Experimental semi-quantum key distribution with classical users

Francesco Massa[1], Preeti Yadav[2,3], Amir Moqanaki[1], Walter O. Krawec[4], Paulo Mateus[2,3], Nikola Paunković[2,3], André Souto[2,5], and Philip Walther[1]

[1]University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), Boltzmanngasse 5, Vienna A-1090, Austria

[2]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal

[3]Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

[4]Computer Science and Engineering Department, University of Connecticut, Storrs, CT 06269, USA

[5]LASIGE, Departamento de Informática, Faculdade de Ciências, Universidade de Lisboa, 1749-016 Lisboa, Portugal

Quantum key distribution, which allows two distant parties to share an unconditionally secure cryptographic key, promises to play an important role in the future of communication. For this reason such technique has attracted many theoretical and experimental efforts, thus becoming one of the most prominent quantum technologies of the last decades. The security of the key relies on quantum mechanics and therefore requires the users to be capable of performing quantum operations, such as state preparation or measurements in multiple bases. A natural question is whether and to what extent these requirements can be relaxed and the quantum capabilities of the users reduced. Here we demonstrate a novel quantum key distribution scheme, where users are fully classical. In our protocol, the quantum operations are performed by an untrusted third party acting as a server, which gives the users access to a superimposed single photon, and the key exchange is achieved via interaction-free measurements on the shared state. We also provide a full security proof of the protocol by computing the secret key rate in the realistic scenario of finite-resources, as well as practical experimental conditions of imperfect photon source and detectors. Our approach deepens the understanding of the fundamental principles underlying quantum key distribution and, at the same time, opens up new interesting possibilities for quantum cryptography networks.

1 Introduction

Quantum key distribution (QKD) is a technique that allows two distant parties, traditionally called Alice and Bob, to exchange a cryptographic key in an information-theoretic secure way. This means that the security of the key relies on information theory and cannot be broken even by an eavesdropper with unlimited resources.

The first QKD proposal was the BB84 protocol, introduced by Bennett and Brassard in 1984 [1] (subsequently, Ekert introduced the E91 protocol in 1991 [2]), which was proven secure several years later [3–5]. Since then, much progress, both theoretical and experimental, has been made in the field. The practicality of this technology is underlined by numerous experimental and even commercial endeavors, supporting its development [6–9].

Most QKD protocols require Alice or Bob to share a quantum state, or a direct quantum channel, and to perform quantum operations, i.e., operations on quantum bits (qubits) that do not have any counterpart in classical communication, such as generation or measurement in multiple bases. On the other hand, it is known that if both parties are restricted to classical communication, unconditional security is unachievable for the key distribution problem. It is therefore relevant for a fundamental understanding of QKD to investigate how quantum the users' operations and resources need to be in order to achieve information-theoretic security.

A first step in this direction was made by introducing the *semi-quantum* model of cryptography in 2007 by Boyer et al. [10]. In this model, at least one party must be "classical" in nature, i.e., restricted to a limited set of operations on qubits, namely measuring and/or preparing qubits in a single basis (usually the computational (Z) basis $\{|0\rangle, |1\rangle\}$), or simply disconnecting from the quantum channel by allowing any received quantum state to reflect back to the sender. The use of "classical" in this terminology is due to the fact that orthogonal quantum states from a single measurement basis and states of classical systems are both fully distinguishable. The other parties may be classical or quantum (naturally, at least one party must be quantum) with a "quantum" user having the ability to perform any quantum operation on qubits allowed by the laws of physics. In the subsequent proposal [11], permuting or reordering the in-

coming qubits using delay lines was considered as another classical operation. Nevertheless, although one can indeed argue that permuting physical systems is inherently classical operation, doing so, especially in photonic applications, is with the current technology far more infeasible than any quantum operation used in cryptographic protocols. Also, preparing and detecting qubit states, albeit in a single basis, is technologically non-trivial.

Further development has shown that Alice's operations can be as limited as Bob's, provided that a third party distributes entangled photons to the users and performs measurements in different bases [12, 13]. Such a scheme, referred to as a mediated SQKD protocol, allows two classical users to establish a shared secret key with one-another, using the help of a quantum server which must prepare, and later measure, quantum bits. However, this quantum server need not be trusted, and in fact could be an all-powerful adversary. Security was proven, but again, only for the perfect-qubit scenario [12].

Since that original mediated-SQKD protocol, there have been several advances both in new protocol design and in new security proof methods. A main research goal in this field is to develop new protocols which further reduce the requirements placed on either the end-users or the server (or both). In terms of reducing the complexity of the end-users, a protocol which did not require users to measure was proposed in [13] (however, attacks against the protocol were later discovered in [14]). On the other hand, in [15, 16], protocols were developed which reduced the server's requirements. Namely, in [15] the server need only send single qubit states to users but later requiring a Bell measurement. In [16] single qubits were used, both in the initial preparation stage and in the subsequent server measurement, however a cycle topology was required.

Beyond reducing end-user or server requirements, another avenue of research in this area is in improving either efficiency or noise tolerance of the protocol (or both) and in developing new security proof methods. In [17] a new multi-mediated model was introduced which could improve noise tolerance at the cost of efficiency, while in [18] a new protocol was introduced which improved efficiency (though at the cost of noise tolerance).

Most SQKD protocols up to this point have been theoretical in nature, and assume perfect qubit channels, i.e., no photon loss or multi-photons are permitted for their security to be valid. A SQKD protocol immune to such imperfections was described recently in [19] and was proven to be robust, meaning that any attack which causes an adversary to gain non-zero information on the key, necessarily creates a disturbance that may be detected with non-zero probability. A second such protocol was proposed in [20], though there security was only proven against a few specific attacks. However, no full proof of security yet exists for these protocols and so, their key rates and noise tolerances are still unknown.

In general, while numerous SQKD protocols have been proposed in the last decade [21], information-theoretic proofs of security were developed only for a few of them [12, 17, 18, 22, 23] and always in the ideal scenario of perfect qubits, ideal devices and infinite resources in the asymptotic regime.

In this work, we propose a novel SQKD protocol in the mediated model, allowing two classical users to share a secret key using the help of an untrusted, potentially adversarial, quantum server. In particular, our protocol requires Alice and Bob to perform two classical operations only, the detection or reflection of a single photon, and hence places even fewer restrictions on the users than prior protocols of this nature, by requiring only a single photon measurement and no state preparation. We are the first to show that such minimal requirements, on the part of the users, is sufficient to generate a secret key. The server's complexity is also reduced compared to prior work, needing only to prepare and measure single qubits. Furthermore, as first for mediated SQKD research, we conduct an information theoretic proof of security of the protocol assuming practical devices, whereas prior work in mediated SQKD was restricted to perfect qubit scenarios, and compute the secret key rate in the finite key setting. Finally, we experimentally demonstrate our protocol under real-life conditions and evaluate the secret key rate by using the results from actual devices. Our methods here may also be broadly applicable to other multi-user (S)QKD protocols in practical settings.

2 The Protocol

Our protocol involves three parties: two classical users, Alice and Bob, whose aim is to exchange a secret cryptographic key, and an untrusted, potentially adversarial, quantum server, which provides the quantum resources for this purpose. Furthermore, we assume that Alice and Bob can communicate through a classical authenticated channel and that the server can send unauthenticated classical messages to the users. In the description below, we discuss the protocol for single photons for simplicity, and also they are the most practical for QKD applications (though our security analysis will also take into account realistic multi-photon sources).

A sketch of the scheme is depicted in Figure 1. The server sends to Alice and Bob a single photon in a balanced superposition of their respective locations. Each user can independently choose to perform two actions: "detect" (D) or "reflect" (R). In the former case, the photon travels to a detector controlled by the user; in the latter, the photon is sent back to a balanced beam splitter controlled by the server, at

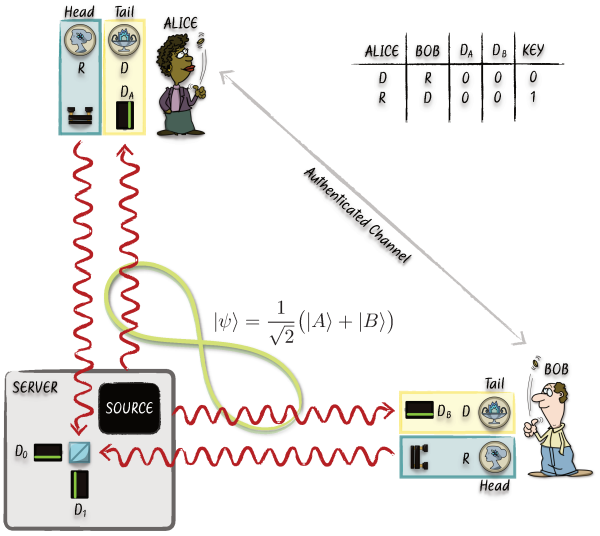

Figure 1: **The QKD protocol with classical users.** A quantum server sends single photons in superposition to the users at predetermined regular intervals, which constitute the rounds of the protocol. For each round, Alice and Bob randomly choose between "detect" (D) and "reflect" (R). The photons reflected back to the server impinge onto a beam splitter at whose outputs two detectors D0 and D1 are placed. When both Alice and Bob reflect the received photon, single-photon interference occurs at the beam splitter and only detector D0 clicks. If only one of the users chooses to detect the photon without registering any detection event, interference is suppressed and the photon has ideally 50% probability to reach detector D1. If the server announces a detection at D1 and none of the users detected photons, a raw key bit is generated according to the table in the figure. The users can communicate through a classical authenticated channel to verify the honesty of the server and to share the necessary information for the evaluation of the secure key rate.

whose output ports two detectors, D_0 and D_1, are placed. When both users choose to reflect, single-photon interference occurs at the beam splitter, with the relative phase of the two interfering photon amplitudes tuned such that only detector D_0 clicks. In the ideal case of perfect detection efficiency, when only one of the users chooses to detect the photon and does not find any, the photon collapses into the other user's location. This corresponds to performing an *interaction-free* measurement [24–26], which suppresses single-photon interference at the server and allows either detector D_0 and D_1 to click with non-zero probability. A click at detector D_1, therefore, enables each user to deduce the action of the other one, thus allowing for the establishment of a raw key digit. In particular, a key digit of 0(1) is set when Alice chooses $D(R)$ and Bob $R(D)$. Other combinations are not considered, as they cannot result in a detection at D_1. Since the raw key bits are generated when the server announces a click at detector D_1, and *neither* Alice *nor* Bob detect a photon, no use of the authenticated channels is needed during those rounds, unlike the standard QKD protocols [1, 2]. In our protocol, classically authenticated information exchange is performed only for the verification and parameter estimation rounds, which are not used to generate the raw key.

The detailed steps of the protocol are described below:

Quantum Communication Stage: Users repeat the following process until a sufficiently large raw key has been established (refer also to Figure 1):

1. The server sends a single photon to both parties in a superposition. Ideally this should be performed by the server sending a single photon through a beam splitter.

2. Alice and Bob choose, independently and randomly, between two available actions: D or R. Since Alice and Bob are completely classical, the detection results only give them information as to whether or not there is a photon at their respective detector D_A or D_B. Their actions determine their raw key bit for this round, namely:

   - **Alice:** If Alice chose D, she will record a raw key-bit of 0; otherwise, if she chose R, she will record a raw key-bit of 1.
   - **Bob:** Bob's encoding is opposite that of Alice; namely if he chose D he will record a raw key bit of 1 and, otherwise, a raw key bit of 0 if he chose R.

3. The server measures the photon coming from Alice/Bob and announces the following results: "0" if the server's detector D_0 clicks; "1" if detector D_1 clicks; "v" if no detector clicks; or "m" if more than one detector clicks. Ideally, this measurement should be performed by the server completing a (folded) Mach-Zehnder interferometer as shown in Figure 1. Note that the last case can arise due to experimental imperfections or the action of an adversary.

4. Alice and Bob perform a minimal sifting step whereby they will keep the round only if the following two conditions are met:

   - The server announces the message "1"
   - *and* Alice and Bob both did *not* detect a photon if they chose to measure.

   All other events will cause the round to be discarded. Note that, for this, Alice and Bob must announce whether they detect a photon or not. In the event parties choose R they will, by default, announce that they did not detect a photon.

Sampling Stage: Users will communicate, through an authenticated channel, their actions and measurement outcomes (if applicable) for a randomly chosen subset of the rounds performed above. This is done to verify the honesty of the server and/or the presence of an adversary. More specifically, these statistics, as

discussed below, will be used to determine a bound on the overall key-rate of the protocol.

Post Processing Stage: After performing the above sampling process and discarding those rounds chosen for sampling, users will perform a standard error correction protocol and privacy amplification protocol resulting in the final secret key of the system. For information on these standard processes, the reader is referred to [6].

It is not difficult to see that, if the server is honest, the protocol is correct. Namely, the only time the server should ever send the message "1" is when Alice and Bob choose opposite actions (thus resulting in a correlated raw key bit since their encoding operations are opposites of one another). We show later that the protocol can lead to a secure secret key even if the server is adversarial.

3 Key generation and parameter estimation

In this section, we discuss the events when raw key bits are generated and the parameter estimation procedure (for details see Appendices A, C, and D).

Let N be the total number of successful rounds in the protocol, i.e., whenever the server announces a message from "v", "0", "1" or "m". At the end of N rounds, Alice and Bob communicate with each other over an authenticated classical channel to proceed to, first, the verification procedure, and then, to estimate the parameters to eventually share a secret key among them. Note that the server is bound to announce the same results to both Alice and Bob, since it can easily be checked by the users when they communicate over an authenticated channel. Therefore, upon having all the indexed results from the server, each user compares it with their own action. During the rounds when the server announced "1", when a user either reflected, or detected vacuum, only then we say that the user's action is "consistent" with the server's result, and no information is sent to the other client. Otherwise, any of the users detecting inconsistency announces it to the other one and the corresponding round is discarded from the rounds for key-generation. Such inconsistencies could be due to receiving a click in their detectors, or receiving clicks even when they reflected due to the failure in the switch used by them to change between the actions reflect (R) or detect (D).

Therefore, when the server announces "1" and both users' actions are consistent with such outcome, then a raw key digit is generated. This occurs on total of $N_{raw} = \mathrm{p}(1)N$ rounds, where $\mathrm{p}(1)$ denotes the probability that the server announces "1" and none of the users detect any click(s). The cases when the server announces "1" and both users reflected or both detected vacuum determine errors in the key.

Note that in the majority of QKD protocols (for instance, BB84), even the very first set of keys shared by Alice and Bob requires them to communicate over an authenticated channel. On the contrary, the first set of shared key in our protocol does not require any communication between the users, but only the message "1" from the server.

Alice and Bob choose each action (R or D) independently at random, with probability 1/2. Thus, the cases when the key can potentially be generated occur with probability 1/2. In those cases, in ideal conditions, there is a probability of 1/2 that the photon collapses into the location of the user that reflects. Finally, the reflected photon has at best a further probability of 1/2 to come out from the beam splitter at the output of detector D_1. Therefore, $\mathrm{p}(1)$ is at best 1/8, which is further reduced by experimental imperfections, eavesdropping or the action of an adversarial server.

For the rest of $(1 - \mathrm{p}(1))N$ rounds, the users exchange the information of their actions and detection results over the classical channel in order to estimate the parameters necessary for the establishment of a secret key between them. Note that it is enough that only one user, say Alice, performs the verification with the information received from the other. This allows for a reduction of the communication complexity. In addition to his action choices and results for the $(1 - \mathrm{p}(1))N$ rounds, Bob can also send the messages announced by the server over all the rounds. Alice will proceed with parameter estimation only if *all* of Bob's messages match with hers.

Using the information received from Bob for the $(1 - \mathrm{p}(1))N$ rounds, Alice can perform an indirect estimation method to evaluate the probability of exchanging a key bit, p_{key}, and the probability of error on the key, p_{err}, without the need to discard any key bit. A drawback of this indirect estimation is that p_{key} and p_{err} are obtained from other directly-measured quantities, therefore, due to error propagation, their uncertainty is higher. Alternatively, the users can exchange full information about their actions for a randomly chosen fraction τ of N_{raw} rounds to directly estimate the necessary probabilities. However, in the direct estimation, the uncertainty of the final probabilities depends on the size τ of the considered sub-sample. The choice of which method to use, therefore, depends on the experimental parameters and the length of the raw key.

4 Experimental implementation

The experimental set-up for the implementation of the protocol is depicted in Figure 2. After setting its polarization to "horizontal"(H), that is parallel to the optical table, a single photon is sent to a beam splitter that creates the superposition between Alice's and Bob's locations. Each of the users controls a liquid-

crystal cell (LCC) at 45° and a polarization beam splitter (PBS). The phase retardation between the two axes of the LCC can be switched between 0 and π by means of a voltage signal. Consequently, the photon polarization is rotated by 0° or 90°, respectively. In the first case, the photon is transmitted by the PBS and steered to a fiber-coupled avalanche photo-diode (APD) for detection, D_A or D_B; in the second case, the photon travels back to the server. The detection efficiency of D_A and D_B is evaluated by comparison with a fully-characterized transition-edge superconducting nanowire detector. The photons going back to the server impinge onto a second beam splitter, at whose outputs two fiber-coupled APDs, D_0 and D_1, are placed. The set-up, therefore, implements a folded Mach-Zehnder interferometer. The phase between the two arms of the interferometer is set such that, when Alice and Bob both decide to reflect back the photon, detector D_0 clicks. The interferometer is passively stabilized, so that the phase is constant for about 100 s. After this time, the phase is actively re-set to the initial value by using a piezo transducer.

The single photons are provided by a source based on spontaneous parametric down-conversion (SPDC) in a 20 mm-long periodically-poled potassium tytanyl phosphate (PPKTP) crystal, which probabilistically converts a photon at 395 nm from a continuous-wave laser into two photons at 790 nm and with orthogonal polarizations. One photon from each produced pair is used to herald the presence of the other one, which is sent to the users. Therefore, all detections in the experiment are in coincidence with the heralding detector, D_H. The server sets intervals of 0.5 s, constituting the rounds of the protocol, in which Alice and Bob can decide to either detect or reflect the photons. Note that this interval can be made shorter, in the order of 10^{-8} s, by using ultra-fast switches and optimized bright single-photon sources [27]. At the end of each round, the server announces the result of the measurement at its detectors. The probabilistic nature of our source implies that, in each round, multiple non-simultaneous single-photon emissions can occur. In some rounds, therefore, the total number of detections is higher than one. The output rate of the source is decreased, so that the total average number of photons sent to the users is about 0.35 per round, in order to reduce the probability of multi-photon emissions.

