Eur. Phys. J. D **41**, 599–627 (2007)
DOI: 10.1140/epjd/e2007-00010-4

THE EUROPEAN PHYSICAL JOURNAL D

Unconditional security of practical quantum key distribution

H. Inamori[1], N. Lütkenhaus[2,a], and D. Mayers[3]

[1] Centre for Quantum Computation, Clarendon Laboratory, Oxford, UK
[2] Helsinki Institute of Physics, Helsinki, Finland
[3] NEC Research Institute, Computer Science Department, Maharishi University of Management, Princeton NJ, USA

Received 30 October 2006
Published online 17 January 2007 – © EDP Sciences, Società Italiana di Fisica, Springer-Verlag 2007

Abstract. We present a complete protocol for BB84 quantum key distribution for a realistic setting (noise, loss, multi-photon signals of the source) that covers many of todays experimental implementations. The security of this protocol is shown against an eavesdropper having unrestricted power to manipulate the signals coherently on their path from sender to receiver. The protocol and the security proof take into account the effects concerning the finite size of the generated key. This paper is identical to the preprint `arXiv:quant-ph/0107017`, which was finalized in 2001. Therefore, some of the more recent developments, including the question of composability, are not addressed.

PACS. 03.67.Dd Quantum cryptography

QICS. 21.20.Kd Quantum key distribution – 22.70.+S Security proofs

Highlight Paper

1 Introduction

We present a proof of unconditional security of a practical quantum key distribution protocol. It is an extension of a previous result obtained by Mayers [2,3], which proves unconditional security provided that a perfect single photon source is used. In present days, perfect single photon sources are not available and, therefore, practical implementations use either dim laser pulses or post-selected states from parametric downconversion. Both practical signal types contain multi-photon contributions which characterise the deviation from the ideal single-photon state. This compromise threatens seriously the security of quantum key distributions when the loss rate in the quantum channel is high [4–6]. Security of such practical realisation has nevertheless been proved in [7] against restricted type of eavesdropping attacks. The salient idea used in [7] is that data associated with multiple photon signals are revealed to a possible eavesdropper, without the legitimate user's knowledge. We show here that this model can be combined with Mayers' proof. The resulting extension guarantees unconditional security of a realistic quantum key distribution protocol against an enemy with unlimited classical or quantum computational power.

By now, Mayers' proof has been followed up by other proof of the security of ideal single-photon quantum key distribution [8,9]. Security assuming some restrictions on eavesdropper's attack can be found in [10–12]. Security of protocols in which honest participants use trusted quantum computers can be found in [13].

Unconditional security of a protocol means a security against a cheater with unlimited computational power, quantum or classical. In other words, it means that there is no condition on the cheater. It does not mean that there is no condition on the apparatus used by the honest participants. This last interpretation would be equivalent to say that we know nothing about the protocol that is actually implemented. So, each proof of unconditional security must use a different type of assumptions on these apparatus. Mayers' original proof applies to an unrestricted eavesdropper's attack on the quantum signals, but assumes the source used in the protocol is perfect. In particular, it assumes that the source emits single photon pulses. In this paper, we present a derivation of the proof in which the last assumption is relaxed: we still consider sources that perform perfect polarisation encoding, but each signal carries now a random number of photons in the ideal polarisation mode. The random variables giving the numbers of photons in the pulses are assumed to be identically and independently distributed, and we require that an upper-bound on the probability that a pulse contains several photons is known. As in Mayers' original paper, there is no assumption on the quantum channel nor on the detection unit, except that, given an input quantum state of any signal, the detector's probability of

[a] *Present affiliation*: Institute for Quantum Computing, University of Waterloo, Ontario, Canada.
e-mail: `nlutkenhaus@iqc.ca`

detecting a signal does not depend on the choice of the measurement basis. A more detailed discussion about assumptions in quantum cryptography together with a new approach to this problem, especially the problem of an untrusted BB84 source, can be found in [14].

This paper is divided into two parts. In the first part we define the assumptions of our proof, the protocol we refer to and the security notion. We then give the result of our proof which give the precise quantitative meaning of our security proof together. In that step the necessary parameters of the protocol leading to secure quantum key cryptography are given. We illustrate the results by giving the asymptotic formulas for the limit of long keys which show, how many secure bits the protocol will obtain for a given error rate of an experimental set-up as a function of the source parameters and the error rate. In the second part, we present the detailed proof of the statements of the first part. We have chosen to give all details of this proof to make it self contained, although it follows closely Mayers original work. The readers are invited to refer to the original paper [3] where a simpler situation was analysed, to get an insight into the main idea of the proof.

2 Security in quantum key distribution

The role of key distribution between two distant legitimate parties, traditionally called Alice and Bob, is to generate a shared random binary string, called the private key, that is guaranteed to be known only by the legitimate parties. A non-authorised party, traditionally called Eve, should not be able to obtain any information about the private key. More precisely, for any eavesdropping strategy Eve chooses, the conditional entropy of the private key, given the data Eve acquires during the protocol, should be very close to the maximum entropy, corresponding to a uniformly and independently distributed key. One requirement for this is that the conditional probability of the private key given Eve's data must be very close to the uniform distribution. Note that it is not sufficient to impose that the private key be independent of the data Eve acquires: a key distribution protocol that returns a specific value for the private key with high probability does not provide any privacy, even if Eve is inactive during the key distribution.

Quantum key distribution protocols do not allow Alice and Bob to share a private key in all circumstances. For example, Eve can usually block signals between the two parties. But even if the signals arrive, Alice and Bob cannot always create a secure key using them. As shown in [6], it is in principle not possible to create a secure key with the BB84 protocol (using ideal signals) once the error rate exceeds 25%. This is true for any post-processing of the data in the sense of advantage distillation or similar ideas. It is therefore characteristic for any full protocol (including the classical post-processing of the data) that it can deliver a secure private key only as long as the parameters describing the transmission of the quantum channel (like the error rate) are within a certain parameter region.

Any protocol therefore provides a validation test that tells whether a key can be generated with unconditional privacy. A key is created only if the test is passed. Otherwise the session is abandoned. Naturally, one would like to find an entropic bound given the validation test is passed. However, it is known that such a bound is inappropriate for the protocol we consider in this paper (see for example [8]): there are simple attacks that give full knowledge about the private key, although with very small probability of success. It is therefore important to choose a good measure of privacy which nevertheless reflects our basic intuition.

We follow Mayers' proof and define formally a key even in the cases that the validation test is not passed. For this purpose Bob formally chooses with uniform distribution a binary sequence as key whenever the test fails. We then bound Eve's entropy on this always defined key, conditioned on her knowledge, to be arbitrarily close to the maximal value. Naturally, in that case Alice and Bob do not share a key, but this is unimportant since they are aware of it.

This choice of security notion assures that Eve's conditional entropy is close to the maximal amount, but this situation can arise from two different scenarios: either Eve applies only gentle eavesdropping, which passes the validation tests and gives her basically no information, or she applies massive eavesdropping, which basically all the time fails the validation test, but in the unlikely event of passing the test, it might reveal substantial amount of information. Nevertheless, in both cases the key will be safe, since in the first scenario Eve has no information on the key, while in the second case, the probability of success will be, in a quantified way, extremely low.

Another important aspect of security of quantum key distribution protocols is the integrity or the faithfulness of the distributed key. We must require that whatever Eve does, it is very unlikely that Alice and Bob fail to share an identical private key while the validation test is passed. One way this situation might arise is the error correction procedure (which is a typical ingredient of a full protocol) failing to correct all errors, for example because of an unusual error distribution.

Finally, we consider families of protocols for which a parameter, quantifying the amount of a resource used in a protocol, characterises its security. Usually, the higher this *security parameter's* value is, the higher is the level of security, but also the amount of a resource required by the protocol. In the protocol we consider the number of quantum signals sent by Alice as security parameter.

We now give a formal definition of security. For this we will introduce some notation. A random variable will always be denoted by a bold letter, and values taken by this random variable by the corresponding plain letter. Only discrete random variables will be considered in this paper. The probability distribution of a random variable $\boldsymbol{x}$ is denoted by $\mathrm{P}_{\boldsymbol{x}}$, i.e. $\mathrm{P}_{\boldsymbol{x}}(x) = \Pr(\boldsymbol{x} = x)$ is the probability that $\boldsymbol{x}$ takes the value x. The joint distribution of two random variables $\boldsymbol{x}$ and $\boldsymbol{y}$ is denoted by $\mathrm{P}_{\boldsymbol{xy}}$, i.e. $\mathrm{P}_{\boldsymbol{xy}}(x, y) = \Pr(\boldsymbol{x} = x, \boldsymbol{y} = y)$. The conditional probability of $\boldsymbol{x}$ given an event $\mathcal{E}$ with positive probability is denoted by $\mathrm{P}_{\boldsymbol{x}\,|\,\mathcal{E}}$, i.e. $\mathrm{P}_{\boldsymbol{x}\,|\,\mathcal{E}}(x) = \Pr(\boldsymbol{x} = x|\mathcal{E})$. The conditional probability of $\boldsymbol{x}$ given that $\boldsymbol{y}$ takes a value y is denoted by $\mathrm{P}_{\boldsymbol{x}\,|\,\boldsymbol{y}=y}$ whenever $\mathrm{P}_{\boldsymbol{y}}(y) > 0$, i.e. $\mathrm{P}_{\boldsymbol{x}\,|\,\boldsymbol{y}=y}(x) = \Pr(\boldsymbol{x} = x|\boldsymbol{y} = y) = \mathrm{P}_{\boldsymbol{xy}}(x, y)/\mathrm{P}_{\boldsymbol{y}}(y)$, whenever $\mathrm{P}_{\boldsymbol{y}}(y)$ is positive. Let f be a function defined on the image of $\boldsymbol{x}$. When no confusion is possible, the notation $\boldsymbol{f}$ will be adopted to denote the random variable $f(\boldsymbol{x})$.

We will denote by $\vec{\boldsymbol{\kappa}}$ the random variable giving the private key generated in a key distribution session. The key is a string of m bits where m is a positive integer specified by the legitimate users. That is $\vec{\boldsymbol{\kappa}}$ takes value in $\{0, 1\}^m$. We denote by **valid** the random variable giving the outcome of the validation test and by **share** the random variable telling whether Alice and Bob share an identical private key. Given an eavesdropping strategy chosen by Eve, we denote by $\boldsymbol{v}$ the random variable giving collectively all data Eve gets during this key distribution session. Henceforth, given the eavesdropping strategy adopted by Eve, $\boldsymbol{v}$ is called the *view* of Eve, and we will denote by $\mathcal{Z}$ the set of all values $\boldsymbol{v}$ may take.

We adopt the following definition of security for quantum key distribution protocols.

Definition 1. *Consider a quantum key distribution protocol returning a key $\vec{\boldsymbol{\kappa}} \in \{0, 1\}^m$ regardless of the outcome of the validation test, where the length of the key, m, is fixed and chosen by the user. We say that the protocol has* (asymptotic) perfect security *if and only if:*

- *the protocol is parametrised by a parameter N taking value in $\mathbb{N}$ called the* security parameter, *and*
- *there exists two functions ϵ_1, ϵ_2: $\mathbb{N} \times \mathbb{N} \to \mathbf{R}^+$ such that $\epsilon_1(N, m)$ and $\epsilon_2(N, m)$ are vanishing exponentially as N grows (i.e. there exist $\alpha > 0$, $\beta > 0$, $N_{min} \in \mathbb{N}$ and a function f: $\mathbb{N} \to \mathbf{R}^+$ such that $\forall N > N_{min}$, $\epsilon_1(N, m)$, $\epsilon_2(N, m) < e^{-\alpha N^\beta} f(m)$), and*
- *there exists a function N_0: $\mathbb{N} \to \mathbb{N}$ such that, for any strategy adopted by Eve,*

$$\begin{aligned} &\forall m, \forall N \geq N_0(m), \\ &(\textbf{privacy}) \quad H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - \epsilon_1(N, m) && (1) \\ &(\textbf{integrity}) \; \Pr(\neg\textbf{share} \text{ and } \textbf{valid}) \leq \epsilon_2(N, m) && (2) \end{aligned}$$

where $\boldsymbol{v}$ is Eve's view given her strategy, and

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \overset{Def}{=} - \sum_{\vec{\kappa}, v | \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa}, v) > 0} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa}, v) \log_2 \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa})$$

is the Shannon entropy [15–17] of the key $\vec{\boldsymbol{\kappa}}$ given Eve's view $\boldsymbol{v}$.

We will show that the protocol presented in the next section will be secure according to this definition. In particular, this means, that the protocol creates a key of length m out of N signals. Then, by choosing N large enough for fixed values of m, we can always assure that Eve's conditional entropy is arbitrarily close to the maximum amount (privacy). Additionally, with a probability arbitrarily close to unity, Alice and Bob share the key given that the validation test is passed (integrity).

3 The protocol

In this section, the quantum key protocol considered in this paper is described. It is an adaptation of the BB84 [18] protocol which takes into account the usage of an imperfect photon source. Note that the usage of imperfect source has been discussed as early as the first experimental implementation of BB84 [19] in the framework of restricted types of eavesdropping attacks. We first make precise which assumptions on the quantum channel we adopt in this paper. Then we give a formal description of the protocol.

3.1 Required technology

In the original proof [3], Mayers considered a practical realisation of quantum key distribution prone to noise and signal loss. However, the legitimate parties were assumed to be using a perfect single photon source — a source that emits exactly one photon in the chosen polarisation state. No restriction was imposed on the photo-detection unit used in the protocol, except that given an incoming signal, the probability of detection was required to be independent of the basis used to measure the signal. It was argued in [3] that Eve can take advantage of a detection unit in which the probability of detection depends on the basis chosen for the measurement, and we will adopt in this paper the same restriction regarding the detection unit.

The new feature in this paper is that we allow the use of imperfect source of photons in the following sense: given a polarisation state specified by the user, the source emits photons exactly in the specified polarisation state, but in a mixture of Fock states. That is, the source emits n photons in the given polarisation state with probability p_n, where $n \in \mathbb{N}$ and $p_0, p_1, p_2, \ldots$ is a probability distribution. The user does not have to know how many photons were actually emitted. The only restriction we impose is that an upper bound M_{max} on the number of emitted signals containing several photons is known within a confidence limit given by the (small) probability $\Pr(M > M_{max})$. We restrict ourselves to provide this bound for signals with identically and independently distributed multi-photon probability p_M. In that case we can choose $M_{max} = (p_M + \tau_M)N$ and obtain $\Pr(M > M_{max}) < \exp(-\tau_M^2 N)$, as explained below. Other methods for providing M_{max} and $\Pr(M > M_{max})$ can be used, where the corresponding terms replace the here derived and easily identifiable expressions in the subsequent results.

The authors believe this relaxation of requirement has practical importance, since single photon sources are not yet available, due to technological limitations. Furthermore, it has been pointed out [6] that in most experimental implementations of quantum key distribution, the quantum signals transmitted by the legitimate parties can be described as mixtures of Fock states.

As an example, consider a practical source emitting a *coherent state* of light in a given polarisation:

$$\big|\,\alpha\big\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{j=0}^{\infty} \frac{\alpha^j}{\sqrt{j!}} \big|\,j\big\rangle \tag{3}$$

where $\big|\,j\big\rangle$, $j \in \mathbb{N}$ is the number state — or Fock state — describing a state of j photons in the considered polarisation (therefore, for $\alpha \neq 0$, a coherent state has an indefinite number of photons). If we write $\alpha = |\alpha| e^{i\phi}$, $|\alpha|$ and ϕ are called *amplitude* and *phase* of the coherent pulse, respectively.

In general, the phase of a pulse is completely unknown, or can be rendered random thanks to a phase randomisation technique. Since the phase is then uniformly distributed, a pulse state in a given polarisation is described by the density matrix:

$$\rho_{\text{source}} = \frac{1}{2\pi} \int_0^{2\pi} \big|\,|\alpha| e^{i\phi}\big\rangle\big\langle |\alpha| e^{i\phi}\,\big| d\phi \tag{4}$$

$$= \frac{1}{2\pi} \int_0^{2\pi} e^{-|\alpha|^2} \sum_{j,j'=0}^{\infty} \frac{|\alpha|^{j+j'}}{\sqrt{j!j'!}} e^{i\phi(j-j')} \big|\,j\big\rangle\big\langle j'\,\big| d\phi \tag{5}$$

$$= \sum_{j=0}^{\infty} e^{-|\alpha|^2} \frac{|\alpha|^{2j}}{j!} \big|\,j\big\rangle\big\langle j\,\big|. \tag{6}$$

Therefore, the signals emitted by a coherent source of light becomes a classical mixture of Fock states due to the lack of a phase reference. Another example of practical source is a source emitting thermal states of light. Such states are already mixtures of Fock states. The above de-phasing argument applies in general for any signal state. Further studies of source characterisation can be found in [20].

We summarise the assumptions on the quantum setup adopted throughout this paper:

- the legitimate parties use a source of photons that sends a mixture of Fock states $\rho = \sum_{n=0}^{\infty} p_n \big|\,n\big\rangle\big\langle n\,\big|$ in the polarisation state exactly as specified by the user. The numbers of photons in the pulses emitted by the source are assumed to be identically and independently distributed. The upper bound M_{max} on the emitted number of multi-photon signals during the protocol is known by the legitimate parties to hold except with a negligible probability $\Pr(M > M_{max})$;
- the legitimate parties use a photo-detection unit such that for any given signal, the probability of detection is independent of the choice of the measurement basis;
- the signals and Alice's and Bob's polarization bases are chosen truly at random;
- Eve cannot intrude Alice's or Bob's apparatus by utilizing the quantum channel. She is restricted to interaction with the signals as they pass along the quantum channel.

3.2 The protocol

The quantum key distribution protocol under consideration based on Bennett and Brassard's BB84 [18] is defined. It comprises three stages: agreement on parameters of the protocol and security constants, the transmission of quantum signals, and the execution of a classical protocol together with the validation test.

Pre-agreement

1. Alice and Bob specify:
   - m, the length (in bits) of the private key to be generated;
   - N, the number of quantum signals to be sent by Alice. This integer is the security parameter of the protocol;
   - δ, the maximum threshold value for the error rate for the validation test;
   - r_{min}, the minimum threshold value for Bob's detection rate ($1 > r_{min} > M_{max}/N$);
   - p_R, the proportion of the shared bits that must be publicly announced for the validation test ($0 < p_R \leq 1/2$);
   - τ_{ec}, τ_f, τ_M, $\hat{\tau}$, and τ_p the security constants of the protocol. They are small strictly positive real numbers chosen so that $\delta + \tau_{ec} < 1$, $\delta + \tau_f < 1$, $r_{min} > M_{max}/N$, $\hat{\tau} < \frac{1-p_R}{2}$, $\tau_p < 1$.

Quantum transmission

2. Alice and Bob initialise the counter of the signals as $i = 0$ and Bob initialises the set of detected signals as $\mathcal{D} = \{\}$. Then until the pre-agreed number of signals have been sent ($i = N$), the following is repeated:
   (a) Alice and Bob increment i by one;
   (b) Alice picks randomly with uniform distribution a basis $a_i \in \{+, \times\}$ and a bit value $g_i \in \{0, 1\}$;
   (c) Alice makes her source emit a pulse of photons in the state $|\Psi(g_i, a_i)\rangle$ where $|\Psi(0,+)\rangle$, $|\Psi(1,+)\rangle$, $|\Psi(0,\times)\rangle$ and $|\Psi(1,\times)\rangle$ correspond to single photon states of polarisation angles 0, $\pi/2$, $\pi/4$ and $-\pi/4$, respectively. We recall that $\{\big|\,\Psi(0,+)\big\rangle, \big|\,\Psi(1,+)\big\rangle\}$ forms an orthonormal basis of $\mathcal{H}_{\text{photon}}$, the Hilbert space for single photon polarisation states, and

$$\big|\,\Psi(0,\times)\big\rangle = \frac{\big|\,\Psi(0,+)\big\rangle + \big|\,\Psi(1,+)\big\rangle}{\sqrt{2}},$$

$$\big|\,\Psi(1,\times)\big\rangle = \frac{\big|\,\Psi(0,+)\big\rangle - \big|\,\Psi(1,+)\big\rangle}{\sqrt{2}};$$

   (d) Bob measures Alice's pulse in the basis b_i where $b_i \in \{+, \times\}$ is chosen randomly at each time. If at least one photon is detected, the index i is added to the set $\mathcal{D}$ of detected signals' indexes, and the outcome of the measurement is recorded as $h_i \in \{0, 1\}$ (if the detection unit finds photons in both modes $h_i = 0, 1$, the value for h_i is chosen randomly in $\{0, 1\}$ by Bob). If no photon is detected at all, h_i is assigned the value $\perp$.

Note that the random choice of basis in step (d) might be provided by a beamsplitter (or a coupler) followed by two measurement setups, each measuring the photons in the basis + and × respectively. It might also be given by an external random number generator acting on a polarisation rotator.

Classical part

We denote by n the number of signals detected by Bob, i.e. $n = |\mathcal{D}|$, and by $\vec{a} = (a_1, \ldots, a_N) \in \{+, \times\}^N$, $\vec{b} = (b_1, \ldots, b_N) \in \{+, \times\}^N$, $\vec{g} = (g_1, \ldots, g_N) \in \{0, 1\}^N$ and $\vec{h} = (h_1, \ldots, h_N) \in \{0, 1, \perp\}^N$ the outcome of the quantum transmission (Step 2). Restrictions of these vectors onto some specified subset $X \subset \{1, \ldots, N\}$ will be denoted by $\vec{a}(X), \vec{b}(X), \vec{g}(X), \vec{h}(X)$.

3. Bob announces the set of detected signals by $\mathcal{D}$ to Alice.
4. Bob picks up randomly a subset of signals which will be revealed for the validation test $R \subset \{1, \ldots, N\}$, where each position $i \in \{1, \ldots, N\}$ is put in R with probability p_R.
5. Bob announces the revealed set R and the measurement basis of all signals $\vec{b}$ to Alice.
6. Bob announces the bit values of the test set $\vec{h}(\mathcal{D} \cap R)$ to Alice.
7. Alice computes the set of corresponding signals $\Omega = \{i \in \mathcal{D}\colon a_i = b_i\}$, the set of corresponding test signals $T = \Omega \cap R$ and the set of untested corresponding signals $E = \Omega \cap \overline{R}$. We denote $|E|$ by l.
8. Alice announces the polarisation basis of all of her signals $\vec{a}$, thus announces implicitly Ω and E as well. The bitstreams $\vec{g}(E)$ and $\vec{h}(E)$ are usually called *sifted keys.*
9. Alice chooses a linear error correcting code [15,16] capable of correcting $\lceil(\delta + \tau_{ec})(1 - p_R)|\Omega|\rceil$ errors in E. Its parity check matrix, F, is a $r \times l$ binary matrix, where r is the number of redundant bits required to correct $\lceil(\delta + \tau_{ec})(1 - p_R)|\Omega|\rceil$ errors in l bits using the linear error correcting code. Alice announces the *syndrome* $\vec{s} = F\vec{g}(E) \pmod 2$ to Bob.
10. Receiving the parity check matrix F and the syndrome $\vec{s}$, Bob runs the error correction on his sifted key $\vec{h}(E)$ and obtains $\vec{h}'(E)$. If there are less than $\lceil(\delta+\tau_{ec})(1-p_R)|\Omega|\rceil$ errors in E, Bob corrects successfully all the errors and obtains $\vec{g}(E)$, i.e. $\vec{h}'(E) = \vec{g}(E)$.
11. Alice picks up randomly with uniform distribution a $m \times l$ binary matrix K to which we will refer as the *privacy amplification matrix.* Alice announces K publicly.
12. Receiving the privacy amplification matrix K, Bob computes $\vec{\kappa}' = K\vec{h}'(E) \pmod 2$.

Validation test

Alice runs the validation test.

