langle\Phi|_{\bar{S}\bar{R}SR}\big(\rho_{SR} \otimes \operatorname{tr}_{S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})]\big)|\Phi\rangle_{\bar{S}\bar{R}SR} \\
&= \langle\Phi|_{\bar{S}\bar{R}SR}\big(\rho_{SR} \otimes \frac{\mathbb{1}_{\bar{S}}}{d_{\bar{S}}} \otimes \operatorname{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})]\big)|\Phi\rangle_{\bar{S}\bar{R}SR}.
\end{aligned} \tag{47}$$

Now, notice that $\operatorname{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})] \in \mathcal{S}(\bar{R}R')$ can be regarded as the Choi state of some quantum CPTP map $\mathcal{E}_{R\to R'} : \mathcal{S}(R) \to \mathcal{S}(R')$, i.e., $\operatorname{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})] = \mathcal{C}(\mathcal{E}_{R\to R'})$. This is because of the fact that complete positivity of the map is equivalent to positivity of the Choi state and the trace preserving property of the map is equivalent to the normalisation of the Choi state. $\mathcal{C}(\mathcal{E}_{SR\to S'R'})$ being the Choi state of a CPTP map ensures that $\operatorname{tr}_{\bar{S}S'}[\mathcal{C}(\mathcal{E}_{SR\to S'R'})]$ too would be the Choi state of a CPTP map between the appropriately reduced spaces. Noticing that the maximally mixed state is the Choi state of the trace map, i.e., $\mathcal{C}(\operatorname{tr}_S) = \frac{\mathbb{1}_S}{d_S}$, we have

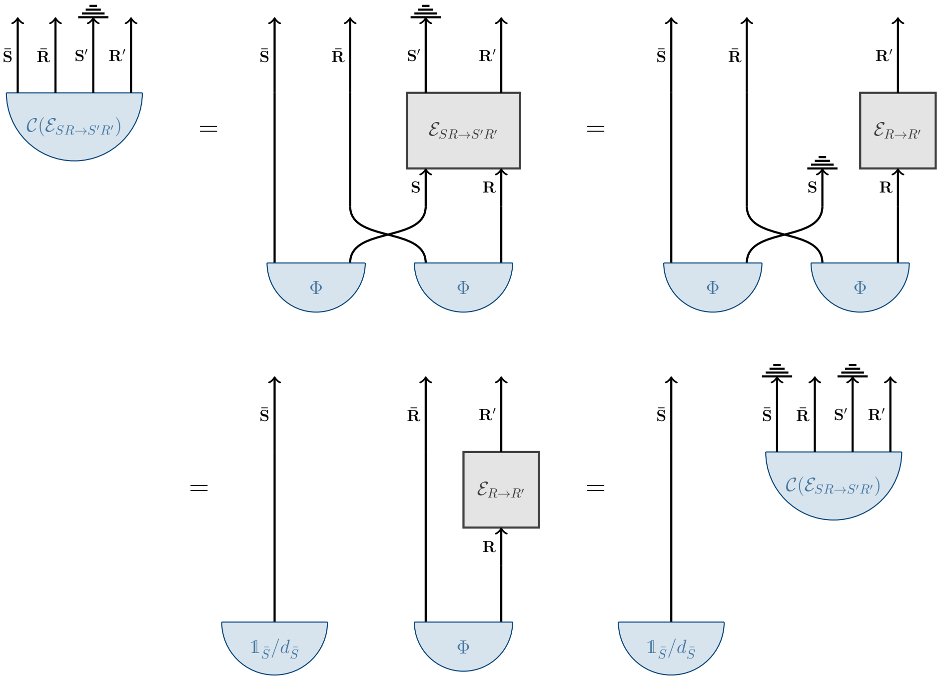


Figure 12: Diagrammatic proof of the necessary part of Lemma 2.11 (cf. (45)).

$$
\begin{aligned}
\operatorname{tr}_{S'}[\mathcal{E}_{SR\to S'R'}(\rho_{SR})] &= \langle\Phi|_{\bar{S}\bar{R}SR}\big(\rho_{SR}\otimes\frac{\mathbb{1}_{\bar{S}}}{d_{\bar{S}}}\otimes\mathcal{C}(\mathcal{E}_{R\to R'})\big)|\Phi\rangle_{\bar{S}\bar{R}SR} \\
&= \langle\Phi|_{\bar{S}\bar{R}SR}\big(\rho_{SR}\otimes\mathcal{C}(\operatorname{tr}_S\otimes\mathcal{E}_{R\to R'})\big)|\Phi\rangle_{\bar{S}\bar{R}SR} \\
&= \operatorname{tr}_S\otimes\mathcal{E}_{R\to R'}(\rho_{SR}).
\end{aligned}
\tag{48}
$$

This establishes the result as it holds for all input states ρ_{SR}.