The possibility of simultaneous multi-photon emission from the source is ruled out by the measurement of the heralded second-order correlation function at zero delay, $g^{(2)}(0)$ [28], which should be exactly 0 for an ideal perfect single-photon source. We obtain $g^{(2)}(0) = 0.004 \pm 0.010$, measured at a total detection rate of about 15×10^3 photons per round (in our case 0.5 s) and a pump power of 7 mW. Our value of $g^{(2)}(0)$ is comparable with the lowest ones obtained in quantum optics experiments [29].

5 Security analysis

We prove security of our protocol under the following assumptions:

1. The server may be compromised by the adversary. In particular, it may prepare an arbitrary initial state and perform an arbitrary quantum operation on the returning signals (both subject to the other constraints listed below). Due to this assumption, we must only analyze the case of a single adversary, namely the server, and any third party adversary's attack may be absorbed into this adversarial server's attack strategy (to the advantage of the adversary).

2. The adversary performs collective attacks only. That is, the adversary attacks by using an identical attack operation at each iteration (both for the initial state preparation strategy and the final quantum operation strategy, including the message sending). The server's initial state may be entangled with a private quantum ancilla and the final operation may also result in a private quantum memory system. The adversary is free to postpone measuring its ancilla until any future point in time and may even perform an arbitrary global measurement of its entire ancilla at that future point in time.

3. The attack performed by the adversary on each iteration of the protocol is not interactive/adaptive. In particular, the adversary must prepare an initial state once at each iteration and send it to Alice and Bob. Although this initial state may consist of multiple photons, the server cannot feed a photon into Alice or Bob's lab, and then, based on the output, immediately feed additional photons into Alice or Bob's lab. While this seems a strong assumption, there are mechanisms to enforce its compliance as we discuss in Appendix B.1. Although a full analysis of interactive attacks would be very interesting, we consider it out of scope of this paper as we are primarily focused on the development, finite key analysis, and experimental demonstration of a novel mediated SQKD protocol with minimal end-user resource requirements. We do, however, consider an interactive attack based on a "quantum bomb" attack in Appendix B.1.

4. The initial state sent by the server consists of zero, one, or two photons prepared in an arbitrary manner. This was done as our experimental implementation consisted of a negligible probability of producing three or more photons. It is also an enforceable condition if Alice and Bob used cascading interferometers to ensure the state, with high probability, does not contain

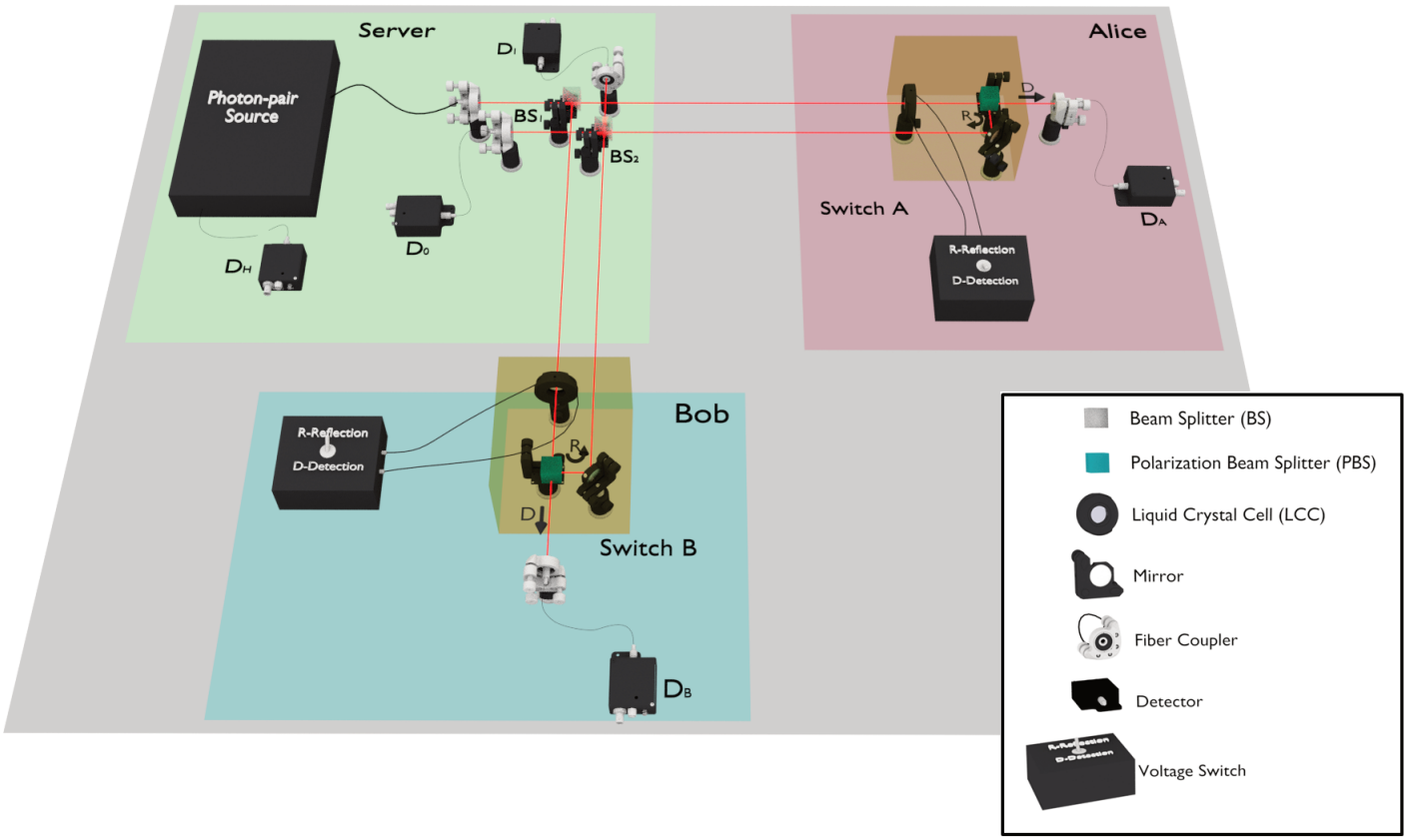

Figure 2: **Experimental set-up.** The regions of space occupied by Alice, Bob and the server are respectively marked in red, blue and green, whereas the path of the photons is indicated by red lines. The server uses a heralded single-photon source and a beam splitter (BS_1) to produce the superposition state that is sent to Alice and Bob. Each of the users controls a switch, composed of a liquid-crystal cell (LCC) at 45°, a polarization beam splitter (PBS) and a mirror. By switching the voltage of the LCC, the users can choose to steer the photon to a detector (D) or reflect it back to the server (R). The server collects the reflected photons at a second beam splitter (BS_2), where single-photon interference takes place in case both users choose to reflect. The server records the detections at D_0 and D_1 and announces the results to the users via a classical channel.

more than two photons. Our proof methodology, however, can be extended to consider the three or more photon case (assuming the attack is non-adaptive in this round as discussed above) if required. While we do not work out the exact algebra in this paper for that case, we do consider a particular multi-photon attack with three or more photons in Appendix B.2.

After Alice and Bob receive quantum states of some form from the server and perform their respective actions, they will receive a classical message from the sever indicating a possible measurement outcome. However, the server is under no obligation in our proof of security to report the measurement outcome honestly, or to even perform any measurement at all. On the rounds where the server announces "1", Alice and Bob generate the raw key of length N_{raw} whenever one of them chose to detect the photon without registering any click at the detector, while the other reflected. Note that due to experimental imperfections and eavesdropping (or server's dishonesty), server can announce "1" even if both agents reflected, or both detected vacuum, in which case they do not share the same raw key and the error is introduced. As mentioned before, from the raw key of size $N_{raw} = \mathrm{p}(1)N$, Alice and Bob may choose to use a (small) subset of size $\mu = \tau N_{raw}$ to directly estimate the statistics used to compute the secret key rate. The portion of the raw key remaining after parameter estimation step is called the sifted key, of the length $N_{sift} = N_{raw} - \mu$. Let the random variables $\mathcal{R}_A$ and $\mathcal{R}_B$ denote Alice's and Bob's respective sifted keys. After the quantum communication and sampling stages, it is not necessarily true that $\mathcal{R}_A$ and $\mathcal{R}_B$ are uniformly distributed or fully correlated. It is also not necessarily true that they are completely secret. Thus, the protocol must perform a classical post processing stage which further processes these raw key strings through error correction (to ensure they are perfectly correlated with high probability) and privacy amplification (which ensures that Eve's ancilla is independent of the final secret key.

The security level of the key shared between Alice and Bob is given by parameter ϵ, which quantifies how

uncorrelated the secret key is from Eve or a dishonest server. More formally, from [30, 31], one should have:

$$\left|\left|\rho_{KE} - \frac{I_K}{2^\ell} \otimes \rho_E\right|\right| \leq \epsilon, \tag{1}$$

where ρ_{KE} is the classical-quantum state modeling the secret key (after error-correction and privacy amplification) and Eve's ancilla, while $I_K/2^\ell \otimes \rho_E$ is an ideal uniform random key of size ℓ-bits independent of Eve. The security criterion requires ϵ to tend to zero as the number of rounds N tends to infinity, thus obtaining perfectly secret key in the asymptotic scenario. One can compute the sifted key rate as $r' = \lim_{N\to\infty} \ell/N_{sif} = S(A|C) - H(A|B)$ using results in [5]. Conditional Shannon entropy $H(A|B)$ can be easily computed using the probabilities $p_{i,j}$ of Alice and Bob establishing the raw key bit values i and j, respectively. Further, the secret key rate is defined as $r = \ell/N = r'(N_{sift}/N)$, which is the same as the sifted key rate in the asymptotic regime: since in order to obtain good enough statistics during the verification procedure, the number μ, albeit big, is still finite, we have $N_{sif} = N - \mu \approx N$, for $N \to \infty$. In the realistic case of limited resources, however, where Alice and Bob can exchange only a finite number of keys, we must take into account the imperfect parameters. Using the security criterion given by [31], let us denote ϵ_{PE} as a given error tolerance for the parameter estimation. One can further compute δ, as a function of ϵ_{PE}, a confidence interval so that the observed parameters are δ close to the actual values, except with probability ϵ_{PE}. Let ϵ be the desired security of the final secret key, and let ϵ_{EC} be the maximal probability that Bob computes error correction incorrectly. All of these are given by the user. Therefore, after μ rounds are used for the direct method of parameter estimation, the proportion of qubits used for estimating the secret key rate is $(\mathrm{p}(1)N - \mu)/N$. Using the results shown in [31], under the assumption of collective attacks, we have the following Theorem:

Theorem 1. *(Modified from [31]): Let $\rho_{AC}^{\otimes N}$ be the state of the quantum system produced by executing the protocol N times. Then, the key-rate r is bounded by:*

$$r \geq \frac{\mathrm{p}(1)N - \mu}{N}\left(S(A|C)_\rho - \frac{\texttt{leak}_{EC} + \Delta}{\mathrm{p}(1)N - \mu}\right), \tag{2}$$

where

$$\Delta = 2\log_2\left(\frac{1}{2(\epsilon - \epsilon_{EC} - \epsilon')}\right) + 7\sqrt{(\mathrm{p}(1)N - \mu)\log_2(2/(\epsilon' - \epsilon_{PE}))}. \tag{3}$$

Above, $S(A|C)_\rho$ is the conditional von Neumann entropy of Alice's raw key bit register conditioned on the server's quantum memory system. The value $\texttt{leak}_{EC}$ quantifies the error-correction leakage (namely, the number of classical bits exchanged between Alice and Bob during the error correction protocol). Finally, ϵ is the desired distance to an ideal key (as in Equation 1); ϵ_{PE} is the user specified error tolerance for the parameter estimation; ϵ_{EC} is the failure probability of the error correction protocol; and ϵ' is arbitrary (chosen by the user to maximize the expression) but bounded by $\epsilon - \epsilon_{EC} > \epsilon' > \epsilon_{PE} \geq 0$.

Of course, users don't have an exact description of ρ needed to directly compute $S(A|C)$ above. Thus, to actually compute the key-rate r, $S(A|C)$ is minimized over all observable statistics within the given confidence interval (so that the actual statistics of the real density operator are within $\delta(\epsilon_{PE})$ of the observed statistics, except with probability ϵ_{PE}). Later, in our security proof, we will use a theorem from [32], stated below as Theorem 2, to actually bound the entropy $S(A|C)$. The value $\texttt{leak}_{EC}$ represents the number of (classical) bits exchanged between Alice and Bob during the error correction. Again, using [31], we take $\texttt{leak}_{EC}/(\mathrm{p}(1)N - \mu) = (1.2)h(Q)$, where $Q = \mathrm{p}_{err}/\mathrm{p}(1)$ and p_{err} is the probability to generate opposite key bits during the entire protocol. Note that μ will also be a function of ϵ_{PE}, since the smaller that is, the larger μ will be.

Theorem 2. *(From [32]): Let ρ_{AC} be a quantum state of the form:*

$$\frac{1}{N}\sum_{a=0}^{2} |a\rangle\langle a|_A \otimes \left(\sum_{i=1}^{N} |F_i^a\rangle\langle F_i^a|_C\right). \tag{4}$$

Then, the von Neumann entropy $S(A|C)_\rho$ may be bounded by

$$S(A|C)_\rho \geq \frac{1}{N}\sum_{i=1,N}\left(\langle F_i^0|F_i^0\rangle + \langle F_i^1|F_i^1\rangle\right) \times \left[h\left(\frac{\langle F_i^0|F_i^0\rangle}{\langle F_i^0|F_i^0\rangle + \langle F_i^1|F_i^1\rangle}\right) - h(\lambda_i)\right],$$

where

$$\lambda_i = \frac{1}{2}\left(1 + \frac{\sqrt{(\langle F_i^0|F_i^0\rangle - \langle F_i^1|F_i^1\rangle)^2 + 4\mathrm{Re}^2\langle F_i^0|F_i^1\rangle}}{\langle F_i^0|F_i^0\rangle + \langle F_i^1|F_i^1\rangle}\right).$$

At a high level, our security proof involves bounding the conditional von Neumann entropy $S(A|C)$ of the system assuming an adversarial server. This is achieved by first writing out an explicit description of the overall state's density operator (including the photons in the interferometer, the agents, and the Server/adversary). We then show how certain important qualities of the state, namely the overlap of various ancilla vectors of the adversary, may be determined through observable statistics (such as, for instance, p_{err}). Finally, we use Theorem 2 to bound the conditional entropy and Theorem 1 to determine a final bound on the secret key rate. These steps are algebraically involved and so are derived in detail in the appendices. Namely, in Appendix C we derive the key rate for the ideal-qubit case. This first stage also

helps to develop the intuition of the proof used for the more complicated scenario involving practical device imperfections, presented in Appendix D. Bounding $S(A|C)$ is the critical, and challenging, element of any QKD security proof. The techniques to bound this quantity developed in this work may be useful in other protocols as well.

Our security analysis takes into account the finite detection efficiencies of commercial single-photon detectors and multi-photon components in the quantum state received by Alice and Bob (see Appendix A), but does not consider other imperfections which can be used by an eavesdropper to gain information about the key. This is in general an issue for all cryptographic protocols, both classical and quantum, as it is in practice very challenging to consider all potential side channels in the security analysis [33–37]. However, specific attacks can be countered by technical adaptations of the experimental set-up. As an example, let us consider the frequency dependence of the APD's detection efficiency. By sending photons at frequencies outside the detection bandwidth of the users' detectors, an eavesdropper can in fact gain information about the agents' actions while remaining completely undetected. This specific issue can be solved by employing bandpass filters that block any incoming light at undetectable frequencies. Similar strategies can be used for other degrees of freedom which the eavesdropper could exploit to prepare undetectable photons (e.g. time, spatial mode, etc.). Current photonic technology provides effective filtering systems for all these degrees of freedom [38–41], which allows the users to counter the described category of attacks at the price of a more complicated set-up and a reduction in the secret key rate.

6 Experimental Results

To obtain the numerical values from the lower-bounds on $S(A|C)$ and other terms from the expression (2) for the secret key rate, r, we measure the probability of the raw key generation, p_{key}, and the probability of error in the raw key, p_{err}, after 10^5 rounds of the protocol. Formally, p_{key} is defined to be the probability of Alice and Bob not rejecting a round, while p_{err} is the probability that, conditioned on a raw key bit being distilled, that the raw key bit contains an error (e.g., Alice has a 0 while Bob has a 1). Note that 10^5 rounds is not sufficient to actually produce a secret key through this protocol under these operating conditions as our later evaluations show; however, it is sufficient as a proof of concept to gather experimental statistics and evaluate what the key-rate *would be* had we continued the experiment for a longer duration.

The values of p_{key} and p_{err} are evaluated in three different ways: direct estimation over the full data set, direct estimation over a randomly chosen subset of 10^4 rounds and indirect estimation. In the direct estimation, the users sacrifice a part of the raw key for verification procedure (see Appendix E.1 for details). In the indirect estimation, discussed in detail in Appendix E.2, Alice obtains p_{key} and p_{err}, using the information received from Bob during the verification phase. This allows the parties to avoid the loss of key digits, at a price of higher uncertainty on the estimated values, which are calculated from several experimentally obtained quantities, each with its error. The results are reported in Table 1.

	Direct Method (full dataset)	Direct Method (subset)	Indirect Method (full dataset)
p_{key}	$1.55(3) \times 10^{-2}$	$1.5(1) \times 10^{-2}$	$1.5(3) \times 10^{-2}$
p_{err}	$7.5(8) \times 10^{-4}$	$5(2) \times 10^{-4}$	$3(3) \times 10^{-3}$

Table 1: **Evaluation of key generation and error rates**. The probabilities of raw-key generation, p_{key} and error on a key digit, p_{err}, respectively, are shown per round (in our case an interval of 0.5 s). In the table, the numbers in parentheses are the errors on the last digits, obtained with the assumption of poissonian uncertainty on the counts.