13. Alice tests whether the following conditions are all satisfied:
    - Bob's detection rate is greater than r_{min}, i.e.
    $$n > r_{min}N; \tag{7}$$
    - the size of $\mathcal{D}$ complies to the following inequalities:
    $$\frac{\widehat{l}_{min}}{2} \geq (\delta + \tau_f)(1 - p_R)n, \tag{8}$$
    $$m + r \leq \widehat{l}_{min} \left[1 - H_1 \left[\frac{2(\delta + \tau_f)\frac{1-p_R}{2}n}{\widehat{l}_{min}}\right] - \tau_p\right], \tag{9}$$
    where
    $$\widehat{l}_{min} = \left(\frac{1 - p_R}{2} - \hat{\tau}\right)(n - M_{max}) \tag{10}$$
    is a probabilistic lower bound on the number of signals on the set E which is due to single photon signals;
    - the number of errors in the tested set T is lower than the maximally allowed value. More precisely,
    $$|\{i \in T\colon g_i \neq h_i\}| < d, \tag{11}$$
    where $d = \delta|\Omega|p_R$.

    The validation test is passed if and only if all the conditions above are satisfied. The private key is the bitstream obtained by Alice as follows:
14. Alice computes the private key, defined as:
    - $\vec{\kappa} = K\vec{g}(E) \pmod 2$ if the validation test is passed,
    - a m-bit string $\vec{\kappa}$ chosen randomly with uniform distribution each time the validation test is not passed.

This protocol defines a key regardless whether the validation test is passed. The choice of the security constants used in the protocol is clarified in the following section.

Note. The matrix K can be prepared in advance, and Eve could know its form before the transmission of the quantum signal. More precisely, Alice and Bob could preagree on some set of matrices K for various values of m, and l. It is the special property 4 of F and K which is required here, and which will be introduced and explained in Section 5.3. This property is satisfied automatically if we choose K as random binary matrix, as specified in the protocol, and the constraint of equation (9) is satisfied. Our security proof can therefore immediately adapted to other choices of F and K together with their respective constraints replacing equation (9) to satisfy the underlying required property 4 of Section 5.3.

4 Security of the protocol

In this section we present the security statement for the protocol described in Section 3.2. If follows the structure of Definition 1. The proof of the security statement is given in the remainder of the paper.

Theorem 1. *The expected conditional Shannon entropy of the key* $\boldsymbol{\vec{\kappa}}$ *returned by the protocol described in Section 3.2 given Eve's view* $\boldsymbol{v}$ *is lower bounded, for any* $N > 0$*, by*

$$H(\boldsymbol{\vec{\kappa}}|\boldsymbol{v}) \geq m - \epsilon_1(N, m) \tag{12}$$

where the difference $\epsilon_1(N,m)$ *between the bound and the maximal value* m *is given by*

$$
\begin{aligned}
\epsilon_1(N,m) = 2\left(m+\frac{1}{\ln 2}\right) h(\delta,\tau_f,p_R,n) \\
+2\sqrt{2\left(m+\frac{1}{\ln 2}\right) mh(\delta,\tau_f,p_R,n)} \\
+m\Big(e^{-2\tau_M^2 N} + e^{-2\hat{\tau}^2(r_{min}N-M_{max})} \\
+2^{-\tau_p\left(\frac{1-p_R}{2}-\hat{\tau}\right)(r_{min}N-M_{max})} \\
+\sqrt{g(\delta,\tau_f,p_R,n)}\Big)
\end{aligned}
\tag{13}
$$

where

$$
\begin{aligned}
g(\delta,\tau_f,p_R,n) = \exp\Bigg[-\frac{1}{2\delta+\tau_f}\tau_f^2\frac{p_R^2}{4}r_{min}N \\
+2\left(\frac{\tau_f}{2\delta+\tau_f}\right)^2\Bigg],
\end{aligned}
\tag{14}
$$

$$
h(\delta,\tau_f,p_R,n) = 2\sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}+\sqrt{g(\delta,\tau_f,p_R,n}}. \tag{15}
$$

Besides, the conditional probability that Alice and Bob share an identical private key given that the validation test is passed is lower bounded for any $N>0$ *by:*

$$
\Pr(\neg\textbf{share} \text{ and } \textbf{valid}) \leq \epsilon_2(N,m), \tag{16}
$$

where

$$
\begin{aligned}
\epsilon_2(N,m) = \\
\min_{\tau_\Omega\in(0,1/2)}\Big[e^{-\frac{1}{2\delta+\tau_{ec}}\tau_{ec}^2 p_R^2(\frac{1}{2}-\tau_\Omega)r_{min}N+2\left(\frac{\tau_{ec}}{2\delta+\tau_{ec}}\right)^2} \\
+e^{-2\tau_\Omega^2 r_{min}N}\Big].
\end{aligned}
\tag{17}
$$

The functions $\epsilon_1(N,m)$ and $\epsilon_2(N,m)$ decrease exponentially with N, as required by the definition of security (Def. 1).

The parameters, the number of emitted signals N out of which the key of length m is created, are chosen in accordance with the performance of the set-up used for preparation, transmission and detection of the quantum signals in view of equation (9). As the number of these transmissions goes to infinity, we can neglect statistical fluctuations of the signal properties and describe the ratio between detected signals and sent signals by a detection rate $p_D = n/N$ and $r_{min} = n/N$. All security constants τ_{ec}, τ_f, τ_p, $\tilde{\tau}$ and τ_M can be chosen to be arbitrarily small, and the asymptotic key generation rate out of one bit of the sifted key reads is given as the length of the sifted key over that of the final key in terms of the observed error rate δ as

$$
\frac{m}{l} = \left(1-\frac{p_M}{p_D}\right)\left[1-H_1\left(\frac{2\delta}{1-\frac{p_M}{p_D}}\right)\right] - H_1(\delta). \tag{18}
$$

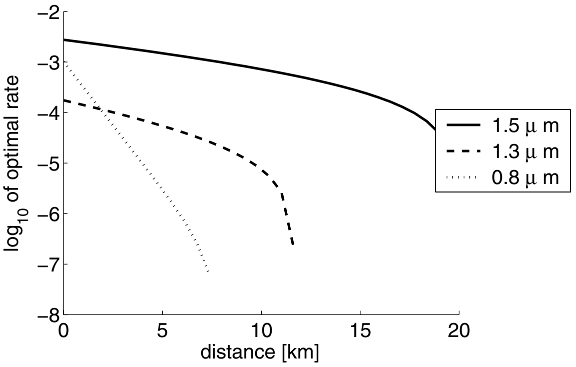

Fig. 1. Asymptotic gain rates using a simulation with the help of experimental parameters. The parameters are drawn from Bourennane et al. [21] for 1.5 μm, Marand and Townsend [22] for 1.3 μm and Townsend [23] for 0.8 μm.

Here we used we used asymptotic equalities for the sifted key length $l \simeq (1-p_R)n/2$ and $\lceil(\delta+\tau_{ec})(1-p_R)|\Omega|\rceil \simeq \lceil\delta l\rceil$. Furthermore, we made use of the Shannon limit [15] $r(\lceil\delta l\rceil, l) \simeq lH_1(\delta)$.

The overall rate of secure key bits per sent signal m/N can be calculated directly by multiplying equation (18) with the asymptotic formula

$$
\frac{l}{N} \simeq \frac{1-p_R}{2}p_D\ . \tag{19}
$$

The ratio G between key length and received signals m/n can be obtained by multiplication with $l/n \simeq (1-p_R)/2$. Moreover, in the limit of arbitrary long keys we can use the limit $p_R \rightarrow 0$ since even testing a 'small' fraction of the long key will have statistical significance sufficient for our purpose. Examples of the resulting values of G as a function of distance are shown in Figure 1 for various wavelength. To put our results into context, we relate our results in Figure 2 to those obtained for the limited security level of security against individual attacks. Note that the difference between the two results is not substantial. More importantly, the difference might be due to the proof technique used in our result. Our results should therefore not be interpreted as to claim that coherent attacks give more information to Eve than individual attacks do. Furthermore, we lay out the relevant bounds on improved security proofs. The rate is bounded due to the photon number statistics of the source, resulting in

$$
G_{bound} = \frac{1}{2}(p_D - p_M) \tag{20}
$$

as shown in [7]. We recover this bound by setting $\delta = 0$ in our asymptotic bound.

The distance, over which secure communication is possible, is bounded by the detector noise. As shown in Brassard et al. [6], the minimal transmission efficiency F_{WCP} in the situation of Poissonian photon number distribution of the source is given by

$$
F_{WCP} \approx 2\frac{\sqrt{d_B}}{\eta_B} \tag{21}
$$

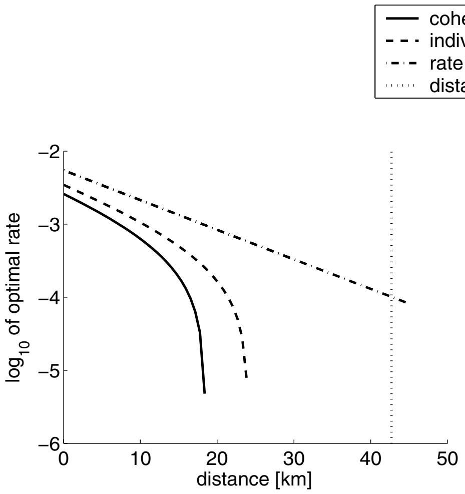

Fig. 2. We use the parameters of Bourennane et al. [21] for 1.5 μm to show the secure gain rate per time slot using our results ('coherent'). For comparison, the corresponding results for security against individual attack [7] are given. The rate is bounded due to the Poissonian photon number distribution of the source and the loss in the quantum channel ('rate bound') as shown in [7]. The combination of the source statistics, the loss and detector dark counts, there is a fundamental bound on the distance over which secure QKD could be proved with more advances proofs than ours, as shown in Brassard et al. [6].

where d_B is the dark count probability of the detector per signal slot and η_B is the single photon detection efficiency of the detector. The corresponding distance (given the parameters of the experiment) is shown in Figure 2.

We have therefore a clear picture of the rates and distances which are shown to be secure by our proof (the area below the curve 'coherent' in Fig. 2), those that are shown to be insecure [6,7] (the area outside of the two bound curves). Note that the area between the 'coherent' line and the two bounds is the area of the unknown. Future classical protocols taking on the error correction and privacy amplification tasks from our protocol in a different way (but leaving the quantum transmission and measurement untouched) and/or improved security proofs can proclaim more of this area 'secure'.

5 Proof of the main result

The structure of the proof follows. In the first section, an important feature of the distribution of errors during the quantum transmission is presented. As an immediate consequence we can proof the integrity of the protocol, meaning that when the validation test is passed, Bob shares the private key with Alice with high probability. The second section deals with the multi-photon signals' issue. It gives an upper bound on the number of bits a spy can get by an attack called photon number splitting attack. In the third section, we explore the method of privacy amplification implemented by binary matrices and taking into account linear error correction tools. It turns out that the privacy of the protocol is equivalent to the "privacy" in a modified protocol . This equivalence is proved in Section 5.4, and the corresponding mathematical model is provided in Section 5.5. Finally, the proof of privacy of the modified protocolis given.

There are several points where our proof deviates from that of Mayers [3]. Most notably this difference can be seen in Section 5.3 where the deviation between the proofs shows up quantitatively. However, changes in the protocol (in our protocol the number of transmitted signals is fixed which are not necessarily all detected, and not the number of detected signals, as in [2]) make it necessary to check in detail that the basic proof idea of Mayers carries through.

5.1 On the distribution of errors and the proof of integrity

We start with a property regarding the distribution of errors which is based solely on basic probability theory. It allows to make statements on the key derived from the set E based on the counting of errors in the set T. As an immediate application this property allows us to proof the integrity of the QKD protocol. Note, that in a practical run of quantum key distribution, we could omit this estimation, since we can learn the exact number of errors in E during the later stage of error correction. However, the kind of estimation presented here serves a second purpose, which is used later on in our proof. This purpose is to make a statement about the eavesdropping strategy and its expected error rate from the observed error rate. Let us explain this by an example: If Eve implements an intercept/resend attack where she measures Alice's bit in a randomly chosen signal basis and she resends a state to Bob corresponding to her measurement result, then she might be lucky an choose always the correct signal basis. In that (unlikely) event, she would cause no errors while obtaining full information on the key. Indirectly, the property below quantifies the idea that the observed numbers of errors will belong to a typical run of the protocol.

Property 1. *Let $\mathcal{S}$ be a set of finite size, s. Let C be a randomly chosen subset of $\mathcal{S}$. The random variable giving the choice of C is denoted by $\boldsymbol{C}$. Let A and B be two subsets of $\mathcal{S}$ chosen randomly as follows:*

1. *each element in $\mathcal{S}$ is put (exclusively) in A or B or neither of these sets with respective probabilities p_A, p_B and $1-(p_A+p_B)$. That is, the random variables giving the set to which the indexes in $\mathcal{S}$ belong to are independently and identically distributed;*
2. *furthermore, the random variables giving the set to which indexes in $\mathcal{S}$ belong to are independent of the random variable $\boldsymbol{C}$.*

We denote by $\boldsymbol{A}$, $\boldsymbol{B}$ the random variables giving the set A and B, respectively. Then for any positive real numbers δ, ϵ such that $0<\delta<\delta+\epsilon<1$,

$$\Pr(|\boldsymbol{A}\cap\boldsymbol{C}|<\delta s p_A \text{ and } |\boldsymbol{B}\cap\boldsymbol{C}|\geq(\delta+\epsilon)s p_B) \leq f(\delta,\epsilon,p_A,p_B,s) \quad (22)$$

Highlight Paper

where

$$f(\delta,\epsilon,p_A,p_B,s) = \exp\left[-\frac{1}{2\delta+\epsilon}\epsilon^2(\min\{p_A,p_B\})^2 s + 2\left(\frac{\epsilon}{2\delta+\epsilon}\right)^2\right]. \quad (23)$$

Proof. For any subset C of $\mathcal{S}$, given $\boldsymbol{C}=C$, each element of C is either in $\boldsymbol{A}$ or in $\boldsymbol{B}$ with respective probabilities p_A and p_B.

Now $c=|C|$ is either smaller than $\lfloor(\delta+\frac{\epsilon}{2})s\rfloor$ or bigger than $\lceil(\delta+\frac{\epsilon}{2})s\rceil$.

- If $c \leq \lfloor(\delta+\frac{\epsilon}{2})s\rfloor$, let $C' = C \cup D$ where D is some subset of $\mathcal{S}\setminus C$ such that $|C'| = c' = \lfloor(\delta+\frac{\epsilon}{2})s\rfloor$. Then $C \subset C'$, and

$$\Pr(|\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)sp_B|\boldsymbol{C}=C) \leq \Pr(|\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)sp_B|\boldsymbol{C}=C'). \quad (24)$$

Furthermore,

$$(\delta+\epsilon)sp_B = \frac{\delta+\epsilon}{\delta+\frac{\epsilon}{2}}p_B\left(\delta+\frac{\epsilon}{2}\right)s \geq \left(1+\frac{\epsilon}{2\delta+\epsilon}\right)p_B c', \quad (25)$$

and using the property 16 from Appendix for the set B and the set C',

$$\begin{aligned}\Pr(|\boldsymbol{B}\cap\boldsymbol{C}| &\geq (\delta+\epsilon)sp_B|\boldsymbol{C}=C') \\ &\leq \Pr\left(|\boldsymbol{B}\cap\boldsymbol{C}| \geq \left(1+\frac{\epsilon}{2\delta+\epsilon}\right)p_B c'|\boldsymbol{C}=C'\right) \quad (26)\\ &\leq \exp\left[-2\left(\frac{\epsilon p_B}{2\delta+\epsilon}\right)^2 c'\right] \quad (27)\\ &\leq f(\delta,\epsilon,p_A,p_B,s), \quad (28)\end{aligned}$$

since $(\min\{p_A,p_B\})^2 \leq p_B^2$ and $c' \geq \left(\delta+\frac{\epsilon}{2}\right)s-1$. Of course this implies that

$$\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| < \delta sp_A \text{ and } |\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)s|\boldsymbol{C}=C) \leq f(\delta,\epsilon,p_A,p_B,s). \quad (29)$$

- If $c \geq \lceil(\delta+\frac{\epsilon}{2})s\rceil$, then

$$\delta sp_A = \frac{\delta}{\delta+\frac{\epsilon}{2}}p_A\left(\delta+\frac{\epsilon}{2}\right)s \leq \left(1-\frac{\epsilon}{2\delta+\epsilon}\right)p_A c \quad (30)$$

and using the Property 16 for the set A and the set C,

$$\begin{aligned}\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| &< \delta sp_A|\boldsymbol{C}=C) \\ &\leq \Pr\left(|\boldsymbol{A}\cap\boldsymbol{C}| < \left(1-\frac{\epsilon}{2\delta+\epsilon}\right)p_A c|\boldsymbol{C}=C\right) \quad (31)\\ &\leq \exp\left[-2c\left(\frac{p_A\epsilon}{2\delta+\epsilon}\right)^2\right] \quad (32)\\ &\leq f(\delta,\epsilon,p_A,p_B,s), \quad (33)\end{aligned}$$

since $(\min\{p_A,p_B\})^2 \leq p_A^2 \leq 1$ and $c \geq \left(\delta+\frac{\epsilon}{2}\right)s > \left(\delta+\frac{\epsilon}{2}\right)s-1$. Again, this implies that

$$\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| < \delta sp_A \text{ and } |\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)s|\boldsymbol{C}=C) \leq f(\delta,\epsilon,p_A,p_B,s). \quad (34)$$

We conclude that for any C,

$$\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| < \delta sp_A \text{ and } |\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)s|\boldsymbol{C}=C) \leq f(\delta,\epsilon,p_A,p_B,s). \quad (35)$$

Thus

$$\begin{aligned}\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| &< \delta sp_A \text{ and } |\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)sp_B)\\ &= \sum_C \mathrm{P}_{\boldsymbol{C}}(C)\Pr(|\boldsymbol{A}\cap\boldsymbol{C}| < \delta sp_A \\ &\qquad \text{and } |\boldsymbol{B}\cap\boldsymbol{C}| \geq (\delta+\epsilon)sp_B|\boldsymbol{C}=C) \quad (36)\\ &\leq f(\delta,\epsilon,p_A,p_B,s), \quad (37)\end{aligned}$$

which concludes the proof. □

An immediate consequence of property 1 is that the error rate in the sifted key is not significantly higher than the error rate observed by Alice and Bob during the validation test. This implies the integrity of the protocol, as defined in Definition 1, or more formally:

Property 2. *The joint probability that Alice and Bob fail to share an identical key and that the validation test is passed is lower bounded by:*

$$\Pr(\neg\textbf{share} \text{ and } \textbf{valid}) \leq \epsilon_2(N,m) \quad (38)$$

where

$$\epsilon_2(N,m) = \min_{\tau_\Omega\in(0,1/2)}\left[e^{-\frac{1}{2\delta+\tau_{ec}}\tau_{ec}^2 p_R^2(\frac{1}{2}-\tau_\Omega)r_{min}N+2\left(\frac{\tau_{ec}}{2\delta+\tau_{ec}}\right)^2} + e^{-2\tau_\Omega^2 r_{min}N}\right]. \quad (39)$$

Proof. We have seen that Alice and Bob run an error-correcting scheme capable of correcting $\lceil(\delta+\tau_{ec})(1-p_R)|\Omega|\rceil$ errors in E. Thus Bob shares exactly the same key after the error correction step if there are less than $(\delta+\tau_{ec})(1-p_R)|\Omega|$ errors in E. Given that $\boldsymbol{\Omega}=\Omega$ where $\Omega \subset \{1,\ldots,N\}$, the probability that the validation test passes while there are more than $(\delta+\tau_{ec})(1-p_R)|\Omega|$ errors in E is bounded by:

$$\begin{aligned}\Pr(&\boldsymbol{\mathcal{P}}(\boldsymbol{T},\delta|\Omega|p_R) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},(\delta+\tau_{ec})|\Omega|(1-p_R)))\\ &= \Pr(|\boldsymbol{T}\cap\boldsymbol{C}| < \delta|\Omega|p_R \text{ and } |\boldsymbol{E}\cap\boldsymbol{C}|\\ &\geq (\delta+\tau_{ec})|\Omega|(1-p_R)) \quad (40)\\ &\leq f(\delta,\tau_{ec},p_R,1-p_R,|\Omega|)\\ &\leq \exp\left[-\frac{1}{2\delta+\tau_{ec}}\tau_{ec}^2 p_R^2|\Omega| + 2\left(\frac{\tau_{ec}}{2\delta+\tau_{ec}}\right)^2\right]. \quad (41)\end{aligned}$$

using the above property for $\mathcal{S}=\Omega$ and where $\boldsymbol{C}$ is the random variable giving the set of discrepancies between

Alice's bits $\vec{g}(\Omega)$ and Bob's bits $\vec{h}(\Omega)$ on Ω. Indeed, $\boldsymbol{R}$ is independent of $\boldsymbol{C}$, and consequently the random variables giving the set (E or T) to which the indexes in Ω belong to are independently and identically distributed ($\Pr(i \in E|i \in \Omega) = (1-p_R)$ and $\Pr(i \in T|i \in \Omega) = p_R$), and independent of $\boldsymbol{C}$. The above implies that the probability that the error correction fails to reconcile Alice's and Bob's sifted keys while the validation test is passed is upper-bounded by an exponentially decreasing function of $|\Omega|$. Now, each index in $\mathcal{D}$ has probability 1/2 to be put in the set $\boldsymbol{\Omega}$. Let τ_Ω be a constant obeying $0 < \tau_\Omega < 1/2$. Suppose we are given that $\boldsymbol{n} = n$ for some positive integer n. Using Property 16 in the Appendix, the probability that there are less than $(\frac{1}{2} - \tau_\Omega)n$ is bounded by:

$$\Pr\left(|\boldsymbol{\Omega}| \leq \left(\frac{1}{2} - \tau_\Omega\right) n|\boldsymbol{n} = n\right) \leq e^{-2\tau_\Omega^2 n}. \qquad (42)$$

Therefore,

$$\begin{aligned}
&\Pr(\neg\textbf{share} \wedge \textbf{valid}) \\
&\quad \leq \Pr(\boldsymbol{\mathcal{P}}(\boldsymbol{T}, \delta|\boldsymbol{\Omega}|p_R) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E}, (\delta+\tau_{ec})|\boldsymbol{\Omega}| \\
&\qquad \times (1-p_R)) \Big| \boldsymbol{n} > r_{min}N) \qquad (43) \\
&\quad \leq \Pr\left(\boldsymbol{\mathcal{P}}(\boldsymbol{T}, \delta|\boldsymbol{\Omega}|p_R) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E}, (\delta+\tau_{ec})|\boldsymbol{\Omega}| \right. \\
&\qquad \left. \times(1-p_R)) \Big| |\boldsymbol{\Omega}| \geq \left(\frac{1}{2} - \tau_\Omega\right)\boldsymbol{n},\ \boldsymbol{n} > r_{min}N\right) \\
&\qquad + \Pr\left(|\boldsymbol{\Omega}| \leq \left(\frac{1}{2} - \tau_\Omega\right)\boldsymbol{n} \Big| \boldsymbol{n} > r_{min}N\right) \\
&\quad \leq e^{-\frac{1}{2\delta+\tau_{ec}}\tau_{ec}^2 p_R^2 (\frac{1}{2}-\tau_\Omega) r_{min}N + 2\left(\frac{\tau_{ec}}{2\delta+\tau_{ec}}\right)^2} + e^{-2\tau_\Omega^2 r_{min}N}, \\
&\qquad\qquad (44)
\end{aligned}$$

since $\boldsymbol{n} > r_{min}N$ if the validation test is passed. Since this equations has to hold for all values $\tau_\Omega \in (0, 1/2)$, we have especially

$$\begin{aligned}
&\Pr(\neg\textbf{share} \wedge \textbf{valid}) \leq \\
&\quad \min_{\tau_\Omega \in (0,1/2)} \left[e^{-\frac{1}{2\delta+\tau_{ec}}\tau_{ec}^2 p_R^2 (\frac{1}{2}-\tau_\Omega) r_{min}N + 2\left(\frac{\tau_{ec}}{2\delta+\tau_{ec}}\right)^2}\right. \\
&\qquad\qquad \left. + e^{-2\tau_\Omega^2 r_{min}N}\right]. \qquad (45)
\end{aligned}$$

This concludes the proof. □

5.2 On multiple photon signals

Let $\mathcal{A} = \{1, \ldots, N\}$ be the set of indexes of all signals Alice sent. Each signal Alice sends contains zero, one or more photons, with respective probabilities denoted by p_V, p_S and p_M. Alice does not know how many photons she actually emits in each individual pulse. However, a potential eavesdropper Eve can learn the actual number of emitted photons without disturbing the quantum signal, thanks to a quantum non demolition measurement (we assume no technological limitation for the enemy). Let's denote by V, S and M the set of indexes of signals containing zero, one and more photons, respectively. Therefore, $V \cup S \cup M = \mathcal{A}$ and the set V, S and M are disjoint. We will denote by $\Sigma = (V, S, M)$ this partition of $\mathcal{A}$. We will deal with the worst case scenario in which the partition Σ is unknown to Alice, but perfectly known to Eve.