C Proof of Theorem 2.13

In this proof we assume that, unless explicitly stated otherwise, sums over N only include terms $N\geq 1$. Similarly we assume that sums over k (l) only include odd (even) terms $\leq N$. We start by rewriting the expressions for $M^{(0)}$ and $M^{(1)}$ in (25) as

$$
M^{(0,1)} = \frac{1}{2}\mathbb{1} - \frac{1}{2}|0,0\rangle\langle 0,0| \pm \frac{1}{2}\sum_{N=1}^{\infty}\left(|N,0\rangle\langle N,0|_{AB} - |0,N\rangle\langle 0,N|_{AB}\right). \tag{49}
$$

Using (20) we can now rewrite the states $|N,0\rangle_{AB}$ and $|0,N\rangle_{AB}$ after the BS in terms of the states on the systems SR before the BS to obtain:

$$
\begin{aligned}
|N,0\rangle_{AB} &= \frac{1}{\sqrt{N!}}\left(a_A^\dagger\right)^N|0,0\rangle = \frac{1}{\sqrt{2^N}}\sum_{m=0}^{N}\sqrt{\binom{N}{m}}|N-m,m\rangle_{SR}, \\
|0,N\rangle_{AB} &= \frac{1}{\sqrt{N!}}\left(a_B^\dagger\right)^N|0,0\rangle = \frac{1}{\sqrt{2^N}}\sum_{m=0}^{N}\sqrt{\binom{N}{m}}(-1)^m|N-m,m\rangle_{SR},
\end{aligned}
\tag{50}
$$

Inserting this into the expressions of (49) yields:

$$
\begin{aligned}
M^{(0,1)} &= \frac{1}{2}\mathbb{1} - \frac{1}{2}|0,0\rangle\langle 0,0|_{SR} \\
&\pm \frac{1}{2}\sum_{N}^{\infty}\sum_{m,n=0}^{N}\frac{1}{2^N}\sqrt{\binom{N}{m}}\sqrt{\binom{N}{n}}\left(1-(-1)^{m+n}\right)|N-m,m\rangle\langle N-n,n|_{SR}.
\end{aligned}
\tag{51}
$$

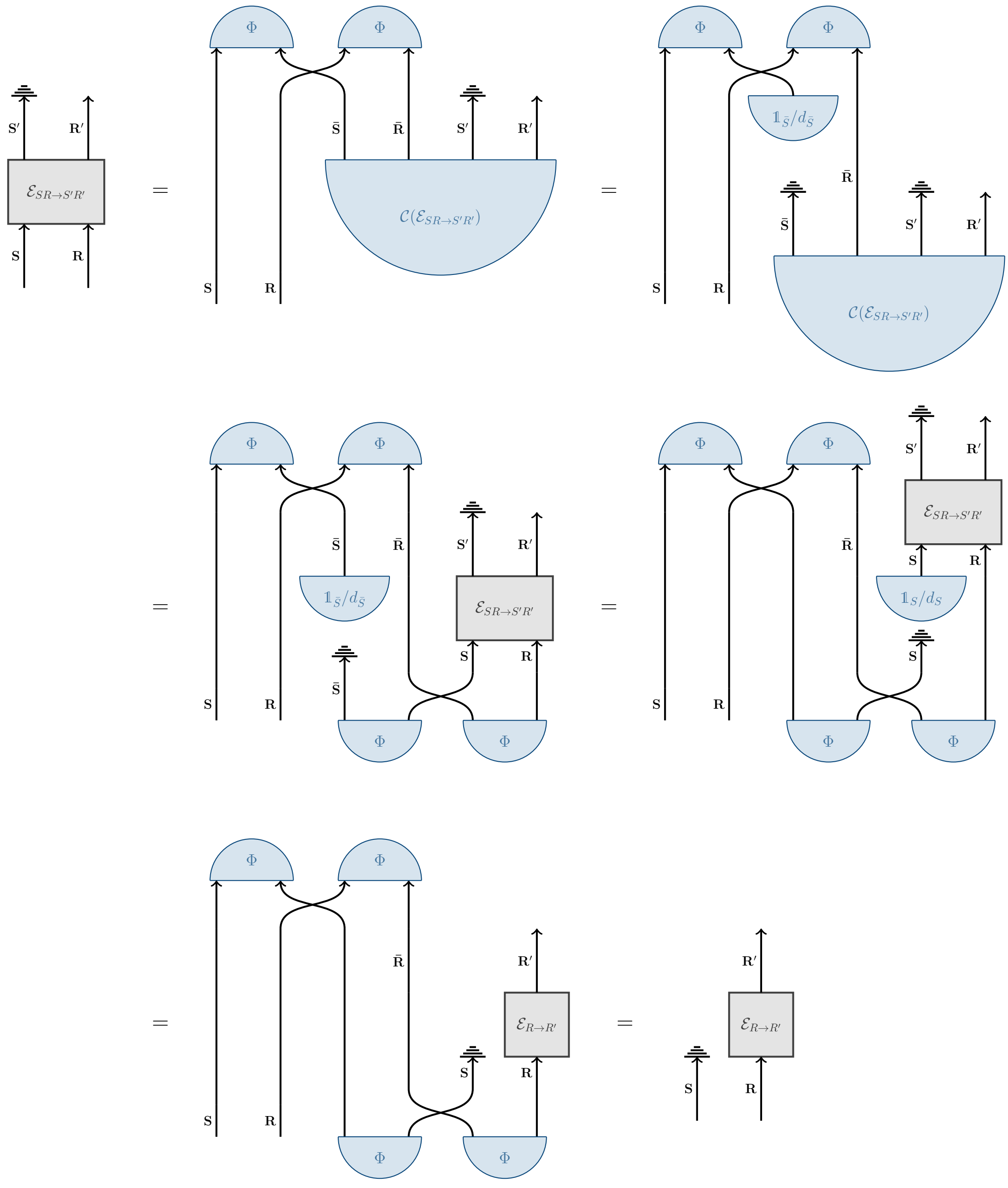


Figure 13: Diagrammatic proof of the sufficient part of Lemma 2.11 (cf. (47)). Here, the upright semi-circles labelled Φ physically represent a post-selection on the outcome corresponding to the Bell state Φ, following a joint measurement in the Bell basis on the associated systems. Mathematically, they correspond to projectors on to the Bell state Φ.