Based on the probabilities in Table 1, we obtain the dependence of the final secret key rate, r, on the number of rounds, N, see Equation (2). This dependence is plotted in Figure 3, for different values of the detection losses of $\mathrm{D_A}$ and $\mathrm{D_B}$, assumed to be the same. The details of how the curves were obtained are discussed in Appendices D and F. As expected, an increase in the detection loss degrades the performance of the protocol.

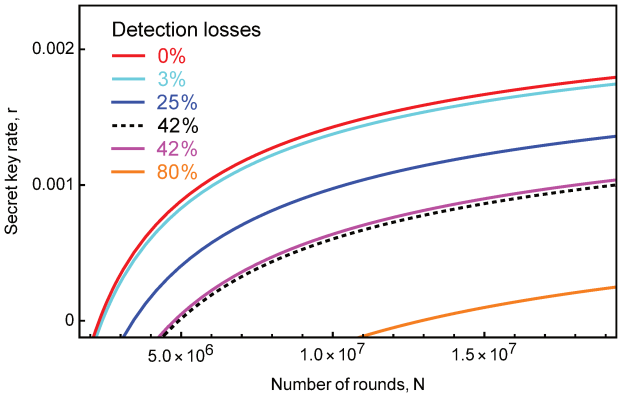

Figure 3: **Secret key rate vs number of rounds, for different values of detection loss**. The black dashed curve refers to the experimental implementation, corresponding to a detection loss of 42% for each Alice and Bob. The red, cyan, blue, magenta and orange curves represent the calculated results for detection losses of $0, 3, 25, 42$ and 80%, respectively. If the detection loss increases, the number of rounds for which r becomes positive also increases, while the asymptotic secret key rate decreases. In the implemented case, the secret key rate becomes positive after about 4.9×10^6 rounds.

We also report in Figure 4 the dependence of the secret key rate on the loss in the quantum channel between the server and each user, assumed to be the same for both, Alice and Bob. We present plots for

different values of the detection efficiency and the quantum bit error rate (QBER), which is defined as the fraction of errors in the sifted key. More details on how these plots are obtained can be found in Appendix G.

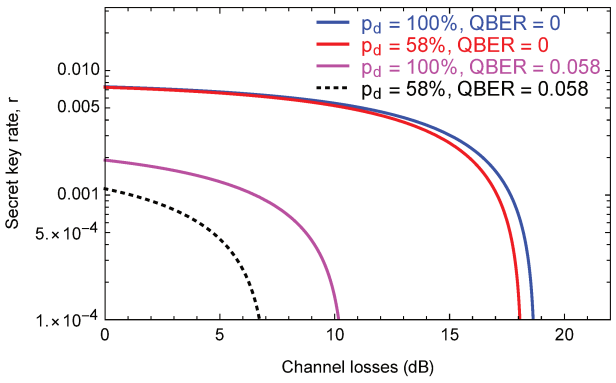

Figure 4: **Secret key rate vs channel transmission loss, for different values of detection efficiency and quantum bit error rate (QBER)**. The black dashed curve corresponds to the experimental parameters, with a detection efficiency of 58% for each Alice and Bob and a QBER of 0.058. The magenta, red and blue curve represent the three following ideal situations, respectively: perfect detectors and experimentally obtained QBER, imperfect detectors and QBER = 0, perfect detectors and QBER = 0. All curves are obtained by considering 10^9 rounds of the protocol and the statistics of the used single-photon source.

Given the results of Figure 4, we can compare the performance of our protocol to that of other QKD schemes. A natural candidate for the comparison is measurement-device-independent (MDI) QKD [42], which also involves an external server performing the detection. To our knowledge the best implementation to date of MDI-QKD achieves a secret key rate of about 10^{-4} for 7 dB of channel transmission loss [43]. We obtain a similar key rate at the same transmission loss, as shown by the dashed line in Figure 4. However, the secret key rate for our experimental parameters quickly decreases for higher losses, contrary to the realization in [43], where a secret key rate of 4.9×10^{-6} is reported for 20.4 dB of loss. Nevertheless, by considering QBER = 0, we obtain rates of the order of 10^{-4} for about 18 dB of channel loss. These results indicate that our protocol can perform as good as MDI-QKD for transmission losses up to about 7 dB, at least within the boundaries of our experimental implementation. At the moment, it is not clear if the performance could be made comparable also for higher losses, which however would require a more advanced experimental realization of our protocol.

Additionally, we stress that our estimated rates are lower-bounds and the actual key rates could be significantly higher. Indeed, to compute these lower bounds on $S(A|C)$, we took advantage of the strong subadditivity of von Neumann entropy by actually discarding several components of the entropy function (components which would only have increased Eve's uncertainty – thus, by discarding them, we are giving an unrealistic advantage to the adversary causing the key rate to drop). Such a method gives a worst-case computation.

7 Conclusions

In our work, we propose and experimentally implement a novel QKD protocol allowing two classical users to establish a shared secret key using the services of an untrusted quantum server, which provides a superimposed single photon as a feasible quantum resource. We underline the applicability of our scheme by providing an information-theoretic security analysis of our protocol in the finite-key setting, which takes into account imperfect detection efficiency and multi-photon emission from the source, and by calculating the secret key rate.

Experimentally, the main challenge of the protocol is that it requires phase stability in the interferometer formed between the users and the server. This issue can be addressed by using intrinsically phase-stable schemes, like Sagnac configurations [44]. In this case, however, a quantum channel between Alice and Bob is also necessary.

As an immediate future line of research, our security analysis of finite keys in the presence of experimental imperfections can be applied to show the same security levels for other cryptographic schemes, such as counterfactual quantum cryptography [45–49], or the key distribution based upon recently proposed two-way communication with one photon [50, 51].

In practical terms, recent progresses in bright deterministic single-photon sources [52], high-efficiency detectors [53] and fast switches [27] promise to push our scheme towards real-world applications.

Acknowledgments

We would like to thank Giulia Rubino for help with some figures and Borivoje Dakić and Ämin Baumeler for useful discussions. P.Y., P.M., N.P. and A.S. acknowledge the support of SQIG – Security and Quantum Information Group, the Instituto de Telecomunicações (IT) Research Unit, ref. UIDB/50008/2020 (actions QuRUNNER, QUESTS), funded by Fundação para a Ciência e Tecnologia (FCT), and the FCT projects QuantumMining POCI-01-0145-FEDER-031826, Predict PTDC/CCI-CIF/29877/2017 and QuantumPrime PTDC/EEI-TEL/8017/2020, supported by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project Q.DOT with Nr. 039728 (POCI-01-0247-FEDER-039728)], and by the Regional Operational Program of Lis-

bon. P.Y. acknowledges the support of DP-PMI and FCT (Portugal) through the scholarship PD/BD/113648/2015. W.K. is partially supported by NSF Grant No. 1812070. N.P. acknowledges FCT project CERN/FIS-PAR/0023/2019, as well as the FCT Estímulo ao Emprego Científico grant no. CEECIND/04594/2017/CP1393/CT000. A.S. acknowledges funds granted to LaSIGE Research Unit, ref. UID/CEC/00408/2013. P.W. acknowledges support from the research platform TURIS, from the European Commission through ErBeStA (No.800942), from the Austrian Science Fund (FWF) through BeyondC (F7113-N48) and Research Group 5 (FG5), and from the U.S. Air Force Office of Scientific Research (FA9550-21-1-0355) **Author contributions:** P.Y., W.K., P.M., N.P., A.S. developed the protocol and analysed its security. F.M., A.M. and P.W. designed and implemented the experiment and analysed the experimental data. All the authors contributed to the writing of the final manuscript. F.M. and P.Y. contributed equally to this work. **Corresponding authors:** correspondence to Francesco Massa (francesco.massa@univie.ac.at) or Philip Walther (philip.walther@univie.ac.at).

A Extraction of the secret key

In order to compute the secret key rate described above, one needs to compute $S(A|C)$ for a given system. Before we proceed to discuss the ideal and experimental scenario, let us first define some useful terminology.

Let us denote the Hilbert spaces corresponding to Alice's and Bob's equipments as $\mathcal{H}_A = \text{span}\{|D_c\rangle_A, |D_v\rangle_A, |D_\ell\rangle_A, |D'_\ell\rangle_A, |D'_c\rangle_A, |R\rangle_A\}$ and $\mathcal{H}_B = \text{span}\{|D_c\rangle_B, |D_v\rangle_B, |D_\ell\rangle_B, |D'_\ell\rangle_B, |D'_c\rangle_B, |R\rangle_B\}$, respectively. Here, $|D_c\rangle$ and $|D_v\rangle$ denote the states of a detector, the first corresponding to the case of a photon causing a click, and the second corresponding to the case when there were no photons, resulting in a no-click. The detectors' state corresponding to the case when an incoming photon was lost is denoted as $|D_\ell\rangle$. The state $|D'_\ell\rangle$ corresponds to a loss, while $|D'_c\rangle$ to a click, of the photon at time $t' \neq t$, when two non-simultaneous photons were emitted by the source at times t and t'. Finally, $|R\rangle$ denotes the state of a reflecting mirror. Note that the states corresponding to a click, $|D_c\rangle$ and $|D'_c\rangle$, and the ones corresponding to no-click, $|D_v\rangle$, $|D_\ell\rangle$ and $|D'_\ell\rangle$ are macroscopically distinguishable between each other as groups of those with or without clicks; and also to $|R\rangle$. However, the first two, $|D_c\rangle$ and $|D'_c\rangle$, are not distinguishable among each other, since in our set-up, Alice and Bob do not keep track of the detection times. Moreover, the latter three states, $|D_v\rangle$, $|D_\ell\rangle$ and $|D'_\ell\rangle$, also cannot be distinguished among each other, since without performing sophisticated quantum measurements, one cannot distinguish whether a detector did not click because there were no photons present, or they were lost.

We denote the server's Hilbert space as $\mathcal{H}_S = \text{span}\{|0\rangle_S, |1\rangle_S, |v\rangle_S, |m\rangle_S\}$ consists of macroscopic orthogonal states modeling classical messages "0", "1", "v" (vacuum) and "m" (multiple clicks), respectively. Additionally, we denote server's ancilla system by C, spanned by the Hilbert space $\mathcal{H}_C$, which a dishonest server can entangle with the photons sent to Alice and Bob to extract information about the exchanged key.

Let us assume Alice tosses a fair coin to decide whether she will detect or reflect the photon, and set the initial state of the apparatus accordingly, resulting in a proper mixture of the two states, $|D_v\rangle_A \langle D_v|$ and $|R\rangle_A \langle R|$, and analogously for Bob. Without the loss of generality, we can always include the coin states into the macroscopic description of the apparatus states, such that the purified initial state of Alice's apparatus is

$$|\phi_0\rangle_A = \frac{1}{\sqrt{2}}\Big(|D_v\rangle_A + |R\rangle_A \Big), \tag{5}$$

and analogously for Bob, making their joint state as

$$|\phi_0\rangle_{AB} = \frac{1}{2}\Big(|D_v,R\rangle_{AB} + |R,D_v\rangle_{AB} + |D_v,D_v\rangle_{AB} + |R,R\rangle_{AB}\Big). \tag{6}$$

Note that due to possible imperfect single-photon sources, and the presence of adversaries, the number of photons present is not necessarily fixed to be one. Thus, we will use a number basis to describe the photonic states. In this paper, we will decompose the overall Fock space of the photons in Alice's and Bob's arms as $\mathcal{F}_f = \text{span}\{|0,0\rangle_f, |1,0\rangle_f, |0,1\rangle_f, |2,0\rangle_f, |1,1'\rangle_f, |1',1\rangle_f, |0,2\rangle_f\} \oplus \mathcal{F}_f^k$, where $|0,0\rangle_f \equiv |v\rangle_f$ represents the vacuum state, $|1,0\rangle_f$ represents a photon in Alice's arm and $|0,1\rangle_f$ to be in Bob's arm. Similarly, $|2,0\rangle_f$, and $|0,2\rangle_f$, represent two non-simultaneous photons in Alice' and Bob's arms, respectively; whereas $|1,1'\rangle_f$ and $|1',1\rangle_f$ represent the case of two non-simultaneous photons when the first one went to Alice's arm while the second to Bob and vice-versa, respectively. $\mathcal{F}_f^k$ denotes the sub-space corresponding to the multi-photon case of $k > 2$ photons. The action of photonic creation operators $\hat{a}^\dagger$ and $\hat{b}^\dagger$, in terms of the number basis $|a,b\rangle_f$, with $a, b \in \mathbb{N}_0$ being the number of photons in Alice's and Bob's arms, respectively, is given by $(\hat{a}^\dagger)^a(\hat{b}^\dagger)^b |0\rangle_f = \sqrt{a!\,b!}\,|a,b\rangle_f$. We can now proceed to analyze the experimental implementation of our protocol with imperfect single-photon sources and detectors, as well as the noisy and lossy channels.

We assume an untrusted server that can attack before Alice and Bob perform their respective operations, as well as after (which is equivalent to allowing Eve to intercept the photons exchanged between an honest server and the agents). We consider a poissonian probabilistic single photon source, emitting vacuum state with probability p_0, single photons with probability p_1, two non-simultaneous photons with probability p_2, etc., within a time slot of interval T, as

$$|\phi_0\rangle_f = \sqrt{\mathrm{p}_0}\,|v\rangle_f + \sqrt{\frac{\mathrm{p}_1}{T}}\int_0^T \hat{a}^\dagger(t)\,|v\rangle_f\,\mathrm{d}t + \frac{\sqrt{\mathrm{p}_2}}{T}\int_0^T\int_0^T\left(\frac{\hat{a}^\dagger(t)\hat{a}^\dagger(t')}{\sqrt{2}}\,|v\rangle_f\right)\mathrm{d}t\,\mathrm{d}t' + \ldots, \tag{7}$$

where $\hat{a}^\dagger(t)$ and $\hat{a}^\dagger(t')$ represent photon creation at times t and t', respectively. In our particular implementation, the average number of photons is 0.35, yielding $\mathrm{p}_0 = 0.705$, $\mathrm{p}_1 = 0.247$, $\mathrm{p}_2 = 0.043$. For simplicity, and in order to compare the theoretical analysis with our experimental data, the probability to emit higher numbers of photons is considered negligible, i.e., $\mathrm{p}_0 + \mathrm{p}_1 + \mathrm{p}_2 \approx 1$. Thus, the initial photon state is

$$|\phi_0\rangle_f = \sqrt{\mathrm{p}_0}\,|v\rangle_f + \sqrt{\mathrm{p}_1}\,|1\rangle_f + \sqrt{\mathrm{p}_2}\,|2\rangle_f\,, \tag{8}$$

where $|v\rangle_f \equiv |0\rangle_f$ is the photon vacuum state, $|1\rangle_f = \hat{a}^\dagger(t)\,|v\rangle_f$, $\sqrt{2}\,|2\rangle_f = \hat{a}^\dagger(t)\hat{a}^\dagger(t')\,|v\rangle_f$. Nevertheless, our analysis can straightforwardly generalised to an arbitrary number of emitted photons. Note that, for simplicity, we omitted the time integrals in the definition of the single- and two-photon states, $|1\rangle_f$ and $|2\rangle_f$, respectively, as we consider that the users do not keep track of the photon detection times, meaning that, at the end of each round, Alice, Bob and the server only have access to the number of detections they recorded. This makes our analysis also applicable to the case of simultaneous multi-photon emission.