In the following sections, a lower bound on the number of bits in the sifted key not arising from multi-photon signals (that is $|E \cap \overline{M}|$) will be required. Most of practical implementations of quantum key distribution today use a quantum channel with high loss rate, due to technological limitations. This loss rate must be taken into account to establish the required lower bound. For, Eve could replace secretly the quantum channel by a perfect quantum channel without loss (again, we assume no technological limitation for Eve). Eve might then stop signals containing only one photon, as long as the resulting loss rate of the quantum channel does not exceed significantly the expected loss rate of the original channel. By doing so, Eve increases the proportion of bits arising from multi-photon signals in the sifted key, without being noticed by the legitimate users. Now if a signal sent by Alice contains several photons, Eve can split off one photon from the pulse without disturbing the polarisation of the remaining photons. She stores the stolen photon until bases are announced and learns deterministically the corresponding bit by measuring it in the correct basis. This attack is usually referred to as the *photon number splitting* attack [6,7]. It is in view of this attack (in a slightly different context) that we will need to estimate the number of bits in the sifted key that are not arising from multi-photon signals.

It is possible to give a probabilistic lower bound on the number of bits in the sifted key that are not arising from multiple photon signals, provided that an upper-bound on the probability p_M is given. More precisely,

Property 3. *Let's denote by $\widehat{l}$ the number of bits in E that are not arising from multi-photon signals, i.e. $\widehat{l} = |E \cap \overline{M}|$. We denote by $\widehat{\boldsymbol{l}} = |\boldsymbol{E} \cap \overline{\boldsymbol{M}}|$ the corresponding random variable. We recall that we defined the random variable $\widehat{\boldsymbol{l}}_{\boldsymbol{min}}$ as:*

$$\widehat{\boldsymbol{l}}_{\boldsymbol{min}} = \left[\frac{1-p_R}{2} - \hat{\tau}\right](\boldsymbol{n} - M_{max}) \qquad (46)$$

where the security constants τ_M and $\hat{\tau}$ are strictly positive real number such that $M_{max}/N < r_{min}$ and $\frac{1-p_R}{2} - \hat{\tau} > 0$. Then the joint probability that $\boldsymbol{n} > r_{min}N$ and that $\widehat{\boldsymbol{l}} < \widehat{\boldsymbol{l}}_{min}$ is bounded by:

$$\Pr(\widehat{\boldsymbol{l}} \leq \widehat{\boldsymbol{l}}_{min} \wedge \boldsymbol{n} > r_{min}N) \leq e^{-2\hat{\tau}^2(r_{min}N - M_{max})} + e^{-2\tau_M^2 N}. \qquad (47)$$

Proof. We consider the worst case scenario in which all losses and errors are caused by Eve's intervention on the quantum channel. Obviously, in order to minimise $\widehat{l}$, Eve intervene in such a way that $M \subset \mathcal{D}$.

Suppose we are given that Bob detected $\boldsymbol{n} = n$ signals and that $\boldsymbol{M} = M$. Then there are at least $n - |M|$ signals in $\mathcal{D}$ that are not arising from multi-photon pulses. Now, each of these non-multiphoton signals in $\mathcal{D}$ has probability

$(1-p_R)/2$ of being put in the set $\boldsymbol{E}$. Therefore, the probability that there are less than $[(1-p_R)/2-\hat{\tau}]\,(n-|M|)$ signals in the sifted key not arising from multi-photon signals is bounded by:

$$\Pr\left(\widehat{\boldsymbol{l}} \le \left[\frac{1-p_R}{2}-\hat{\tau}\right](n-|M|)\Big|\boldsymbol{n}=n, \boldsymbol{M}=M\right) \le e^{-2\hat{\tau}^2(n-|M|)} \qquad (48)$$

using Property 16 in Appendix.

Now, the marginal probability that Alice sent more than $(p_M+\tau_M)N$ multi-photon signals is bounded using property 16 in Appendix:

$$\Pr(|\boldsymbol{M}| \ge (p_M+\tau_M)N) \le e^{-2\tau_M^2 N} \qquad (49)$$

since each signal Alice sends has probability p_M of being in $\boldsymbol{M}$.

Note that $[(1-p_R)/2-\hat{\tau}]\,(n-|M|) \ge \widehat{l}_{min}$ whenever $|M| \le (p_M+\tau_M)N$. Therefore, given that $\boldsymbol{n}=n$, the probability that there are less than $\widehat{l}_{min}$ signals in the sifted key that were not emitted with several photons is bounded by:

$$\begin{aligned}\Pr(\widehat{\boldsymbol{l}} \le \widehat{l}_{min}|\boldsymbol{n}=n) &\le \Pr(|\boldsymbol{M}| \ge (p_M+\tau_M)N\,|\,\boldsymbol{n}=n)\\ &\quad + \Pr(\widehat{\boldsymbol{l}} \le \widehat{l}_{min} \text{ and } |\boldsymbol{M}| \le (p_M+\tau_M)N|\boldsymbol{n}=n) \qquad (50)\\ &\le \Pr(|\boldsymbol{M}| \ge (p_M+\tau_M)N\,|\,\boldsymbol{n}=n)\\ &\quad + e^{-2\hat{\tau}^2(n-(p_M+\tau_M)N)}. \qquad (51)\end{aligned}$$

Multiplying both side by $\mathrm{P}_{\boldsymbol{n}}(n)$ and summing over $n > r_{min}N$, we get:

$$\begin{aligned}\Pr(\widehat{\boldsymbol{l}} \le \widehat{l}_{min} \wedge \boldsymbol{n} > r_{min}N) &\le \Pr(|\boldsymbol{M}| \ge (p_M+\tau_M)\\ &\quad\times N \wedge \boldsymbol{n} > r_{min}N) + \sum_{n>r_{min}N} e^{-2\hat{\tau}^2(n-(p_M+\tau_M)N)}\mathrm{P}_{\boldsymbol{n}}(n) \qquad (52)\\ &\le \Pr(|\boldsymbol{M}| \ge (p_M+\tau_M)N)\\ &\quad + e^{-2\hat{\tau}^2(r_{min}N-(p_M+\tau_M)N)} \qquad (53)\\ &\le e^{-2\tau_M^2 N} + e^{-2\hat{\tau}^2(r_{min}N-M_{max})}, \qquad (54)\end{aligned}$$

which concludes the proof. □

5.3 On privacy amplification

In this section, diverse notions used in connection with privacy amplification are defined. In particular, we define $\widehat{d}_w$, the minimal weight of a privacy amplification code, used in conjunction with an error-correcting code and an imperfect source. Finally, an important probabilistic lower bound on this weight is proved. This bound will be used in the last part of the proof. It is this minimal weight which will keep track of the multi-photon signals. The changed estimation of the minimum weight is therefore the most important change of this proof as respect to Mayers proof [3], although other details need to be adapted.

The privacy amplification is specified by a $m \times l$ binary matrix K. The linear error correction code is specified by a $r \times l$ binary parity check matrix F. We introduce some notations. Let G be the $(r+m) \times l$ matrix:

$$G = \begin{pmatrix} F \\ K \end{pmatrix}. \qquad (55)$$

For any matrix A, $A_{(i)}$ denotes its ith row and $A^{(i)}$ its ith column.

Recall that $\widehat{l} = |E \cap \overline{M}|$ is the number of signals in E that are not arising from pulses sent with several photons.

Let $\widehat{G}$ be the $(r+m) \times \widehat{l}$ matrix obtained from G by removing the columns $G^{(i)}$, $i \in M \cap E$, corresponding to the multi-photon signals. Equivalently, $\widehat{G}$ is the matrix formed by the $\widehat{l}$ columns of G corresponding to signals in $E \cap \overline{M}$. Let $\check{G}$ be the $(r+m) \times (l-\widehat{l})$ matrix formed by the $(l-\widehat{l})$ columns $G^{(i)}$, $i \in E \cap M$. Similarly, we define $\widehat{F}$, $\widehat{K}$ obtained from F, K by removing the $l-\widehat{l}$ columns $F^{(i)}, G^{(i)}$, $i \in E \cap M$ respectively. And $\check{F}$, $\check{K}$ are the matrices formed by the $l-\widehat{l}$ columns $F^{(i)}, G^{(i)}$, $i \in E \cap M$ respectively. Thus

$$\widehat{G} = \begin{pmatrix} \widehat{F} \\ \widehat{K} \end{pmatrix}, \quad \check{G} = \begin{pmatrix} \check{F} \\ \check{K} \end{pmatrix}. \qquad (56)$$

Let $\widehat{\mathcal{G}}$ be the set of linear combinations of rows of $\widehat{G}$. Let $\widehat{\mathcal{G}}^*$ be the set of linear combinations of rows of $\widehat{G}$ which contain at least one row of $\widehat{K}$, i.e.

$$\widehat{\mathcal{G}}^* = \left\{ \sum_{i=1}^{r+m} z_i \widehat{G}_{(i)} \pmod 2 \;:\; \vec{z} \in \{0,1\}^{r+m}, z_j = 1 \right.$$
$$\left. \text{for at least one } j \in \{r+1, \ldots r+m\} \right\}. \qquad (57)$$

We define $\widehat{\mathcal{C}}$ as:

$$\widehat{\mathcal{C}} = \left\{ \vec{x} \in \{0,1\}^{\widehat{l}} \;:\; \widehat{G}\vec{x} = \vec{0} \right\} = \left(\widehat{\mathcal{G}}\right)^{\perp}. \qquad (58)$$

Note that $\widehat{\mathcal{C}}^{\perp} = \widehat{\mathcal{G}}$. We define the *minimum weight* of $\widehat{\mathcal{G}}^*$ as the integer:

$$\widehat{d}_w = \min_{\vec{x} \in \widehat{\mathcal{G}}^*} w(\vec{x}). \qquad (59)$$

Equivalently,

$$\widehat{d}_w = \min_{\vec{u} \in \{0,1\}^r, \vec{v} \in \{0,1\}^m \setminus \{\vec{0}\}} w(\vec{u}^T \widehat{F} + \vec{v}^T \widehat{K}). \qquad (60)$$

The minimum weight is an important characterisation of the combination of the error correction code matrix F and the privacy amplification matrix K. It denotes the minimum number of signals contributing to key bits or parities of sets of key bits after taking into account publicly known parities from the error correction code and the knowledge from multi-photon signals. We need a probabilistic bound on this quantity. Here we will derive it for the case of random coding where K is a random binary matrix, but we would like to point out that other suitable choices for K are indeed possible, and might lead to increased performance of the protocol in terms of the yield of secure bits. The important property to be fulfilled is Property 4.

We approach the bound on $\widehat{d}_w$ via the following lemma taken directly from [3]:

Lemma 1. *Let k, a and b be positive integers. Let A be any $a \times k$ binary matrix. Let B be a $b \times k$ binary matrix, picked at random with uniform distribution. We denote by $\boldsymbol{B}$ the corresponding random variable. Let d_{AB} be the minimum weight of linear combinations of rows of A and B that contain at least one row of B:*

$$d_{AB} = \min_{\vec{u} \in \{0,1\}^a, \vec{v} \in \{0,1\}^b \setminus \{\vec{0}\}} w(\vec{u}^T A + \vec{v}^T B). \tag{61}$$

Then for any positive real number x such that $x/k < 1/2$ and for any positive real number τ,

$$\frac{a+b}{k} \le 1 - H_1\left(\frac{x}{k}\right) - \tau \quad \Rightarrow \quad \Pr(d_{\boldsymbol{AB}} < x) \le 2^{-\tau k} \tag{62}$$

where H_1 is the binary entropy function.

Proof of the lemma. Let C be the $(a+b) \times k$ matrix defined by:

$$C = \begin{pmatrix} A \\ B \end{pmatrix}. \tag{63}$$

Define the real number R as $R = kH_1^{-1}(1 - \frac{a+b}{k} - \tau)$ where H_1^{-1} is the inverse function of the restricted bijective function $H_1 : [0, \frac{1}{2}] \to [0,1]$. Assume that $\frac{a+b}{k} \le 1 - H_1(\frac{x}{k}) - \tau$. This implies that $x \le R$. Let $\mathcal{B}$ be the sphere in $\{0,1\}^k$ centred at the zero string $\vec{0}$ and of radius R. For $i \in \{1, \ldots b\}$, let's denote by q_i the probability that there exists $\vec{z} \in \{0,1\}^{a+i-1}$ such that $\boldsymbol{B}_{(i)} + \sum_{j=1}^{a+i-1} z_j C_{(j)}$ is in $\mathcal{B}$ (equivalently, q_i is the probability that the coset $\boldsymbol{B}_{(i)} + \text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right)$ intersects $\mathcal{B}$). Then

$$\begin{aligned} \Pr(d_{\boldsymbol{AB}} < x) &\le \Pr(d_{\boldsymbol{AB}} < R) & (64) \\ &= q_1 + q_2(1-q_1) + \cdots + q_b \prod_{i=1}^{b-1}(1-q_i) & (65) \\ &\le \sum_{i=1}^{b} q_i, & (66) \end{aligned}$$

since the probability that $d_{AB} < R$ is the probability that, if one picks successively at random the rows $\boldsymbol{B}_{(1)}, \boldsymbol{B}_{(2)}, \ldots, \boldsymbol{B}_{(b)}$, at some step $i \in \{1, \ldots, b\}$ the set $B_{(i)} + \text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right)$ intersects $\mathcal{B}$.

Now,

$$\begin{aligned} &\left(\boldsymbol{B}_{(i)} + \text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right)\right) \cap \mathcal{B} \neq \emptyset \Leftrightarrow \\ &\qquad \boldsymbol{B}_{(i)} \in \left\{\vec{x} + \text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right) \,:\, \vec{x} \in \mathcal{B}\right\}, \end{aligned} \tag{67}$$

where the size of the last set is upper bound by $|\mathcal{B}| \times |\text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right)|$. Since $\boldsymbol{B}_{(i)}$ is chosen randomly out of 2^k strings,

$$\begin{aligned} q_i &\le \frac{|\mathcal{B}| \times |\text{Span}\left(\{C_{(j)}\}_{j \le a+i-1}\right)|}{2^k} & (68) \\ &\le 2^{a+i-1-k} |\mathcal{B}|, & (69) \end{aligned}$$

and using the binomial tail inequality (Property 13):

$$|\mathcal{B}| = \sum_{q=0}^{\lfloor R \rfloor} \binom{k}{q} \le 2^{kH_1(R/k)} \quad \text{for } \frac{R}{k} \le \frac{1}{2}, \tag{70}$$

we find

$$q_i \le 2^{a+i-1-k+k\left(1 - \frac{a+b}{k} - \tau\right)} = 2^{-b-\tau k+i-1}, \tag{71}$$

thus

$$\Pr(d_{\boldsymbol{AB}} < R) \le \sum_{i=1}^{b} q_i = 2^{-b-\tau k} \sum_{i=0}^{b-1} 2^i \le 2^{-\tau k}. \tag{72}$$

Therefore, the expected probability that $d_{\boldsymbol{AB}} \le R$ is smaller than $2^{-\tau k}$. Thus,

$$\frac{a+b}{k} \le 1 - H_1(\frac{x}{k}) - \tau \quad \Rightarrow \quad \Pr(d_{\boldsymbol{AB}} < x) \le 2^{-\tau k} \tag{73}$$

which concludes the proof of the lemma. □

This bound allows us to prove the following crucial property:

Property 4. *Let $\widehat{\boldsymbol{d}}_{\boldsymbol{w}}$ be the random variable giving the minimum weight $\widehat{d}_w$ defined above. Then, given that $\boldsymbol{n} = n$ for some positive integer n and $\widehat{\boldsymbol{l}} \ge \widehat{l}_{min}$,*

$$\begin{aligned} \Pr\Bigg(\frac{\widehat{\boldsymbol{d}}_{\boldsymbol{w}}}{2} < (\delta + \tau_f)\frac{1-p_R}{2}n \,\Bigg|\, \widehat{\boldsymbol{l}} \ge \widehat{l}_{min}, \\ \boldsymbol{n} = n, \textbf{valid} = \textit{True}\Bigg) \le 2^{-\tau_p \widehat{l}_{min}}. \end{aligned} \tag{74}$$

Proof. Given that $\boldsymbol{n} = n$ and $\widehat{\boldsymbol{l}} = \widehat{l} \ge \widehat{l}_{min}$, note that the random variable $\widehat{\boldsymbol{K}}$ is uniformly distributed and independent of other variables. Passing the validation test in the protocol requires that the Constraint 9

$$\frac{m+r}{\widehat{l}_{min}} \le 1 - H_1\left[\frac{2(\delta+\tau_f)\frac{1-p_R}{2}n}{\widehat{l}_{min}}\right] - \tau_p \tag{75}$$

is satisfied. Since the validation test is passed, especially equation (8), the argument of $H_1(x)$ satisfies $x < 1/2$. Moreover, we have $\frac{m+r}{\widehat{l}} \le \frac{m+r}{\widehat{l}_{min}}$ and $1 - H_1(\frac{2(\delta+\tau_f)\frac{1-p_R}{2}n}{\widehat{l}}) - \tau_p \ge 1 - H_1(\frac{2(\delta+\tau_f)\frac{1-p_R}{2}n}{\widehat{l}_{min}}) - \tau_p$. Therefore, the number of rows of $\widehat{F}$ and $\widehat{K}$ verify:

$$\frac{m+r}{\widehat{l}} \le 1 - H_1\left[\frac{2(\delta+\tau_f)\frac{1-p_R}{2}n}{\widehat{l}}\right] - \tau_p. \tag{76}$$

Highlight Paper

We can therefore apply the above lemma for $A = \widehat{F}$, $\boldsymbol{B} = \widehat{\boldsymbol{K}}$, $k = \widehat{l}$ and $x = 2(\delta + \tau_f)(1 - p_R)n/2$. We obtain that:

$$\Pr\left(\widehat{\boldsymbol{d}}_{\boldsymbol{w}} < 2(\delta+\tau_f)\frac{1-p_R}{2}n \,\middle|\, \widehat{\boldsymbol{l}} = \widehat{l} \geq \widehat{l}_{min}, \boldsymbol{n} = n, \textbf{valid} = \text{True}\right) \leq 2^{-\tau_p \widehat{l}} \tag{77}$$

or,

$$\Pr\left(\frac{\widehat{\boldsymbol{d}}_{\boldsymbol{w}}}{2} < (\delta+\tau_f)\frac{1-p_R}{2}n \,\middle|\, \widehat{\boldsymbol{l}} \geq \widehat{l}_{min}, \boldsymbol{n} = n, \textbf{valid} = \text{True}\right) \leq 2^{-\tau_p \widehat{l}_{min}} \tag{78}$$

which concludes the proof of the property. □

5.4 Reduction to a modified situation

In this section, a modified situation of the original protocol is defined. This modified situation does not correspond to a key distribution, but nevertheless, a "key" is defined at Alice's side. Surprisingly, the "privacy" in the modified situation implies the privacy of the original protocol, and this implication is proved.

5.4.1 Equivalence with the modified protocol

We first describe the *modified protocol* which is similar to the original protocol, except that Bob measures the photons in the sifted set E in the wrong bases (therefore Bob does not share the private key with Alice). We show that the security of the modified protocol is equivalent to the security of the original protocol.

In the subsequent discussion, we will consider — without loss of generality as far as the security of the protocol is concerned — that Bob's choice of measurement bases $\vec{b}$ and the set R are provided by a randomising box at Bob's side: the box generates randomly a choice for R and for $\vec{b}$ at the beginning of the protocol. It then provides Bob with the generated data as required by the protocol, that is, it gives $\vec{b}$ during step 2 and R at the step 4 to Bob. We now define the intermediate protocol as follows. In the intermediate protocol,

- Alice behaves exactly as in the original protocol;
- Bob's randomising box generates R and $\vec{b}$ as before, but gives $\tilde{\vec{b}}$ instead of $\vec{b}$ to Bob at step 2, where:

$$\tilde{b}_i \overset{Def}{=} \begin{cases} b_i \text{ if } i \in R \\ \neg b_i \text{ if } i \notin R. \end{cases} \tag{79}$$

  The box announces R to Bob at step 4 as in the original protocol;
- Bob behaves exactly as in the original situation, except that, in step 5, after he learned the choice for R, he computes and announces $\vec{b}$ rather than $\tilde{\vec{b}}$.

Therefore, in the modified protocol, Bob measures Alice's signals in the bases $\tilde{\vec{b}}$ and announces $\vec{b}$. The underlying idea is that the original and the modified protocols are identical, except that Bob measures the signals indexed in $\overline{R}$ in the wrong bases (without actually knowing R). Consequently, Alice's sifted key and Bob's sifted key are uncorrelated: Bob does not share the key with Alice. The private key is only defined in Alice's hand. Therefore, this situation does not describe a key exchange. It is only an abstract stepping stone towards the proof of unconditional privacy, thanks to the following property:

Property 5. *Whichever strategy a potential eavesdropper Eve chooses, the random variable giving jointly Alice's private key and Eve's view has the same probability distribution in both protocol.*

Proof. In the following, we say that a random variable in the original protocol and the corresponding random variable in the modified protocol are *indistinguishable* if and only if their probability distributions are identical. A quantum system whose state is not a priori known is characterised by an ensemble description. Given a system having probability p_i to be in the state ρ_i for $i = 1, 2, \ldots, k$, its *ensemble description* is the list $\{(p_i, \rho_i)\}_i$, that is, the list of its possible states together with the corresponding probabilities. We say that a quantum system in the original protocol and the corresponding quantum system in the modified protocol are *indistinguishable* if and only if their ensemble descriptions are identical. Throughout the proof of this property, we consider an arbitrary but fixed strategy adopted by Eve. By strategy, we mean the algorithm or the "program" followed by Eve to eavesdrop. Therefore, if Eve is given the same input, she will act identically. We have to prove that the data Eve accesses and the private key Alice gets in the original protocol and in the modified protocol are indistinguishable if Eve follows this given strategy. Recall that in the original protocol, Eve learns the values of $\mathcal{D}$, R, $\vec{b}$, $\vec{h}(\mathcal{D} \cap R)$, $\mathcal{P}(T, d)$, $\vec{a}$, F, $\vec{s}$ and K via the public discussions. Eve may also attempt to eavesdrop the quantum channel. If a pulse contains several photons, Eve might keep one photon and store it until bases are announced, thus obtaining deterministically the corresponding bit. Eve may also entangle a quantum probe P to Alice's single photon signals, and measure P after public discussions. She might also stop some single photon signals, leaving pulses in vacuum state to Bob. Let $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ldots, \boldsymbol{D})$ be a set of random variables (and/or quantum systems) in the original protocol. Let $(\boldsymbol{A'}, \boldsymbol{B'}, \boldsymbol{C'}, \ldots, \boldsymbol{D'})$ be the set of corresponding random variables (and/or quantum systems) in the modified protocol. Note that one can show that the set $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ldots, \boldsymbol{D})$ is indistinguishable from the set $(\boldsymbol{A'}, \boldsymbol{B'}, \boldsymbol{C'}, \ldots, \boldsymbol{D'})$ by showing successively that: $\boldsymbol{A}$ and $\boldsymbol{A'}$ are indistinguishable. Given $\boldsymbol{A}$ and $\boldsymbol{A'}$ take the same value (denoted as $\boldsymbol{A} = \boldsymbol{A'}$), $\boldsymbol{B}$ and $\boldsymbol{B'}$ are indistinguishable. Given $\boldsymbol{A} = \boldsymbol{A'}$ and $\boldsymbol{B} = \boldsymbol{B'}$, $\boldsymbol{C}$ and $\boldsymbol{C'}$ are indistinguishable, etc. Now:

- the choice for $\vec{a}$, $\vec{g}$, $\vec{b}$ and R are indistinguishable in both protocol. Given that the choice for $\vec{a}$, $\vec{g}$, $\vec{b}$ and

R takes the same values in both protocol, Alice announces the same $\vec{a}$ in step 8 and Bob announces the same $\vec{b}$ and R in step 5;

- given that Alice's choice for $\vec{a}$ and $\vec{g}$ take the same value in both protocol, Alice's quantum signals are indistinguishable in both protocol;
- given that Alice's quantum signals are in the same state in both protocols, Eve acts on them in the same manner: the interaction of the quantum signals with Eve's apparatus and the probe P remains the same. Thus the resulting quantum signals (disturbed and/or suppressed by Eve) received by Bob are indistinguishable in both protocol. Likewise, the resulting states of Eve's apparatus and probe P are indistinguishable in both protocol. Naturally, after the above coupling, the density matrix describing P does not depend on Bob's choice of bases or outcomes of the measurements;
- we assumed that given a quantum signal, the probability that Bob detects at least one photon in this signal is independent of his choice of basis. Therefore, given that Alice's quantum signals are identical in both protocol, the set of detected signals in the modified protocol is indistinguishable from the set $\mathcal{D}$ of detected signals in the original protocol. Given that the choice for $\vec{b}$ and R is the same in both protocol, since $\tilde{b}_i = b_i$ for $i \in R$, the measurement outcome h_i in the modified protocol is indistinguishable from the h_i in the original protocol, for $i \in R$. Therefore Bob's announcement of $\vec{h}(R \cap \mathcal{D})$ in the modified protocol is indistinguishable from its counterpart in the original protocol;
- as a result, the sets Ω, T and E computed by Alice in the modified protocol are indistinguishable from the corresponding sets computed in the original protocol;
- the above implies that the outcome of the test $\mathcal{P}(T, d)$ is indistinguishable in both protocol;
- in both protocol, Alice's choices for K and F are indistinguishable. Given $\vec{g}$, E and F take the same value in both protocol, Alice announces the same syndrome $\vec{s}$;
- the private data Eve wishes to discover is the private key $\vec{\kappa} = K\vec{g}(E) \pmod 2$ in both situation.