In a similar fashion we can write:

$$N^{(0,1)} = \frac{1}{2}\mathbb{1} - \frac{1}{2}|00\rangle\langle 00| \pm \frac{1}{2}\big(|\phi^+\rangle\langle\phi^+| - |\phi^-\rangle\langle\phi^-|\big). \tag{52}$$

We are now ready to prove the theorem. We need to show three statements:

1. Λ is trace-preserving, i.e. $\big(K^{(0)}\big)^* K^{(0)} + \sum_{N,k,l}(K_{k,l}^{(N)})^* K_{k,l}^{(N)} = \mathbb{1}$.
2. Λ preserves the statistics, i.e. $\operatorname{tr}\Big[M_{SR}^{(v)}\rho_{SR}\Big] = \operatorname{tr}\Big[N_{S'R'}^{(v)}\Lambda[\rho_{SR}]\Big]$.
3. Λ is non-signalling from S to R', i.e. $\operatorname{tr}_{S'}\Lambda[\rho_{SR}]$ only depends on ρ_R.

We proceed in the order outlined above:

1. We have

$$\begin{aligned}&\Big(K^{(0)}\Big)^* K^{(0)} + \sum_{N,k,l}\Big(K_{k,l}^{(N)}\Big)^* K_{k,l}^{(N)}\\ =&|0,0\rangle\langle 0,0| + \sum_{N,k,l}\frac{2}{2^N}\left(\binom{N}{l}|N-k,k\rangle\langle N-k,k| + \binom{N}{k}|N-l,l\rangle\langle N-l,l|\right).\end{aligned} \tag{53}$$

   We can now use the formula $\sum_l \binom{N}{l} = \sum_k \binom{N}{k} = 2^{N-1}$ to simplify the expression above:

$$\begin{aligned}&|0,0\rangle\langle 0,0| + \sum_{N,k}|N-k,k\rangle\langle N-k,k| + \sum_{N,l}|N-l,l\rangle\langle N-l,l|\\ =&\sum_{N=0}^{\infty}\sum_{m=0}^{N}|N-m,m\rangle\langle N-m,m| = \sum_{m,n}|n,m\rangle\langle n,m| = \mathbb{1}.\end{aligned} \tag{54}$$

2. We see directly that $\operatorname{tr}\Big[M_{SR}^{(\perp)}\rho_{SR}\Big] = \operatorname{tr}\Big[N_{S'R'}^{(\perp)}\Lambda[\rho_{SR}]\Big]$. Comparing the expressions in (51) with those in (52) we see that for the two remaining measurement outcomes it is sufficient to show that the third term (after the $\pm$) is preserved between (51) and (52). Hence we compute:

$$\begin{aligned}&\langle\phi^+|\Lambda[\rho_{SR}]|\phi^+\rangle - \langle\phi^-|\Lambda[\rho_{SR}]|\phi^-\rangle = \langle 01|\Lambda[\rho_{SR}]|10\rangle + \langle 10|\Lambda[\rho_{SR}]|01\rangle\\ =&\sum_{N,k,l}\frac{2}{2^N}\sqrt{\binom{N}{l}}\sqrt{\binom{N}{k}}(\langle N-k,k|\rho_{SR}|N-l,l\rangle + \langle N-l,l|\rho_{SR}|N-k,k\rangle)\\ =&\sum_{N}^{\infty}\sum_{m,n=0}^{N}\frac{1}{2^N}\sqrt{\binom{N}{m}}\sqrt{\binom{N}{n}}(1-(-1)^{m+n})\langle N-n,n|\rho_{SR}|N-m,m\rangle,\end{aligned} \tag{55}$$

   as desired.

3. We compute

$$\begin{aligned}\operatorname{tr}_{S'}\Lambda[\rho_{SR}] &= |0\rangle\langle 0|_{R'}\langle 0,0|\rho_{SR}|0,0\rangle + |1\rangle\langle 1|_{R'}\sum_{N,k,l}\frac{2}{2^N}\binom{N}{l}\langle N-k,k|\rho_{SR}|N-k,k\rangle\\ &+ |0\rangle\langle 0|_{R'}\sum_{N,k,l}\frac{2}{2^N}\binom{N}{k}\langle N-l,l|\rho_{SR}|N-l,l\rangle\\ &= |1\rangle\langle 1|_{R'}\sum_{N,k}\langle N-k,k|\rho_{SR}|N-k,k\rangle\\ &+ |0\rangle\langle 0|_{R'}\left(\langle 0,0|\rho_{SR}|0,0\rangle + \sum_{N,l}\langle N-l,l|\rho_{SR}|N-l,l\rangle\right)\\ &= |1\rangle\langle 1|_{R'}\sum_{k}\langle k|\operatorname{tr}_S\rho_{SR}|k\rangle + |0\rangle\langle 0|_{R'}\sum_{l}\langle l|\operatorname{tr}_S\rho_{SR}|l\rangle,\end{aligned} \tag{56}$$

where we again used the expression from before to get rid of the binomials. We now see that the final expression only depends on the state of ρ_{SR} on the system R and hence Λ is non-signalling from S to R'.