After passing through the first 50/50 beam splitter of our interferometer, described by $\hat{a}^\dagger(t) \to (\hat{a}^\dagger(t) + \hat{b}^\dagger(t))/\sqrt{2}$ and $\hat{a}^\dagger(t') \to (\hat{a}^\dagger(t') + \hat{b}^\dagger(t'))/\sqrt{2}$, the above state becomes

$$|\phi_0\rangle_f = \sqrt{\mathrm{p}_0}\,|v\rangle_f + \sqrt{\frac{\mathrm{p}_1}{2}}\Big(\,|1,0\rangle_f + |0,1\rangle_f\,\Big) + \frac{\sqrt{\mathrm{p}_2}}{2}\Big(\,|2,0\rangle_f + |1,1'\rangle_f + |1',1\rangle_f + |0,2\rangle_f\,\Big). \tag{9}$$

Upon possible further action of the adversary, the most general photon-server (normalized) state is given by

$$\begin{aligned}
|\phi_0\rangle_{fC} &= \sum_{\substack{a,b\geq 0\\ a+b\leq 2}} |a,b\rangle_f\,|c_{a,b}\rangle_C \\
&= |0,0\rangle_f \otimes |c_{0,0}\rangle_C \\
&\quad + |1,0\rangle_f \otimes |c_{1,0}\rangle_C + |0,1\rangle_f \otimes |c_{0,1}\rangle_C \\
&\quad + |2,0\rangle_f \otimes |c_{2,0}\rangle_C + |0,2\rangle_f \otimes |c_{0,2}\rangle_C + |1,1'\rangle_f \otimes |c_{1,1'}\rangle_C + |1',1\rangle_f \otimes |c_{1',1}\rangle_C\,.
\end{aligned} \tag{10}$$

where $|c_{a,b}\rangle_C \in \mathcal{H}_C$ (not necessarily orthogonal, nor normalized states) are associated to the cases when there are a and b photons entering Alice's and Bob's arms, respectively. Nevertheless, the states $|c_{a,b}\rangle_C$ are arbitrary and contain any number of photons. Therefore, the overall state before the photon(s) enter Alice's and Bob's labs is

$$\begin{aligned}
|\phi_0\rangle_{ABfC} &= |\phi_0\rangle_{AB} \otimes |\phi_0\rangle_{fC} \\
&= \frac{1}{2}\Big(|D_v,D_v\rangle_{AB} + |D_v,R\rangle_{AB} + |R,D_v\rangle_{AB} + |R,R\rangle_{AB}\Big) \\
&\quad \otimes \Big(|0,0\rangle_f \otimes |c_{0,0}\rangle_C \\
&\qquad + |1,0\rangle_f \otimes |c_{1,0}\rangle_C + |0,1\rangle_f \otimes |c_{0,1}\rangle_C \\
&\qquad + |2,0\rangle_f \otimes |c_{2,0}\rangle_C + |0,2\rangle_f \otimes |c_{0,2}\rangle_C + |1,1'\rangle_f \otimes |c_{1,1'}\rangle_C + |1',1\rangle_f \otimes |c_{1',1}\rangle_C\Big).
\end{aligned} \tag{11}$$

Let us denote Alice's and Bob's respective detectors' efficiencies as p_d^A and p_d^B, with the respective losses being $\mathrm{p}_\ell^A = 1 - \mathrm{p}_d^A$ and $\mathrm{p}_\ell^B = 1 - \mathrm{p}_d^B$. In our experimental implementation, the two efficiencies are almost the

same, with $\mathrm{p}_d^A \approx \mathrm{p}_d^B \approx 58\%$. The individual actions of, say, Alice, in this practical scenario are

$$
\begin{aligned}
&|D_v\rangle_A |0\rangle_f \to |D_v\rangle_A |0\rangle_f ,\\
&|D_v\rangle_A |1\rangle_f \to \left(\sqrt{\mathrm{p}_\ell^A}\,|D_\ell\rangle_A + \sqrt{\mathrm{p}_d^A}\,|D_c\rangle_A\right)|0\rangle_f ,\\
&|D_v\rangle_A |2\rangle_f \to \Big(\mathrm{p}_\ell^A\,|D_\ell D'_\ell\rangle_A + \sqrt{\mathrm{p}_\ell^A \mathrm{p}_d^A}\,|D_c D'_\ell\rangle_A\\
&\qquad\qquad + \sqrt{\mathrm{p}_\ell^A \mathrm{p}_d^A}\,|D_\ell D'_c\rangle_A + \mathrm{p}_d^A\,|D_c D'_c\rangle_A\Big)|0\rangle_f ,\\
&|R\rangle_A |0\rangle_f \to |R\rangle_A |0\rangle_f ,\\
&|R\rangle_A |1\rangle_f \to |R\rangle_A |1\rangle_f ,\\
&|R\rangle_A |2\rangle_f \to |R\rangle_A |2\rangle_f ,
\end{aligned}
\tag{12}
$$

where primed and unprimed states of the apparatuses correspond to at times t' and t, respectively. Note that we assume that Alice and Bob trust their detectors with their finite detection efficiencies. Therefore, upon applying U_1, given in terms of Alice's and Bob's local actions described by (12), we obtain the state $|\phi_1\rangle_{AB\mathfrak{f}C} = U_1\,|\phi_0\rangle_{AB\mathfrak{f}C}$.

Upon leaving Alice's and Bob's labs, the server (or Eve) will apply a quantum instrument to the returning photon-server state. This can be modelled as an isometry $\mathcal{I} : \mathcal{F}_f \otimes \mathcal{H}_C \to \mathcal{H}_S \otimes \mathcal{H}_C$, given by

$$
\mathcal{I}\,|a', b'\rangle_f\,|c_{a,b}\rangle_C = |0\rangle_S\,|e^{a,b}_{a',b'}\rangle_C + |1\rangle_S\,|f^{a,b}_{a',b'}\rangle_C + |v\rangle_S\,|g^{a,b}_{a',b'}\rangle_C + |m\rangle_S\,|h^{a,b}_{a',b'}\rangle_C ,
\tag{13}
$$

where states $|e^{a,b}_{a',b'}\rangle_C, |f^{a,b}_{a',b'}\rangle_C, |g^{a,b}_{a',b'}\rangle_C, |h^{a,b}_{a',b'}\rangle_C \in \mathcal{H}_C$ are again not necessarily normalized, nor orthogonal. Note that, due to the action of U_1, the photon numbers a, b are no longer correlated to $a', b' \in \{0, 1, 2\}$; nevertheless, we still have $a' + b' \leq 2$. From this, one obtains the final state between the users and the server, $|\phi_2\rangle_{ABSC} = \mathcal{I}\,|\phi_1\rangle_{AB\mathfrak{f}C}$. Using Theorem 2, one can lower bound the conditional entropy $S(A|C)$, as explained in detail in the next section.

B Two particular attacks

B.1 Adaptive attack with a single photon

The adaptive attack with a single photon that is fed in an agent's laboratory several times during a single round of the key distribution protocol is based on the interaction-free measurement proposed in [54], depict in Figure 5. An agent, say Alice, is placed in one arm of an interferometer which consist of an input polarizing beam splitter and standard balanced beam splitter on its output. Before entering the interferometer, the initial polarization state, say horizontal state $|\psi_0\rangle = |H\rangle$, is rotated by a certain angle θ, so that before the polarizing beam splitter it is $|\psi_\theta\rangle = \cos\theta\,|H\rangle + \sin\theta\,|V\rangle$. In case Alice decided to "reflect", at the output of the interferometer the polarization state of the photon will stay the same, $|\psi_\theta\rangle$. In case she decided to "detect", with probability $\sin^2\theta$ the photon will end up in Alice's laboratory and be absorbed, while with probability $\cos^2\theta$ it will leave the interferometer in polarization state $|\psi_0\rangle$. In the case of the latter, the process is repeated, up to M times. If the rotation angle is chosen to be $\theta = \pi/2M$, after M iterations the polarization state will be $|\psi_{\pi/2}\rangle = |V\rangle$ in case Alice decided to "reflect", while it will stay "frozen" to $|\psi_0\rangle = |H\rangle$ in case she decided to "detect", i.e., the two states will be fully distinguishable, and Eve would know Alice's action. The probability that a photon will not end in Alice's arm M consecutive times when she decided to "detect" is $p = \cos^{2M}\theta = (\cos\frac{\pi}{2M})^{2M}$, which for large M behaves like $p \sim 1 - \pi^2/4M \to 1$. Thus, with probability arbitrarily close to 1 Eve can learn Alice's action without triggering her detector ("activating the bomb" from the original scenario discussed in [54]).

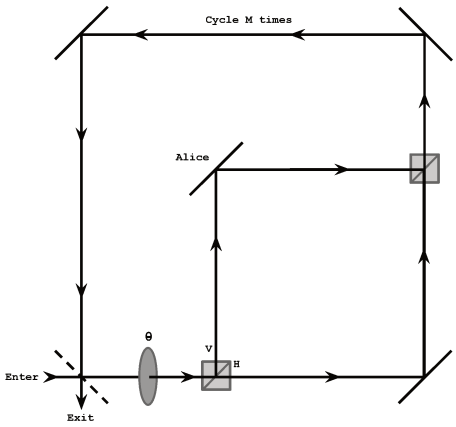

Figure 5: **Eve's attack based on interaction-free measurement.**

But in our case, the aim of Eve is to simulate, as much as possible, the honest scenario, in which Alice's detector will click in about half of the cases. This is achieved with pretty good accuracy for $M = 4$ already, as we have that $p = (\cos\frac{\pi}{8})^8 \approx 0.53$. Nevertheless, if Eve wanted to learn the actions of both agents, she would need to perform two such measurements performed on both agents. But this would inevitably lead to increased double clicks in rounds when both agents decide to "detect" (Note that in order to learn the action of a single agent, say Alice, Eve should perform measurement after her laboratory, thus destroying any possible coherence between photon(s) state in Alice's and Bob's labs). During the parameter estimation phase, Alice and Bob can infer such increased probability of coincidences, and thus detect eavesdropping.

B.2 Multi-photon attack

This is a version of the above interaction attack in which instead of sending a single photon through the interferometer M times, Eve sends M photons only once, in order to learn action of a single agent. Thus, it suffers from the same deficiency as the previous attack: Alice's photon detection is not correlated with Bob's one and therefore will change the joint detection statistics. Again, note that in order to learn the action of a single agent, Eve must perform her measurement on the photons outside her/his lab, thus destroying any possible coherence. In other words, sending a coherent superposition between photon states sent to Alice and Bob offers no advantage.

But this attack features additional problem, in that Eve cannot fully distinguish between an agent's actions, leading her to announce inconsistent messages allowing Alice and Bob to additionally detect cheating. Let us first describe this attack in more detail. Eve sends a multi-photon state $|\Psi_\theta(M)\rangle = |\psi_\theta\rangle^{\otimes M} = (\cos\theta\,|H\rangle + \sin\theta\,|V\rangle)^{\otimes M}$. If Alice decides to "reflect", Eve will receive the same M-photon state $|\Psi_\theta(M)\rangle$ at the output of the interferometer. In case she decides to "detect" and at least one of the photons ends in her arm, there will be less then M photons at the output of the interferometer, and Eve can thus infer Alice's action. But if not a single photon gets detected by Alice, at the output of the interferometer we would have the M-photon state $|\Psi_0(M)\rangle = |\psi_0\rangle^{\otimes M} = |H\rangle^{\otimes M}$. Thus, Eve cannot distinguish the two actions by measuring the photon number, and she needs to subsequently perform polarization measurement. The optimal discrimination probability for the two states is given in terms of the transition probability $\tilde{p} = |\langle\Psi_0|\Psi_\theta\rangle|^2 = |\langle\psi_0|\psi_\theta\rangle|^{2M} = \cos^{2M}\theta$, which is precisely the probability that in the case of deciding to "detect" none of M photons end up in Alice's arm. On the other hand, as before we want that this probability is equal to $1/2$, to match the honest scenario. Thus, if Eve wants to emulate the honest scenario, she must set θ such that the output polarization states are far from fully distinguishable. In other words, the adversary will necessarily occasionally announce messages that are inconsistent with the agents' actions, thus revealing eavesdropping. One can straightforwardly apply our methodology to this case to obtain quantitative expression for the secret key rate. Therefore, we omit this rather complex, but straightforward analysis.

C Security Analysis - Ideal case

In Appendix D, we show how to prove the security of our protocol in the general case, assuming practical devices. To develop the intuition behind the proof in that section, however, we first consider the ideal case scenario. Here, we assume that the server has a perfect single-photon source, Alice's and Bob's detectors are

perfect, which means they have 100% detection efficiency and zero dark counts, but there may be channel loss. Therefore, the perfect single photon state that Alice and Bob expect to be sent is

$$|\phi_0\rangle_f = \left(\frac{\hat{a}^\dagger + \hat{b}^\dagger}{\sqrt{2}}\right)|0,0\rangle_f = \frac{|1,0\rangle_f + |0,1\rangle_f}{\sqrt{2}}, \tag{14}$$

with $|1,0\rangle_f$ and $|0,1\rangle_f$ representing the photon located in Alice's and Bob's arms, respectively. However, we assume that the following entangled state is sent to Alice and Bob by the server (or Eve)

$$|\phi_0\rangle_{fC} = |0,0\rangle_f \otimes |c_{0,0}\rangle + |1,0\rangle_f \otimes |c_{1,0}\rangle_C + |0,1\rangle_f \otimes |c_{0,1}\rangle_C \tag{15}$$

where $|c_{a,b}\rangle_C \in \mathcal{H}_C$ are not necessarily orthogonal nor normalized. Note that, this is the state arriving at A and B's lab, and so it also incorporates channel loss in the $|0,0\rangle_f \otimes |c_{0,0}\rangle$ term. Moreover, as per usual in QKD security proofs, Alice and Bob can enforce symmetry, and so, we may assume $\langle c_{0,1}|c_{0,1}\rangle_C = \langle c_{1,0}|c_{1,0}\rangle$. Therefore, we can write the joint initial state as

$$\begin{aligned} |\phi_0\rangle_{ABfC} &= |\phi_0\rangle_{AB} \otimes |\phi_0\rangle_{fC} \\ &= \frac{1}{2}\Big(|D_v,R\rangle_{AB} + |R,D_v\rangle_{AB} + |D_v,D_v\rangle_{AB} + |R,R\rangle_{AB}\Big) \\ &\quad \otimes \Big(|0,0\rangle_f |c_{0,0}\rangle_C + |1,0\rangle_f |c_{1,0}\rangle_C + |0,1\rangle_f |c_{0,1}\rangle_C\Big). \end{aligned} \tag{16}$$

Alice's and Bob's actions on a given initial photon state are given by

$$\begin{aligned} &|D_v,R\rangle|1,0\rangle \to |D_c,R\rangle|0,0\rangle, && |R,D_v\rangle|1,0\rangle \to |R,D_v\rangle|1,0\rangle, \\ &|D_v,R\rangle|0,1\rangle \to |D_v,R\rangle|0,1\rangle, && |R,D_v\rangle|0,1\rangle \to |R,D_c\rangle|0,0\rangle, \\ &|D_v,D_v\rangle|1,0\rangle \to |D_c,D_v\rangle|0,0\rangle, && |R,R\rangle|1,0\rangle \to |R,R\rangle|1,0\rangle, \\ &|D_v,D_v\rangle|0,1\rangle \to |D_v,D_c\rangle|0,0\rangle, && |R,R\rangle|0,1\rangle \to |R,R\rangle|0,1\rangle, \\ &|D_v,D_v\rangle|0,0\rangle \to |D_v,D_v\rangle|0,0\rangle, && |R,R\rangle|0,0\rangle \to |R,R\rangle|0,0\rangle, \\ &|D_v,R\rangle|0,0\rangle \to |D_v,R\rangle|0,0\rangle, && |R,D_v\rangle|0,0\rangle \to |R,D_v\rangle|0,0\rangle, \end{aligned} \tag{17}$$

and, therefore

$$\begin{aligned} |\phi_1\rangle_{ABfC} = \frac{1}{2}\Big[&|D_c,R\rangle|0,0\rangle|c_{1,0}\rangle + |D_v,R\rangle|0,1\rangle|c_{0,1}\rangle + |R,D_v\rangle|1,0\rangle|c_{1,0}\rangle_C + |R,D_c\rangle|0,0\rangle|c_{0,1}\rangle \\ &+ |D_c,D_v\rangle|0,0\rangle|c_{1,0}\rangle + |D_v,D_c\rangle|0,0\rangle|c_{0,1}\rangle + |R,R\rangle\big(|1,0\rangle|c_{1,0}\rangle + |0,1\rangle|c_{0,1}\rangle \\ &+ |D_v,D_v\rangle|0,0\rangle|c_{0,0}\rangle + |D_v,R\rangle|0,0\rangle|c_{0,0}\rangle + |R,D_v\rangle|0,0\rangle|c_{0,0}\rangle + |R,R\rangle|0,0\rangle|c_{0,0}\rangle\Big]. \end{aligned} \tag{18}$$

Following this, as in the experimental case, the adversary will apply a quantum instrument to the returning photon state which, as before, can be modeled as an isometry, whose action is defined as

$$\mathcal{I}|a',b'\rangle_f |c_{a,b}\rangle_C = |0\rangle_S |e^{a,b}_{a',b'}\rangle_C + |1\rangle_S |f^{a,b}_{a',b'}\rangle_C + |v\rangle_S |g^{a,b}_{a',b'}\rangle_C, \tag{19}$$

where states from $\mathcal{H}_C$ are not necessarily normalized nor orthogonal, and a, b are no longer correlated with a', b' due to Alice's and Bob's actions given by Equation (17). Note that since we are assuming an ideal case, the term corresponding to the message "m" is absent from the above equation.

We are interested only in the rounds when the server announces "1" and neither Alice nor Bob detect a photon, and the users generate the key. Thus, while writing the state after the server applies $\mathcal{I}$ on $|\phi_1\rangle_{ABfC}$, we will omit writing the server's message state $|1\rangle_S$ (corresponding to announcing a result "1"). The final density operator representing the state of the system ABC, conditioned on the event that the server sends the message "1" and none of the users detects a photon (only the rounds used for key generation), is

$$|\phi_2\rangle_{ABC} = \frac{1}{\sqrt{\mathcal{N}}}\Big\{|D_v,R\rangle \otimes |k_{0,0}\rangle + |R,D_v\rangle \otimes |k_{1,1}\rangle + |R,R\rangle \otimes |k_{1,0}\rangle + |D_v,D_v\rangle \otimes |k_{0,1}\rangle\Big\}, \tag{20}$$

where the states $|k_{i,j}\rangle_C$ are associated to Alice establishing the value i and Bob j as a key bit, are given by

$$\begin{aligned}
|k_{0,0}\rangle_C &= \frac{1}{2}\left[|f_{0,1}^{0,1}\rangle + |f_{0,0}^{0,0}\rangle\right], \\
|k_{1,1}\rangle_C &= \frac{1}{2}\left[|f_{1,0}^{1,0}\rangle + |f_{0,0}^{0,0}\rangle\right], \\
|k_{0,1}\rangle_C &= \frac{1}{2}|f_{0,0}^{0,0}\rangle, \\
|k_{1,0}\rangle_C &= \frac{1}{2}\left[|f_{1,0}^{1,0}\rangle + |f_{0,1}^{0,1}\rangle + |f_{0,0}^{0,0}\rangle\right].
\end{aligned} \tag{21}$$

Note that, though we are assuming in this ideal setting, that A and B's devices are ideal, the adversarial server may still "simulate" imperfect detectors which may have, for instance, dark counts (incorporated in the term $\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle$ which is the probability the server sends a positive message in the event a vacuum actually enters its lab). The normalization constant $\mathcal{N}$ is, again, the probability to obtain the result 1, p(1), when there were no clicks at the users' detectors, and is given by

$$\mathcal{N} = \langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle + \langle k_{0,1}|k_{0,1}\rangle = \mathrm{p}(1). \tag{22}$$