Therefore, the public announcements, Eve's apparatus and probe, and Alice's private key are indistinguishable in both protocol. Thus the random variables giving the results Eve gets from measuring her apparatus and probe are indistinguishable in both situation. This concludes the proof. □

5.4.2 Further reduction

The previous section has shown that it is sufficient to prove privacy of the modified protocol to prove that the original protocol is secure. It turns out that it is simpler to prove security for the modified protocol since Bob has no information about the private key. The privacy of the modified protocol can be proved even in the following situation where:

- Alice announces generously $\vec{g}(\overline{E})$ after she announces $\vec{a}$ in step 8, and
- Bob announces generously $\vec{h}(\mathcal{D})$ in step 3 (i.e. before announcement of the revealed set R), instead of announcing $\vec{h}(\mathcal{D} \cap R)$ in step 6.

Of course, this can only weaken the security of the modified protocol, and the security of the resulting protocol implies the security of the original protocol.

Provided the randomising box is not corrupted and the random choice of R and $\vec{b}$ are announced honestly in step 5 by the box, the security of the modified protocol can be proved even if we furthermore assume that Bob is corrupted by Eve. That is, Bob tells Eve the output $\vec{\tilde{b}}$ of the randomising box in step 2 and Eve and Bob together make the measurement they want on the quantum signals sent by Alice. Bob then announces $\mathcal{D}$ and $\vec{h}(\mathcal{D})$ as told by Eve in step 3. Thus we can regard the couple Eve-Bob as a single enemy, provided that the randomising box is not corrupted and that the public announcement of R and $\vec{b}$ in step 5 is made directly by the box.

Of course, $\vec{h}(T)$ should be close enough to $\vec{g}(T)$ so that the couple Eve-Bob passes the test. The eavesdropping fails if Alice declares $\neg\mathcal{P}(T, d)$. After the public discussion, Eve may execute another measurement on the residual state of the photons to refine her information.

5.4.3 Reduction related to multiple photon signals

We now present a reduction related to the multiple photon signals. By assuming that the enemy has full knowledge about the multiple photon signals prior to any public announcement, this reduction will allow us to work with a simpler situation in which the enemy is performing a conditional measurement on single photon signals only.

Since Eve has no technological limitation, we must assume that Eve-Bob have perfect detectors. We also consider the worst case scenario in which Eve replaces the quantum channel by a perfect one. Therefore, Eve-Bob are cheating when the set $\mathcal{D}$ containing all signals in which Bob officially detected at least one photon is not equal to $S \cup M$. Eve-Bob choose the set $\mathcal{D}$ at their convenience, while ensuring that the observed transmission rate n/N is not significantly lower than the expected transmission rate. Now, if Alice emits a signal of index i with several photons, Eve-Bob may pick up one photon from the signal and measure it in basis $\tilde{b}_i$, giving the outcome h_i. Then they measure the remaining photons in the pulse in the other basis $\neg\tilde{b}_i$, yielding a result h'_i. The bit h_i allows Eve-Bob to pass the test for the index i, if $i \in T$. After announcement of Alice's basis a_i, Eve-Bob knows whether $a_i = \tilde{b}_i$ or $a_i = \neg\tilde{b}_i$. In either case, Eve-Bob learn deterministically g_i (since $g_i = h_i$ if $a_i = \tilde{b}_i$ and $g_i = h'_i$ if $a_i = \neg\tilde{b}_i$). That is, for any signal i emitted with several photons, Eve-Bob can learn deterministically g_i while passing the test for the index i with certainty, if $i \in T$. In order to take into account this extra knowledge gained by Eve-Bob from the multi-photon signals, we consider a slightly worse scenario. We henceforth assume that:

- in addition to sending the photon pulses exactly as described previously, Alice's source tells secretly Eve-Bob the partition $\Sigma = (V, S, M)$, the number of photons n_i in each pulse i in M (collectively denoted by $\vec{n}(M)$), Alice's bases $\vec{a}(M)$ and Alice's bits $\vec{g}(M)$. These secret announcements are made at the same time as the source emits the quantum signals and we denote them collectively by $\mathcal{M} = (\Sigma, \vec{n}(M), \vec{a}(M), \vec{g}(M))$.

Again, this assumption can only weaken the security of the protocol. Now given $\mathcal{M}$, Eve-Bob can re-create the signals sent by Alice on M. That is, provided Eve-Bob learn $\mathcal{M}$, we can assume that Eve-Bob receive only photon pulses that are in S, without modifying the security of the protocol.

To summarise, the security of the original key distribution protocol is implied by the security of the modified protocol in which Bob is corrupted by Eve and in which:

- $\mathcal{M} = (\Sigma, \vec{n}(M), \vec{a}(M), \vec{g}(M))$ are given secretly to Eve-Bob during step 2;
- Eve-Bob receive only photon pulses that are in S;
- Eve-Bob must announce publicly $\vec{h}(\mathcal{D})$ in step 3;
- Bob's randomising box is not corrupted and announces publicly R and $\vec{b}$ honestly in step 5.

5.5 Mathematical model of eavesdropping in the modified situation

We define the view of Eve-Bob as the set of all data Eve-Bob acquired during the modified protocol. The random variable describing this view is denoted by $\boldsymbol{v}$, and takes value in the set of all possible view values, $\mathcal{Z}$. Following our model, the view v has the following form:

$$\boldsymbol{v} = (\boldsymbol{\mathcal{M}}, \boldsymbol{\mathcal{D}}, \vec{\boldsymbol{h}}(\boldsymbol{\mathcal{D}}), \boldsymbol{R}, \boldsymbol{P}, \boldsymbol{j}) \tag{80}$$

where

- $\boldsymbol{\mathcal{M}} = (\boldsymbol{\Sigma}, \vec{\boldsymbol{n}}(\boldsymbol{M}), \vec{\boldsymbol{a}}(\boldsymbol{M}), \vec{\boldsymbol{g}}(\boldsymbol{M}))$ is the random variable giving collectively the secret announcements of Alice's source ($\boldsymbol{\Sigma} = (\boldsymbol{V}, \boldsymbol{S}, \boldsymbol{M})$),
- $\boldsymbol{P} = (\vec{\boldsymbol{a}}, \vec{\boldsymbol{g}}(\overline{\boldsymbol{E}}), \boldsymbol{F}, \boldsymbol{K}, \vec{\boldsymbol{s}})$ is the random variable giving collectively Alice's public announcements, and
- $\boldsymbol{j}$ is the random variable giving collectively the rest of classical data Eve-Bob obtain by performing measurements on the quantum signals. The structure of $\boldsymbol{j}$ depends, of course, on Eve-Bob's attack.

Note that from the beginning Eve-Bob learn $\tilde{\vec{b}}$ from the random number generating box. Since the privacy results in the modified situation will not depend on $\tilde{\vec{b}}$, we will consider $\tilde{\vec{b}}$ as a parameter of the protocol, known by everybody. This is why the corresponding random variable is omitted from $\boldsymbol{v}$.

We now present the formalism to describe the whole situation just after Eve-Bob learn $\mathcal{M}$ from the source, that is before they determine $\mathcal{D}$. Just after Eve-Bob get an outcome $\boldsymbol{\mathcal{M}} = \mathcal{M}$, the situation is modeled as follows.

The system as seen by Eve-Bob is described in a Hilbert space $\mathcal{H}_{sys} = \mathcal{H}_C \otimes \mathcal{H}_S$ where $\mathcal{H}_C$ is the Hilbert space describing the classical data $\vec{a}$, $\vec{g}$, R, F, K processed by Alice or the randomising box and $\mathcal{H}_S$ is the Hilbert space describing single photon signals in S.

We will denote by $\boldsymbol{c} = (\vec{\boldsymbol{a}}, \vec{\boldsymbol{g}}, \boldsymbol{R}, \boldsymbol{F}, \boldsymbol{K})$ the random variable giving collectively $\vec{a}$, $\vec{g}$, R, F, K. Each possible value $c = (\vec{a}, \vec{g}, R, F, K)$ for $\boldsymbol{c}$ is represented by a state (i.e. a normalised vector) $\big|\, c \big\rangle \in \mathcal{H}_C$ such that the set $\{\big|\, c\big\rangle\}_c$ forms an orthonormal basis of $\mathcal{H}_C$. The Hilbert space $\mathcal{H}_S$ is $\mathcal{H}_S = \otimes_{i \in S} \mathcal{H}_{\text{photon}}$. The single photon polarisation Hilbert space $\mathcal{H}_{\text{photon}}$ has been defined previously.

For any quantum system described in a Hilbert space $\mathcal{H}$, the state of the system is fully defined by a Hermitian non negative matrix ρ of unit trace called the *density operator*. When the system has probability p_i to be in the state $\big|\, \Psi_i \big\rangle$ for $i = 1, 2, \ldots, k$ (we say the system is in a *statistical mixture* of states), then the corresponding density operator is $\rho = \sum_{i=1}^{k} p_i \big|\, \Psi_i \big\rangle\big\langle \Psi_i \,\big|$. The result of a general measurement on a system described in $\mathcal{H}$ can be seen as an outcome of a random variable $\boldsymbol{q}$ where q is the measured physical quantity. A general measurement $\boldsymbol{q}$ on a system described in a Hilbert space $\mathcal{H}$ is described by a *positive operator valued measure* (POVM henceforth) $\{(q, F_q)\}_{q \in \mathcal{Q}}$ where $\mathcal{Q}$ is the set of all possible outcomes for $\boldsymbol{q}$. It is a set of Hermitian non negative operators F_q on $\mathcal{H}$ such that $\sum_{q \in \mathcal{Q}} F_q = \mathbf{1}_{\mathcal{H}}$. Then the probability that the measurement yields a particular value q is given by

$$\mathrm{P}_{\boldsymbol{q}}(q) = \mathrm{Tr}(F_q \rho) \tag{81}$$

where ρ is the density operator of the system. For any $q \in \mathcal{Q}$, the Hermitian nonnegative operator F_q is called the *positive operator* associated with the outcome q. A more detailed description of the general measurement formalism can be found in [24].

This formalism can be applied to our system $\mathcal{H}_{sys} = \mathcal{H}_C \otimes \mathcal{H}_S$. However, we need to describe c as classically encoded variable. This is done by adding the following restrictions to the above formalism:

- any state in $\mathcal{H}_C \otimes \mathcal{H}_S$ should be described as a mixture of states in the canonical or the *computational* basis of $\mathcal{H}_C$, i.e. its density matrix must be of the form:

$$\rho_{sys} = \sum_c \mathrm{P}_{\boldsymbol{c}}(c) \big|\, c \big\rangle\big\langle c \,\big| \otimes \big|\, \Phi_c \big\rangle\big\langle \Phi_c \,\big| \tag{82}$$

  where computational basis means that no other basis than the canonical one $\{\big|\, \vec{a}, \vec{g}, R, F, K \big\rangle\}_c$ should be used (i.e. we shall not use basis containing cat-state vectors such as $\frac{|\, c_1 \rangle + |\, c_2 \rangle}{\sqrt{2}}$). The probability $\mathrm{P}_{\boldsymbol{c}}(c)$ is the probability of occurrence of c;
- any positive operator describing a general measurement on $\mathcal{H}_C \otimes \mathcal{H}_S$ should be of the form:

$$\Pi^C \otimes E^Q \tag{83}$$

  where Π^C (acting on $\mathcal{H}_C$) is some projection operator on the computational basis of $\mathcal{H}_C$ (i.e. on the subspace spanned by some set of vectors of the canonical basis). In other words,

$$\Pi^C = \sum_{c \in A} \big|\, c \big\rangle\big\langle c \,\big| \tag{84}$$

for some set A of values c may take. The set A corresponds to the set of values c that are compatible with the outcome associated with the positive operator.

The operator E^Q (acting on $\mathcal{H}_S$) is some positive operator in $\mathcal{H}_S$. This model allows global measurement in which two-way classical communication between Alice and Eve-Bob occurs. This is necessary since variables such as $\boldsymbol{E}$, and $\boldsymbol{\mathcal{P}}(\boldsymbol{T}, d)$ depend on Bob's announcements.

In our model, Eve-Bob execute two measurements on the system. The first one, allowing to find $\mathcal{D}$, $\vec{h}(\mathcal{D})$ given $\mathcal{M}$ but before public announcement occurs, the second one, allowing Eve-Bob to refine their information once P is known.

However, technically, it is more convenient to think that Eve-Bob execute one single POVM measurement on the whole product space $\mathcal{H}_C \otimes \mathcal{H}_S$. This POVM should obey certain constraints reflecting the fact that $\mathcal{D}$ and $\vec{h}(\mathcal{D})$ should be measured before the public announcements by Alice and the box.

Let's now describe more precisely the density matrix of the system and the POVM associated with various possible measurements during the protocol.

Once Eve-Bob have learned the value taken by $\boldsymbol{\mathcal{M}}$, the density matrix of the system as seen by Eve-Bob reads, prior to any further measurement,

$$\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{c\in C_{\mathcal{M}}} \mathrm{P}_{\boldsymbol{c}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(c)\,\big|\,c\big\rangle\big\langle c\,\big| \otimes \big|\,\Psi(\vec{g}(S),\vec{a}(S))\big\rangle\big\langle\Psi(\vec{g}(S),\vec{a}(S))\,\big| \tag{85}$$

where

$$C_{\mathcal{M}} \overset{Def}{=} \{c' = (\vec{a}', \vec{g}', R', F', K') : \vec{a}'(M) = \vec{a}(M),\ \vec{g}'(M) = \vec{g}(M)\}, \tag{86}$$

$$\big|\,\Psi(\vec{g}(S),\vec{a}(S))\big\rangle \overset{Def}{=} \otimes_{i\in S}\big|\,\Psi(g_i, a_i)\big\rangle \tag{87}$$

(in the definition of $C_{\mathcal{M}}$, $\vec{a}(M)$ and $\vec{g}(M)$ are given by $\mathcal{M}$). The subscript "$|\boldsymbol{\mathcal{M}} = \mathcal{M}$" stands for "given $\boldsymbol{\mathcal{M}} = \mathcal{M}$". The probability distribution of $\mathrm{P}_{\boldsymbol{c}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}$ is normalised for each possible value for the size of E, that is, for each possible value for the number of columns in the matrices F and K (recall that the size of the parity check matrix and the privacy amplification matrix is given by the set E). This is to ensure that the sum of probabilities of all outcomes $c = (\vec{a}, \vec{g}, R, F, K)$ that are compatible with $|\boldsymbol{E}| = n$ is equal to unity, for any possible value n. In other words, $\sum_{F \text{ and } K \text{ have } n \text{ columns}} \mathrm{P}_{\boldsymbol{c}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(c) = 1$.

Eve-Bob learn the outcome of $\boldsymbol{\mathcal{M}}$ which is part of the view $\boldsymbol{v}$. The remaining part of the view is provided by a single generalised measurement defined by the POVM

$$\big\{\big(v,\ E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\big)\big\}_{v\in\mathcal{Z}_{\mathcal{M}}} \tag{88}$$

where $\mathcal{Z}_{\mathcal{M}}$ is the set of views giving $\mathcal{M}$ for the announcement regarding the multiple photon signals. We have seen that for any $v \in \mathcal{Z}_{\mathcal{M}}$, $E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ reads

$$E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \Pi^C_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} \otimes E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} \tag{89}$$

where $\Pi^C_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ is the projection onto the span of states $\big|\,c\big\rangle \in \mathcal{H}_C$ for all c compatible with the view v.

Now $\vec{a}$, R, F and K are given explicitly by v (of course, the number of columns in F and K is $|E|$ where E is given by v). The view v tells as well that $\vec{\boldsymbol{g}}(M) = \vec{g}(M)$ (secret announcement of Alice's source), $\vec{\boldsymbol{g}}(\overline{E}) = \vec{g}(\overline{E})$ (announcement of $\vec{\boldsymbol{g}}(\overline{E})$) and $\boldsymbol{F}\vec{\boldsymbol{g}}(\boldsymbol{E}) = F\vec{\boldsymbol{g}}(E) = \vec{s}$ (announcement of $\vec{s}$, and note that F and E are given by v). Therefore, the set of all values for $\boldsymbol{c}$ compatible with v is

$$\Big\{(\vec{a}, \vec{y}, R, F, K) : \vec{y} \in C_{\vec{s},\vec{g}(\overline{E}\cup M)}\Big\} \quad \text{where}$$
$$C_{\vec{s},\vec{g}(\overline{E}\cup M)} = \big\{\vec{x} \in \{0,1\}^N : \vec{x}(\overline{E}\cup M) = \vec{g}(\overline{E}\cup M) \text{ and } F\vec{x}(E) = \vec{s} \pmod 2\big\} \tag{90}$$

that is,

$$\Pi^C_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{\vec{x}\in C_{\vec{s},\vec{g}(\overline{E}\cup M)}} \big|\,\vec{a}, \vec{x}, R, F, K\big\rangle\big\langle\vec{a}, \vec{x}, R, F, K\,\big|. \tag{91}$$

Suppose now that at the end of the protocol, and after Eve-Bob get the view v, Alice announces the key $\vec{\kappa}$. Then the POVM associated to this situation reads

$$E_{(v,\vec{\kappa})|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \Pi^C_{(v,\vec{\kappa})|\boldsymbol{\mathcal{M}}=\mathcal{M}} \otimes E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} \tag{92}$$

where $E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ remains the same, since the additional data come from Alice's announcement only, after the attack. The set of all values for $\boldsymbol{c}$ compatible with $(v, \vec{\kappa})$ in this situation is

$$\Big\{(\vec{a}, \vec{y}, R, F, K) : \vec{y} \in C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Big\} \quad \text{where}$$
$$C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = \Big\{\vec{x} \in \{0,1\}^N : \vec{x}(\overline{E}\cup M) = \vec{g}(\overline{E}\cup M) \text{ and } F\vec{x}(E) = \vec{s} \pmod 2 \quad \text{and } K\vec{x}(E) = \vec{\kappa} \pmod 2\Big\}. \tag{93}$$

Therefore,

$$\Pi^C_{(v,\vec{\kappa})|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{\vec{x}\in C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}} \big|\,\vec{a}, \vec{x}, R, F, K\big\rangle\big\langle\vec{a}, \vec{x}, R, F, K\,\big|. \tag{94}$$

Of course, Alice will not announce publicly $\vec{\kappa}$ during the protocol. The above POVM has just been derived so that we can compute $\mathrm{P}_{\boldsymbol{v}\vec{\boldsymbol{\kappa}}}(v, \vec{\kappa})$, the probability that Eve-Bob get the view v and that the key takes the value $\vec{\kappa}$.

Finally, we can assume that for any v, the positive operators $E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ are of the rank one, i.e.

$$E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \big|\,\phi_v\big\rangle\big\langle\phi_v\,\big| \tag{95}$$

where $\big|\,\phi_v\big\rangle$ are some vectors in $\mathcal{H}_S$. The vectors $\big|\,\phi_v\big\rangle$ are in general neither normalised nor orthogonal. The reasons for this assumption follows: suppose a positive operator $E^Q_{v_0|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ has a rank greater than one, namely:

$$E_{v_0|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{i\in I}\big|\,\eta_i\big\rangle\big\langle\eta_i\,\big| \tag{96}$$

where the vectors $\left|\,\eta_i\right\rangle \in \mathcal{H}_S$ are possibly not normalised (such decomposition is always possible since $E_{v_0|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ is Hermitian positive). I is a set of size greater than 1. Then the modified POVM

$$\{(v, E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}})\}_{v\neq v_0} \cup \{((v_0, i), \Pi^C_{v_0|\boldsymbol{\mathcal{M}}=\mathcal{M}} \otimes \left|\,\eta_i\right\rangle\left\langle\eta_i\,\right|)\}_{i\in I} \tag{97}$$

gives more precise information than the original POVM. This justifies our assumption.

Finally, we examine the constraint on the POVM $\{\left(v, E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\right)\}_{v\in\mathcal{Z}_{\mathcal{M}}}$ related to the fact that given $\mathcal{M}$, Eve-Bob must determine $\mathcal{D}$ and $\vec{h}(\mathcal{D}\cap\overline{M})$ ($\vec{g}(M)$ is already known and Eve-Bob do not commit error on M) prior to Alice's public announcements. We have seen that Eve-Bob may choose the set $\mathcal{D}$ at their convenience. Since signals in M give perfect information about Alice's bits and signals in V give no information at all, we assume that Eve-Bob follow the optimal strategy by choosing $\mathcal{D}$ such that:

$$M \subset \mathcal{D} \quad \text{and} \quad \mathcal{D}\cap V = \emptyset. \tag{98}$$

Now, since $\mathcal{M}$, $\mathcal{D}$ and $\vec{h}(\mathcal{D}\cap\overline{M})$ are parts of the view v, we can define the POVM

$$\left\{\left((\mathcal{M}, \mathcal{D}, \vec{h}(\mathcal{D}\cap\overline{M})), E_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}}\right)\right\}_{\mathcal{D}\,:\,M\subset\mathcal{D},\mathcal{D}\cap V=\emptyset}$$
$$\text{with } E_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{v\ \text{gives}\ \mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})} E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} \tag{99}$$

which is the positive operator associated with the outcome $(\boldsymbol{\mathcal{D}}, \vec{\boldsymbol{h}}(\boldsymbol{\mathcal{D}}\cap\overline{\boldsymbol{M}})) = (\mathcal{D}, \vec{h}(\mathcal{D}\cap\overline{M}))$ given that $\boldsymbol{\mathcal{M}} = \mathcal{M}$. When Eve-Bob make a measurement to determine $\mathcal{D}$ and $\vec{h}(\mathcal{D}\cap\overline{M})$, the only data they have about $\boldsymbol{c}$ are $\vec{a}(M)$ and $\vec{g}(M)$. Therefore,

$$E_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \Pi^C_{\mathcal{M}} \otimes E^Q_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}} \tag{100}$$

where $E^Q_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ is some positive operator acting on $\mathcal{H}_S$ and

$$\Pi^C_{\mathcal{M}} = \sum_{c\in C_{\mathcal{M}}} \left|\,c\right\rangle\left\langle c\,\right|. \tag{101}$$

To recapitulate, for any positive real number $e > 0$, the test $\boldsymbol{\mathcal{P}}(\boldsymbol{A}, e)$ on a subset $\boldsymbol{A}$ of $\mathcal{D}$ is modeled as follows:

- Eve-Bob get an outcome $\boldsymbol{\mathcal{M}} = \mathcal{M}$ for the multiple photon signals, thanks to Alice's source;
- given $\boldsymbol{\mathcal{M}} = \mathcal{M}$ Eve-Bob determine the value taken by $\boldsymbol{\mathcal{D}}$ and $\vec{\boldsymbol{h}}(\boldsymbol{\mathcal{D}}\cap\overline{M})$ thanks to the POVM

$$\left\{\left((\mathcal{M}, \mathcal{D}, \vec{h}(\mathcal{D}\cap\overline{M})), E_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \Pi^C_{\mathcal{M}} \otimes E^Q_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}}\right)\right\}_{\mathcal{D}\,:\,M\subset\mathcal{D},\mathcal{D}\cap V=\emptyset}; \tag{102}$$

- Eve-Bob do not commit any error on $A\cap M$.