D General considerations for the security proofs

In this section we present the steps that are shared between the two security proofs. The remainder of the steps is then presented in the respective chapters. Throughout this section we will make use of the following events (formally defined as subsets of $A^n\tilde{A}^nC^n$):

Ω_{EC}	The protocol did not abort in the EC step, i.e. $h(A^n) = h(\tilde{A}^n)$.
$\Omega_{\mathrm{EC}}^{\mathrm{fail}}$	The protocol did not abort in the EC step and $\tilde{A}^n \neq A^n$.
$\Omega_{\mathrm{EC}}^{\mathrm{cor}}$	The protocol did not abort in the EC step and $\tilde{A}^n = A^n$. This event can also be written as $\Omega_{\mathrm{EC}}^{\mathrm{cor}} = \Omega_{\mathrm{EC}} \cap (\Omega_{\mathrm{EC}}^{\mathrm{fail}})^c$.
Ω_{PE}	The protocol did not abort in the parameter estimation step, i.e. $f(\mathrm{freq}(C^n)) \geq H_{\mathrm{exp}}$.

We also define the event of not aborting the protocol which is given by $\Omega = \Omega_{\mathrm{EC}} \cap \Omega_{\mathrm{PE}}$. Security consists of two components: Completeness and Soundness. Proving those two properties is the content of the following two subsections. The completeness condition will put a lower bound on the admissible value of $\mathrm{leak}_{\mathrm{EC}}$ while the soundness condition will put an upper bound on the admissible key length l.

D.1 Completeness

In this section we show completeness, i.e., we show that there exists an (honest) implementation that aborts with low probability. The main result is summarised in the following theorem:

Theorem D.1. *Let $\delta, \bar{\varepsilon}_s, \varepsilon_{\mathrm{EC}}^{\mathrm{com}} > 0$ and $p \in \mathbb{P}_{\mathcal{C}}$ be the expected statistics of the honest implementation. If*

$$\mathrm{leak}_{\mathrm{EC}} \geq nH(A|JB)_{\mathrm{hon}} + 2\sqrt{n}\log 7\sqrt{\log\frac{2}{\bar{\varepsilon}_s^2}} + 2\log\frac{1}{\varepsilon_{\mathrm{EC}}^{\mathrm{com}} - \bar{\varepsilon}_s} + 4, \tag{57}$$

and $H_{\mathrm{exp}} \leq f(p) - \delta$ then there exists an (honest) implementation of the protocol with abort probability

$$\Pr[\mathrm{abort}] \leq \varepsilon_{\mathrm{EC}}^{\mathrm{com}} + \exp\left(-n\frac{\delta^2/2}{\mathrm{Var}(f) + (\mathrm{Max}(f) - \mathrm{Min}(f))\delta/3}\right). \tag{58}$$

In the expression above $H(A|JB)_{\mathrm{hon}} = H(A_i|J_iB_i)_{\mathrm{hon}}$ refers to the entropy of Alice's raw key conditioned on Bob's information for the honest implementation.

Proof. Let ρ_{hon} be the state at the end of the protocol when Eve is passive. There are two places where the protocol could abort. The first is during error correction, the second is during parameter estimation. Formally, this can be expressed as $\Omega_{\mathrm{abort}} = \Omega^c = \Omega_{\mathrm{EC}}^c \cup \Omega_{\mathrm{PE}}^c$. Using the union bound, we find that

$$\rho_{\mathrm{hon}}[\Omega_{\mathrm{abort}}] = \rho_{\mathrm{hon}}[\Omega_{\mathrm{EC}}^c \cup \Omega_{\mathrm{PE}}^c] \leq \rho_{\mathrm{hon}}[\Omega_{\mathrm{EC}}^c] + \rho_{\mathrm{hon}}[\Omega_{\mathrm{PE}}^c]. \tag{59}$$

We will now bound the two terms in this expression separately.

To bound the first term we note that according to [RR12], there exists an EC protocol with failure probability at most $\varepsilon_{\mathrm{EC}}^{\mathrm{com}}$ as long as:

$$\mathrm{leak}_{\mathrm{EC}} \geq H_{\max}^{\bar{\varepsilon}_s}(A^n|J^nB^n) + 2\log\frac{1}{\varepsilon_{\mathrm{EC}}^{\mathrm{com}} - \bar{\varepsilon}_s} + 4. \tag{60}$$

Next, we apply [DFR20, Corollary 4.10] to bound the smooth max-entropy:

$$H_{\max}^{\bar{\varepsilon}_s}(A^n|J^nB^n) \leq nH(A|JB)_{\mathrm{hon}} + 2\sqrt{n}\log(1 + 2|\mathcal{A}|)\sqrt{\log\frac{2}{\bar{\varepsilon}_s^2}}. \tag{61}$$

Therefore we can conclude that since inequality (57) is satisfied by assumption (we have $|\mathcal{A}| = 3$), there exists an EC protocol such that $\rho_{\text{hon}}[\Omega_{\text{EC}}^c] \leq \varepsilon_{\text{EC}}^{\text{com}}$.