As in the experimental case, we define $\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1) = \langle k_{0,0}|k_{0,0}\rangle$ as the joint probability for the event when Alice detects vacuum and Bob reflects, and the server announces the result "1", and analogously $\mathrm{p}_{1,1}$, $\mathrm{p}_{0,1}$ and $\mathrm{p}_{1,0}$. Again, we use the semicolon (;) to denote logical AND operation between two propositions. Therefore, we can define the probability to share the key as $\mathrm{p}_{key} = \mathrm{p}_{0,0} + \mathrm{p}_{1,1}$ and the probability of an error as $\mathrm{p}_{err} = \mathrm{p}_{0,1} + \mathrm{p}_{1,0}$. When we evaluate our key rate bound, we use $\mathcal{Q}$ to be the probability that the server announces the result "1", given both Alice and Bob reflected, conditioned on a photon arriving at the server. Finally, we allow the adversarial server to "simulate" dark counts at a rate of p_d (to its advantage), and we use T to mean the probability of transmittance in one direction, namely $1-T$ is the probability the photon is dropped before it gets to A or B (the probability the photon returns to the server if A and B reflect is T^2). In the ideal case, it is easy to see that

$$\begin{aligned}
\mathrm{p}_{0,0} = \langle k_{0,0}|k_{0,0}\rangle &= \frac{1}{4}\left(\frac{T^2}{4} + \frac{T(1-T)p_d}{2}\right), \quad \mathrm{p}_{0,1} = \langle k_{0,1}|k_{0,1}\rangle = \frac{(1-T)p_d}{4}, \\
\mathrm{p}_{1,1} = \langle k_{1,1}|k_{1,1}\rangle &= \frac{1}{4}\left(\frac{T^2}{4} + \frac{T(1-T)p_d}{2}\right), \quad \mathrm{p}_{1,0} = \langle k_{1,0}|k_{1,0}\rangle = \frac{\mathcal{Q}\cdot T^2}{4}.
\end{aligned} \tag{23}$$

Expanding $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$, needed for the entropy bound computation, we find:

$$\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle = \frac{1}{4}(\mathrm{Re}\,\langle f_{0,1}^{0,1}|f_{1,0}^{1,0}\rangle + \mathrm{Re}\,\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \mathrm{Re}\,\langle f_{0,1}^{0,1}|f_{0,0}^{0,0}\rangle + \mathrm{Re}\,\langle f_{0,0}^{0,0}|f_{1,0}^{1,0}\rangle) \tag{24}$$

Expanding $\langle k_{1,0}|k_{1,0}\rangle$ we find:

$$\begin{aligned}
\langle k_{1,0}|k_{1,0}\rangle &= \frac{1}{4}(\langle f_{1,0}^{1,0}|f_{1,0}^{1,0}\rangle + \langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle + \langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + 2\mathrm{Re}(\langle f_{0,1}^{0,1}|f_{1,0}^{1,0}\rangle + \langle f_{0,1}^{0,1}|f_{0,0}^{0,0}\rangle + \langle f_{1,0}^{1,0}|f_{0,0}^{0,0}\rangle)). \\
\Rightarrow \mathrm{Re}(\langle f_{0,1}^{0,1}|f_{1,0}^{1,0}\rangle + \langle f_{0,1}^{0,1}|f_{0,0}^{0,0}\rangle + \langle f_{1,0}^{1,0}|f_{0,0}^{0,0}\rangle) &= \frac{4\,\langle k_{1,0}|k_{1,0}\rangle - (\langle f_{1,0}^{1,0}|f_{1,0}^{1,0}\rangle + \langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle + \langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle)}{2}
\end{aligned} \tag{25}$$

Substituting Equation (25) into Equation (24) we have:

$$\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle = \frac{1}{2}\,\langle k_{1,0}|k_{1,0}\rangle - \frac{1}{8}(\langle f_{1,0}^{1,0}|f_{1,0}^{1,0}\rangle + \langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle + \langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle). \tag{26}$$

The term $\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle$ is an observable quantity, it is simply $4\,\langle k_{0,1}|k_{0,1}\rangle = 4p_{0,1}$. The values of $\langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle$ and $\langle f_{1,0}^{1,0}|f_{1,0}^{1,0}\rangle$ can be bounded by solving the following quadratic equation (derived from the expansion of $\langle k_{0,0}|k_{0,0}\rangle$ and $\langle k_{1,1}|k_{1,1}\rangle$ respectively):

$$\langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle + 2\cos\theta\sqrt{\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle}\sqrt{\langle f_{0,1}^{0,1}|f_{0,1}^{0,1}\rangle} + (\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle - 4\,\langle k_{0,0}|k_{0,0}\rangle). \tag{27}$$

Similarly for $\langle f_{1,0}^{1,0}|f_{1,0}^{1,0}\rangle$. This allows us to minimize $|\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle|$, thus minimizing the adversary's uncertainty (i.e., minimizing $S(A|C)$).

At this point, we compute the conditional entropy between Alice and the adversary, $S(A|C)$, for the rounds where raw key bits are generated. Using Equation (20), the density operator, after dropping off-diagonal terms, with $|k_{i,j}\rangle_C\langle k_{l,m}|$, for $(i,j) \neq (l,m)$, is

$$\rho_{ABC} = \frac{1}{\mathcal{N}} \Big(|D_v,R\rangle_{AB}\langle D_v,R| \otimes |k_{0,0}\rangle_C\langle k_{0,0}| + |R,D_v\rangle_{AB}\langle R,D_v| \otimes |k_{1,1}\rangle_C\langle k_{1,1}| + |R,R\rangle_{AB}\langle R,R| \otimes |k_{1,0}\rangle_C\langle k_{1,0}| + |D_v,D_v\rangle_{AB}\langle D_v,D_v| \otimes |k_{0,1}\rangle_C\langle k_{0,1}| \Big). \tag{28}$$

The state $|D_v,R\rangle\langle D_v,R|$, describing Alice detecting without a click and Bob reflecting, is associated to a shared key bit 0. Similarly, $|R,D_v\rangle\langle R,D_v|$ is associated to a key bit 1. Whereas, $|R,R\rangle\langle R,R|$ and $|D_v,D_v\rangle\langle D_v,D_v|$ corresponds to errors in the key, when the two users establish opposite key bit values.

Now that we have a description of the quantum state, we can use Theorem 2 to compute a bound on the conditional entropy $S(A|C)$ leading us to:

$$S(A|C) \geq \frac{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle}{\mathcal{N}} \left[h\left(\frac{\langle k_{0,0}|k_{0,0}\rangle}{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle} \right) - h(\lambda_0) \right], \tag{29}$$

with λ_0 is defined as in Equation (37).

We present the dependence of the secret key rate r on the total number of rounds N for different values of $\mathcal{Q}$ (including the one obtained from the experimental set-up) in Figure 6 for $T = 1$. Other parameters are taken from [31] as $\epsilon = 10^{-5}$, $\epsilon_{EC} = 10^{-10}$ and $\epsilon' = 10^{-7}$. We also assume $\epsilon_{PE} = 10^{-11}$. In Figure 7, we report key-rate as a function of total transmission loss in one direction where we set p_d to be a negligible 10^{-8} to consider ideal devices on the server also.

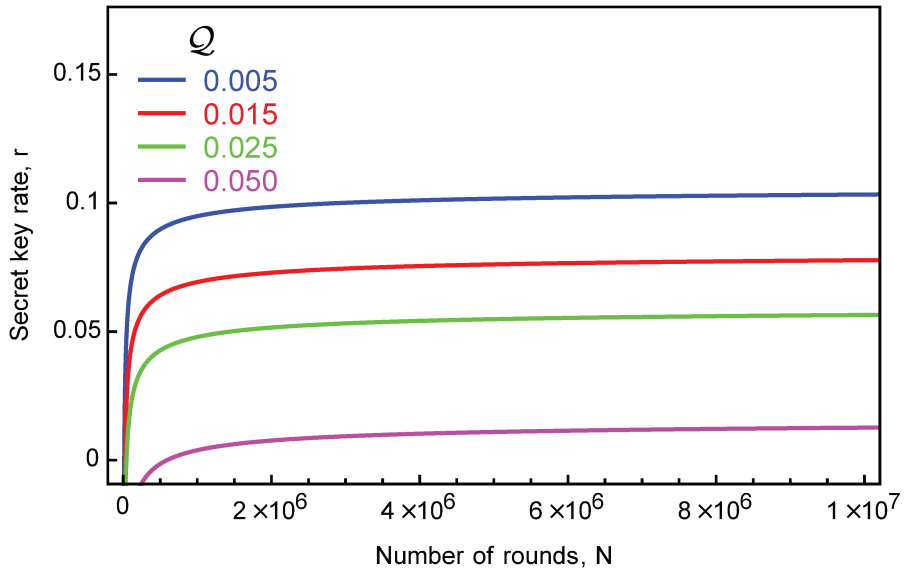

Figure 6: The secret key rate r is plotted against N, for the ideal case of perfect single-photon sources and detectors. The blue, green and magenta curves correspond to the values of $\mathcal{Q}$ to be $0.005, 0.025$ and 0.05, respectively. Whereas, the red curve represents the experimentally observed value of $\mathcal{Q}$, 0.015.

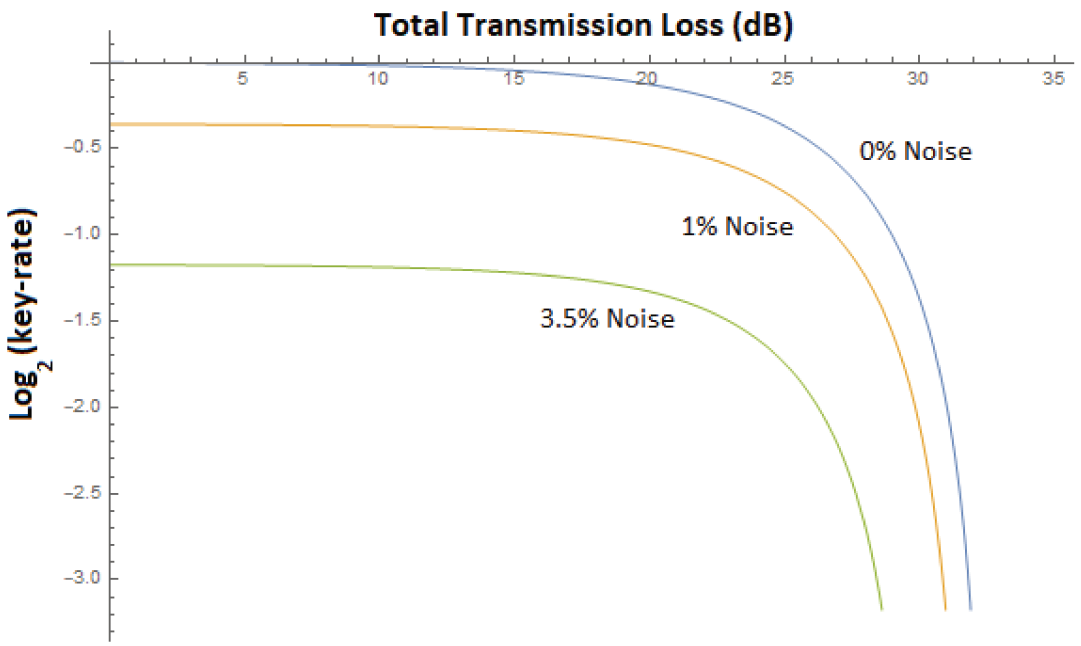

Figure 7: The secret key rate r is plotted against transmission loss in one direction (server to end-users), for the ideal case of perfect single-photon sources and detectors in the asymptotic setting (taking the number of iterations to be infinite and with perfect error correction).

D Security Analysis - General Case

By straightforward algebra, from Equations (11), (12) and (13), we get $|\phi_2\rangle_{ABSC} = \mathcal{I}\,|\phi_1\rangle_{ABfC}$. However, we are only interested in the key-generation rounds, i.e., we condition to the event when the server announces "1" and neither Alice nor Bob receives a click. Hence, omitting writing the message state $|1\rangle_S$, the final density operator (without the off-diagonal terms) of the system ABC is

$$\begin{aligned}\rho_{ABC} = \frac{1}{\mathcal{N}}\Big[& |D_v,R\rangle_{AB}\langle D_v,R| \otimes |k_{0,0}\rangle_C\langle k_{0,0}| + |R,D_v\rangle_{AB}\langle R,D_v| \otimes |k_{1,1}\rangle_C\langle k_{1,1}| \\ & + |D_\ell,R\rangle_{AB}\langle D_\ell,R| \otimes |k^1_{0,0}\rangle_C\langle k^1_{0,0}| + |R,D_\ell\rangle_{AB}\langle R,D_\ell| \otimes |k^1_{1,1}\rangle_C\langle k^1_{1,1}| \\ & + |D'_\ell,R\rangle_{AB}\langle D'_\ell,R| \otimes |k^2_{0,0}\rangle_C\langle k^2_{0,0}| + |R,D'_\ell\rangle_{AB}\langle R,D'_\ell| \otimes |k^2_{1,1}\rangle_C\langle k^2_{1,1}| \\ & + |D_\ell D'_\ell,R\rangle_{AB}\langle D_\ell D'_\ell,R| \otimes |k^3_{0,0}\rangle_C\langle k^3_{0,0}| + |R,D_\ell D'_\ell\rangle_{AB}\langle R,D_\ell D'_\ell| \otimes |k^3_{1,1}\rangle_C\langle k^3_{1,1}| \\ & + |D_v,D_v\rangle_{AB}\langle D_v,D_v| \otimes |k_{0,1}\rangle_C\langle k_{0,1}| + |R,R\rangle_{AB}\langle R,R| \otimes |k_{1,0}\rangle_C\langle k_{1,0}| \\ & + |D_\ell,D_v\rangle_{AB}\langle D_\ell,D_v| \otimes |k^1_{0,1}\rangle_C\langle k^1_{0,1}| + |D_v,D_\ell\rangle_{AB}\langle D_v,D_\ell| \otimes |k^2_{0,1}\rangle_C\langle k^2_{0,1}| \\ & + |D_\ell,D'_\ell\rangle_{AB}\langle D_\ell,D'_\ell| \otimes |k^3_{0,1}\rangle_C\langle k^3_{0,1}| + |D'_\ell,D_\ell\rangle_{AB}\langle D'_\ell,D_\ell| \otimes |k^4_{0,1}\rangle_C\langle k^4_{0,1}| \\ & + |D_\ell D'_\ell,D_v\rangle_{AB}\langle D_\ell D'_\ell,D_v| \otimes |k^5_{0,1}\rangle_C\langle k^5_{0,1}| + |D_v,D_\ell D'_\ell\rangle_{AB}\langle D_v,D_\ell D'_\ell| \otimes |k^6_{0,1}\rangle_C\langle k^6_{0,1}|\Big].\end{aligned} \tag{30}$$

Note that, as before, we use commas in the states from $\mathcal{H}_A \otimes \mathcal{H}_B$ to separate the quantum numbers defining Alice's and Bob's apparatus states: $|D_\ell D'_\ell,R\rangle_{AB}$ means that Alice opted to detect, unsuccessfully (due to finite detection efficiency) the two photons present in her lab, while Bob set his apparatus to reflect, etc. The states $|k_{i,j}\rangle_C$, etc., are associated to the cases when Alice establishes the value i and Bob j as a key bit, and are given

by

$$
\begin{aligned}
|k_{0,0}\rangle &= \frac{1}{2}\left[|f^{0,0}_{0,0}\rangle + |f^{0,1}_{0,1}\rangle + |f^{0,2}_{0,2}\rangle\right], & |k_{1,1}\rangle &= \frac{1}{2}\left[|f^{0,0}_{0,0}\rangle + |f^{1,0}_{1,0}\rangle + |f^{2,0}_{2,0}\rangle\right],\\
|k^1_{0,0}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\left[|f^{1,0}_{0,0}\rangle + |f^{1,1}_{0,1}\rangle\right], & |k^1_{1,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\left[|f^{0,1}_{0,0}\rangle + |f^{1,1}_{1,0}\rangle\right],\\
|k^2_{0,0}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\,|f^{1',1}_{0,1}\rangle, & |k^2_{1,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\,|f^{1,1'}_{1,0}\rangle,\\
|k^3_{0,0}\rangle &= \frac{1}{2}\mathrm{p}^A_\ell\,|f^{2,0}_{0,0}\rangle, & |k^3_{1,1}\rangle &= \frac{1}{2}\mathrm{p}^B_\ell\,|f^{0,2}_{0,0}\rangle,\\
|k_{0,1}\rangle &= \frac{1}{2}\,|f^{0,0}_{0,0}\rangle, & |k_{1,0}\rangle &= \frac{1}{2}\big[\,|f^{0,0}_{0,0}\rangle + |f^{1,0}_{1,0}\rangle + |f^{0,1}_{0,1}\rangle + |f^{2,0}_{2,0}\rangle,\\
& & & \quad + |f^{1,1'}_{1,1'}\rangle + |f^{1',1}_{1',1}\rangle + |f^{0,2}_{0,2}\rangle\,\big],\\
|k^1_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\,|f^{1,0}_{0,0}\rangle, & |k^4_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell\,\mathrm{p}^B_\ell}\,|f^{1',1}_{0,0}\rangle,\\
|k^2_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\,|f^{0,1}_{0,0}\rangle, & |k^5_{0,1}\rangle &= \frac{1}{2}\mathrm{p}^A_\ell\,|f^{2,0}_{0,0}\rangle,\\
|k^3_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell\,\mathrm{p}^B_\ell}\,|f^{1,1'}_{0,0}\rangle, & |k^6_{0,1}\rangle &= \frac{1}{2}\mathrm{p}^B_\ell\,|f^{0,2}_{0,0}\rangle.
\end{aligned}
\tag{31}
$$

Above, as well as in rest of the Appendix, for simplicity we omit writing the labels of the quantum states (A, B, C, S and f), whenever it is implicitly unambiguous to which space they belong by their quantum numbers (D_v, $0,0$, etc.).