5.6 Bound on the conditional entropy of the key in the modified situation

In this section, we derive the bound on the conditional entropy of the key in the modified situation. Throughout this section, we consider a given eavesdropping strategy chosen by Eve-Bob that fits the model we gave previously.

The structure of the proof follows. We define the subset $\mathcal{P}$ of views in which Eve-Bob succeed to pass the validation test (recall that in our protocol, the outcome of the validation test is publicly announced). We define two subsets $\mathcal{L}$ and $\mathcal{R}$ of $\mathcal{P}$. The subset $\mathcal{L}$ is the set of views for which the associated positive operators obey a certain constraint. This constraint is related to the fact that it is very unlikely that Eve-Bob pass the validation test while they have a substantial knowledge about Alice's sifted key: indeed, if a quantum signal is in the revealed set R, Eve-Bob want to learn the outcome of the measurement in the basis indicated by the randomising box. If it is not in R, then Eve-Bob want to learn the measurement's outcome in the conjugate basis (since $\tilde{b}_i = \neg b_i$ if $i \notin R$). The trouble for Eve-Bob is that they do not know R before they have to announce their bits $\vec{h}(\mathcal{D})$ and this can be translated in the form of the above constraint. The second subset $\mathcal{R}$ corresponds to the set of views in which probabilistic properties we have seen previously actually hold. We prove useful identities on $\mathcal{R}$ that are necessary in the subsequent part of the proof. We then prove that: (1) when the view is in the intersection of $\mathcal{R}$ and $\mathcal{L}$, Alice's private key is almost uniformly distributed and independent of Eve-Bob's view, and (2) this intersection covers almost completely the set $\mathcal{P}$ of views passing the test. Then conclusive calculations lead to the privacy of the protocol.

The following lemma will be useful in this section.

Lemma 2. *Let the density matrix of the system be of the form:*

$$\rho_{sys} = \sum_c \mathrm{P}_{\boldsymbol{c}}(c)\left|\,c\right\rangle\left\langle c\,\right| \otimes \left|\,\Phi_c\right\rangle\left\langle\Phi_c\,\right| \tag{103}$$

where $\{\left|\,\Phi_c\right\rangle\}_c$ is an orthonormal set of vectors in $\mathcal{H}_S$, and let a positive operator acting on $\mathcal{H}_{sys}$ be of the form:

$$F = \left(\sum_{c\in A}\left|\,c\right\rangle\left\langle c\,\right|\right) \otimes F^Q \tag{104}$$

where A is some set of values for c. Then for any operators V and W acting on $\mathcal{H}_S$,

$$\mathrm{Tr}\left(FV\rho_{sys}W\right) = \mathrm{P}_{\boldsymbol{c}}(A)\mathrm{Tr}\left(F^Q V \rho_{sys,A} W\right) \tag{105}$$

provided $\mathrm{P}_{\boldsymbol{c}}(A) > 0$, *where*

$$\mathrm{P}_{\boldsymbol{c}}(A) = \sum_{c'\in A} \mathrm{P}_{\boldsymbol{c}}(c') \ \textit{and} \tag{106}$$

$$\rho_{sys,A} = \frac{1}{\mathrm{P}_{\boldsymbol{c}}(A)} \sum_{c\in A} \mathrm{P}_{\boldsymbol{c}}(c)\left|\,\Phi_c\right\rangle\left\langle\Phi_c\,\right|. \tag{107}$$

Proof. We have:

$$\mathrm{Tr}(FV\rho_{sys}W) = \sum_{c\in A}\sum_{c'} \mathrm{P}_{\boldsymbol{c}}(c')\underbrace{|\langle c|c'\rangle|^2}_{\delta_{c,c'}} \times \mathrm{Tr}(F^Q V \left|\Phi_{c'}\right\rangle\left\langle\Phi_{c'}\right| W) \quad (108)$$

$$\text{where } \delta_{X,X'} = \begin{cases} 0 & \text{if } X \neq X' \\ 1 & \text{if } X = X' \end{cases}$$

$$= \sum_{c\in A} \mathrm{P}_{\boldsymbol{c}}(c)\mathrm{Tr}(F^Q V \left|\Phi_c\right\rangle\left\langle\Phi_c\right| W) \quad (109)$$

$$= \mathrm{Tr}\big(F^Q V \sum_{c\in A} \mathrm{P}_{\boldsymbol{c}}(c) \left|\Phi_c\right\rangle\left\langle\Phi_c\right| W\big). \quad (110)$$

Now if $\mathrm{P}_{\boldsymbol{c}}(A) = \sum_{c'\in A} \mathrm{P}_{\boldsymbol{c}}(c') > 0$, then

$$\mathrm{Tr}(FV\rho_{sys}W) = \mathrm{P}_{\boldsymbol{c}}(A)\mathrm{Tr}\big(F^Q V \underbrace{\frac{1}{\mathrm{P}_{\boldsymbol{c}}(A)} \sum_{c\in A} \mathrm{P}_{\boldsymbol{c}}(c) \left|\Phi_c\right\rangle\left\langle\Phi_c\right|}_{=\rho_{sys,A}} W\big). \quad (111)$$

The factor $\mathrm{P}_{\boldsymbol{c}}(A)$ has been only introduced so that $\rho_{sys,A}$ is normalised:

$$\mathrm{Tr}(\rho_{sys,A}) = \frac{1}{\mathrm{P}_{\boldsymbol{c}}(A)} \sum_{c\in A} \mathrm{P}_{\boldsymbol{c}}(c) \underbrace{\mathrm{Tr}(\left|\Phi_c\right\rangle\left\langle\Phi_c\right|)}_{=1\,\forall c} = 1. \quad (112)$$

This concludes the proof. □

5.6.1 Small sphere property

In this section we define $\mathcal{L}$, the set of views passing the test and for which the associated positive operators obey a certain constraint. We then prove that $\mathcal{L}$ covers almost completely $\mathcal{P}$.

Definition 2. *The set $\mathcal{P}$ is defined as the set of all views of Eve in which the validation test is passed.*

$$\mathcal{P} := \{v \in \mathcal{Z} \; : \; \textbf{valid} = \mathit{true}\}\,. \quad (113)$$

Definition 3. *For any view*

$$v = (\mathcal{M}, \mathcal{D}, \vec{h}(\mathcal{D}), R, P, j) \in \mathcal{Z} \quad (114)$$

where $\mathcal{M} = (\Sigma, \vec{n}(M), \vec{a}(M), \vec{g}(M))$ *and* $P = (\vec{a}, \vec{g}(\overline{E}), F, K, \vec{s})$, *define the* partial view z *as*

$$z = (\mathcal{M}, \mathcal{D}, \vec{h}(\mathcal{D}\cap\overline{M}), \vec{a}, R) \text{ part of } v. \quad (115)$$

The partial view describes the data Eve-Bob have after receiving $\mathcal{M}$ and after measurement of $\mathcal{D}$ and $\vec{h}(\mathcal{D}\cap\overline{M})$, followed by announcements of $(\vec{a}, R)$ by Alice and the randomising box. Recall that Eve-Bob do not make any mistake on M thanks to Alice's source, and that they need only to get $\vec{h}(\mathcal{D}\cap\overline{M})$ using the POVM (102). Given any partial view $z = (\mathcal{M}, \mathcal{D}, \vec{h}(\mathcal{D}\cap\overline{M}), \vec{a}, R)$, define $\Pi_0(z)$ as the orthogonal projection operator onto $\mathrm{Span}(\{\left|\Psi(\vec{j}, \tilde{\vec{b}})\right\rangle | d_{E\cap\overline{M}}(\vec{j}, \vec{h}) \geq d_2\})$ where $d_2 = (\delta + \tau_f)(1-p_R)n/2$ and where E, M and $\vec{h}(\mathcal{D}\cap\overline{M})$ are given by the partial view z. We have restricted to $E\cap\overline{M}$ and $T\cap\overline{M}$ because Eve-Bob do not commit any error on M. We prove now the following property (referred to as the small sphere property in [3]).

Property 6. *Let the subset of views $\mathcal{L}\subset\mathcal{P}$ be defined by:*

$$\mathcal{L} \overset{Def}{=} \Big\{v\in\mathcal{P} \; : \; \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\big] \leq \sqrt{g(\delta, \tau_f, p_R, n)}\mathrm{P}_{\boldsymbol{v}}(v)\Big\}, \quad (116)$$

where

$$g(\delta, \tau_f, p_R, n) = \exp\left[-\frac{1}{2\delta+\tau_f}\tau_f^2\frac{p_R^2}{4}r_{min}N + 2\left(\frac{\tau_f}{2\delta+\tau_f}\right)^2\right]. \quad (117)$$

Then the probability weight of $\mathcal{L}$ is lower bounded by:

$$\mathrm{P}_{\boldsymbol{v}}(\mathcal{L}) \geq \mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) - \sqrt{g(\delta, \tau_f, p_R, n)}. \quad (118)$$

Proof. Define $\mathcal{Z}_{r_{min}} \subset \mathcal{Z}$ as the subset of views for which the size of $\mathcal{D}$ satisfies the first condition of the validation test, i.e. $n > r_{min}N$ or $\mathcal{Z}_{r_{min}} = \{v \in \mathcal{Z} : |\mathcal{D}| > r_{min}N$ where $\mathcal{D}$ is given by $v.\}$. Likewise, define $\mathcal{W}_{r_{min}}$ as the subset of partial views z for which the size of $\mathcal{D}$ satisfies the condition $n > r_{min}N$, that is $\mathcal{W}_{r_{min}} = \{z : |\mathcal{D}| > r_{min}N\}$. We can assume that $\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}})$ and $\mathrm{P}_{\boldsymbol{z}}(\mathcal{W}_{r_{min}})$ are strictly positive. Otherwise, since $\mathcal{P}$ is in $\mathcal{Z}_{r_{min}}$, this would imply $\mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) = 0$ which implies trivial security of the protocol. Define the positive operator $\Pi_1(z)$ as the orthogonal projection operator onto $\mathrm{Span}(\{\left|\Psi(\vec{j}, \tilde{\vec{b}})\right\rangle | d_{T\cap\overline{M}}(\vec{j}, \vec{h}) \geq d_1\})$ where $d_1 = \delta\frac{p_R}{2}n$, and where T, M and $\vec{h}(\mathcal{D}\cap\overline{M})$ are given by z as before. We also define $\overline{\Pi}_1(z)$ as $\overline{\Pi}_1(z) = \mathbf{1} - \Pi_1(z)$.

We first prove that the set of views $\mathcal{Q}$ defined by:

$$\mathcal{Q} \overset{Def}{=} \Big\{v\in\mathcal{Z}_{r_{min}} \; : \; \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big] \leq \sqrt{g(\delta, \tau_f, p_R, n)}\mathrm{P}_{\boldsymbol{v}}(v)\Big\}. \quad (119)$$

has probability bounded from below by:

$$\mathrm{P}_{\boldsymbol{v}}(\mathcal{Q}) \geq \left(1 - \sqrt{g(\delta, \tau_f, p_R, n)}\right)\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}}). \quad (120)$$

Let's assume that we are given that $\boldsymbol{\mathcal{D}} = \mathcal{D}$ for some set $\mathcal{D}$. The starting point is the following: as mentioned already, Eve-Bob do not know Alice's bases $\vec{a}$ nor the choice of R during the quantum transmission. This means that in a fictional situation $\mathcal{F}$ in which the single photons sent by Alice are in the state $\left|\Psi(\vec{g}(S),\tilde{\vec{b}}(S))\right\rangle$ instead of $|\Psi(\vec{g}(S),\vec{a}(S))\rangle$ (the classically stored $\vec{a}$ remains however unchanged), Property 1 holds for the subsets T and E of $\mathcal{D}$. Let $\boldsymbol{C}$ be the random variable giving the set of discrepancies between Alice's bits $\vec{g}(\mathcal{D})$ and Bob's bits $\vec{h}(\mathcal{D})$ on $\mathcal{D}$. Then in such a situation, the error set $\boldsymbol{C}$ is independent of $\boldsymbol{\Omega}$ and $\boldsymbol{R}$. This implies that $\boldsymbol{T}$ and $\boldsymbol{E}$ are independent of $\boldsymbol{C}$. Using Property 1 for $\mathcal{S}=\mathcal{D}$, $\boldsymbol{A}=\boldsymbol{T}$, $\boldsymbol{B}=\boldsymbol{E}$ and $\boldsymbol{C}$ with $p_A=p_T=p_R/2$, $p_B=p_E=(1-p_R)/2$ (the factor 1/2 is the probability that $a_i=\tilde{b}_i$ (for T) and $a_i\neq\tilde{b}_i$ (for E) respectively), we have

$$\Pr\left(\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F},\,\boldsymbol{\mathcal{D}}=\mathcal{D}\right)\leq f\left(\delta,\tau_f,\frac{p_R}{2},\frac{1-p_R}{2},n\right). \quad (121)$$

Multiplying the above relation by $\mathrm{P}_{\boldsymbol{\mathcal{D}}}(\mathcal{D})$ and summing for all $\mathcal{D}$ that satisfy $|\mathcal{D}|>r_{min}N$, one gets:

$$\Pr\left((\boldsymbol{n}>r_{min}N)\wedge\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\right)\leq g(\delta,\tau_f,p_R,n)\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}}) \quad (122)$$

remarking that $f(\delta,\tau_f,p_R/2,(1-p_R)/2,r_{min}N) = g(\delta,\tau_f,p_R,n)$ and that $\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}}) = \sum_{\mathcal{D}\,:\,|\mathcal{D}|>r_{min}N}\mathrm{P}_{\boldsymbol{\mathcal{D}}}(\mathcal{D})$.

But the lhs above reads:

$$\Pr\left((\boldsymbol{n}>r_{min}N)\wedge\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\right)= \sum_{c}\sum_{z'\in\mathcal{W}_{r_{min}}}\mathrm{P}_{\boldsymbol{c}}(c)\mathrm{P}_{\boldsymbol{\mathcal{M}}\,|\,\boldsymbol{c}=c}(\mathcal{M}')\mathrm{P}_{\boldsymbol{z}\,|\,\mathcal{F},\boldsymbol{c}=c,\boldsymbol{\mathcal{M}}=\mathcal{M}'}(z') \times\Pr(\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F},\boldsymbol{c}=c,\boldsymbol{z}=z') \quad (123)$$

where $\mathcal{M}'$ is given uniquely by the partial view $z'=(\mathcal{M}',\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'}))$. Note that $\boldsymbol{c}$ and $\boldsymbol{\mathcal{M}}$ are independent of the event $\mathcal{F}$.

It is easy to see from (102) that, given $\boldsymbol{\mathcal{M}}=\mathcal{M}$, the POVM associated with the partial view $z\in\mathcal{W}_{\mathcal{M}}$ (where $\mathcal{W}_{\mathcal{M}}$ is the set of partial views that are compatible with $\boldsymbol{\mathcal{M}}=\mathcal{M}$) is:

$$\left\{z=(\mathcal{M},\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M}),\vec{a},R),E_{z|\boldsymbol{\mathcal{M}}=\mathcal{M}}= \mathit{\Pi}^{C}_{\mathcal{M},\vec{a},R}\otimes E^{Q}_{\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M})|\boldsymbol{\mathcal{M}}=\mathcal{M}}\right\}_{z\in\mathcal{W}_{\mathcal{M}}} \quad (124)$$

where

$$\mathit{\Pi}^{C}_{\mathcal{M},\vec{a},R}= \sum_{F',K',\vec{g}'\,:\,\vec{g}'(M)=\vec{g}(M)}\left|\vec{a},\vec{g}',R,F',K'\right\rangle\!\left\langle\vec{a},\vec{g}',R,F',K'\right| \quad (125)$$

is the projection onto states giving $\vec{a}$, $\vec{g}(M)$ and R for Alice's choice of bases, Alice's bits on M and the randomising box's choice for the revealed set, respectively.

Using this POVM, we have:

$$\begin{aligned}\mathrm{P}_{\boldsymbol{z}\,|\,\mathcal{F},\boldsymbol{c}=c,\boldsymbol{\mathcal{M}}=\mathcal{M}'}(z')&=\mathrm{Tr}\big[E_{z'|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\big|c\big\rangle\big\langle c\big|\\&\quad\otimes\Psi(\vec{g}(S'),\tilde{\vec{b}}(S')))\rangle\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S')|\big] && (126)\\&=\mathrm{Tr}\big[\mathit{\Pi}^{C}_{\mathcal{M}',\vec{a}',R'}\otimes E^{Q}_{\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'})|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\big|c\big\rangle\big\langle c\big|\\&\quad\otimes\big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\,\big|\big] && (127)\\&=\delta_{\vec{a},\vec{a}'}\delta_{R,R'}\delta_{\vec{g}(M'),\vec{g}'(M')}\\&\quad\times\mathrm{Tr}\big[E^{Q}_{\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'})|\boldsymbol{\mathcal{M}}=\mathcal{M}'}|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))|\rangle\\&\quad\times\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))|\big] && (128)\end{aligned}$$

where S', M' and $\vec{g}'(M')$ are given by $\mathcal{M}'$, $\vec{a}'$, R', $\mathcal{D}'$ and $\vec{h}'(\mathcal{D}'\cap\overline{M'})$ are given by z' and $\vec{a}$, R and $\vec{g}$ are given by c. We recall that $\mathcal{M}'$ is part of z'.

Since Eve-Bob do not commit any error on $\boldsymbol{M}$,

$$\begin{aligned}&\Pr(\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F},\boldsymbol{c}=c,\boldsymbol{z}=z')\\&=\Pr(\boldsymbol{\mathcal{P}}(\boldsymbol{T}\cap\overline{\boldsymbol{M}},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E}\cap\overline{\boldsymbol{M}},d_2)|\mathcal{F},\boldsymbol{c}{=}c,\boldsymbol{z}{=}z') && (129)\\&=\Pr(d_{T'\cap\overline{M'}}(\vec{g},\vec{h}')<d_1\text{ and }d_{E'\cap\overline{M'}}(\vec{g},\vec{h}')\geq d_2) && (130)\\&=\mathrm{Tr}\Big(\overline{\mathit{\Pi}}_1(z')\mathit{\Pi}_0(z')\big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\,\big|\\&\quad\times\mathit{\Pi}_0(z')\overline{\mathit{\Pi}}_1(z')\Big) && (131)\end{aligned}$$

where the sets T', E' and M' are uniquely given by the partial view z'.

Note that

$$\overline{\mathit{\Pi}}_1(z')\mathit{\Pi}_0(z')\big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle \times\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\,\big|\mathit{\Pi}_0(z')\overline{\mathit{\Pi}}_1(z')= \begin{cases}\big|\Psi(\tilde{\vec{b}}(S'),\vec{g}(S'))\big\rangle\big\langle\Psi(\tilde{\vec{b}}(S'),\vec{g}(S'))\,\big|\\ \qquad\text{if }d_{T'\cap\overline{M'}}(\vec{g},\vec{h}')<d_1\text{ and }d_{E'\cap\overline{M'}}(\vec{g},\vec{h}')\geq d_2\\[2ex] 0\qquad\qquad\qquad\text{otherwise.}\end{cases} \quad (132)$$

Therefore, the above term can be integrated in the other trace so that:

$$\begin{aligned}&\Pr\left((\boldsymbol{n}>r_{min}N)\wedge\boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1)\wedge\neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\right)\\&=\sum_{c}\sum_{z'\in\mathcal{W}_{r_{min}}}\mathrm{P}_{\boldsymbol{c}\boldsymbol{\mathcal{M}}}(c,\mathcal{M}')\delta_{\vec{a},\vec{a}'}\delta_{R,R'}\delta_{\vec{g}(M'),\vec{g}'(M')}\\&\times\mathrm{Tr}\big[E^{Q}_{\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'})|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\overline{\mathit{\Pi}}_1(z')\mathit{\Pi}_0(z')\big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle\\&\times\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\,\big|\mathit{\Pi}_0(z')\overline{\mathit{\Pi}}_1(z')\big] && (133)\end{aligned}$$

but

$$\mathrm{P}_{\boldsymbol{c}\boldsymbol{\mathcal{M}}}(c,\mathcal{M}') = \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}')\mathrm{P}_{\boldsymbol{c}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}'}(c) \tag{134}$$

$$= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}')\mathrm{P}_{\boldsymbol{\vec{g}}(S')}(\vec{g}(S')) \times \mathrm{P}_{\boldsymbol{\vec{a}}\boldsymbol{\vec{g}}(\overline{S'})\boldsymbol{RFK}|\boldsymbol{\mathcal{M}}=\mathcal{M}'}(\vec{a},\vec{g}(\overline{S'}),R,F,K) \tag{135}$$

$$= \frac{1}{2^{|S'|}}\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}') \times \mathrm{P}_{\boldsymbol{\vec{a}}\boldsymbol{\vec{g}}(\overline{S'})\boldsymbol{RFK}|\boldsymbol{\mathcal{M}}=\mathcal{M}'}(\vec{a},\vec{g}(\overline{S'}),R,F,K) \tag{136}$$

since $\boldsymbol{\vec{g}}(S')$ is uniformly distributed and independent of $\boldsymbol{M}$, $\boldsymbol{\vec{a}}$, $\boldsymbol{\vec{g}}(\overline{S'})$, $\boldsymbol{R}$, $\boldsymbol{F}$ and $\boldsymbol{K}$. Recall that Σ is not chosen by Eve-Bob, but randomly by the source. Therefore,

$$\begin{aligned}
&\Pr\big((\boldsymbol{n} > r_{min}N) \wedge \boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\big) = \\
&\sum_{z'\in\mathcal{W}_{r_{min}}} \sum_{\vec{a},\vec{g}(\overline{S'}),R,F,K} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}') \\
&\times \mathrm{P}_{\boldsymbol{\vec{a}}\boldsymbol{\vec{g}}(\overline{S'})\boldsymbol{RFK}|\boldsymbol{\mathcal{M}}=\mathcal{M}'}(\vec{a},\vec{g}(\overline{S'}),R,F,K) \\
&\times \delta_{\vec{a},\vec{a}'}\delta_{R,R'}\delta_{\vec{g}(M'),\vec{g}'(M')} \\
&\times \mathrm{Tr}\big[E^{Q}_{\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'})|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\overline{\Pi}_1(z')\Pi_0(z') \sum_{\vec{g}(S')}\frac{1}{2^{|S'|}} \\
&\times \big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big|\Pi_0(z')\overline{\Pi}_1(z')\big].
\end{aligned} \tag{137}$$

The important point to remark is that

$$\sum_{\vec{g}(S')}\frac{1}{2^{|S'|}}\big|\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\tilde{\vec{b}}(S'))\big| = \frac{\mathbf{1}_{S'}}{2^{|S'|}}$$

$$= \sum_{\vec{g}(S')}\frac{1}{2^{|S'|}}\big|\Psi(\vec{g}(S'),\vec{a}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\vec{a}(S'))\big|. \tag{138}$$

Therefore, setting back the sum over $\vec{g}(S')$ and writing back the trace over classical spaces in the original form, we obtain:

$$\begin{aligned}
&\Pr\big((\boldsymbol{n} > r_{min}N) \wedge \boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\big) \\
&= \sum_{c}\sum_{z'\in\mathcal{W}_{r_{min}}} \mathrm{P}_{\boldsymbol{c}\boldsymbol{\mathcal{M}}}(c,\mathcal{M}')\delta_{\vec{a},\vec{a}'}\delta_{R,R'}\delta_{\vec{g}(M'),\vec{g}'(M')} \\
&\quad\times\mathrm{Tr}\big[E^{Q}_{\mathcal{D}',\vec{h}'(\mathcal{D}'\cap\overline{M'})|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\overline{\Pi}_1(z')\Pi_0(z') \\
&\quad\times\big|\Psi(\vec{g}(S'),\vec{a}(S'))\big\rangle\big\langle\Psi(\vec{g}(S'),\vec{a}(S'))\big|\Pi_0(z')\overline{\Pi}_1(z')\big]
\end{aligned} \tag{139}$$

$$\begin{aligned}
&= \sum_{z'\in\mathcal{W}_{r_{min}}}\sum_{c\in C_{\mathcal{M}'}} \underbrace{\mathrm{P}_{\boldsymbol{c}\boldsymbol{\mathcal{M}}}(c,\mathcal{M}')}_{=\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}')\mathrm{P}_{\boldsymbol{c}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}'}(c)} \quad \mathrm{Tr}\big[E_{z'|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\big|c\big\rangle \\
&\quad\times\big\langle c\big|\otimes\overline{\Pi}_1(z')\Pi_0(z')\big|\Psi(\vec{a}(S'),\vec{g}(S'))\big\rangle \\
&\quad\times\big\langle\Psi(\vec{a}(S'),\vec{g}(S'))\big|\Pi_0(z')\overline{\Pi}_1(z')\big]
\end{aligned} \tag{140}$$

$$\begin{aligned}
&= \sum_{z'\in\mathcal{W}_{r_{min}}} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}')\mathrm{Tr}\big[E_{z'|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\overline{\Pi}_1(z') \\
&\quad\times\Pi_0(z')\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}'}\Pi_0(z')\overline{\Pi}_1(z')\big], \text{ or,}
\end{aligned} \tag{141}$$

$$\begin{aligned}
&= \sum_{z\in\mathcal{W}_{r_{min}}} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{z|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z) \\
&\quad\times\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big],
\end{aligned} \tag{142}$$

where $\mathcal{M}$ is given by z.