To bound the second term in (59) we note that the honest implementation is IID. We follow the steps in [MR22] to see that

$$\rho_{\text{hon}}[\Omega_{\text{PE}}^c] \leq \exp\left(-n\frac{\delta^2/2}{\operatorname{Var}(f) + (\operatorname{Max}(f) - \operatorname{Min}(f))\delta/3}\right). \tag{62}$$

Combining the two bounds then yields the result. □

D.2 Soundness

Soundness is the statement that for any attack either the protocol aborts with high probability or Eve's knowledge about the key is small. Our soundness statement is summarized in the following theorem:

Theorem D.2. *Let $\alpha' \in (1, 3/2)$ and $\varepsilon_{\text{PA}}, \varepsilon_s \in (0,1)$. Let V and $K(\alpha')$ be as in Theorem 2.9 for the min-tradeoff function f of the protocol. If*

$$\begin{aligned} l \leq & nH_{\exp} - n\frac{\alpha'-1}{2-\alpha'}\frac{\ln(2)}{2}V^2 - \frac{g(\varepsilon_s) + \alpha' \log\left(\frac{1}{2\varepsilon_s + \varepsilon_{\text{PA}}}\right)}{\alpha'-1} - n\left(\frac{\alpha'-1}{2-\alpha'}\right)^2 K(\alpha') \\ & - \text{leak}_{\text{EC}} - \lceil \log(1/\varepsilon_{\text{EC}}) \rceil - 2\log(1/\varepsilon_{\text{PA}}) + 2, \end{aligned} \tag{63}$$

then the protocol is $(\varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + 2\varepsilon_s)$-sound.

Proof. The proof more or less follows the steps from [TSB⁺20, MR22]. Let E_n denote Eve's quantum system at the end of the protocol. Let us denote with O_{EC} the (classical) information exchanged during the error correction procedure of the protocol and with F the information exchanged during privacy amplification. Write $\Sigma = E_n I^n J^n O_{\text{EC}}$ for Eve's total information before privacy amplification and let $\rho_{K_A^l K_B^l A^n \tilde{A}^n C^n F \Sigma}$ be the state at the end of the protocol. The goal is to upper-bound the quantity (see Definition 2.2):

$$\frac{1}{2}\left\|(\rho_{\wedge\Omega})_{K_A^l K_B^l F\Sigma} - \tau_{K_A^l K_B^l} \otimes (\rho_{\wedge\Omega})_{F\Sigma}\right\|_1. \tag{64}$$

The event Ω includes the event where the protocol did not abort but error correction produced incorrect outputs, i.e. $\tilde{A}^n \neq A^n$ and hence $K_B^l \neq K_A^l$. To address this we write $\Omega = (\Omega \cap \Omega_{\text{EC}}^{\text{fail}}) \cup (\Omega \cap (\Omega_{\text{EC}}^{\text{fail}})^c) = \Omega_1 \cup \Omega_2$ with $\Omega_1 = \Omega \cap \Omega_{\text{EC}}^{\text{fail}}$ and $\Omega_2 = \Omega \cap (\Omega_{\text{EC}}^{\text{fail}})^c$. Since $\Omega_1 \cap \Omega_2 = \emptyset$, we have $\rho_{\wedge\Omega} = \rho_{\wedge\Omega_1} + \rho_{\wedge\Omega_2}$. Inserting this into (64) and applying the triangle inequality we get:

$$\begin{aligned} & \frac{1}{2}\left\|(\rho_{\wedge\Omega})_{K_A^l K_B^l F\Sigma} - \tau_{K_A^l K_B^l} \otimes (\rho_{\wedge\Omega})_{F\Sigma}\right\|_1 \\ \leq & \frac{1}{2}\left\|(\rho_{\wedge\Omega_1})_{K_A^l K_B^l F\Sigma} - \tau_{K_A^l K_B^l} \otimes (\rho_{\wedge\Omega_1})_{F\Sigma}\right\|_1 + \frac{1}{2}\left\|(\rho_{\wedge\Omega_2})_{K_A^l K_B^l F\Sigma} - \tau_{K_A^l K_B^l} \otimes (\rho_{\wedge\Omega_2})_{F\Sigma}\right\|_1 \\ \leq & \varepsilon_{\text{EC}} + \frac{1}{2}\left\|(\rho_{\wedge\Omega_2})_{K_A^l K_B^l F\Sigma} - \tau_{K_A^l K_B^l} \otimes (\rho_{\wedge\Omega_2})_{F\Sigma}\right\|_1, \end{aligned} \tag{65}$$

where in the last line we noted that by the properties of universal hashing we have that $\rho[\Omega_1] \leq \rho[\Omega_{\text{EC}}^{\text{fail}}] \leq \varepsilon_{\text{EC}}$. We now focus on bounding the second term. Since this term is conditioned on $\Omega_2 = \Omega \cap (\Omega_{\text{EC}}^{\text{fail}})^c$, we know that $\tilde{A}^n = A^n$ and hence $K_A^l = K_B^l$. Therefore we can trace out the systems K_B^l in the trace distance above to recover a situation similar to the one in the leftover hashing lemma.

We let $\varepsilon_s, \varepsilon_{\text{PA}} > 0$ and our goal will now be to upper-bound the second term in the expression above by $2\varepsilon_s + \varepsilon_{\text{PA}}$. We can expand $\Omega_2 = \Omega_{\text{PE}} \cap \Omega_{\text{EC}} \cap (\Omega_{\text{EC}}^{\text{fail}})^c = \Omega_{\text{PE}} \cap \Omega_{\text{EC}}^{\text{cor}}$. If now either $\rho[\Omega_{\text{PE}}] < 2\varepsilon_s + \varepsilon_{\text{PA}}$ or $\rho_{|\Omega_{\text{PE}}}[\Omega_{\text{EC}}^{\text{cor}}] < 2\varepsilon_s + \varepsilon_{\text{PA}}$ then $\rho[\Omega_2] < 2\varepsilon_s + \varepsilon_{\text{PA}}$ and the statement holds trivially. Hence we can from now on assume that both $\rho[\Omega_{\text{PE}}] \geq 2\varepsilon_s + \varepsilon_{\text{PA}}$ and $\rho_{|\Omega_{\text{PE}}}[\Omega_{\text{EC}}^{\text{cor}}] \geq 2\varepsilon_s + \varepsilon_{\text{PA}}$.

