Algorithmica (2002) 34: 340–365
DOI: 10.1007/s00453-002-0983-4

Algorithmica

Security of Practical Time-Reversed EPR Quantum Key Distribution[1]

Hitoshi Inamori[2]

Abstract. We propose a proof of the security of a time-reversed EPR quantum key distribution protocol against enemies with unlimited computational power. The considered protocol uses interactive key distillation, and the proof holds for implementations using imperfect photon sources.

Key Words. Quantum cryptography, Quantum key distribution.

1. Introduction. Quantum key distribution is a cryptographic task that uses properties of quantum mechanics to allow two legitimate parties to share a secret random number. This random number can be used as a key for a symmetric classical cipher to establish a perfectly secure communication channel between the legitimate parties. The first quantum key distribution protocol, called BB84, was proposed by Bennett and Brassard [1]. It was followed by other protocols, such as [2]–[5] and the security of these protocols were analysed [6]–[13]. The unconditional security of quantum key distribution—i.e. security against enemies with unlimited computational power—was obtained by Mayers [14], [15] for the BB84 protocol and many notions and techniques introduced in the proof are used in the present paper. Other proofs of the unconditional security of quantum key distribution followed [16]–[22].

In this paper we present a proof of the security of the *time-reversed EPR protocol*, which was proposed in [5] by Biham et al. Here, the considered protocol uses a two-way public communication for key distillation, and may be implemented with imperfect devices. More precisely, the legitimate users may use imperfect photon sources that emit a perfect single-photon signal with limited probability. Besides, they may be vulnerable to *Trojan Horse attacks*, in which an enemy tries to read the settings of the legitimate users' apparatus by sending in a probe. The present proof holds against a limited class of Trojan Horse attacks, in which the potential enemy is restricted to acquiring information about a limited number of signals during the quantum transmission. Under these conditions, the protocol is proved secure against enemies with unlimited computational power.

The protocol assumes the existence of an untrusted third party performing measurements on signals sent by the legitimate parties. The key distribution is possible only when the third party performs honestly efficient Bell measurements on polarisations of pairs of photons. The key distribution session is otherwise rejected by the protocol's validation test. Therefore the time-reversed EPR protocol is not yet practical with current

[1] This work was supported by the European TMR Network ERP-4061PL95-1412.
[2] Centre for Quantum Computation, Oxford University, Oxford, England.

Received February 28, 2001. Communicated by M. Mosca and A. Tapp.
Online publication September 16, 2002.

technology, as no efficient technique performing such measurements is available. Nevertheless, the present proof has practical relevance as one can derive from it the security of a realistic BB84 protocol [23], which can be implemented with today's technology.

2. Definition of Security. We adopt the same definition of security as described in [15] and [24]. The role of key distribution between two distant legitimate parties, traditionally called Alice and Bob, is to generate a shared random number, 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, whichever eavesdropping strategy she might adopt. However, most quantum key distribution protocols do not allow Alice and Bob to share a private key in all circumstances. It is only when some conditions are satisfied that Alice and Bob can ascertain a potential eavesdropper will only have negligible information about the key. The 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. Nevertheless, as in [15] and [24] we adopt the convention that when the validation test is not passed, Alice chooses a random value for the private key with uniform probability distribution. As a result, the private key is defined regardless of the outcome of the validation test, but, of course, when the validation test is not passed, Bob does not share the key with Alice.

Finally, we consider families of protocols for which a parameter quantifying the amount of a resource used in a protocol characterises its security. Such a parameter is called the *security parameter*. Usually, the higher the security parameter's value, the higher the level of security, but also the higher amount of a resource required by the protocol. We now give a formal definition of security.

A random variable is always denoted by a bold letter, and values taken by this random variable are denoted by the corresponding plain letter. Only discrete random variables are 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 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. $\mathrm{P}_{\boldsymbol{x}|\boldsymbol{y}=y}(x) = \Pr(\boldsymbol{x} = x \mid \boldsymbol{y} = y) = \mathrm{P}_{\boldsymbol{xy}}(x, y)/\mathrm{P}_{\boldsymbol{y}}(y)$, 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 $\boldsymbol{f}$ is adopted to denote the random variable $f(\boldsymbol{x})$.