But $E_{z|\boldsymbol{\mathcal{M}}=\mathcal{M}} = \sum_{v\,\text{gives}\,z} E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ and we get

$$\begin{aligned}
&\Pr\big((\boldsymbol{n} > r_{min}N) \wedge \boldsymbol{\mathcal{P}}(\boldsymbol{T},d_1) \wedge \neg\boldsymbol{\mathcal{P}}(\boldsymbol{E},d_2)|\mathcal{F}\big) \\
&\qquad= \sum_{v\in\mathcal{Z}_{r_{min}}} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z) \\
&\qquad\qquad\times\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big]
\end{aligned} \tag{143}$$

where $\mathcal{M}$ and z are given by v, and recalling the inequality (122), we get

$$\begin{aligned}
&\sum_{v\in\mathcal{Z}_{r_{min}}} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z) \\
&\times\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big] \le g(\delta,\tau_f,p_R,n)\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}}).
\end{aligned} \tag{144}$$

At this point we use the following lemma.

Lemma 3. *Let μ be a strictly positive real number. Let $\boldsymbol{y}$ be a random variable taking values in a set $\mathcal{Y}$. Let $\{a_y\}_{y\in\mathcal{Y}}$ be a set of $|\mathcal{Y}|$ real nonnegative numbers such that $\sum_{y\in\mathcal{Y}} a_y \le \mu$. Let q be a strictly positive number. If we define the subset $\mathcal{X} \subset \mathcal{Y}$ by*

$$\mathcal{X} = \{y \in \mathcal{Y} \,:\, a_y \le \mu q \mathrm{P}_{\boldsymbol{y}}(y)\} \tag{145}$$

Then $\mathrm{P}_{\boldsymbol{y}}(\mathcal{X}) \ge 1 - 1/q$.

Proof. Assume to the contrary that the set $S = \mathcal{Y}\setminus\mathcal{X} = \{y \in \mathcal{Y} \,:\, a_y > \mu q\mathrm{P}_{\boldsymbol{y}}(y)\}$ has probability $\mathrm{P}_{\boldsymbol{y}}(S)$ greater than $1/q$. Then

$$\sum_{y} a_y \ge \sum_{y\in S} a_y > \mu q \sum_{y\in S}\mathrm{P}_{\boldsymbol{y}}(y) = \mu q\mathrm{P}_{\boldsymbol{y}}(S) \ge \mu. \tag{146}$$

Therefore $\sum_y a_y > \mu$ which is a contradiction. This concludes the proof. □

Define the set of views $\mathcal{Q}$ as:

$$\mathcal{Q} \overset{Def}{=} \Big\{ v \in \mathcal{Z}_{r_{min}} \ : \\ \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big] \\ \le \sqrt{g(\delta,\tau_f,p_R,n)}\mathrm{P}_{\boldsymbol{v}}(v)\Big\}. \tag{147}$$

Then applying the above lemma for $\mu = g(\delta,\tau_f,p_R,n)\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}})$, $q = 1/\sqrt{g(\delta,\tau_f,p_R,n)}$ and the probability distribution on $\mathcal{Z}_{r_{min}}$ given by the conditional distribution $\mathrm{P}_{\boldsymbol{v}}(v)/\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}})$, we find that

$$\mathrm{P}_{\boldsymbol{v}}(\mathcal{Q}) \ge \left(1 - \sqrt{g(\delta,\tau_f,p_R,n)}\right)\mathrm{P}_{\boldsymbol{v}}(\mathcal{Z}_{r_{min}}). \tag{148}$$

Thus, for any view $v \in \mathcal{Q} \cap \mathcal{P}$, we have:

$$\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}\big[E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)\big] \\ \le \sqrt{g(\delta,\tau_f,p_R,n)}\mathrm{P}_{\boldsymbol{v}}(v). \tag{149}$$

However, since $v \in \mathcal{P}$ we also have:

$$\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)) \tag{150}$$

$$= \mathrm{P}_{\boldsymbol{\mathcal{M}\vec{a}RFK}}(\mathcal{M},\vec{a},R,F,K)\mathrm{P}_{\vec{\boldsymbol{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)}) \\ \times \mathrm{Tr}\big[E^{Q}_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\frac{1}{|C_{\vec{s},\vec{g}(\overline{E}\cup M)}|} \\ \times \sum_{\vec{x}\in C_{\vec{s},\vec{g}(\overline{E}\cup M)}} \big|\Psi(\vec{x},\vec{a})\big\rangle\big\langle\Psi(\vec{x},\vec{a})\big|\Pi_0(z)\overline{\Pi}_1(z)\big] \tag{151}$$

using Lemma 2, and since for any $\vec{x} \in C_{\vec{s},\vec{g}(\overline{E}\cup M)}$ (note that $a_i = \tilde{b}_i$ for $i \in T$),

$$\overline{\Pi}_1(z)\big|\Psi(\vec{x},\vec{a})\big\rangle\big\langle\Psi(\vec{x},\vec{a})\big|\overline{\Pi}_1(z) = \big|\Psi(\vec{x},\vec{a})\big\rangle\big\langle\Psi(\vec{x},\vec{a})\big| \tag{152}$$

(that is, $z = (\mathcal{M},\mathcal{D},\vec{h}(\mathcal{D}\cap\overline{M}),\vec{a},R)$ verifies $d_{T\cap\overline{M}}(\vec{h},\vec{x}) < d_1$ for any $\vec{x} \in C_{\vec{s},\vec{g}(\overline{E}\cup M)}$). Note that $\Pi_0(z)$ and $\overline{\Pi}_1(z)$ commute. Thus we have:

$$\forall v \in \mathcal{Q}\cap\mathcal{P} \\ \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\overline{\Pi}_1(z)\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\overline{\Pi}_1(z)) \\ = \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}\Pi_0(z)) \tag{153}$$

$$\le \mathrm{P}_{\boldsymbol{v}}(v)\sqrt{g(\delta,\tau_f,p_R,n)} \tag{154}$$

since $\Pi_0(z)$ acts only on $\mathcal{H}_{E\cap\overline{M}}$. This proves that $\mathcal{Q}\cap\mathcal{P} \subset \mathcal{L}$. Therefore the probability of $\mathcal{L}$ is bounded from below by:

$$\mathrm{P}_{\boldsymbol{v}}(\mathcal{L}) \ge \mathrm{P}_{\boldsymbol{v}}(\mathcal{Q}\cap\mathcal{P}) \tag{155}$$

$$\ge \mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{Q}}\cap\mathcal{Z}_{r_{min}}) \tag{156}$$

$$\ge \mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) - \sqrt{g(\delta,\tau_f,p_R,n)}, \tag{157}$$

which concludes the proof of the small sphere property.□

5.6.2 Identities on $\mathcal{R}$

Here we define another big subset of $\mathcal{P}$, corresponding to the set of views in which probabilistic assumptions such as $\widehat{l} \ge \widehat{l}_{min}$, $\widehat{d}_w \ge 2(\delta+\tau_f)(1-p_R)n/2$ holds. We require as well that for any $v \in \mathcal{R}$, $\mathrm{P}_{\boldsymbol{v}}(v) > 0$. Formally,

$$\mathcal{R} = \{v \in \mathcal{P} \ : \ v \ \text{ verifies} \\ \widehat{l} \ge \widehat{l}_{min}, \\ \widehat{d}_w \ge 2(\delta+\tau_f)\frac{1-p_R}{2}n, \\ \mathrm{P}_{\boldsymbol{v}}(v) > 0\} \tag{158}$$

remembering that $\widehat{l}$, $\widehat{l}_{min}$ and $\widehat{d}_w$ are all uniquely defined by Eve-Bob's view v.

In the last section of this proof, a bound on the probability of the set of views $\overline{\mathcal{R}}\cap\mathcal{P}$ will be needed. We have, using Properties 3 and 4,

$$\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) \le \mathrm{Pr}(\widehat{\boldsymbol{l}} \le \widehat{l}_{min} \wedge \boldsymbol{n} > r_{min}N) \\ + \mathrm{Pr}\left(\frac{\widehat{\boldsymbol{d}}_{\boldsymbol{w}}}{2} < (\delta+\tau_f)\frac{1-p_R}{2}n \wedge \widehat{\boldsymbol{l}} \ge \widehat{l}_{min} \wedge \boldsymbol{n} > r_{min}N\right) \tag{159}$$

$$\le e^{-2\tau_M^2 N} + e^{-2\hat{\tau}^2(r_{min}N-M_{max})} \\ + 2^{-\tau_p\left(\frac{1-p_R}{2}-\hat{\tau}\right)(r_{min}N-M_{max})}. \tag{160}$$

We now prove the following properties on $\mathcal{R}$, i.e. for

$$v = (\mathcal{M},\mathcal{D},\vec{h}(\mathcal{D}),R,P,j) \in \mathcal{R} \tag{161}$$

where $\mathcal{M} = (\Sigma,\vec{n}(M),\vec{a}(M),\vec{g}(M))$, $\Sigma = (V,S,M)$ and $P = (\vec{a},\vec{g}(\overline{E}),F,K,\vec{s})$. This implies for instance that $\widehat{d}_w$ verifies $\widehat{d}_w \ge 2(\delta+\tau_f)(1-p_R)n/2$ in this section. It might be useful to realise that the following properties are exactly equivalent to the properties proved in the original paper [3] in which the sifted keys $\vec{g}(E)$ and $\vec{h}(E)$ are replaced by the single-photon encoded sifted keys $\vec{g}(E\cap\overline{M})$ and $\vec{h}(E\cap\overline{M})$.

Property 7.

$$\forall v \in \mathcal{R}, \forall \vec{\kappa} \in \{0,1\}^m, \quad |C_{\vec{s},\vec{g}(\overline{E}\cup M)}| = 2^m|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}|. \tag{162}$$

Proof. We remark that:

$$C_{\vec{s},\vec{g}(\overline{E}\cup M)} = \{\vec{x} \in \{0,1\}^N \ : \\ \vec{x}(\overline{E}\cup M) = \vec{g}(\overline{E}\cup M) \text{ and} \\ \widehat{F}\vec{x}(E\cap\overline{M}) = \vec{s} + \check{F}\vec{g}(E\cap M) \pmod 2\} \tag{163}$$

(+ and − are equivalent in arithmetics modulo 2), and

$$C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = \{\vec{x} \in \{0,1\}^N \ : \\ \vec{x}(\overline{E}\cup M) = \vec{g}(\overline{E}\cup M) \text{ and} \\ \widehat{F}\vec{x}(E\cap\overline{M}) = \vec{s} + \check{F}\vec{g}(E\cap M) \pmod 2, \\ \widehat{K}\vec{x}(E\cap\overline{M}) = \vec{\kappa} + \check{K}\vec{g}(E\cap M) \pmod 2\}. \tag{164}$$

Now, for $v \in \mathcal{R}$, $\widehat{d}_w > 0$, that is, rows of $\widehat{K}$ are linearly independent and each row of $\widehat{K}$ is linearly independent of rows of $\widehat{F}$. Therefore $\widehat{K}\vec{x}(E \cap \overline{M}) = \vec{\kappa} + \check{K}\vec{g}(E \cap M)$ (mod 2) introduces m additional linearly independent constraints in $C_{\vec{s},\vec{g}(\overline{E}\cup M)}$. Thus $|C_{\vec{s},\vec{g}(\overline{E}\cup M)}| = 2^m|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}|$. □

Property 8. *For any $\vec{\kappa} \in \{0,1\}^m$ and $v \in \mathcal{R}$, the mutual probability of the outcome $(v, \vec{\kappa})$ reads:*

$$\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v,\vec{\kappa}) = \frac{1}{2^m}\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\big\langle \tilde{\phi}_v \big| \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} \big| \tilde{\phi}_v \big\rangle \tag{165}$$

where

- $\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R) = \sum_{\vec{x}\in C_{\vec{s},\vec{g}(\overline{E}\cup M)}} \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})$ $\mathrm{P}_{\boldsymbol{\vec{a}\vec{g}RFK}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(\vec{a},\vec{x},R,F,K)$ *is the probability that Alice announces $P = (\vec{a},\vec{g}(\overline{E}),F,K,\vec{s})$, the box announces R and Eve-Bob get $\mathcal{M}$ thanks to the photon number splitting attack;*
- $\big|\Psi(\vec{g}(A),\vec{a}(A))\big\rangle = \otimes_{i\in A}\big|\Psi(g_i,a_i)\big\rangle \in \mathcal{H}_A$ *for any set $A \subset S$, where $\mathcal{H}_A$ stands for the Hilbert space describing the photons in A;*
- $\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = \frac{1}{|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}|}\sum_{\vec{x}\in C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}} \big|\Psi(\vec{x}(E\cap \overline{M}),\vec{a}(E\cap\overline{M}))\big\rangle\big\langle\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\big|$;
- $\big|\tilde{\phi}_v\big\rangle = \langle\Psi(\vec{g}(\overline{E}\cup M),\vec{a}(\overline{E}\cup M))\big|\phi_v\big\rangle \in \mathcal{H}_{E\cap\overline{M}}$.

Note that in the above notation, $\mathcal{M}$, P, R, $C_{\vec{s},\vec{g}(\overline{E}\cup M)}$ and $C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}$ are all given by v.

Property 9. *For any view $v \in \mathcal{R}$ and for any operators V and W acting on the restricted space $\mathcal{H}_{E\cap\overline{M}} \subset \mathcal{H}_S$,*

$$\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}V\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}W) = \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\big\langle\tilde{\phi}_v\big|V\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}W\big|\tilde{\phi}_v\big\rangle \tag{166}$$

where

- $\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} = \frac{1}{|C_{\vec{s},\vec{g}(\overline{E}\cup M)}|}\sum_{\vec{x}\in C_{\vec{s},\vec{g}(\overline{E}\cup M)}} \big|\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\big\rangle\big\langle\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\big|$
- *and other elements defined as previously.*

Proof. Using Lemma 2 for $\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}$, $E_{(v,\vec{\kappa})|\boldsymbol{\mathcal{M}}=\mathcal{M}}$ and $E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}$, we get (recall that $\mathcal{M}$ is given by v)

$$\begin{aligned}\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v,\vec{\kappa}) &= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{P}_{\boldsymbol{v\vec{\kappa}}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(v,\vec{\kappa}) &(167)\\ &= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{(v,\vec{\kappa})|\boldsymbol{\mathcal{M}}=\mathcal{M}}\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}) &(168)\\ &= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{P}_{\boldsymbol{\vec{a}RFK}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(\vec{a},R,F,K)\\ &\quad\times\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)})\mathrm{Tr}(E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\rho_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}) &(169)\end{aligned}$$

where

$$\rho_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = \frac{1}{\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)})} \times \sum_{\vec{x}\in C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}} \mathrm{P}_{\boldsymbol{\vec{g}}}(\vec{x})\big|\Psi(\vec{x},\vec{a})\big\rangle\big\langle\Psi(\vec{x},\vec{a})\big| \tag{170}$$

and

$$\begin{aligned}&\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}V\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}}W)\\ &\quad= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{P}_{\boldsymbol{\vec{a}RFK}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(\vec{a},R,F,K)\\ &\quad\times\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)})\mathrm{Tr}(E^Q_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}V\rho_{\vec{s},\vec{g}(\overline{E}\cup M)}W) \qquad (171)\end{aligned}$$

where

$$\rho_{\vec{s},\vec{g}(\overline{E}\cup M)} = \frac{1}{\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)})} \times \sum_{\vec{x}\in C_{\vec{s},\vec{g}(\overline{E}\cup M)}} \mathrm{P}_{\boldsymbol{\vec{g}}}(\vec{x})\big|\Psi(\vec{x},\vec{a})\big\rangle\big\langle\Psi(\vec{x},\vec{a})\big|. \tag{172}$$

Now V and W act only on $\mathcal{H}_{E\cap\overline{M}}$ and for any $\vec{x} \in C_{\vec{s},\vec{g}(\overline{E}\cup M)}$ or $C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}$, $\vec{x}(\overline{E}\cup M) = \vec{g}(\overline{E}\cup M)$. Thus

$$\big\langle\Psi(\vec{x},\vec{a})\big|X\big|\phi_v\big\rangle = \big\langle\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\big|X\big|\tilde{\phi}_v\big\rangle \tag{173}$$

where X is V or W. Noting that $\mathrm{P}_{\boldsymbol{\vec{g}}}$ is uniform, for any $\vec{x}$, we have $\mathrm{P}_{\boldsymbol{\vec{g}}}(\vec{x})/\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)}) = 1/|C_{\vec{s},\vec{g}(\overline{E}\cup M)}|$ and $\mathrm{P}_{\boldsymbol{\vec{g}}}(\vec{x})/\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}) = 1/|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}|$. Finally we use the identities $\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}) = \frac{1}{2^m}\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)})$ and $\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{P}_{\boldsymbol{\vec{a}RFK}\,|\,\boldsymbol{\mathcal{M}}=\mathcal{M}}(\vec{a},R,F,K)\mathrm{P}_{\boldsymbol{\vec{g}}}(C_{\vec{s},\vec{g}(\overline{E}\cup M)}) = \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)$. This concludes the proof. □

It follows that the marginal probability of $v \in \mathcal{R}$ reads:

$$\begin{aligned}\mathrm{P}_{\boldsymbol{v}}(v) &= \mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M})\mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}}\rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}})\\ &= \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\big\langle\tilde{\phi}_v\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\tilde{\phi}_v\big\rangle. \qquad (174)\end{aligned}$$

Finally, for any ket $\big|\chi\big\rangle \in \mathcal{H}_{E\cap\overline{M}}$, for any $\vec{\kappa} \in \{0,1\}^m$, we denote by $r_{v,\vec{\kappa}}(\big|\chi\big\rangle)$ the ratio:

$$r_{v,\vec{\kappa}}(\big|\chi\big\rangle) = \frac{\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle}{\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle} \tag{175}$$

whenever $\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle > 0$ and $r_{v,\vec{\kappa}}(\big|\chi\big\rangle) = 1$ otherwise.

It is easy to see that, for any view $v \in \mathcal{R}$, any key $\vec{\kappa}$ and any ket $\big|\chi\big\rangle \in \mathcal{H}_{E\cap\overline{M}}$ such that $\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle > 0$

$$\begin{aligned}\sum_{\vec{\kappa}\in\{0,1\}^m} r_{v,\vec{\kappa}}(\big|\chi\big\rangle) &= \frac{\big\langle\chi\big|\sum_{\vec{\kappa}\in\{0,1\}^m}\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle}{\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle} &(176)\\ &= 2^m &(177)\end{aligned}$$

where we have used the identity $\sum_{k\in\{0,1\}^m}\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = 2^m\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}$ which follows directly from Property 7. The identity $\sum_{\vec{\kappa}\in\{0,1\}^m} r_{v,\vec{\kappa}}(\big|\xi\big\rangle) = 2^m$ holds for $\big\langle\chi\big|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\big|\chi\big\rangle = 0$ as well.

5.6.3 Quasi-independence of the key and the view on $\mathcal{R}\cap\mathcal{L}$

We are going to prove in this section that the probability of the joint event in which Eve-Bob get the view v and

Alice gets the key $\vec{\kappa}$ reads, provided $v \in \mathcal{R} \cap \mathcal{L}$,

$$\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v, \vec{\kappa}) = \pi_v + \eta_{v,\vec{\kappa}} \tag{178}$$

where π_v is independent of $\vec{\kappa}$ and an upper bound is found on $|\eta_{v,\vec{\kappa}}|$.

For any view $v \in \mathcal{R}$ and any key value $\vec{\kappa} \in \{0,1\}^m$, we have seen that (Property 8),

$$\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v, \vec{\kappa}) = \frac{1}{2^m} \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M}, P, R) \big\langle \tilde{\phi}_v \,\big|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)}\big|\, \tilde{\phi}_v \big\rangle. \tag{179}$$

Let $\mathit{\Pi}_w(z)$ be the orthogonal projection onto the subspace $\mathcal{H}_w = \mathrm{Span}\{ \big| \Psi(\vec{j}, \tilde{\vec{b}}) \big\rangle \mid d_{E \cap \overline{M}}(\vec{j}, \vec{h}) \geq \frac{\widehat{d}_w}{2} \} \subset \mathcal{H}_S$. The minimum weight $\widehat{d}_w$ has been defined in Section 5.3. As before, the partial view z is specified by the view v. Let $\overline{\mathit{\Pi}}_w(z) = \mathbf{1} - \mathit{\Pi}_w(z)$. Then $\mathit{\Pi}_w(z)$ and $\overline{\mathit{\Pi}}_w(z)$ act non trivially only on $\mathcal{H}_{E \cap \overline{M}}$, and

$$\begin{aligned} \big\langle \tilde{\phi}_v \,\big|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)}\big|\, \tilde{\phi}_v \big\rangle &= \big\langle \tilde{\phi}_v \,\big|(\mathit{\Pi}_w(z) + \overline{\mathit{\Pi}}_w(z)) \\ &\times \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} (\mathit{\Pi}_w(z) + \overline{\mathit{\Pi}}_w(z))\big|\, \tilde{\phi}_v \big\rangle. \end{aligned} \tag{180}$$

Therefore,

$$\begin{aligned} &\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v, \vec{\kappa}) = \\ &\frac{1}{2^m} \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M}, P, R) \Big[\big\langle \tilde{\phi}_v \,\big|\overline{\mathit{\Pi}}_w(z) \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \overline{\mathit{\Pi}}_w(z)\big|\, \tilde{\phi}_v \big\rangle \\ &+ \big\langle \tilde{\phi}_v \,\big|\mathit{\Pi}_w(z) \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)}\big|\, \tilde{\phi}_v \big\rangle + \big\langle \tilde{\phi}_v \,\big|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \mathit{\Pi}_w(z)\big|\, \tilde{\phi}_v \big\rangle \\ &- \big\langle \tilde{\phi}_v \,\big|\mathit{\Pi}_w(z) \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \mathit{\Pi}_w(z)\big|\, \tilde{\phi}_v \big\rangle \Big]. \end{aligned} \tag{181}$$

We show that the first term in the rhs in equation (181) corresponds to the term independent of $\vec{\kappa}$ and we derive a bound on the modulus of the remaining terms in the following parts.