We can write $\rho_{\wedge\Omega_2} = \rho_{\wedge(\Omega_{\mathrm{PE}}\cap\Omega_{\mathrm{EC}}^{\mathrm{cor}})} = \rho[\Omega_{\mathrm{PE}}](\rho_{|\Omega_{\mathrm{PE}}})_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}$ and to simplify the notation we introduce $\sigma = \rho_{|\Omega_{\mathrm{PE}}}$. With this we get

$$\begin{aligned}\left\|(\rho_{\wedge\Omega_2})_{K_A^l F\Sigma} - \tau_{K_A^l}\otimes(\rho_{\wedge\Omega_2})_{F\Sigma}\right\|_1 &= \rho[\Omega_{\mathrm{PE}}]\left\|(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{K_A^l F\Sigma} - \tau_{K_A^l}\otimes(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{F\Sigma}\right\|_1 \\ &\leq \left\|(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{K_A^l F\Sigma} - \tau_{K_A^l}\otimes(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{F\Sigma}\right\|_1 .\end{aligned} \tag{66}$$

We now apply Lemma 2.4 to upper-bound the trace distance:

$$\frac{1}{2}\left\|(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{K_A^l F\Sigma} - \tau_{K_A^l}\otimes(\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}})_{F\Sigma}\right\|_1 \leq 2\varepsilon_s + 2^{\frac{1}{2}\left(l - H_{\min}^{\varepsilon_s}(A^n|\Sigma)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} - 2\right)} \overset{!}{\leq} 2\varepsilon_s + \varepsilon_{\mathrm{PA}}, \tag{67}$$

where the smooth min-entropy is evaluated on the state before the PA part of the protocol. To arrive at our desired result we now need to upper-bound the second term by $\varepsilon_{\mathrm{PA}}$:

$$2^{\frac{1}{2}\left(l - H_{\min}^{\varepsilon_s}(A^n|\Sigma)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} - 2\right)} \leq \varepsilon_{\mathrm{PA}} \iff l \leq H_{\min}^{\varepsilon_s}(A^n|\Sigma)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} - 2\log\frac{1}{\varepsilon_{\mathrm{PA}}} + 2. \tag{68}$$

To find an upper bound on the admissible values of l, we now need to lower-bound the smooth min-entropy. Since the EAT applies to the state before the error correction procedure, we first need to eliminate this side information. This can be achieved using the chain rule in [Tom16, Lemma 6.8]

$$\begin{aligned}H_{\min}^{\varepsilon_s}(A^n|\Sigma)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} &\geq H_{\min}^{\varepsilon_s}(A^n|E_n I^n J^n)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} - \log(\dim O_{\mathrm{EC}}) \\ &\geq H_{\min}^{\varepsilon_s}(A^n|E_n I^n J^n)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} - \mathrm{leak}_{\mathrm{EC}} - \lceil\log(1/\varepsilon_{\mathrm{EC}})\rceil,\end{aligned} \tag{69}$$

where we noted that $\log(\dim O_{\mathrm{EC}}) \leq \mathrm{leak}_{\mathrm{EC}} + \lceil\log(1/\varepsilon_{\mathrm{EC}})\rceil$. We now note that since $\sqrt{\sigma[\Omega_{\mathrm{EC}}^{\mathrm{cor}}]} \geq \sqrt{2\varepsilon_s + \varepsilon_{\mathrm{PA}}} > \varepsilon_s$ we can apply [TL17, Lemma 10]:

$$H_{\min}^{\varepsilon_s}(A^n|E_n I^n J^n)_{\sigma_{\wedge\Omega_{\mathrm{EC}}^{\mathrm{cor}}}} \geq H_{\min}^{\varepsilon_s}(A^n|E_n I^n J^n)_{\sigma}. \tag{70}$$

Remembering that $\sigma = \rho_{|\Omega_{\mathrm{PE}}}$ and applying Theorem 2.9 with $\rho[\Omega_{\mathrm{PE}}] \geq 2\varepsilon_s + \varepsilon_{\mathrm{PA}}$ to the remaining smooth min-entropy term then yields the desired result. □

E Security of relativistic QKD

Here we show the remaining steps for proving security of the relativistic protocol. Namely this includes finding a valid min-tradeoff function (the parameter f of the protocol). A min-tradeoff function is an affine function $f : \mathbb{P}_{\mathcal{C}} \to \mathbb{R}$ satisfying:

$$f(p) \leq \inf_{\nu\in\Sigma(p)} H(A_i|E_i I_i J_i \tilde{E}_{i-1})_\nu \qquad \forall p \in \mathbb{P}_{\mathcal{C}}, i \in [n], \tag{71}$$

where $\tilde{E}_{i-1}$ is a system isomorphic to $E_{i-1}I^{i-1}J^{i-1}$ and $\Sigma(p)$ is the set of all states that can be produced by our channels and that are compatible with the statistics p. To simplify the construction of our min-tradeoff function we follow the steps outlined in [DF19] i.e. we split our protocol into key rounds where $T_i = 0$ and test rounds where $T_i = 1$. For this we separate $\mathcal{C} = \mathcal{C}' \cup \{\varnothing\}$ with $\mathcal{C}' = \{\mathrm{corr}, \mathrm{err}, \perp\}$. We then apply [DF19, Lemma V.5] which states that if