We 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 a value in $\{0, 1\}^m$. 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 denote by $\mathcal{V}$ 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 offers *perfect privacy* if and only if:

- the protocol is parameterised by a parameter N taking a value in $\mathbf{N}$ called the security parameter, and
- there exists a function $\varepsilon\colon \mathbf{N}\times\mathbf{N}\to\mathbf{R}^+$ such that $\varepsilon(N,m)$ vanishes exponentially as N grows (i.e. there exist $\alpha>0$, $\beta>0$, $N_{\min}\in\mathbf{N}$ and a function $f\colon \mathbf{N}\to\mathbf{R}^+$ such that $\forall N>N_{\min},\ \varepsilon(N,m)<e^{-\alpha N^{\beta}}f(m)$), and
- there exists a function $N_0\colon \mathbf{N}\to\mathbf{N}$ such that, for any strategy adopted by Eve,

$$\forall m,\ \forall N\geq N_0(m),\qquad H(\vec{\boldsymbol{\kappa}}\mid \boldsymbol{v})\geq m-\varepsilon(N,m),$$

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

$$H(\vec{\boldsymbol{\kappa}}\mid \boldsymbol{v})\stackrel{\text{Def}}{=}-\sum_{\vec{\kappa},v:\ P_{\vec{\kappa}v}(\vec{\kappa},v)>0} P_{\vec{\kappa}v}(\vec{\kappa},v)\log_2 \mathrm{P}_{\vec{\kappa}|\boldsymbol{v}=v}(\vec{\kappa})$$

is the Shannon entropy [25]–[27] of the key $\vec{\boldsymbol{\kappa}}$ given Eve's view $\boldsymbol{v}$.

Another important aspect of the security of 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. However, the integrity of the protocol depends mainly on the efficiency of the error detection/correction scheme that is used. The reader is referred for instance to [28] for a detailed explanation.

3. Idea Behind the Protocol and Its Security. In the framework of quantum mechanics, any physical system is described in an associated Hilbert space $\mathcal{H}$ of appropriate dimension. The *state* of the system is fully defined by a Hermitian non-negative operator ρ acting on $\mathcal{H}$, and of unit trace, called the *density operator*. When the system has probability p_i of being in the state ρ_i for $i=1,2,\ldots,k$ (we say the system is in a *statistical mixture* of states), then the corresponding density operator is $\rho=\sum_{i=1}^{k}p_i\rho_i$. A state given by a density matrix of rank one is said to be *pure*. A pure state of density operator ρ can be alternatively described as a normalised vector in the Hilbert space, $|\psi\rangle$, such that $\rho=|\psi\rangle\langle\psi|$. This vector is referred to as a *ket* associated to the pure state. For any vectors $|\varphi\rangle$ and $|\psi\rangle$ of $\mathcal{H}$, $|\varphi\rangle\langle\psi|$ denotes the operator which maps any $|\chi\rangle\in\mathcal{H}$ to $|\varphi\rangle\langle\psi\mid\chi\rangle=\langle\psi\mid\chi\rangle|\varphi\rangle$, where $\langle\psi\mid\chi\rangle$ is the scalar product of $|\psi\rangle$ and $|\chi\rangle$.

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

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

where ρ is the density operator of the system. For any $q \in \mathcal{Q}$, the Hermitian non-negative 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 [29].

In the present paper we are mainly interested in the description of pulses of light. We concentrate our study to light pulses with a definite number of particles of light, called *photons*. Each photon has a degree of freedom called *polarisation*, which is described in a two-dimensional Hilbert space. We assume in this paper that the legitimate parties have the technical ability to emit—at least with a certain probability—a light pulse such that (1) it contains exactly one photon in a specified polarisation state and (2) its other degrees of freedom are independent of the chosen polarisation state. We therefore ignore, in the following part of this paper, the other degrees of freedom for successfully emitted single-photon pulses.