The term independent of the key

Property 10. *For any view v in $\mathcal{R} \cap \mathcal{L}$, the first term in the rhs of (181) is independent of $\vec{\kappa}$. This term will be denoted by π_v subsequently, for any $v \in \mathcal{R} \cap \mathcal{L}$. That is,*

$$\begin{aligned} \pi_v \overset{Def}{=} &\frac{1}{2^m} \mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M}, P, R) \\ &\times \big\langle \tilde{\phi}_v \,\big|\overline{\mathit{\Pi}}_w(z) \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \overline{\mathit{\Pi}}_w(z)\big|\, \tilde{\phi}_v \big\rangle. \end{aligned} \tag{182}$$

Proof. We need the following identity:

Lemma 4.

$$\forall \vec{\alpha}, \vec{\beta} \in \{0,1\}^{\widehat{l}}, \tag{183}$$

$$\begin{aligned} &\Big\langle \Psi(\vec{\alpha}, \tilde{\vec{b}}(E \cap \overline{M})) \,\Big|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \Big|\, \Psi(\vec{\beta}, \tilde{\vec{b}}(E \cap \overline{M})) \Big\rangle = \\ &\frac{1}{2^{\widehat{l}}} \times \begin{cases} 0 \;\; \mathit{if}\; (\vec{\alpha} + \vec{\beta}) \notin \widehat{\mathcal{G}} \\ (-1)^{(\vec{\alpha}+\vec{\beta}) \cdot \vec{\theta}} \;\; \mathit{if}\; (\vec{\alpha} + \vec{\beta}) \in \widehat{\mathcal{G}}. \end{cases} \end{aligned} \tag{184}$$

where $\vec{\theta}$ is a vector in $\{0,1\}^{\widehat{l}}$ such that $\widehat{G}\vec{\theta} = \begin{pmatrix} \vec{s} \\ \vec{\kappa} \end{pmatrix} + \check{G}\vec{g}(E \cap M)$ ($\vec{\theta}$ exists since $|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)}| > 0$ for $v \in \mathcal{R}$). We recall that $\widehat{\mathcal{G}}$ has been defined in Section 5.3.

Proof of the lemma. First we need some definitions. For $y \in \{0,1\}$ and for $a \in \{+, \times\}$, define the unitary operator U^a_y acting on a single photon Hilbert space:

$$\forall x \in \{0,1\}, \quad U^a_y \big| \Psi(x, a) \big\rangle = \big| \Psi(x + y, a) \big\rangle. \tag{185}$$

It is easy to verify that on the opposite basis U^a_y acts as:

$$U^a_y \big| \Psi(x, \neg a) \big\rangle = (-1)^{xy} \big| \Psi(x, \neg a) \big\rangle. \tag{186}$$

Likewise, for $\vec{y} \in \{0,1\}^{\widehat{l}}$ define the unitary operator $U^{\vec{a}(E \cap \overline{M})}_{y}$ acting on $H_{E \cap \overline{M}}$ as:

$$\begin{aligned} \forall \vec{x} \in \{0,1\}^{\widehat{l}}, \quad U^{\vec{a}(E \cap \overline{M})}_{\vec{y}} \big| \Psi(\vec{x}, \vec{a}(E \cap \overline{M})) \big\rangle = \\ \big| \Psi(\vec{x} + \vec{y}, \vec{a}(E \cap \overline{M})) \big\rangle. \end{aligned} \tag{187}$$

It is easy to see that $U^{\vec{a}(E \cap \overline{M})}_{\vec{y}}$ is involutive, that is $U^{\vec{a}(E \cap \overline{M})\,-1}_{\vec{y}} = U^{\vec{a}(E \cap \overline{M})}_{\vec{y}}$. Since $\tilde{b}_i = \neg a_i$ for $i \in E \cap \overline{M}$, we have, using equation (186),

$$\begin{aligned} \forall \vec{x}, \quad U^{\vec{a}(E \cap \overline{M})}_{\vec{y}} \big| \Psi(\vec{x}, \tilde{\vec{b}}(E \cap \overline{M})) \big\rangle = \\ (-1)^{\vec{x} \cdot \vec{y}} \big| \Psi(\vec{x}, \tilde{\vec{b}}(E \cap \overline{M})) \big\rangle. \end{aligned} \tag{188}$$

Returning to our proof, we express $\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)}$ (defined in Property 9), recalling that $\widehat{G} = \begin{pmatrix} \widehat{F} \\ \widehat{K} \end{pmatrix}$. Furthermore, we use the fact that for any $\vec{y} \in \{0,1\}^{\widehat{l}}$,

$$\widehat{G}\vec{y} = \begin{pmatrix} \vec{s} \\ \vec{\kappa} \end{pmatrix} + \check{G}\vec{g}(E \cap M) \Leftrightarrow \vec{y} \in \vec{\theta} + \widehat{\mathcal{C}} \tag{189}$$

where θ is a vector in $\{0,1\}^{\widehat{l}}$ such that $\widehat{G}\vec{\theta} = \begin{pmatrix} \vec{s} \\ \vec{\kappa} \end{pmatrix} + \check{G}\vec{g}(E \cap M)$ (such $\vec{\theta}$ exists since $C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E} \cup M)} \neq \emptyset$). This gives, recalling that $\widehat{\mathcal{C}} = \left(\widehat{\mathcal{G}}\right)^{\perp}$,

$$\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} = \frac{1}{\left|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\right|} \sum_{\substack{\vec{x}\in\{0,1\}^N \mid \\ \vec{x}(\overline{E}\cup M)=\vec{g}(\overline{E}\cup M) \\ \widehat{G}\vec{x}(E\cap\overline{M})=\binom{\vec{s}}{\vec{\kappa}}+\check{G}\vec{g}(E\cap M)}} \left|\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\right\rangle \times \left\langle\Psi(\vec{x}(E\cap\overline{M}),\vec{a}(E\cap\overline{M}))\right| \tag{190}$$

$$= \frac{1}{\left|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\right|} \sum_{\vec{y}\in\vec{\theta}+\widehat{\mathcal{C}}} \left|\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right| \tag{191}$$

$$= \frac{1}{\left|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\right|} \times \sum_{\vec{y}\in\widehat{\mathcal{C}}} \left|\Psi(\vec{y}+\vec{\theta},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{y}+\vec{\theta},\vec{a}(E\cap\overline{M}))\right|, \tag{192}$$

and, using equation (188), for all $\vec{\alpha},\vec{\beta}\in\{0,1\}^{\hat{l}}$,

$$\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle$$
$$= \left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right| \frac{1}{\left|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\right|} \times \sum_{\vec{y}\in\widehat{\mathcal{C}}} U_{\vec{\theta}}^{\vec{a}(E\cap\overline{M})}\left|\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right\rangle \times \left\langle\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right| U_{\vec{\theta}}^{\vec{a}(E\cap\overline{M})}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle \tag{193}$$

$$= (-1)^{(\vec{\alpha}+\vec{\beta})\cdot\vec{\theta}}\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho_0\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle, \tag{194}$$

where

$$\rho_0 = \frac{1}{\left|C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\right|} \times \sum_{\vec{y}\in\widehat{\mathcal{C}}} \left|\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{y},\vec{a}(E\cap\overline{M}))\right|. \tag{195}$$

Let $q = \dim\widehat{\mathcal{C}}$, and $\{\vec{\theta}_1,\dots\vec{\theta}_q\}$ be a basis of $\widehat{\mathcal{C}}$. Let $\widehat{\mathcal{C}}^{(j)}$ be the span of $\{\vec{\theta}_1,\dots\vec{\theta}_j\}$ for $j\in\{1,\dots q\}$. For $j\in\{1,\dots q\}$, define $\rho^{(j)}$ as:

$$\rho^{(j)} = \frac{1}{2^j}\sum_{\vec{x}\in\widehat{\mathcal{C}}^{(j)}} \left|\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right|. \tag{196}$$

We show by induction on $j\in\{0,\dots q\}$ that

$$\forall\vec{\alpha},\vec{\beta}\in\{0,1\}^{\hat{l}},\quad \left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho^{(j)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \begin{cases} 1/2^{\hat{l}} & \text{if } \vec{\alpha}+\vec{\beta}\in\widehat{\mathcal{C}}^{(j)\perp} \\ 0 & \text{if } \vec{\alpha}+\vec{\beta}\notin\widehat{\mathcal{C}}^{(j)\perp} \end{cases}. \tag{197}$$

For $j = 0$, we have $\widehat{\mathcal{C}}^{(0)} = \{\vec{0}\}$ and $\widehat{\mathcal{C}}^{(0)\perp} = \{0,1\}^{\hat{l}}$ and $\rho^{(0)} = \left|\Psi(\vec{0},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{0},\vec{a}(E\cap\overline{M}))\right|$. Thus

$$\forall\vec{\alpha},\vec{\beta},\quad \left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho^{(0)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \frac{1}{2^{\hat{l}}}, \tag{198}$$

and (197) holds (Recall $a_i = \neg\tilde{b}_i$ on $E\cap\overline{M}$).

Suppose (197) holds for some $j\in\{0,\dots q-1\}$. Since $\widehat{\mathcal{C}}^{(j+1)} = \widehat{\mathcal{C}}^{(j)}\cup(\vec{\theta}_{j+1}+\widehat{\mathcal{C}}^{(j)})$, we have

$$\rho^{(j+1)} = \frac{1}{2}\left(\frac{1}{2^j}\sum_{\vec{x}\in\widehat{\mathcal{C}}^{(j)}} \left|\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right| + \frac{1}{2^j}\sum_{\vec{x}\in\vec{\theta}_{j+1}+\widehat{\mathcal{C}}^{(j)}} \left|\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{x},\vec{a}(E\cap\overline{M}))\right|\right) \tag{199}$$

$$= \frac{1}{2}\left(\rho^{(j)} + U_{\vec{\theta}_{j+1}}^{\vec{a}(E\cap\overline{M})}\rho^{(j)}U_{\vec{\theta}_{j+1}}^{\vec{a}(E\cap\overline{M})}\right). \tag{200}$$

Thus,

$$\forall\vec{\alpha},\vec{\beta},\quad \left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho^{(j+1)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \frac{1}{2}\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho^{(j)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle \times \underbrace{\left(1+(-1)^{(\vec{\alpha}+\vec{\beta})\cdot\vec{\theta}_{j+1}}\right)}_{=\begin{cases} 2 & \text{if } \vec{\alpha}+\vec{\beta}\in\vec{\theta}_{j+1}^{\perp} \\ 0 & \text{if } \vec{\alpha}+\vec{\beta}\notin\vec{\theta}_{j+1}^{\perp}.\end{cases}} . \tag{201}$$

And since (197) holds for j, we get

$$\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\rho^{(j+1)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \begin{cases} 1/2^{\hat{l}} & \text{if } \vec{\alpha}+\vec{\beta}\in\widehat{\mathcal{C}}^{(j+1)\perp}, \\ 0 & \text{if } \vec{\alpha}+\vec{\beta}\notin\widehat{\mathcal{C}}^{(j+1)\perp}. \end{cases} \tag{202}$$

which concludes our induction. Noting that $\widehat{\mathcal{C}}^{(q)} = \widehat{\mathcal{C}}$, $|\widehat{\mathcal{C}}| = |C_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}|$, $\widehat{\mathcal{C}}^{\perp} = \widehat{\mathcal{G}}$, and $\rho^{(q)} = \rho_0$, for any $\vec{\alpha}$, $\vec{\beta}\in\{0,1\}^{\hat{l}}$,

$$\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\left|\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \frac{1}{2^{\hat{l}}}\times\begin{cases} 0 \text{ if } (\vec{\alpha}+\vec{\beta})\notin\widehat{\mathcal{G}} \\ (-1)^{(\vec{\alpha}+\vec{\beta})\cdot\vec{\theta}} \text{ if } (\vec{\alpha}+\vec{\beta})\in\widehat{\mathcal{G}}. \end{cases} \tag{203}$$

which concludes the proof of the lemma. □

Now by definition of $\widehat{\mathcal{G}}$, for any vector $\vec{\gamma}\in\widehat{\mathcal{G}}$, there exists a vector $\vec{\lambda}_{\vec{\gamma}}\in\{0,1\}^{r+m}$ such that

$$\vec{\lambda}_{\vec{\gamma}}^T\widehat{G} = \gamma \tag{204}$$

and the above property reads:

$$\left\langle\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle = \frac{1}{2^{\hat{l}}}\times\begin{cases}0 \text{ if } (\vec{\alpha}+\vec{\beta})\notin\widehat{\mathcal{G}}\\ (-1)^{\vec{\lambda}_{(\vec{\alpha}+\vec{\beta})}\cdot\left(\binom{\vec{s}}{\vec{\kappa}}+\check{G}\vec{g}(E\cap M)\right)} & \text{if } (\vec{\alpha}+\vec{\beta})\in\widehat{\mathcal{G}}.\end{cases} \tag{205}$$

To see that the first term in (181) is independent of $\vec{\kappa}$, recalling the definition of $\overline{\Pi}_w(z)$, write

$$\begin{aligned}&\left\langle\tilde{\phi}_v\,\middle|\overline{\Pi}_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\overline{\Pi}_w(z)\middle|\,\tilde{\phi}_v\right\rangle\\ &\quad=\sum_{\substack{\vec{\alpha},\vec{\beta}\in\{0,1\}^{\hat{l}}|\\ w(\vec{\alpha}-\vec{h}(E\cap\overline{M}))<\hat{d}_w/2\\ w(\vec{\beta}-\vec{h}(E\cap\overline{M}))<\hat{d}_w/2}}\left\langle\tilde{\phi}_v\middle|\,\Psi(\alpha,\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle\\ &\quad\times\left\langle\Psi(\alpha,\tilde{\vec{b}}(E\cap\overline{M}))\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\Psi(\beta,\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle\\ &\quad\times\left\langle\Psi(\beta,\tilde{\vec{b}}(E\cap\overline{M}))\,\middle|\tilde{\phi}_v\right\rangle\end{aligned} \tag{206}$$

and the $\vec{\alpha}$'s and the $\vec{\beta}$'s contributing to the above sum obey

$$w(\vec{\alpha}+\vec{\beta})\leq w(\vec{\alpha}-\vec{h}(E\cap\overline{M}))+w(\vec{\beta}-\vec{h}(E\cap\overline{M}))<\hat{d}_w \tag{207}$$

thus $\vec{\alpha}+\vec{\beta}\notin\widehat{\mathcal{G}}^*$ (the set $\widehat{\mathcal{G}}^*$ has been defined in Sect. 5.3). The $\vec{\alpha}$ and $\vec{\beta}$ of the terms contributing in the sum are such that their sum is in $\widehat{\mathcal{G}}$ (according to the previous lemma) but not in $\widehat{\mathcal{G}}^*$. Since (by definition of $\widehat{\mathcal{G}}^*$) for $\vec{\alpha}+\vec{\beta}\in\widehat{\mathcal{G}}\backslash\widehat{\mathcal{G}}^*$, $\vec{\lambda}_{\vec{\alpha}+\vec{\beta}}$ is of the form $\binom{\vec{z}}{\vec{0}}$ where $\vec{z}\in\{0,1\}^r$, the terms

$$\begin{aligned}&\left\langle\tilde{\phi}_v\middle|\,\Psi(\alpha,\tilde{\vec{b}}(E\cap\overline{M})\right\rangle\\ &\quad\times\left\langle\Psi(\alpha,\tilde{\vec{b}}(E\cap\overline{M})\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\Psi(\beta,\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle\\ &\qquad\times\left\langle\Psi(\beta,\tilde{\vec{b}}(E\cap\overline{M}))\,\middle|\tilde{\phi}_v\right\rangle\\ &\qquad=\frac{1}{2^{\hat{l}}}(-1)^{\vec{\lambda}_{\vec{\alpha}+\vec{\beta}}\cdot\left(\binom{\vec{s}}{\vec{\kappa}}+\check{G}\vec{g}(E\cap M)\right)}\\ &\quad\times\left\langle\tilde{\phi}_v\,\middle|\,\Psi(\vec{\alpha},\tilde{\vec{b}}(E\cap\overline{M}))\right\rangle\left\langle\Psi(\vec{\beta},\tilde{\vec{b}}(E\cap\overline{M}))\,\middle|\tilde{\phi}_v\right\rangle\end{aligned} \tag{208}$$

contributing in the above sum (i.e. for $\vec{\alpha}+\vec{\beta}\in\widehat{\mathcal{G}}\setminus\widehat{\mathcal{G}}^*$) does not depend on $\vec{\kappa}$. Therefore $\left\langle\tilde{\phi}_v\,\middle|\overline{\Pi}_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\overline{\Pi}_w(z)\middle|\,\tilde{\phi}_v\right\rangle$ does not depend on $\vec{\kappa}$. Now $\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)$ is independent of $\vec{\kappa}$ since the m rows of $\widehat{K}$ are linearly independent between themselves and linearly independent of the rows of $\widehat{F}$ (since $\hat{d}_w>0$ on $\mathcal{R}$ by definition (Eq. (158))).

Therefore, the term in the rhs of (182) is independent of $\vec{\kappa}$. This concludes the proof of the property. □

The deviation from the key-independent term

We now derive an upper bound on $|\mathrm{P}_{\boldsymbol{\vec{\kappa}v}}(\vec{\kappa},v)-\pi_v|$.

Property 11. *For any $v\in\mathcal{R}\cap\mathcal{L}$ and $\vec{\kappa}\in\{0,1\}^m$, define $\eta_{v,\vec{\kappa}}$ as*

$$\eta_{v,\vec{\kappa}}\overset{Def}{=}\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v,\vec{\kappa})-\pi_v. \tag{209}$$

The modulus of $\eta_{v,\vec{\kappa}}$ is then upper bounded for any $v\in\mathcal{R}\cap\mathcal{L}$ and any $\vec{\kappa}\in\{0,1\}^m$ by

$$\begin{aligned}|\eta_{v,\vec{\kappa}}|\leq{}&\frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\left(r_{v,\vec{\kappa}}(\Pi_w(z)\big|\,\tilde{\phi}_v\big\rangle)+r_{v,\vec{\kappa}}(\big|\,\tilde{\phi}_v\big\rangle)\right)\\ &\times\left[2\sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}+\sqrt{g(\delta,\tau_f,p_R,n)}}\right].\end{aligned} \tag{210}$$

Proof. For any $v\in\mathcal{R}\cap\mathcal{L}$ and $\vec{\kappa}\in\{0,1\}^m$, we have from equation (181),

$$\eta_{v,\vec{\kappa}}=\mathrm{P}_{\boldsymbol{v\vec{\kappa}}}(v,\vec{\kappa})-\pi_v \tag{211}$$

$$\begin{aligned}&=\frac{1}{2^m}\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\Big[\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle\\ &\quad+\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle\\ &\quad-\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle\Big].\end{aligned} \tag{212}$$

Remarking that the second term in the bracket is only the complex conjugate of the first term, we have

$$\begin{aligned}|\eta_{v,\vec{\kappa}}|\leq{}&\frac{1}{2^m}\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\\ &\times\Big[2\left|\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle\right|\\ &+\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle\Big].\end{aligned} \tag{213}$$

Now, the first term in the bracket verifies

$$\begin{aligned}&\left|\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}^{1/2}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\tilde{\rho}^{1/2}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle\right|\\ &\quad\leq\left\|\tilde{\rho}^{1/2}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\big|\,\tilde{\phi}_v\big\rangle\right\|\times\left\|\tilde{\rho}^{1/2}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\big|\,\tilde{\phi}_v\big\rangle\right\|\\ &\qquad\text{using the Schwartz inequality and the fact}\\ &\qquad\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\text{ is Hermitian non negative}\end{aligned} \tag{214}$$

$$\begin{aligned}&=\sqrt{\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle}\\ &\quad\times\sqrt{\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle}.\end{aligned} \tag{215}$$

Now recalling the definition of $r_{v,\vec{\kappa}}$, we have

$$\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle=r_{v,\vec{\kappa}}\left[\big|\,\tilde{\phi}_v\big\rangle\right]\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle \tag{216}$$

since $\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle>0$, for any $v\in\mathcal{R}$ (recall that $\mathrm{P}_{\boldsymbol{v}}(v)=\mathrm{P}_{\boldsymbol{\mathcal{M}PR}}(\mathcal{M},P,R)\left\langle\tilde{\phi}_v\,\middle|\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\middle|\,\tilde{\phi}_v\right\rangle$). And

$$\begin{aligned}&\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle=\\ &\quad r_{v,\vec{\kappa}}\left[\Pi_w(z)\big|\,\tilde{\phi}_v\big\rangle\right]\left\langle\tilde{\phi}_v\,\middle|\Pi_w(z)\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}\Pi_w(z)\middle|\,\tilde{\phi}_v\right\rangle\end{aligned} \tag{217}$$

(recall that if $\left\langle \tilde{\phi}_v \left| \Pi_w(z) \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \Pi_w(z) \right| \tilde{\phi}_v \right\rangle = 0$ then $\left\langle \tilde{\phi}_v \left| \Pi_w(z) \tilde{\rho}_{\vec{s},\vec{\kappa},\vec{g}(\overline{E}\cup M)} \Pi_w(z) \right| \tilde{\phi}_v \right\rangle = 0$ as well).

The latter can be bounded using the small sphere property (Property 6). If $v \in \mathcal{R} \cap \mathcal{L}$,

$$\begin{aligned}
&\mathrm{P}_{\boldsymbol{\mathcal{M}}}(\mathcal{M}) \mathrm{Tr}(E_{v|\boldsymbol{\mathcal{M}}=\mathcal{M}} \Pi_0(z) \rho_{|\boldsymbol{\mathcal{M}}=\mathcal{M}} \Pi_0(z)) \\
&\quad = \mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R) \left\langle \tilde{\phi}_v \left| \Pi_0(z) \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \Pi_0(z) \right| \tilde{\phi}_v \right\rangle \qquad (218) \\
&\quad \le \mathrm{P}_{\boldsymbol{v}}(v) \sqrt{g(\delta,\tau_f,p_R,n)}. \qquad (219)
\end{aligned}$$

Now for $z \in \mathcal{R}$, $\widehat{d}_w/2 > d_2$, thus $\operatorname{Im} \Pi_w(z) \subset \operatorname{Im} \Pi_0(z)$ (refer to the beginning of Section 5.6.1), that is $\Pi_w(z)$ projects onto a space contained in the space on which $\Pi_0(z)$ projects. In other words, $\mathrm{Span}\{\left| \Psi(\vec{j},\tilde{\vec{b}}) \right\rangle | d_{E\cap\overline{M}}(\vec{j},\vec{h}) \ge \widehat{d}_w/2\} \subset \mathrm{Span}\{\left| \Psi(\vec{j},\tilde{\vec{b}}) \right\rangle | d_{E\cap\overline{M}}(\vec{j},\vec{h}) \ge d_2\}$.