$$g(p') \leq \inf H(A|E_i I_i J_i \tilde{E}_{i-1}) \qquad \forall p' \in \mathbb{P}_{\mathcal{C}'}, i \in [n] \tag{72}$$

is a valid min-tradeoff function for the protocol rounds constrained on obtaining statistics p' in the test rounds, then the affine function defined by

$$\begin{aligned} f(\delta_c) &= \mathrm{Max}(g) + \frac{1}{\gamma}(g(\delta_c) - \mathrm{Max}(g)) \quad \forall c \in \mathcal{C}', \\ f(\delta_\varnothing) &= \mathrm{Max}(g)\end{aligned} \tag{73}$$

is a valid min-tradeoff function for the full protocol (which includes both the key and the test rounds). The main difference between the min-tradeoff functions given in (71) and (72) is that

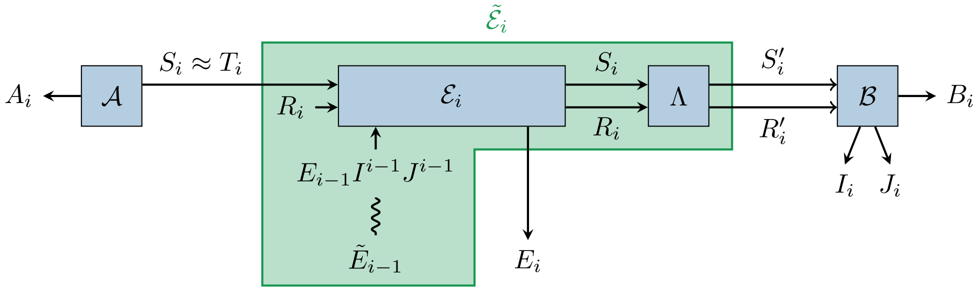


Figure 14: A diagrammatic representation of the channel $\mathcal{M}_i$ in the i-th round of the protocol. Formally we need to consider attack channels with inputs R_i and $E_{i-1}I^{i-1}J^{i-1}$ (which might be entangled with a system $\tilde{E}_{i-1}$) and outputs E_i, R_i and S_i. However, the systems $R_iE_{i-1}I^{i-1}J^{i-1}\tilde{E}_{i-1}$ can be absorbed into the definition of $\tilde{\mathcal{E}}_i$. Similarly we can include the squashing map Λ into Eve's attack (this can only decrease the key rate). Since both $\mathcal{E}_i$ and Λ are non-signalling, $\tilde{\mathcal{E}}_i$ will also be non-signalling (from T_i to R_i').

in the former the optimization is constrained on obtaining the correct statistics in all the rounds (including key rounds), whereas in the latter the optimization is constrained only on obtaining the correct statistics in the test rounds. The properties of the two min-tradeoff functions can be related by

$$\begin{aligned} \mathrm{Max}(f) &= \mathrm{Max}(g), \\ \mathrm{Min}_\Sigma(f) &\geq \mathrm{Min}(g), \\ \mathrm{Var}(f) &\leq \frac{1}{\gamma}(\mathrm{Max}(g) - \mathrm{Min}(g))^2. \end{aligned} \tag{74}$$

The remaining task now is to find a min-tradeoff function as in (72). To ease this task there are a number of simplifications that can be made to Eve's attack channel (see Figure 14). By the existence of the squashing map (see Theorem 2.13) we conclude that we can replace our photonic systems S_i and R_i with qubit systems S_i' and R_i'. Additionally we can absorb the systems $E_{i-1}I^{i-1}J^{i-1}$ and $\tilde{E}_{i-1}$ into Eve's attack map. Next, we note that since the state of the reference is identical for all rounds (and hence is uncorrelated with the key), we can allow Eve to prepare this state herself. Finally we note that, in principle, we would also need to consider the full Fock space on the input to Eve's channel. However because in our protocol the inputs live in $T_i = \mathrm{span}\{|\alpha\rangle, |-\alpha\rangle\}$ we can restrict Eve's input to this reduced subspace (restricting the real attack channel to this subspace yields a new channel with the same key rate).

In conclusion: we can restrict ourselves to attack channels which take a single qubit as input (the system T_i) and produce qubit outputs S_i' and R_i' together with some side-information E_i. Furthermore, this simplified attack channel is non-signalling from T_i to R_i'. By strong subadditivity, we can also assume that E_i is a purifying system.