The normalization constant $\mathcal{N}$ from Equation (30) is the probability to obtain the result "1" when there were no clicks at the agents' detectors, given by

$$
\begin{aligned}
\mathcal{N} = \;& \langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle\\
& + \langle k_{0,1}|k_{0,1}\rangle + \langle k^1_{0,1}|k^1_{0,1}\rangle + \langle k^2_{0,1}|k^2_{0,1}\rangle + \langle k^3_{0,1}|k^3_{0,1}\rangle + \langle k^4_{0,1}|k^4_{0,1}\rangle + \langle k^5_{0,1}|k^5_{0,1}\rangle + \langle k^6_{0,1}|k^6_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle\,.
\end{aligned}
\tag{32}
$$

In ρ_{ABC}, given by Equation (30), the state $|D_v,R\rangle\langle D_v,R|$ describes Alice detecting without a click and Bob reflecting, and is associated to a shared key bit of 0. Let us define $\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1) = \langle k_{0,0}|k_{0,0}\rangle$ as the joint probability for the event when Alice detects vacuum and Bob reflects, and the server announces the result "1", which corresponds to the users sharing a key bit of 0. Here we use the semicolon (;) to denote logical AND operation between two propositions. Note that $|D_\ell,R\rangle\langle D_\ell,R|$, $|D'_\ell,R\rangle\langle D'_\ell,R|$, and $|D_\ell D'_\ell,R\rangle\langle D_\ell D'_\ell,R|$ also correspond to a shared key bit of 0, and are a consequence of Alice's imperfect detector and multi-photon events. Therefore, one can analogously define the probabilities $\mathrm{p}^1_{0,0}, \mathrm{p}^2_{0,0}$ and $\mathrm{p}^3_{0,0}$, such that the total probability of the users sharing a key bit of 0 can be given by $\tilde{\mathrm{p}}_{0,0} = \mathrm{p}_{0,0} + \mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} + \mathrm{p}^3_{0,0}$. Analogously, the probabilities, $\mathrm{p}_{1,1}, \mathrm{p}^1_{1,1}, \mathrm{p}^2_{1,1}$ and $\mathrm{p}^3_{1,1}$, associated to a key bit 1 are defined. The k_{ij}'s with $i \neq j$ are associated to the errors, i.e., when the two users establish opposite key bit values. From the above definitions, using k_{ij} and $\mathcal{N}$, we have

$$
\frac{\langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle}{\mathcal{N}} = \mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R|1).
\tag{33}
$$

Here, by $\mathrm{p}(\mathcal{P}|\mathcal{C})$ we denote the conditional probability that the proposition $\mathcal{P}$ holds (in the above case, Alice detects and observes no clicks, while Bob reflects), given that the condition $\mathcal{C}$ is satisfied (in the above case, the server announces "1"). Therefore, using the following terminology for different probabilities (to be used in parameter estimation described in the next section), the probability to share the key is given by

$$
\begin{aligned}
\mathrm{p}_{key} &= \left[\langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle\right] + \left[\langle k_{1,1}|k_{1,1}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle\right]\\
&= \left[\mathrm{p}_{0,0} + \mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} + \mathrm{p}^3_{0,0}\right] + \left[\mathrm{p}_{1,1} + \mathrm{p}^1_{1,1} + \mathrm{p}^2_{1,1} + \mathrm{p}^3_{1,1}\right]\\
&= \tilde{\mathrm{p}}_{0,0} + \tilde{\mathrm{p}}_{1,1}\\
&= \mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;1) + \mathrm{p}(R,D_v \vee R,D_\ell \vee R,D'_\ell \vee R,D_\ell D'_\ell\,;1),
\end{aligned}
\tag{34}
$$

where $\mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;1)$ represents the joint probability of the following event: Alice detects vacuum, Bob reflects, and the server announces the result "1"; and analogously for the other term. As before, we use the semicolon (;) to denote logical AND operation between two propositions, instead of introducing the

additional parenthesis for the first one, and using the standard symbol $\wedge$. The probability of error in the raw key is given by

$$\begin{aligned}
\mathrm{p}_{err} &= \left[\langle k_{0,1}|k_{0,1}\rangle + \langle k^1_{0,1}|k^1_{0,1}\rangle + \langle k^2_{0,1}|k^2_{0,1}\rangle + \langle k^3_{0,1}|k^3_{0,1}\rangle + \langle k^4_{0,1}|k^4_{0,1}\rangle + \langle k^5_{0,1}|k^5_{0,1}\rangle + \langle k^6_{0,1}|k^6_{0,1}\rangle\right] + \langle k_{1,0}|k_{1,0}\rangle \\
&= \left[\mathrm{p}_{0,1} + \mathrm{p}^1_{0,1} + \mathrm{p}^2_{0,1} + \mathrm{p}^3_{0,1} + \mathrm{p}^4_{0,1} + \mathrm{p}^5_{0,1} + \mathrm{p}^6_{0,1}\right] + \mathrm{p}_{1,0} \\
&= \tilde{\mathrm{p}}_{0,1} + \tilde{\mathrm{p}}_{1,0} \\
&= \mathrm{p}(D_v, D_v \vee D_\ell, D_v \vee D_v, D_\ell \vee D_\ell, D'_\ell \vee D'_\ell, D_\ell \vee D_v, D_\ell D'_\ell \vee D'_\ell D_\ell, D_v\,; 1) + \mathrm{p}(RR\,; 1),
\end{aligned} \tag{35}$$

where $\mathrm{p}(D_v, D_v \vee D_\ell, D_v \vee D_v, D_\ell \vee D_\ell, D'_\ell \vee D'_\ell, D_\ell \vee D_v, D_\ell D'_\ell \vee D'_\ell D_\ell, D_v\,; 1)$ represents the joint probability of the event: Alice and Bob both detect vacuum, and that the server announces the result "1"; and analogously for the other term. Note that the probabilities $\tilde{\mathrm{p}}_{i,j}$ can be observed from the experiment directly.

To obtain the secret key rate, we again use the bound given in Theorem 2, as

$$\begin{aligned}
S(A|C) \;\geq\; & \frac{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k_{0,0}|k_{0,0}\rangle}{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle}\right] - h(\lambda_0)\right) \\
& + \frac{\langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^1_{0,0}|k^1_{0,0}\rangle}{\langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle}\right] - h(\lambda_1)\right) \\
& + \frac{\langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^2_{0,0}|k^2_{0,0}\rangle}{\langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle}\right] - h(\lambda_2)\right) \\
& + \frac{\langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^3_{0,0}|k^3_{0,0}\rangle}{\langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle}\right] - h(\lambda_3)\right) \\
& + \frac{\langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k_{0,1}|k_{0,1}\rangle}{\langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle}\right] - h(\lambda_4)\right),
\end{aligned} \tag{36}$$

where $h(\cdot)$ is the binary Shannon entropy, and λ_i's are defined in the following way

$$\begin{aligned}
\lambda_0 &= \frac{1}{2}\left(1 + \frac{\sqrt{\left(\langle k_{0,0}|k_{0,0}\rangle - \langle k_{1,1}|k_{1,1}\rangle\right)^2 + 4\mathrm{Re}^2\,\langle k_{0,0}|k_{1,1}\rangle}}{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle}\right), \\
\lambda_1 &= \frac{1}{2}\left(1 + \frac{\sqrt{\left(\langle k^1_{0,0}|k^1_{0,0}\rangle - \langle k^1_{1,1}|k^1_{1,1}\rangle\right)^2 + 4\mathrm{Re}^2\,\langle k^1_{0,0}|k^1_{1,1}\rangle}}{\langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle}\right), \\
\lambda_2 &= \frac{1}{2}\left(1 + \frac{\sqrt{\left(\langle k^2_{0,0}|k^2_{0,0}\rangle - \langle k^2_{1,1}|k^2_{1,1}\rangle\right)^2 + 4\mathrm{Re}^2\,\langle k^2_{0,0}|k^2_{1,1}\rangle}}{\langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle}\right), \\
\lambda_3 &= \frac{1}{2}\left(1 + \frac{\sqrt{\left(\langle k^3_{0,0}|k^3_{0,0}\rangle - \langle k^3_{1,1}|k^3_{1,1}\rangle\right)^2 + 4\mathrm{Re}^2\,\langle k^3_{0,0}|k^3_{1,1}\rangle}}{\langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle}\right), \\
\lambda_4 &= \frac{1}{2}\left(1 + \frac{\sqrt{\left(\langle k_{0,1}|k_{0,1}\rangle - \langle k_{1,0}|k_{1,0}\rangle\right)^2 + 4\mathrm{Re}^2\,\langle k_{0,1}|k_{1,0}\rangle}}{\langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle}\right).
\end{aligned} \tag{37}$$

The first four terms in $S(A|C)$ correspond to the keys shared between Alice and Bob, while the last term corresponds to errors in the key. However, we estimate the lower bound on $S(A|C)$ by considering only the first term since its contribution to the entropy is far larger than that of any of the other terms. From the expression (37) for λ_0, we see that minimizing $S(A|C)$ essentially means minimizing $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$. Therefore, in addition to different probabilities obtained from the experiment, we also need to estimate $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$. We proceed by computing the lower bound for $\mathrm{Re}^2\,\langle k_{0,0}|k_{1,1}\rangle$, i.e., for $|\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle\,|$. Notice that the lower it is, the closer to 1/2 λ_0 is, i.e., the closer to 1 the $h(\lambda_0)$ is, and the worst case scenario for $S(A|C)$, has the lowest value.

Let us use the following notation for simplification,

$$|x\rangle = |f^{1,0}_{1,0}\rangle + |f^{2,0}_{2,0}\rangle\,, \qquad |y\rangle = |f^{0,1}_{0,1}\rangle + |f^{0,2}_{0,2}\rangle\,, \qquad |z\rangle = |f^{1,1'}_{1,1'}\rangle + |f^{1',1}_{1',1}\rangle\,. \tag{38}$$

We can rewrite $|k_{0,0}\rangle$ and $|k_{1,1}\rangle$ from Equation (31), to obtain $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ as

$$\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle = \frac{1}{4}\left[\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \mathrm{Re}\,\langle x|f_{0,0}^{0,0}\rangle + \mathrm{Re}\,\langle f_{0,0}^{0,0}|y\rangle + \mathrm{Re}\,\langle x|y\rangle\right]. \tag{39}$$

From the error term, we have $\langle k_{1,0}|k_{1,0}\rangle = \mathrm{p}(R,R|1)\mathrm{p}(R,R) = \mathcal{Q}/4$, where $\mathcal{Q} = \mathrm{p}(R,R|1)$ is the probability that the server announces the result "1", given both Alice and Bob reflected, and $\mathrm{p}(R,R) = 1/4$. With straightforward substitution from the above into Equation (39), with $\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle = 4\,\langle k_{0,1}|k_{0,1}\rangle = 4\mathrm{p}_{0,1}$, we get

$$\langle k_{0,0}|k_{1,1}\rangle = \frac{\mathcal{Q}}{8} + \frac{\mathrm{p}_{0,1}}{2} - \frac{1}{8}\left[\langle x|x\rangle + \langle y|y\rangle + \langle z|z\rangle\right] - \frac{1}{4}\left[\langle x|z\rangle + \langle y|z\rangle + \langle f_{0,0}^{0,0}|z\rangle\right]. \tag{40}$$

In the ideal case, with no vacuum or multi-photon pulses, when $\langle x|x\rangle = 4\,\langle k_{0,0}|k_{0,0}\rangle = 4\mathrm{p}_{0,0}$ and $\langle y|y\rangle = 4\,\langle k_{1,1}|k_{1,1}\rangle = 4\mathrm{p}_{1,1}$, we recover the ideal case expression 26 from Appendix C. By writing $\langle x|z\rangle = |\,\langle x|z\rangle\,|e^{\varphi_{x,z}}$, we have

$$\mathrm{Re}\,\langle x|z\rangle = |\,\langle x|z\rangle\,|\cos\varphi_{x,y} = ||\,|x\rangle\,|| \cdot ||\,|z\rangle\,|| \cdot |\cos\chi_{x,z}|\cos\varphi_{x,z} = \sqrt{\langle x|x\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{x,z}, \tag{41}$$

where $\chi_{x,z}$ denotes the angle between $|x\rangle$ and $|z\rangle$ and $\cos\theta_{x,z} \equiv |\cos\chi_{x,z}|\cos\varphi_{x,z}$, and analogously for $\mathrm{Re}\,\langle y|z\rangle$ and so on. Therefore, the final expression for $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ is

$$\begin{aligned}\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle = \frac{\mathcal{Q}}{8} + \frac{\mathrm{p}_{0,1}}{2} - \frac{1}{8}\left[\langle x|x\rangle + \langle y|y\rangle + \langle z|z\rangle\right] - \frac{1}{4}\left[\sqrt{\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{f,z}\right] \\ -\frac{1}{4}\left[\sqrt{\langle x|x\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{x,z} + \sqrt{\langle y|y\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{y,z}\right].\end{aligned} \tag{42}$$

To obtain $\langle x|x\rangle$ and $\langle y|y\rangle$, consider again $|k_{0,0}\rangle$ and $|k_{1,1}\rangle$ from Equation (31)

$$\begin{aligned}\langle k_{1,1}|k_{1,1}\rangle &= \frac{1}{4}\left[\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \langle x|x\rangle + 2\mathrm{Re}\,\langle f_{0,0}^{0,0}|x\rangle\right], \\ \langle k_{0,0}|k_{0,0}\rangle &= \frac{1}{4}\left[\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \langle y|y\rangle + 2\mathrm{Re}\,\langle f_{0,0}^{0,0}|y\rangle\right].\end{aligned} \tag{43}$$

Note that $\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle = 4\,\langle k_{0,1}|k_{0,1}\rangle = 4\mathrm{p}_{0,1}, \langle k_{0,0}|k_{0,0}\rangle = \mathrm{p}_{0,0}$ and $\langle k_{1,1}|k_{1,1}\rangle = \mathrm{p}_{1,1}$. Therefore, solving the quadratic equations obtained from (43), we get the following positive roots of $\sqrt{\langle x|x\rangle}$ and $\sqrt{\langle y|y\rangle}$,

$$\begin{aligned}\sqrt{\langle x|x\rangle} &= 2\left[-\sqrt{\mathrm{p}_{0,1}}\cos\theta_{x,f} + \sqrt{\mathrm{p}_{1,1} - (1 - \cos^2\theta_{x,f})\,\mathrm{p}_{0,1}}\right], \\ \sqrt{\langle y|y\rangle} &= 2\left[-\sqrt{\mathrm{p}_{0,1}}\cos\theta_{y,f} + \sqrt{\mathrm{p}_{0,0} - (1 - \cos^2\theta_{y,f})\,\mathrm{p}_{0,1}}\right].\end{aligned} \tag{44}$$

Analogously, for $\langle z|z\rangle$ we have

$$\begin{aligned}\langle z|z\rangle + \underbrace{2\left[\sqrt{\langle x|x\rangle}\,\cos\,\theta_{x,z} + \sqrt{\langle y|y\rangle}\,\cos\,\theta_{y,z} + 2\sqrt{\mathrm{p}_{0,1}}\,\cos\,\theta_{f,z}\right]}_{\beta}\sqrt{\langle z|z\rangle} \\ \underbrace{+\,4\left[\mathrm{p}_{0,1} - \mathrm{p}_{1,0}\right] + \left[\langle x|x\rangle + \langle y|y\rangle + 2\sqrt{\langle x|x\rangle}\sqrt{\langle y|y\rangle}\,\cos\,\theta_{x,y}\right] + 4\sqrt{\mathrm{p}_{0,1}}\left[\sqrt{\langle x|x\rangle}\,\cos\,\theta_{x,f} + \sqrt{\langle y|y\rangle}\,\cos\,\theta_{y,f}\right]}_{\gamma} = 0,\end{aligned} \tag{45}$$

where $\cos\theta_{x,z} \equiv |\cos\chi_{x,z}|\cos\varphi_{x,z}$ and analogously for $\cos\theta_{y,z}$, $\cos\theta_{f,z}$, etc. Again, solving the above quadratic equation, we can obtain the positive root of $\sqrt{\langle z|z\rangle}$.

E Parameter estimation

Here, we briefly explain how to estimate the relevant probabilities, $\mathrm{p}_{0,0}, \mathrm{p}_{1,1}$ and $\mathrm{p}_{0,1}$, to compute $S(A|C)$ in Equation (36), to eventually obtain the secret key rate given by Equation (1) from the main text.

Due to the nature of this protocol, in the ideal case, one expects $\mathrm{p}(1) = 1/8$ (see Appendix C for details), which is further reduced in the experimental case of imperfect detectors, etc. Therefore, it is useful if these probabilities could be computed without sacrificing any key-generation rounds. Below, we discuss the case with direct estimation where Alice and Bob use part of the key to obtain these probabilities, as well as the case of indirect estimation where no key-generation rounds are wasted.