Since $\tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)}$ is Hermitian non negative, it implies that

$$\left\langle \tilde{\phi}_v \left| \Pi_w(z) \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \Pi_w(z) \right| \tilde{\phi}_v \right\rangle \le \left\langle \tilde{\phi}_v \left| \Pi_0(z) \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \Pi_0(z) \right| \tilde{\phi}_v \right\rangle. \qquad (220)$$

Therefore, using Property 6, we have, $\forall \vec{\kappa} \in \{0,1\}^m$, $\forall v \in \mathcal{R} \cap \mathcal{L}$,

$$\mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R) \left\langle \tilde{\phi}_v \left| \Pi_w(z) \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \Pi_w(z) \right| \tilde{\phi}_v \right\rangle \le \mathrm{P}_{\boldsymbol{v}}(v) \sqrt{g(\delta,\tau_f,p_R,n)}. \qquad (221)$$

Linking the results (213, 215, 216, 217, 221) together, we obtain

$$\begin{aligned}
&\forall \vec{\kappa} \in \{0,1\}^m, \forall v \in \mathcal{R} \cap \mathcal{L}, \\
&|\eta_{v,\vec{\kappa}}| \le \frac{1}{2^m} \mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R) \\
&\times \left[2 \sqrt{\frac{\mathrm{P}_{\boldsymbol{v}}(v)}{\mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R)} \sqrt{g(\delta,\tau_f,p_R,n)} r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right)} \right. \\
&\qquad \times \sqrt{r_{v,\vec{\kappa}}\left(\left| \tilde{\phi}_v \right\rangle\right) \left\langle \tilde{\phi}_v \left| \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \right| \tilde{\phi}_v \right\rangle} \\
&\quad \left. + \frac{\mathrm{P}_{\boldsymbol{v}}(v)}{\mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R)} \sqrt{g(\delta,\tau_f,p_R,n)} r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right) \right] \qquad (222)
\end{aligned}$$

and using $\left\langle \tilde{\phi}_v \left| \tilde{\rho}_{\vec{s},\vec{g}(\overline{E}\cup M)} \right| \tilde{\phi}_v \right\rangle = \mathrm{P}_{\boldsymbol{v}}(v)/\mathrm{P}_{\boldsymbol{\mathcal{MPR}}}(\mathcal{M},P,R)$, we get

$$\begin{aligned}
|\eta_{v,\vec{\kappa}}| &\le \frac{1}{2^m} \left[2 \sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}} \right. \\
&\quad \times \sqrt{r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right) r_{v,\vec{\kappa}}\left(\left| \tilde{\phi}_v \right\rangle\right)} \\
&\quad \left. + \sqrt{g(\delta,\tau_f,p_R,n)} r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right) \right] \mathrm{P}_{\boldsymbol{v}}(v) \qquad (223) \\
&\le \frac{1}{2^m} \max\left(\left\{ r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right), r_{v,\vec{\kappa}}\left(\left| \tilde{\phi}_v \right\rangle\right) \right\} \right) \\
&\quad \times \left[2 \sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}} + \sqrt{g(\delta,\tau_f,p_R,n)} \right] \mathrm{P}_{\boldsymbol{v}}(v) \qquad (224) \\
&\le \frac{1}{2^m} \left[r_{v,\vec{\kappa}}\left(\Pi_w(z) \left| \tilde{\phi}_v \right\rangle\right) + r_{v,\vec{\kappa}}\left(\left| \tilde{\phi}_v \right\rangle\right) \right] \\
&\quad \times \left[2 \sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}} + \sqrt{g(\delta,\tau_f,p_R,n)} \right] \mathrm{P}_{\boldsymbol{v}}(v). \qquad (225)
\end{aligned}$$

This concludes our proof. □

5.6.4 Bound on the conditional entropy

In this section we conclude the privacy proof by deriving from the previous result the following property.

Property 12. *The conditional Shannon entropy of the key $\vec{\boldsymbol{\kappa}}$ given Eve's view $\boldsymbol{v}$ is lower bounded by*

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \ge m - \epsilon_1(N,m) \qquad (226)$$

where

$$\begin{aligned}
\epsilon_1(N,m) &= 2\left(m + \frac{1}{\ln 2}\right) h(\delta,\tau_f,p_R,n) \\
&\quad + 2\sqrt{2\left(m + \frac{1}{\ln 2}\right) m h(\delta,\tau_f,p_R,n)} \\
&\quad + m\left(\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}} \cap \mathcal{P}) + \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}} \cap \mathcal{P})\right) \qquad (227)
\end{aligned}$$

and

$$h(\delta,\tau_f,p_R,n) = 2\sqrt{\sqrt{g(\delta,\tau_f,p_R,n)}} + \sqrt{g(\delta,\tau_f,p_R,n)} \quad \textit{as defined previously.} \qquad (228)$$

Proof. We first prove that for any strictly positive real number q and for any view $v \in \mathcal{R} \cap \mathcal{L}$, there exists a set $\mathcal{K}_v \subset \{0,1\}^m$ such that

- $|\mathcal{K}_v| \ge 2^m(1 - \frac{1}{q})$, and
- $\forall \vec{\kappa} \in \mathcal{K}_v$,

$$\left| \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) - \frac{1}{2^m} \right| \le \frac{1}{2^m}(2q+2) h(\delta,\tau_f,p_R,n). \qquad (229)$$

From that we prove the bound on the conditional entropy (Eq. (226)).

For any view $v \in \mathcal{R}\cap\mathcal{L}$, summing over $\vec{\kappa}\in\{0,1\}^m$ the joint probability $\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) = \pi_v + \eta_{v,\vec{\kappa}}$, we get, using Property 10

$$\forall v \in \mathcal{R}\cap\mathcal{L},\quad \sum_{\vec{\kappa}\in\{0,1\}^m} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) = \mathrm{P}_{\boldsymbol{v}}(v) = 2^m\pi_v + \sum_{\vec{\kappa}\in\{0,1\}^m}\eta_{v,\vec{\kappa}} \tag{230}$$

but

$$\begin{aligned}\left|\sum_{\vec{\kappa}}\eta_{v,\vec{\kappa}}\right| &\le \sum_{\vec{\kappa}}|\eta_{v,\vec{\kappa}}| &(231)\\ &\le \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)h(\delta,\tau_f,p_R,n)\\ &\quad\times\left(\sum_{\vec{\kappa}} r_{v,\vec{\kappa}}\left(\mathit{\Pi}_w(z)|\,\tilde{\phi}_v\rangle\right) + \sum_{\vec{\kappa}} r_{v,\vec{\kappa}}\left(|\,\tilde{\phi}_v\rangle\right)\right) &(232)\\ &\le 2\mathrm{P}_{\boldsymbol{v}}(v)h(\delta,\tau_f,p_R,n) &(233)\end{aligned}$$

using Property 11 and the identity (177).

Therefore,

$$|\mathrm{P}_{\boldsymbol{v}}(v) - 2^m\pi_v| \le 2\mathrm{P}_{\boldsymbol{v}}(v)h(\delta,\tau_f,p_R,n) \tag{234}$$

that is

$$\begin{aligned}&|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)|\\ &\le |\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v) - \pi_v| + |\pi_v - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)| &(235)\\ &\le \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)h(\delta,\tau_f,p_R,n)\\ &\quad\times\left[r_{v,\vec{\kappa}}\left(\mathit{\Pi}_w(z)|\,\tilde{\phi}_v\rangle\right) + r_{v,\vec{\kappa}}\left(|\,\tilde{\phi}_v\rangle\right) + 2\right] &(236)\end{aligned}$$

or

$$\begin{aligned}|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) - \frac{1}{2^m}| &\le \frac{1}{2^m}h(\delta,\tau_f,p_R,n)\\ &\quad\times\left[r_{v,\vec{\kappa}}\left(\mathit{\Pi}_w(z)|\,\tilde{\phi}_v\rangle\right) + r_{v,\vec{\kappa}}\left(|\,\tilde{\phi}_v\rangle\right) + 2\right]. &(237)\end{aligned}$$

Let $a_{v,\vec{\kappa}} = r_{v,\vec{\kappa}}(\mathit{\Pi}_w(z)|\,\tilde{\phi}_v\rangle) + r_{v,\vec{\kappa}}(|\,\tilde{\phi}_v\rangle)$. Then using again identity (177), we have

$$\sum_{\vec{\kappa}\in\{0,1\}^m} a_{v,\vec{\kappa}} = 2^{m+1}. \tag{238}$$

Let q be a strictly positive real number. Let $\boldsymbol{U}$ be a random variable taking value in $\{0,1\}^m$ with uniform probability distribution, i.e. $\forall\vec{\kappa}\in\{0,1\}^m$, $\mathrm{P}_{\boldsymbol{U}}(\vec{\kappa}) = 1/2^m$. Then using Lemma 3 for $\boldsymbol{U}$ with $\mu = 2^{m+1}$, we find that

$$\mathrm{P}_{\boldsymbol{U}}(\mathcal{K}_v) \ge 1 - \frac{1}{q} \tag{239}$$

where the set $\mathcal{K}_v$ is defined by:

$$\mathcal{K}_v = \left\{\vec{\kappa}\in\{0,1\}^m\,:\,a_{v,\vec{\kappa}} < 2^{m+1}q\frac{1}{2^m} = 2q\right\}. \tag{240}$$

In other words,

$$|\mathcal{K}_v| \ge 2^m\left(1 - \frac{1}{q}\right). \tag{241}$$

Let $\mathcal{I}$ be the set defined by

$$\mathcal{I} = \cup_{v\in\mathcal{R}\cap\mathcal{L}}\mathcal{K}_v\times\{v\} \subset \{0,1\}^m\times\mathcal{Z}. \tag{242}$$

It follows that

$$\forall(\vec{\kappa},v)\in\mathcal{I},\quad \left|\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v} - \frac{1}{2^m}\right| \le \frac{1}{2^m}(2q+2)h(\delta,\tau_f,p_R,n), \tag{243}$$

and

$$\begin{aligned}\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\mathcal{I}) &= \sum_{v\in\mathcal{R}\cap\mathcal{L}}\mathrm{P}_{\boldsymbol{v}}(v)\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\mathcal{K}_v) &(244)\\ &= \sum_{v\in\mathcal{R}\cap\mathcal{L}}\left[\mathrm{P}_{\boldsymbol{v}}(v)\sum_{\vec{\kappa}\in\mathcal{K}_v}\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa})\right] &(245)\\ &\ge \sum_{v\in\mathcal{R}\cap\mathcal{L}}\left[\mathrm{P}_{\boldsymbol{v}}(v)\sum_{\vec{\kappa}\in\mathcal{K}_v}\frac{1}{2^m}(1-(2q+2)\right.\\ &\qquad\left.\times h(\delta,\tau_f,p_R,n))\right] &(246)\\ &\ge \left(1-\frac{1}{q}\right)(1-(2q+2)h(\delta,\tau_f,p_R,n))\,\mathrm{P}_{\boldsymbol{v}}(\mathcal{R}\cap\mathcal{L}) &(247)\\ &\ge \left(1-\frac{1}{q}\right)(1-(2q+2)h(\delta,\tau_f,p_R,n))\\ &\qquad\times\left(\mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}}\cap\mathcal{P})\right) &(248)\\ &\ge \mathrm{P}_{\boldsymbol{v}}(\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}}\cap\mathcal{P})\\ &\qquad-\frac{1}{q} - (2q+2)h(\delta,\tau_f,p_R,n). &(249)\end{aligned}$$

Now,

$$\begin{aligned}H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) &= -\sum_{\vec{\kappa},v}\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) &(250)\\ &= -\sum_{\vec{\kappa},v\in\overline{\mathcal{P}}}\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa})\\ &\quad-\sum_{\vec{\kappa},v\in\mathcal{P}}\mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}). &(251)\end{aligned}$$

For any $v\in\overline{\mathcal{P}}$ and $\vec{\kappa}\in\{0,1\}^m$, we have $\mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) = 1/2^m$ since Alice chooses randomly and independently the value for $\vec{\boldsymbol{\kappa}}$ when the validation test is not passed. Therefore,

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) = m\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{P}}) - \sum_{\vec{\kappa},v\in\mathcal{P}} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2 \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) \tag{252}$$

$$\geq m\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{P}}) - \sum_{(\vec{\kappa},v)\in\mathcal{I}} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2 \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) \tag{253}$$

since for any v and $\vec{\kappa}$, $-\log_2 \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa})$ is nonnegative. Using the relation:

$$\forall(\vec{\kappa},v)\in\mathcal{I},\quad \mathrm{P}_{\vec{\boldsymbol{\kappa}}\,|\,\boldsymbol{v}=v}(\vec{\kappa}) = \frac{1}{2^m}(1+\xi_{\vec{\kappa},v}) \tag{254}$$

where $\xi_{\vec{\kappa},v} \leq (2q+2)h(\delta,\tau_f,p_R,n)$ for any $(\vec{\kappa},v)\in\mathcal{I}$, we get

$$\begin{aligned} H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) &\geq m\left(\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{P}}) + \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\mathcal{I})\right) \\ &\quad - \sum_{(\vec{\kappa},v)\in\mathcal{I}} \mathrm{P}_{\vec{\boldsymbol{\kappa}}\boldsymbol{v}}(\vec{\kappa},v)\log_2(1+\xi_{\vec{\kappa},v}) \qquad (255) \\ &\geq m\Big(1-\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) - \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}}\cap\mathcal{P}) \\ &\quad -\frac{1}{q} - (2q+2)h(\delta,\tau_f,p_R,n)\Big) \\ &\quad -\frac{1}{\ln 2}(2q+2)h(\delta,\tau_f,p_R,n) \qquad (256) \\ &= m - \left(m+\frac{1}{\ln 2}\right)(2q+2)h(\delta,\tau_f,p_R,n) \\ &\quad -\frac{m}{q} - m(\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) + \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}}\cap\mathcal{P})) \qquad (257) \end{aligned}$$

where we used equation (249) and the inequality $\log_2(1+x) \leq |x|/\ln 2$ for any $x > -1$.

The above inequality holds for any positive real number $q \geq 1$. Especially it holds for

$$q = \sqrt{\frac{m}{2\left(m+\frac{1}{\ln 2}\right)h(\delta,\tau_f,p_R,n)}} \tag{258}$$

obtained by maximising the rhs in Eq. (257). We therefore obtain the bound on the conditional Shannon entropy of the key $\vec{\boldsymbol{\kappa}}$ given the view $\boldsymbol{v}$

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - \epsilon_1(N,m) \tag{259}$$

where

$$\begin{aligned} \epsilon_1(N,m) &= 2\left(m+\frac{1}{\ln 2}\right)h(\delta,\tau_f,p_R,n) \\ &\quad +2\sqrt{2\left(m+\frac{1}{\ln 2}\right)mh(\delta,\tau_f,p_R,n)} \\ &\quad +m\left(\mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{R}}\cap\mathcal{P}) + \mathrm{P}_{\boldsymbol{v}}(\overline{\mathcal{L}}\cap\mathcal{P})\right). \qquad (260) \end{aligned}$$

This concludes the proof of privacy. □

This work was partially supported by the ESF programme on quantum information theory (QIT). HI gratefully acknowledges support provided by the European TMR Network ERP-4061PL95-1412. NL gratefully acknowledges support provided by the Academy of Finland under project number 43336. We would like to thank Artur Ekert, Patrick Hayden, Michele Mosca, Nicolas Gisin for interesting discussions and helpful comments.

Appendix A: Binomial tail inequalities

The following properties have been used throughout this paper.

Property 13. *Let α be a positive number such that $0 \leq \alpha \leq 1/2$. Then*

$$\sum_{0\leq i\leq \alpha n} \binom{n}{i} \leq 2^{H_1(\alpha)n} \tag{261}$$

where $H_1(\alpha) = -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)$ is the binary entropy function.

Property 14. *Let p, t be positive number such that $0 < p \leq p+t < 1$. Then*

$$\sum_{(p+t)n\leq i\leq n} \binom{n}{i} p^i(1-p)^{n-i} \leq e^{-2t^2 n}. \tag{262}$$

Property 15. *Let p, t be positive number such that $0 < p-t \leq p < 1$. Then*

$$\sum_{0\leq i\leq (p-t)n} \binom{n}{i} p^i(1-p)^{n-i} \leq e^{-2t^2 n}. \tag{263}$$

Property 16. *Let A be a set of size $|A|$. Let B be a set. Suppose each element of A is contained in B with probability p. Let τ be a positive number such that $0 < p-\tau < p < p+\tau < 1$. Then the probability that B contains more than $(p+\tau)|A|$ elements of A (i.e. $|A\cap B| \geq (p+\tau)|A|$) is bounded by*

$$\Pr(|A\cap B| \geq (p+\tau)|A|) \leq \exp[-2\tau^2|A|]. \tag{264}$$

Likewise, the probability that B contains less than $(p-\tau)|A|$ elements of A is bounded by

$$\Pr(|A\cap B| \leq (p-\tau)|A|) \leq \exp[-2\tau^2|A|]. \tag{265}$$

Proof. [25] Suppose $0 \leq p \leq p+t \leq 1$, $q = 1-p$. For any $x \geq 1$, we have

$$\begin{aligned} \sum_{k\leq i\leq n} \binom{n}{i} p^i q^{n-i} &\leq \sum_{k\leq i\leq n} \binom{n}{i} p^i q^{n-i} x^{i-k} \\ &\leq \sum_{0\leq i\leq n} \binom{n}{i} p^i q^{n-i} x^{i-k} \\ &= \frac{1}{x^k}(q+px)^n \\ &\leq \frac{1}{x^{(p+t)n}}(q+px)^n \end{aligned}$$

where $k = \lceil (p+t)n \rceil$. The minimum of the last expression as function of x ($x \geq 1$) is reached for $\vec{x} = \frac{q(p+t)}{p(q-t)}$ and the above inequality gives

$$\sum_{k \leq i \leq n} \binom{n}{i} p^i q^{n-i} \leq \left[\left(\frac{p}{p+t} \right)^{p+t} \left(\frac{q}{q-t} \right)^{q-t} \right]^n . \tag{266}$$

The inequality above reads, for $p = 1/2$ (therefore $q = 1/2$) and $t = \beta - 1/2$ where $\beta = 1 - \alpha \in [1/2, 1]$,

$$\sum_{\beta n \leq i \leq n} \binom{n}{i} \leq 2^{nh(\beta)}. \tag{267}$$

Using the identity

$$\binom{n}{i} = \frac{n!}{(n-i)!i!} = \binom{n}{n-i} \tag{268}$$

and remarking that $H_1(\alpha) = H_1(1-\beta) = H_1(\beta)$, we get Property 13:

$$\forall 0 \leq \alpha \leq \frac{1}{2}, \quad \sum_{0 \leq i \leq \alpha n} \binom{n}{i} \leq 2^{H_1(\alpha)n}. \tag{269}$$

Let's write (266) as

$$\sum_{k \leq i \leq n} \binom{n}{i} p^i q^{n-i} \leq e^{ng(t)} \tag{270}$$

where

$$g(t) = \ln \left[\left(\frac{p}{p+t} \right)^{p+t} \left(\frac{q}{q-t} \right)^{q-t} \right]. \tag{271}$$

Then g is $\mathcal{C}^\infty$ on $[0, q[$, and applying Taylor's formula at order 2, we get

$$g(t) = g(0) + tg'(0) + \int_0^t g''(u)(t-u)du. \tag{272}$$

It is easy to check that $g(0) = g'(0) = 0$ and that $g''(u) = -\frac{1}{(p+u)(q-u)} \leq -4$ for any $u \in]0, q[$. Therefore

$$\begin{aligned} g(t) &= \int_0^t g''(u)(t-u)du \\ &\leq -4 \int_0^t (t-u)du \\ &\leq -2t^2. \end{aligned}$$

Since the exponential function is monotonically increasing, we get

$$e^{g(t)} \leq e^{-2t^2}, \tag{273}$$

therefore

$$\sum_{(p+t)n \leq i \leq n} \binom{n}{i} p^i q^{n-i} \leq e^{-2t^2 n} \tag{274}$$

which gives Property 14.

Suppose now that $0 < p - t \leq p < 1$. Using the identity (268), we get

$$\begin{aligned} \sum_{0 \leq i \leq (p-t)n} \binom{n}{i} p^i q^{n-i} &= \sum_{0 \leq i \leq (p-t)n} \binom{n}{n-i} q^{n-i} p^i \\ &= \sum_{n-(p-t)n \leq j \leq n} \binom{n}{j} q^j p^{n-j} \\ &= \sum_{(q+t)n \leq j \leq n} \binom{n}{j} q^j p^{n-j}, \end{aligned}$$

where $0 < q \leq q + t < 1$. Applying Property 14, we get

$$\sum_{0 \leq i \leq (p-t)n} \binom{n}{i} p^i (1-p)^{n-i} \leq e^{-2t^2 n} \tag{275}$$

which concludes the proofs for the binomial tail inequalities. We now prove Property 16.

The probability that B contains exactly k elements of A, for $0 \leq k \leq |A|$, reads

$$\Pr(|A \cap B| = k) = \binom{|A|}{k} p^k (1-p)^{|A|-k}. \tag{276}$$

Therefore, the probability that A contains more than $(p+\tau)|A|$ elements of A reads

$$\begin{aligned} &\Pr(|A \cap B| \geq (p+\tau)|A|) \\ &\quad = \sum_{(p+\tau)n \leq k \leq |A|} \Pr(|A \cap B| = k) && (277) \\ &\quad = \sum_{(p+\tau)n \leq k \leq |A|} \binom{|A|}{k} p^k (1-p)^{|A|-k} && (278) \\ &\quad \leq \exp[-2\tau^2 |A|], && (279) \end{aligned}$$

using the binomial tail inequality (Property 14). Likewise, the probability that A contains less than $(p-\tau)|A|$ elements of A reads

$$\begin{aligned} &\Pr(|A \cap B| \leq (p-\tau)|A|) \\ &\quad = \sum_{0 \leq k \leq (p-\tau)|A|} \Pr(|A \cap B| = k) && (280) \\ &\quad = \sum_{0 \leq k \leq (p-\tau)|A|} \binom{|A|}{k} p^k (1-p)^{|A|-k} && (281) \\ &\quad \leq \exp[-2\tau^2 |A|], && (282) \end{aligned}$$

using the binomial tail inequality (Property 15). This concludes the proof. □

References

1. H. Inamori, N. Lütkenhaus, D. Mayers, Inconditional Security for Practical Quantum Key Distribution, `arXiv:quant-ph/0107017` (2001)

2. D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, In *Advances in Cryptology — Proceedings of Crypto '96*; available as `arXiv:quant-ph/9606003` (Springer, Berlin, 1996), pp. 343–357
3. D. Mayers, Unconditional security in quantum cryptography, J. ACM (2001) (to appear); also available at `arXiv:quant-ph/9802025`
4. B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A **51**, 1863 (1995)
5. H.P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996)
6. G. Brassard, N. Lütkenhaus, T. Mor, B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000)
7. N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000)
8. E. Biham, M. Boyer, P.O. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, `arXiv:quant-ph/9912053` (1999)
9. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)
10. B. Huttner, A. Ekert, J. Mod. Opt. **41**, 2455 (1994); C. Fuchs, N. Gisin, R. Griffiths, C.-S. Niu, A. Peres, Phys. Rev. A **56**, 1163 (1997); B. Slutsky, R. Rao, P. Sun, Y. Fainman, Phys. Rev. A **57**, 2383 (1998); N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999)
11. J. Cirac, N. Gisin, Phys. Lett. A **229**, 1 (1997); H. Bechmann-Pasquinucci, N. Gisin, Phys. Rev. A **59**, 4238 (1999)
12. E. Biham, T. Mor, Phys. Rev. Lett. **78**, 2256 (1997); E. Biham, M. Boyer, G. Brassard, J. van de Graaf, T. Mor, `arXiv:quant-ph/9801022` (1998)
13. H.-K. Lo, H.F. Chau. Science **283**, 2050 (1999)
14. D. Mayers, A. Yao, `arXiv:quant-ph/9809039` (1998); D. Mayers, C. Tourenne, "Violation of Locality and Self-Checking Source", to appear in: *Proceedings of Quantum Communication, Computing, and Measurement 3*, held in Capri 2000 (Kluwer Academic/Plenum Publishers)
15. C. Shannon, Bell Syst. Technical Jour. **28**, 657 (1949)
16. D. Welsh, *Code and Cryptography* (Clarendon Press, Oxford, 1988)
17. D. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995)
18. C.H. Bennett, G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175–179
19. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin. J. Cryptology **5**, 3 (1992)
20. D.F. Walls, G.J. Milburn, *Quantum Optics* (Springer, Berlin, 1994)
21. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, E. Sundberg, Opt. Expr. **4**, 383 (1999)
22. C. Marand, P.T. Townsend, Opt. Lett. **20**, 1695 (1995)
23. P.D. Townsend, IEEE Photon. Technol. Lett. **10**, 1048 (1998)
24. A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993)
25. Lectures on Communication Theory by D. Welsh, C. McDiarmid, Mathematical Institute, Oxford (1998)