Assuming E_i to be a purifying system gives Eve too much power in general (Eve cannot purify an unknown state). To resolve this, we switch to an entanglement based version of the protocol. Explicitly we note that the post-measurement state would be identical if Alice had instead prepared the entangled state (for brevity we drop the index i)

$$|\psi\rangle_{\tilde{V}T} = \frac{1}{\sqrt{2}}|0\rangle_{\tilde{V}} \otimes |\alpha\rangle_T + \frac{1}{\sqrt{2}}|1\rangle_{\tilde{V}} \otimes |-\alpha\rangle_T, \tag{75}$$

followed by measuring $\tilde{V}$ locally to obtain her key bit V. However, in contrast to the usual literature, we do not give this source to Eve. The reason for this is that it is not obvious how the non-signalling constraint would look like in that scenario. In this entanglement based picture we can then define the POVM associated to the evaluation function in (32) (now restricted to only test rounds where $J \neq \varnothing$):

$$\begin{aligned} \Gamma^{(\mathrm{cor})}_{\tilde{V}S'R'} &= |0\rangle\langle 0|_{\tilde{V}} \otimes N^{(0)}_{S'R'} + |1\rangle\langle 1|_{\tilde{V}} \otimes N^{(1)}_{S'R'} \\ \Gamma^{(\mathrm{err})}_{\tilde{V}S'R'} &= |0\rangle\langle 0|_{\tilde{V}} \otimes N^{(1)}_{S'R'} + |1\rangle\langle 1|_{\tilde{V}} \otimes N^{(0)}_{S'R'} \\ \Gamma^{(\perp)}_{\tilde{V}S'R'} &= \mathbb{1}_{\tilde{V}} \otimes N^{(\perp)}_{S'R'}, \end{aligned} \tag{76}$$

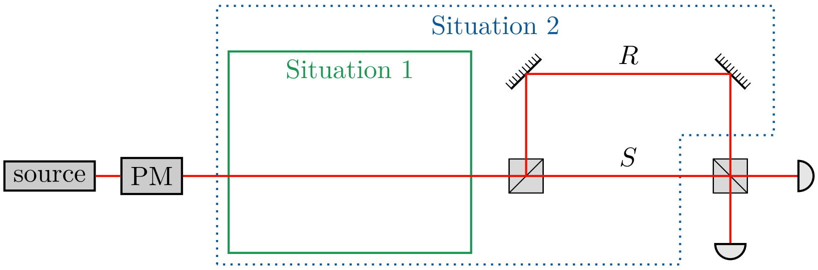


Figure 15: The different possible regions of Eve's influence. Situation 1 is the actual situation of the DPS protocol which does not satisfy the non-signalling constraint. So instead we give Eve access to the memory system R (the upper arm of the interferometer) as well as one of Bob's beam splitters. This is shown as situation 2. This change can only decrease the secret key rate.

where $\{N^{(b)}_{S'R'}\}_b$ are as defined in (27). With this we can compute the expected statistics of any state $\sigma_{\tilde{V}S'R'}$ as

$$\sigma_C(c) = \mathrm{tr}\left[\sigma_{\tilde{V}S'R'}\Gamma^{(c)}_{\tilde{V}S'R'}\right]. \tag{77}$$

Next, we parametrize $g : \mathbb{P}_{\mathcal{C}'} \to \mathbb{R}$ as $g(p') = c_\lambda + \lambda \cdot p'$ with $\lambda \in \mathbb{R}^{|\mathcal{C}'|}$ and note that if

$$c_\lambda \leq \inf_\nu \{H(A|IJE)_\nu - \lambda \cdot \nu_C\}, \tag{78}$$

then g is a valid min-tradeoff function (the minimization is over all states compatible with our channels $\mathcal{M}_i$). The parameter λ is optimized using standard numerical optimization techniques (choosing a non-optimal λ decreases the key rate but does not compromise security). Conservatively, we assume that in the test rounds ($J \neq \varnothing$) no entropy is produced. This means that we can get rid of the conditioning system J at the cost of reducing the entropy by a factor of $1-\gamma$. Hence the final optimization problem that we need to solve is:

$$\begin{aligned} \inf_{\rho_{TS'R'}} \quad & ((1-\gamma)H(A|IE, J=\varnothing)_{\nu(\rho)} - \lambda \cdot \nu_C(\rho)) \\ \text{s.t.} \quad & \rho_{TS'R'} \geq 0, \\ & \mathrm{tr}[\rho_{TS'R'}] = 1, \\ & \rho_{TR'} = \frac{\mathbb{1}_T}{d_T} \otimes \rho_{R'}, \end{aligned} \tag{79}$$

where $\nu(\rho)$ is the state after Alice and Bob measure a purification of $\mathcal{I}_{\tilde{V}} \otimes \mathcal{C}^{-1}(\rho)[|\psi_{\tilde{V}T}\rangle\langle\psi_{\tilde{V}T}|]$ ($\rho_{TS'R'}$ is the Choi state of Eve's attack channel). It is also worth noting that by the Stinespring representation theorem, giving Eve a purification does not give her more power (the input states are pure). The last constraint in (79) originates from the non-signalling condition (see Lemma 2.11). The optimization problem in (79) can then be evaluated using the methods in [AHN+22][5].

F A note about memory in DPS QKD

One of the main technical challenges when trying to prove security of the DPS protocol is that we need to consider memory effects (the system R in Figure 15). Naively one might hope to be able to include these memory effects in the EAT using the register R_i. After all, this is precisely what this register is for. There is however a problem: Bob's outputs and hence the sifting information I_i depends on the state of the memory system R. But the register I_i will also become available to Eve thus breaking the non-signalling condition of the EAT. We circumvent this problem by including the memory system R in Eve's register E_i (situation 2 in Figure 15). Now the non-signalling constraint is trivially satisfied since the register R_i is the trivial (one dimensional) system. On the

[5] Technically we need a slight generalization of the method where we absorb the conditioning on I into the normalization of ν.

other hand this also means that we now have to condition on this additional system (to which Eve in reality has no access). When computing entropies for situation 1 in Figure 15 we observe that the entropy decreases with increasing photon number. This indicates that it is not possible to find (an obvious) squashing map for this scenario.