E.1 Direct estimation

Here, we sacrifice μ instances of the total N_{raw} key-generation rounds, to directly compute the relevant probabilities. However, since Alice's and Bob's detectors are imperfect, they cannot compute $\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1)$ and $\mathrm{p}_{1,1} = \mathrm{p}(R,D_v\,;1)$ directly, as they cannot differentiate the event D_v,R from the events D_ℓ,R, D'_ℓ,R and $D_\ell D'_\ell,R$, and analogously for R,D_v. However, they can obtain $\tilde{\mathrm{p}}_{0,0} = \mathrm{p}_{0,0} + \mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} + \mathrm{p}^3_{0,0} = \mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;1)$ directly, and also $\tilde{\mathrm{p}}_{1,1}$. They can then compute $\mathrm{p}^1_{0,0} = \langle k^1_{0,0}|k^1_{0,0}\rangle$, $\mathrm{p}^2_{0,0} = \langle k^2_{0,0}|k^2_{0,0}\rangle$ and $\mathrm{p}^3_{0,0} = \langle k^3_{0,0}|k^3_{0,0}\rangle$, to eventually obtain $\mathrm{p}_{0,0}$. From Equation (31) one has

$$\begin{aligned}
\mathrm{p}^1_{0,0} &= \mathrm{p}(D_\ell,R\,;1) = \frac{\mathrm{p}^A_\ell}{4}\left(\left|\left|\,|f^{1,0}_{0,0}\rangle + |f^{1,1'}_{0,1'}\rangle\,\right|\right|^2\right),\\
\mathrm{p}^2_{0,0} &= \mathrm{p}(D'_\ell,R\,;1) = \frac{\mathrm{p}^A_\ell}{4}\,\langle f^{1',1}_{0,1}|f^{1',1}_{0,1}\rangle\,,\\
\mathrm{p}^3_{0,0} &= \mathrm{p}(D_\ell D'_\ell,R\,;1) = \frac{\mathrm{p}_\ell^{A^2}}{4}\,\langle f^{2,0}_{0,0}|f^{2,0}_{0,0}\rangle\,.
\end{aligned} \tag{46}$$

Even though Alice and Bob cannot compute the above probabilities, they can estimate them by looking at the events corresponding to the clicks, using the expressions

$$\begin{aligned}
\mathrm{p}(D_c,R\,;1) &= \frac{\mathrm{p}^A_d}{4}\left(\left|\left|\,|f^{1,0}_{0,0}\rangle + |f^{1,1'}_{0,1'}\rangle\,\right|\right|^2\right),\\
\mathrm{p}(D'_c,R\,;1) &= \frac{\mathrm{p}^A_d}{4}\,\langle f^{1',1}_{0,1}|f^{1',1}_{0,1}\rangle\,,\\
\mathrm{p}(D_cD'_c,R\,;1) &= \frac{\mathrm{p}_d^{A^2}}{4}\,\langle f^{2,0}_{0,0}|f^{2,0}_{0,0}\rangle\,.
\end{aligned} \tag{47}$$

Therefore, we can write $\left(\mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0}\right)$ and $\mathrm{p}^3_{0,0}$ as

$$\mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} = \left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)\mathrm{p}(D_c,R \vee D'_c,R\,;1), \qquad \mathrm{p}^3_{0,0} = \left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)^2\mathrm{p}(D_cD'_c,R\,;1), \tag{48}$$

where only $\mathrm{p}(D_cD'_c,R\,;1)$ can be obtained using the rounds when Alice gets double clicks in her detector. However, $\mathrm{p}(D_c,R \vee D'_c,R \vee D_\ell D'_c,R \vee D_cD'_\ell,R\,;1)$, corresponding to a single click in Alice's detector, can also be obtained directly. Hence,

$$\mathrm{p}(D_c,R \vee D'_c,R\,;1) = \mathrm{p}(D_c,R \vee D'_c,R \vee D_\ell D'_c,R \vee D_cD'_\ell,R\,;1) - \mathrm{p}(D_\ell D'_c,R\,;1) - \mathrm{p}(D_cD'_\ell,R\,;1). \tag{49}$$

Also, we have

$$\mathrm{p}(D_\ell D'_c,R\,;1) = \frac{\mathrm{p}^A_\ell \mathrm{p}^A_d}{4}\,\langle f^{2,0}_{0,0}|f^{2,0}_{0,0}\rangle = \mathrm{p}(D_cD'_\ell,R\,;1). \tag{50}$$

Therefore, the required probabilities $\mathrm{p}_{0,0}$ and $\mathrm{p}_{1,1}$ are

$$\begin{aligned}
\mathrm{p}_{0,0} &= \tilde{\mathrm{p}}_{0,0} - \left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)\mathrm{p}(D_c,R \vee D'_c,R \vee D_\ell D'_c,R \vee D_cD'_\ell,R\,;1) + \left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)^2\mathrm{p}(D_cD'_c,R\,;1),\\
\mathrm{p}_{1,1} &= \tilde{\mathrm{p}}_{1,1} - \left(\frac{\mathrm{p}^B_\ell}{\mathrm{p}^B_d}\right)\mathrm{p}(R,D_c \vee R,D'_c \vee R,D_\ell D'_c \vee R,D_cD'_\ell\,;1) + \left(\frac{\mathrm{p}^B_\ell}{\mathrm{p}^B_d}\right)^2\mathrm{p}(D_cD'_c,R\,;1).
\end{aligned} \tag{51}$$

Additionally, to compute $\mathrm{p}_{0,1}$, required to estimate $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ from Equation (42), we use $\mathrm{p}_{0,1} = \tilde{\mathrm{p}}_{0,1} - \mathrm{p}^1_{0,1} - \mathrm{p}^2_{0,1} - \mathrm{p}^3_{0,1} - \mathrm{p}^4_{0,1} - \mathrm{p}^5_{0,1} - \mathrm{p}^6_{0,1}$. Again, using straightforward algebra, we have

$$\begin{aligned}
\mathrm{p}_{0,1} = \tilde{\mathrm{p}}_{0,1} &- \left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)\mathrm{p}(D_c,D_v \vee D_c,D'_\ell \vee D'_c,D_\ell \vee D_cD'_\ell,D_v \vee D_\ell D'_c,D_v\,;1)\\
&- \left(\frac{\mathrm{p}^B_\ell}{\mathrm{p}^B_d}\right)\mathrm{p}(D_v,D_c \vee D_\ell,D'_c \vee D'_\ell,D_c \vee D_v,D_cD'_\ell \vee D_v,D_\ell D'_c\,;1)\\
&- 3\left(\frac{\mathrm{p}^A_\ell}{\mathrm{p}^A_d}\right)^2\mathrm{p}(D_cD'_c,D_v\,;1) - 3\left(\frac{\mathrm{p}^B_\ell}{\mathrm{p}^B_d}\right)^2\mathrm{p}(D_v,D_cD'_c\,;1) - 3\left(\frac{\mathrm{p}^A_\ell\,\mathrm{p}^B_\ell}{\mathrm{p}^A_d\,\mathrm{p}^B_d}\right)\mathrm{p}(D_c,D'_c \vee D'_c,D_c\,;1).
\end{aligned} \tag{52}$$

Using the direct estimation method to compute all the relevant probabilities, we obtain the secret key rate r (from Equation (1) from the main text) in Figure 8. We consider the implemented number of rounds, 10^5, as a

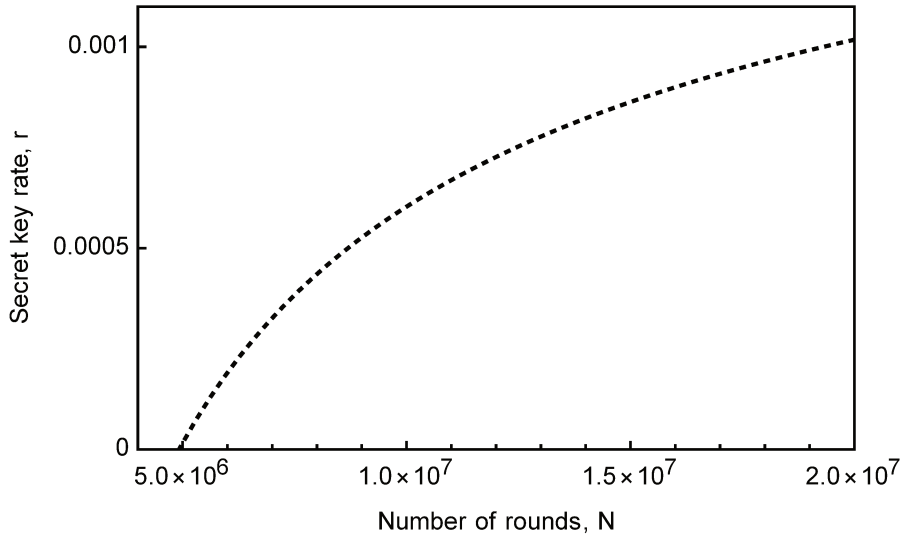

Figure 8: Secret key rate, r, vs number of rounds, N, for the case of imperfect single-photon sources and detectors. The probability necessary for the plot are obtained from the experimental data.

subset of a larger implementation and, therefore, use them to estimate the secret key rate. The probability of server announcing "1" during these rounds is $\mathrm{p}(1) = 0.0162$. Therefore, the amount of keys wasted during the parameter estimations is 1620 bits.

The probabilities of Equations (51) and (52) are the following: $\mathrm{p}_{0,0} = (7.3 \pm 0.3) \times 10^{-3}$, $\mathrm{p}_{1,1} = (5.5 \pm 0.3) \times 10^{-3}$, $\mathrm{p}_{0,1} = (1.1 \pm 0.9) \times 10^{-4}$ and $\mathrm{p}_{1,0} = (5.1 \pm 0.7) \times 10^{-4}$.

We assume $\epsilon = 10^{-5}$, $\epsilon_{EC} = 10^{-10}$ and $\epsilon_{PE} = 10^{-11}$. The value ϵ' is a factor in the min-entropy expression used for the key rate computation and may actually be set by the user arbitrarily to maximize the key rate (see Lemma 1 from [31]). However, for our evaluations we simply set $\epsilon' = 10^{-7}$ (optimizing this could only improve our results). For parameter estimation, we take $\epsilon_{PE} = 10^{-11}$ and assume a confidence interval $\delta = 10^{-4}$, given our experimental errors. The calculated secret key rate corresponds to the minimum lower bound of the entropy $S(A|C)$ (see Equation (36)) over the confidence interval of the experimental probabilities. This minimum occurs for the highest value of the error probability p_{err} and the lowest of p_{key}, and therefore represents the worst possible key rate within our experimental uncertainty.

E.2 Indirect estimation

To avoid wasting the rounds used for key-generation (when "1" was announced without any clicks at Alice's and Bob's detectors), we can use the remaining rounds (when "0","v" or "m" was announced or "1" was announced with click(s) at Alice's and Bob's detectors) for parameter estimation. For these cases, Alice and Bob can communicate over an authenticated channel to convey their respective action choices and resulting states to each other. Therefore, they can communicate for the non-useful rounds where server announces "0","v" or "m", as well as the rounds where any of them detects a photon in case the server announces "1". This method can be applied also in the ideal case described in Section C, but we present it only once for brevity.

We know that $\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1) = \mathrm{p}(D_v,R) - \mathrm{p}(D_v,R\,;0) - \mathrm{p}(D_v,R\,;v) - \mathrm{p}(D_v,R\,;m)$, where $\mathrm{p}(D_v,R) = \mathrm{p}(D,R) - \mathrm{p}(D_\ell,R) - \mathrm{p}(D'_\ell,R) - \mathrm{p}(D_c,R) - \mathrm{p}(D'_c,R) - \mathrm{p}(D_\ell D'_\ell,R) - \mathrm{p}(D_c D'_\ell,R) - \mathrm{p}(D_\ell D'_c,R) - \mathrm{p}(D_c D'_c,R)$. Note that $\mathrm{p}(D,R)$ is the probability of Alice choosing to detect and Bob to reflect. Since Alice and Bob choose their actions at random, ideally $\mathrm{p}(D,D) = \mathrm{p}(D,R) = \mathrm{p}(R,D) = \mathrm{p}(R,R) = 1/4$. However, considering the finite sample size and the inefficiency of switching between the actions, Alice and Bob do not take these probabilities to be $1/4$ but compute them considering only the non-useful rounds. Therefore, we have

$$\begin{aligned}\mathrm{p}_{0,0} = {} & \mathrm{p}(D,R) - \mathrm{p}(D_\ell,R) - \mathrm{p}(D'_\ell,R) - \mathrm{p}(D_c,R) - \mathrm{p}(D'_c,R) - \mathrm{p}(D_\ell D'_\ell,R) - \mathrm{p}(D_c D'_\ell,R) \\ & - \mathrm{p}(D_\ell D'_c,R) - \mathrm{p}(D_c D'_c,R) - \mathrm{p}(D_v,R\,;0) - \mathrm{p}(D_v,R\,;v) - \mathrm{p}(D_v,R\,;m). \end{aligned} \tag{53}$$

Note that Alice and Bob cannot directly compute all the quantities from the above expression, say, $\mathrm{p}(D_v,R\,;0)$, $\mathrm{p}(D_v,R\,;1)$, etc. They can compute $\mathrm{p}(D_\ell,R)$, $\mathrm{p}(D'_\ell,R)$ and $\mathrm{p}(D_c D'_\ell,R)$ analogously as in the previous subsection, given by Equation (48). However, $\mathrm{p}(D_c,R \vee D'_c,R \vee D_\ell D'_c,R \vee D_c D'_\ell,R)$ can be computed directly. We use $\mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;0)$, directly observable, to estimate $\mathrm{p}(D_v,R\,;0)$. Therefore,

$$\mathrm{p}(D_v,R\,;0) = \mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;0) - \mathrm{p}(D_\ell,R\,;0) - \mathrm{p}(D'_\ell,R\,;0) - \mathrm{p}(D_\ell D'_\ell,R\,;0), \tag{54}$$

$\mathrm{p}(D_\ell,R\,;0),\mathrm{p}(D'_\ell,R\,;0)$ and $\mathrm{p}(D_cD'_\ell,R\,;0)$, etc., can again be computed in the same way as before. Therefore, the final expressions for $\mathrm{p}_{0,0}$ and $\mathrm{p}_{1,1}$, in terms of probabilities computed indirectly, are

$$\begin{aligned}\mathrm{p}_{0,0}=\ &\mathrm{p}(D,R)-\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R)-\mathrm{p}(D_cD'_c,R)-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;0)\\&-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;v)-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;m)\\&+\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\left[\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R\,;0)+\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R\,;v)\right.\\&\left.+\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R\,;m)-\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R)\right]\\&-\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\left[\mathrm{p}(D_cD'_c,R\,;0)+\mathrm{p}(D_cD'_c,R\,;v)+\mathrm{p}(D_cD'_c,R\,;m)-\mathrm{p}(D_cD'_c,R)\right],\end{aligned}\tag{55}$$

$$\begin{aligned}\mathrm{p}_{1,1}=\ &\mathrm{p}(R,D)-\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell)-\mathrm{p}(R,D_cD'_c)-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;0)\\&-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;v)-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;m)\\&+\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)\left[\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell\,;0)+\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell\,;v)\right.\\&\left.+\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell\,;m)-\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell)\right]\\&-\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2\left[\mathrm{p}(R,D_cD'_c\,;0)+\mathrm{p}(R,D_cD'_c\,;v)+\mathrm{p}(R,D_cD'_c\,;m)-\mathrm{p}(R,D_cD'_c)\right].\end{aligned}\tag{56}$$

We can analogously estimate $\mathrm{p}_{0,1}$ by computing $\tilde{\mathrm{p}}_{1,0}$ as

$$\tilde{\mathrm{p}}_{1,0}=\mathrm{p}(R,R\,;1)=\mathrm{p}(RR)-\mathrm{p}(R,R\,;0)-\mathrm{p}(R,R\,;v)-\mathrm{p}(R,R\,;m).\tag{57}$$

Therefore,

$$\begin{aligned}\mathrm{p}_{0,1}=\ &\mathrm{p}(1)-\tilde{\mathrm{p}}_{0,0}-\tilde{\mathrm{p}}_{1,1}-\tilde{\mathrm{p}}_{1,0}-\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\mathrm{p}(D_c,D_v\vee D_c,D'_\ell\vee D'_c,D_\ell\vee D_cD'_\ell,D_v\vee D_\ell D'_c,D_v\,;1)\\&-\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)\mathrm{p}(D_v,D_c\vee D_\ell,D'_c\vee D'_\ell,D_c\vee D_v,D_cD'_\ell\vee D_v,D_\ell D'_c\,;1)\\&-3\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\mathrm{p}(D_cD'_c,D_v\,;1)-3\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2\mathrm{p}(D_v,D_cD'_c\,;1)-3\left(\frac{\mathrm{p}_\ell^A\,\mathrm{p}_\ell^B}{\mathrm{p}_d^A\,\mathrm{p}_d^B}\right)\mathrm{p}(D_c,D'_c\vee D'_c,D_c\,;1).\end{aligned}\tag{58}$$

Note that, to compute $\mathrm{p}_{key}=\tilde{\mathrm{p}}_{00}+\tilde{\mathrm{p}}_{11}$ using the indirect method, we have

$$\begin{aligned}\tilde{\mathrm{p}}_{0,0}=\ &\mathrm{p}(D,R)-\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_cD'_\ell,R)-\mathrm{p}(D_cD'_c,R)-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;0)\\&-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;v)-\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;m),\end{aligned}\tag{59}$$

$$\begin{aligned}\tilde{\mathrm{p}}_{1,1}=\ &\mathrm{p}(R,D)-\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_cD'_\ell)-\mathrm{p}(R,D_cD'_c)-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;0)\\&-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;v)-\mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;m).\end{aligned}\tag{60}$$

From our experimental data, we obtain $\mathrm{p}_{0,0}=(8\pm2)\times10^{-3}$, $\mathrm{p}_{1,1}=(6\pm2)\times10^{-3}$, $\mathrm{p}_{0,1}=(3\pm2)\times10^{-3}$ and $\mathrm{p}_{1,0}=(0.5\pm2)\times10^{-3}$. All these values are compatible with those obtained with the direct estimation within experimental uncertainties, which can be reduced by employing a larger sample and improving the single-photon sources and detectors.

F Dependence on detection efficiency

In this section, we discuss the dependence of the secret key rate on the detection efficiencies of Alice's and Bob's detectors, p_d^A and p_d^B, respectively. Note that, since we only consider the first term in Equation (36) to estimate a bound on $S(A|C)$, we only need to compute the probabilities $\mathrm{p}_{0,0},\mathrm{p}_{1,1},\mathrm{p}_{0,1},\mathrm{p}_{1,0}$ and $\mathrm{p}(1)$. However, $\mathrm{p}_{0,0},\mathrm{p}_{1,1},\mathrm{p}_{0,1},\mathrm{p}_{1,0}$ are independent of p_d^A and p_d^B, and it is only $\mathrm{p}(1)$ that has this dependence. Therefore, using the experimental data corresponding to $\mathrm{p}_\ell^A=1-\mathrm{p}_d^A=0.42$ and $\mathrm{p}_\ell^B=1-\mathrm{p}_d^B=0.42$, we can rewrite $\mathrm{p}(1)$ with

the explicit dependence on the general parameters, $\tilde{\mathrm{p}}_\ell^A$ and $\tilde{\mathrm{p}}_\ell^B$, as

$$\begin{aligned}\mathcal{N}(\tilde{\mathrm{p}}_\ell^A, \tilde{\mathrm{p}}_\ell^B) \;&= \langle k_{0,0}|k_{0,0}\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)\left(\langle k_{0,0}^1|k_{0,0}^1\rangle + \langle k_{0,0}^2|k_{0,0}^2\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)^2 \langle k_{0,0}^3|k_{0,0}^3\rangle \\ &+ \langle k_{1,1}|k_{1,1}\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)\left(\langle k_{1,1}^1|k_{1,1}^1\rangle + \langle k_{1,1}^2|k_{1,1}^2\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)^2 \langle k_{1,1}^3|k_{1,1}^3\rangle \\ &+ \langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)\langle k_{0,1}^1|k_{0,1}^1\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)\langle k_{0,1}^2|k_{0,1}^2\rangle \\ &+ \left(\frac{\tilde{\mathrm{p}}_\ell^A\,\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^A\,\mathrm{p}_\ell^B}\right)\left(\langle k_{0,1}^3|k_{0,1}^3\rangle + \langle k_{0,1}^4|k_{0,1}^4\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)^2 \langle k_{0,1}^5|k_{0,1}^5\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)^2 \langle k_{0,1}^6|k_{0,1}^6\rangle \\ &= \mathrm{p}(1)(\tilde{\mathrm{p}}_\ell^A, \tilde{\mathrm{p}}_\ell^B).\end{aligned} \tag{61}$$

Moreover, $\mathrm{p}_{err} = \mathrm{p}(1) - \mathrm{p}_{key}$ is also modified accordingly, to be used in computing $Q = \mathrm{p}_{err}/\mathrm{p}(1)$ to obtain the secret key rate presented in Figure 3 from the main paper.

G Dependence on transmission loss

In this section, we provide a brief analysis of the dependence of the key rate on the channel losses, for the case of imperfect photon sources and detectors. The channel loss, after photons passing a distance L through a medium described by the absorption coefficient α (in dB/unit distance), is given by $\ell = \alpha L$. In our protocol, the photons are traveling from the server to the agents, and back, meaning that the total distance L is twice the distance between the server and the agents. This is also the maximal distance between Alice and Bob, achieved when the two are at the opposite sides of the server.

First, note that in general, the all-powerful adversary is bounded only by the laws of physics. In particular, it can vary the number of photons in front of Alice's and Bob's labs at will. But such assumption would seem to turn senseless the whole loss analysis. Moreover, the agents can check the photon number statistics in their labs, thus the adversary must keep them at the levels of the honest case. Finally, note that the overall photon-adversary state in front of the agents has the same shape as in the lossless case. Indeed, expression 11 represents the most general photon-adversary state that contains up to two photons, in which the probabilities of having zero, one, or two photons are incorporated in the norms of vectors $|c_{a,b}\rangle_C \in \mathcal{H}_C$.

In our table-top experimental implementation, due to the low transmission loss in air for the considered distance, we can assume that the loss is for all practical purposes zero. Let us fix the source parameters p_1 and p_2 (the probabilities of single- and double-photon emission per pulse, respectively), the detector efficiency p_d (for simplicity, we assume that the agent's detectors have the same efficiency), and take a certain number of rounds N. For that, we can calculate the key rate $r(\ell = 0; N)$, presented in Figure 4 from the main text. We have that $N = N_0 + N_1 + N_2$, where N_i is the number of rounds with $i = 0, 1, 2$ emitted photons.

Given the transmission probability $T(\ell) = e^{-\frac{\ell}{10}}$, one can calculate

$$\begin{aligned} N_0(\ell) &= N_0 + (1-T)N_1 + (1-T)^2 N_2 \\ N_1(\ell) &= TN_1 + 2T(1-T)N_2 \\ N_2(\ell) &= T^2 N_2, \end{aligned} \tag{62}$$

where $N_i(\ell)$ are the expected numbers of rounds with $i = 0, 1, 2$ photons present. Note that $N_0(\ell) + N_1(\ell) + N_2(\ell) = N_0 + N_1 + N_2 = N$.

Consider the number of rounds $N' < N$, for which $N_1(\ell) = \mathrm{p}_1 N'$ and calculate the secret key $r(0; N')$. Then, we have that $r(\ell; N) \geq r(0; N')$, the secret key for N' rounds in the configuration with $L = 0$ is the lower bound of the secret key for N rounds with the loss ℓ. This bound is based on the following two arguments:

1. The vacuum pulses neither contribute to the key generation, nor to eavesdropping (they leak no information to the adversary). Thus, only the numbers of single-photon emissions and double-photon emissions are relevant, i.e., whenever we have the key rate for the number of rounds that involve certain numbers of the single-photon and double-photon emissions, we can take this result as valid for any case of having the same single- and double-photon rounds (provided there are no higher-photon rounds).

2. Given a certain number of rounds, N, as ℓ grows, both $N_1(\ell)$ and $N_2(\ell)$ decrease. But their ratio does not stay the same, i.e., there exists no N', such that both requirements $N_1(\ell) = \mathrm{p}_1 N'$ and $N_2(\ell) = \mathrm{p}_2 N'$ are

satisfied. In other words, the profile of the source changes with ℓ. But, the ratio $N_1(\ell)/N_2(\ell)$ increases: as ℓ grows, there are proportionally more single-photon rounds than double-photon ones, meaning it is more likely that Alice and Bob receive a single photon than two photons. Since double-photon rounds are the ones that, on one side might induce errors in the key, and on the other help the adversary, we actually have that our $r(\ell = 0; N')$ is in fact the lower bound for $r(\ell > 0; N)$.

Thus, having our results $r(N)$ for $\ell = 0$, our key rate as a function of the loss ℓ is given by

$$\tilde{r}(\ell) \equiv r(N') = r\left(\frac{N_1(\ell)}{\mathrm{p}_1}\right), \tag{63}$$

where by $\tilde{r}$ we denote the functional dependence of the key rate on the losses, which is different from the dependence of r on the number of rounds for $\ell = 0$. Using the second line of (62), $N_1 = \mathrm{p}_1 N$ and $N_2 = \mathrm{p}_2 N$, we finally have

$$\tilde{r}(\ell) = r\Big(\big[10^{-\ell/10}\mathrm{p}_1 + 2\cdot 10^{-\ell/10}\big(1 - 10^{-\ell/10}\big)\mathrm{p}_2\big]N\Big). \tag{64}$$

References

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. volume 560, pages 7–11, 2014. DOI: https://doi.org/10.1016/j.tcs.2014.05.025.

[2] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. DOI: https://doi.org/10.1103/PhysRevLett.67.661.

[3] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. DOI: https://doi.org/10.1103/PhysRevLett.85.441.

[4] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005. DOI: https://doi.org/10.1103/PhysRevA.72.012332.

[5] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005. DOI: https://doi.org/10.1098/rspa.2004.1372.

[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4): 1012–1236, Dec 2020. DOI: https://doi.org/10.1364/AOP.361502.

[7] Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna. Quantum cryptography: Key distribution and beyond. *Quanta*, 6(1):1–47, 2017. ISSN 1314-7374. DOI: https://doi.org/10.12743/quanta.v6i1.57.

[8] Mohsen Razavi, Anthony Leverrier, Xiongfeng Ma, Bing Qi, and Zhiliang Yuan. Quantum key distribution and beyond: introduction. *J. Opt. Soc. Am. B*, 36(3):QKD1–QKD2, Mar 2019. DOI: https://doi.org/10.1364/JOSAB.36.00QKD1.

[9] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020. DOI: https://doi.org/10.1103/RevModPhys.92.025002.

[10] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical bob. *Phys. Rev. Lett.*, 99:140501, Oct 2007. DOI: https://doi.org/10.1103/PhysRevLett.99.140501.

[11] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. *Phys. Rev. A*, 79:032341, Mar 2009. DOI: https://doi.org/10.1103/PhysRevA.79.032341.

[12] Walter O. Krawec. Mediated semiquantum key distribution. *Phys. Rev. A*, 91:032323, Mar 2015. DOI: https://doi.org/10.1103/PhysRevA.91.032323.

[13] Zhi-Rou Liu and Tzonelih Hwang. Mediated semi-quantum key distribution without invoking quantum measurement. *Annalen der Physik*, 530(4):1700206, 2018. DOI: https://doi.org/10.1002/andp.201700206.

[14] Xiangfu Zou, Zhenbang Rong, and Nan-Run Zhou. Three attacks on the mediated semi-quantum key distribution without invoking quantum measurement. *Annalen der Physik*, 532(8):2000251, 2020. DOI: https://doi.org/10.1002/andp.202000251.

[15] Po-Hua Lin, Chia-Wei Tsai, and Tzonelih Hwang. Mediated semi-quantum key distribution using single photons. *Annalen der Physik*, 531(8):1800347, 2019. DOI: https://doi.org/10.1002/andp.201800347.

[16] Lingli Chen, Qin Li, Chengdong Liu, Yu Peng, and Fang Yu. Efficient mediated semi-quantum key distribution. *Physica A: Statistical Mechanics and its Applications*, 582:126265, 2021. DOI: https://doi.org/10.1016/j.physa.2021.126265.

[17] Walter O Krawec. Multi-mediated semi-quantum key distribution. In *2019 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2019. DOI: https://doi.org/10.1109/GCWkshps45667.2019.9024404.

[18] Julia Guskind and Walter O Krawec. Mediated semi-quantum key distribution with improved efficiency. *Quantum Science and Technology*, 7(3):035019, 2022. DOI: https://doi.org/10.1088/2058-9565/ac7412.

[19] Michel Boyer, Matty Katz, Rotem Liss, and Tal Mor. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A*, 96:062335, Dec 2017. DOI: https://doi.org/10.1103/PhysRevA.96.062335.

[20] Walter O. Krawec. Practical security of semi-quantum key distribution. In Eric Donkor and Michael Hayduk, editors, *Quantum Information Science, Sensing, and Computation X*, volume 10660, pages 33 – 45. International Society for Optics and Photonics, SPIE, 2018. DOI: https://doi.org/10.1117/12.2303759.

[21] Hasan Iqbal and Walter O. Krawec. Semi-quantum cryptography. *arXiv*, 1910.05368, 2019. DOI: https://doi.org/10.48550/arXiv.1910.05368.

[22] Walter O. Krawec. Security proof of a semi-quantum key distribution protocol. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 686–690, 2015. DOI: https://doi.org/10.1109/ISIT.2015.7282542.

[23] Wei Zhang, Daowen Qiu, and Paulo Mateus. Security of a single-state semi-quantum key distribution protocol. *Quantum Information Processing*, 17(6), 2018. ISSN 1570-0755. DOI: https://doi.org/10.1007/s11128-018-1904-z.

[24] R. H. Dicke. Interaction-free quantum measurements: A paradox? *American Journal of Physics*, 49(10): 925–930, 1981. DOI: https://doi.org/10.1119/1.12592.

[25] Avshalom C. Elitzur and Lev Vaidman. Quantum mechanical interaction-free measurements. *Found. Phys.*, 23(7):987–997, Jul 1993. ISSN 1572-9516. DOI: https://doi.org/10.1007/BF00736012.

[26] Paul Kwiat, Harald Weinfurter, Thomas Herzog, Anton Zeilinger, and Mark A. Kasevich. Interaction-free measurement. *Phys. Rev. Lett.*, 74:4763–4766, Jun 1995. DOI: https://doi.org/10.1103/PhysRevLett.74.4763.

[27] Francesco Lenzini, Ben Haylock, Juan C. Loredo, Raphael A. Abrahão, Nor A. Zakaria, Sachin Kasture, Isabelle Sagnes, Aristide Lemaitre, Hoang-Phuong Phan, Dzung Viet Dao, Pascale Senellart, Marcelo P. Almeida, Andrew G. White, and Mirko Lobino. Active demultiplexing of single photons from a solid-state source. *Laser & Photonics Reviews*, 11(3):1600297, 2017. DOI: https://doi.org/10.1002/lpor.201600297.

[28] Leonard Mandel and Emil Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995.

[29] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 2011. DOI: https://doi.org/10.1063/1.3610677.

[30] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6 (01):1–127, 2008. DOI: https://doi.org/10.1142/S0219749908003256.

[31] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008. DOI: https://doi.org/10.1103/PhysRevLett.100.200501.

[32] Walter O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. *Quantum Info. Comput.*, 17(3–4):209–241, 2017. ISSN 1533-7146. DOI: https://doi.org/10.26421/QIC17.3-4-2.

[33] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009. DOI: https://doi.org/10.1103/RevModPhys.81.1301.

[34] Suhri Kim, Sunghyun Jin, Yechan Lee, Byeonggyu Park, Hanbit Kim, and Seokhie Hong. Single trace side channel analysis on quantum key distribution. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 736–739, 2018. DOI: https://doi.org/10.1109/ICTC.2018.8539703.

[35] Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alleaume. Experimental vulnerability analysis of qkd based on attack ratings. *Scientific Report*, 11(9564), 2021. DOI: https://doi.org/10.1038/s41598-021-87574-4.

[36] Dongjun Park, GyuSang Kim, Donghoe Heo, Suhri Kim, HeeSeok Kim, and Seokhie Hong. Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures. *ICT Express*, 7(1):36–40, 2021. ISSN 2405-9595. DOI: https://doi.org/10.1016/j.icte.2021.01.013.

[37] Shahid Anwar, Zakira Inayat, Mohamad Fadli Zolkipli, Jasni Mohamad Zain, Abdullah Gani, Nor Badrul Anuar, Muhammad Khurram Khan, and Victor Chang. Cross-vm cache-based side channel attacks and proposed prevention mechanisms: A survey. *Journal of Network and Computer Applications*, 93:259–279, 2017. ISSN 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.06.001.

[38] Monika Patel, Joseph B. Altepeter, Yu-Ping Huang, Neal N. Oza, and Prem Kumar. Erasing quantum distinguishability via single-mode filtering. *Phys. Rev. A*, 86:033809, Sep 2012. DOI: https://doi.org/10.1103/PhysRevA.86.033809.

[39] Nino Walenta, Tommaso Lunghi, Olivier Guinnard, Raphael Houlmann, Hugo Zbinden, and Nicolas Gisin. Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature. *Journal of Applied Physics*, 112(6):063106, 2012. DOI: https://doi.org/10.1063/1.4749802.

[40] W. J. Zhang, X. Y. Yang, H. Li, L. X. You, C. L. Lv, L. Zhang, C. J. Zhang, X. Y. Liu, Z. Wang, and X. M. Xie. Fiber-coupled superconducting nanowire single-photon detectors integrated with a band-pass filter on the fiber end-face. *Superconductor Science and Technology*, 31(3):035012, feb 2018. DOI: https://doi.org/10.1088/1361-6668/aaa6b4.

[41] S. Gao, O. Lazo-Arjona, B. Brecht, K. T. Kaczmarek, S. E. Thomas, J. Nunn, P. M. Ledingham, D. J. Saunders, and I. A. Walmsley. Optimal coherent filtering for single noisy photons. *Phys. Rev. Lett.*, 123: 213604, Nov 2019. DOI: https://doi.org/10.1103/PhysRevLett.123.213604.

[42] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012. DOI: https://doi.org/10.1103/PhysRevLett.108.130503.

[43] Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, Teng-Yun Chen, Sheng-Kai Liao, Cheng-Zhi Peng, Feihu Xu, and Jian-Wei Pan. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X*, 10:031030, Aug 2020. DOI: https://doi.org/10.1103/PhysRevX.10.031030.

[44] Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.*, 123:100506, Sep 2019. DOI: https://doi.org/10.1103/PhysRevLett.123.100506.

[45] Tae-Gon Noh. Counterfactual quantum cryptography. *Phys. Rev. Lett.*, 103:230501, Dec 2009. DOI: https://doi.org/10.1103/PhysRevLett.103.230501.

[46] Yang Liu, Lei Ju, Xiao-Lei Liang, Shi-Biao Tang, Guo-Liang Shen Tu, Lei Zhou, Cheng-Zhi Peng, Kai Chen, Teng-Yun Chen, Zeng-Bing Chen, and Jian-Wei Pan. Experimental demonstration of counterfactual quantum communication. *Phys. Rev. Lett.*, 109:030501, Jul 2012. DOI: https://doi.org/10.1103/PhysRevLett.109.030501.

[47] G. Brida, A. Cavanna, I.P. Degiovanni, M. Genovese, and P. Traina. Experimental realization of counterfactual quantum cryptography. *Laser Physics Letters*, 9(3):247–252, jan 2012. DOI: https://doi.org/10.1002/lapl.201110120.

[48] Yang Liu, Lei Ju, Xiao-Lei Liang, Shi-Biao Tang, Guo-Liang Shen Tu, Lei Zhou, Cheng-Zhi Peng, Kai Chen, Teng-Yun Chen, Zeng-Bing Chen, and Jian-Wei Pan. Experimental demonstration of counterfactual quantum communication. *Phys. Rev. Lett.*, 109:030501, Jul 2012. DOI: https://doi.org/10.1103/PhysRevLett.109.030501.

[49] Yuan Cao, Yu-Huai Li, Zhu Cao, Juan Yin, Yu-Ao Chen, Hua-Lei Yin, Teng-Yun Chen, Xiongfeng Ma, Cheng-Zhi Peng, and Jian-Wei Pan. Direct counterfactual communication via quantum zeno effect. *Proceedings of the National Academy of Sciences*, 114(19):4920–4924, 2017. DOI: https://doi.org/10.1073/pnas.1614560114.

[50] F. Del Santo and B. Dakić. Two-way communication with a single quantum particle. *Phys. Rev. Lett.*, 120:060503, Feb 2018. DOI: https://doi.org/10.1103/PhysRevLett.120.060503.

[51] Francesco Massa, Amir Moqanaki, Ämin Baumeler, Flavio Del Santo, Joshua A. Kettlewell, Borivoje Dakić, and Philip Walther. Experimental two-way communication with one photon. *Advanced Quantum Technologies*, 2(11):1900050, 2019. DOI: https://doi.org/10.1002/qute.201900050.

[52] Pascale Senellart, Glenn Solomon, and Andrew White. High-performance semiconductor quantum-dot single-photon sources. *Nat. Nanotechnol.*, 12(11):1026, 2017. DOI: https://doi.org/10.1038/nnano.2017.218.

[53] Eric A. Dauler, Matthew E. Grein, Andrew J. Kerman, Francesco Marsili, Shigehito Miki, Sae Woo Nam, Matthew D. Shaw, Hirotaka Terai, Varun B. Verma, and Taro Yamashita. Review of superconducting nanowire single-photon detector system design options and demonstrated performance. *Optical Engineering*, 53(8):1 – 13, 2014. DOI: https://doi.org/10.1117/1.OE.53.8.081907.

[54] T Rudolph and L Grover. Quantum searching a classical database (or how we learned to stop worrying and love the bomb). *arXiv*, 0206066:1–3, 2002. DOI: https://doi.org/10.48550/arXiv.quant-ph/0206066.