The polarisation of one photon is described in a two-dimensional Hilbert space. Let "+" denote one of its orthonormal basis, with basis vectors $|0\rangle_+$ and $|1\rangle_+$. Let "×" be its *conjugate* basis, of basis vectors $|0\rangle_\times = (|0\rangle_+ + |1\rangle_+)/\sqrt{2}$ and $|1\rangle_\times = (|0\rangle_+ - |1\rangle_+)/\sqrt{2}$.

The polarisation state of a system of two distinguishable photons can be described in the tensor product space of two single-photon polarisation spaces. For any $\alpha \in \{0, 1\}$, $\beta \in \{0, 1\}$ and bases $a \in \{+, \times\}$, $b \in \{+, \times\}$, the ket $|\alpha\rangle_a \otimes |\beta\rangle_b$ describes the state of a system in which the first photon is in state $|\alpha\rangle_a$ and the second photon in state $|\beta\rangle_b$. The *Bell basis* of basis vectors $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ is defined in the basis $+$ by

$$
\begin{aligned}
|0\rangle &= \frac{|0,0\rangle_+ + |1,1\rangle_+}{\sqrt{2}}, \\
|1\rangle &= \frac{|0,0\rangle_+ - |1,1\rangle_+}{\sqrt{2}}, \\
|2\rangle &= \frac{|0,1\rangle_+ + |1,0\rangle_+}{\sqrt{2}}, \\
|3\rangle &= \frac{|0,1\rangle_+ - |1,0\rangle_+}{\sqrt{2}},
\end{aligned}
$$

where for any $\alpha \in \{0, 1\}$, $\beta \in \{0, 1\}$ and bases $a \in \{+, \times\}$, $b \in \{+, \times\}$, $|\alpha, \beta\rangle_{ab}$ and $|\alpha, \beta\rangle_a$ are shorthand notations for $|\alpha\rangle_a \otimes |\beta\rangle_b$ and $|\alpha\rangle_a \otimes |\beta\rangle_a$, respectively. It can be shown that the Bell basis reads, in the conjugate basis $\times$:

$$
\begin{aligned}
|0\rangle &= \frac{|0,0\rangle_\times + |1,1\rangle_\times}{\sqrt{2}}, \\
|1\rangle &= \frac{|0,1\rangle_\times + |1,0\rangle_\times}{\sqrt{2}}, \\
|2\rangle &= \frac{|0,0\rangle_\times - |1,1\rangle_\times}{\sqrt{2}}, \\
|3\rangle &= -\frac{|0,1\rangle_\times - |1,0\rangle_\times}{\sqrt{2}}.
\end{aligned}
$$

For any $c \in \{0, 1, 2, 3\}$ and any basis $a \in \{+, \times\}$, we define $(\pi_a^c, \sigma_a^c, \lambda_a^c)$ as the unique

triplet of binary numbers such that

$$|c\rangle = (-1)^{\lambda_a^c} \left(\frac{|0, \pi_a^c\rangle_a + (-1)^{\sigma_a^c} |1, \neg\pi_a^c\rangle_a}{\sqrt{2}} \right).$$

The binary numbers π_a^c and σ_a^c are called respectively the *parity* and the *phase* of the Bell state $|c\rangle$ in the basis a.

We now describe the principal idea of the time-reversed EPR protocol, following [5]. Suppose that Alice sends a single photon in the state $|\alpha\rangle_a$ where the bit α and the basis a are chosen secretly and randomly by Alice. Similarly, Bob sends a single photon in the state $|\beta\rangle_b$ where the bit β and the basis b are chosen secretly and randomly by Bob. The legitimate parties ask a third party, Eve, to perform a projective measurement on the Bell basis, i.e. a POVM measurement with the four positive operators $|g\rangle\langle g|$ where $g \in \{0, 1, 2, 3\}$. After Eve announces her result, g, Alice and Bob publicly announce their bases a and b. If they are identical, then Alice and Bob know whether their bits—which are still secret—are identical or not. For instance, if Alice and Bob chose the basis $+$ and Eve announces $g = 2$, then Alice knows that if her bit is 1, then Bob's bit should be 0. More generally, if Alice and Bob chose the basis a, then Alice's bit and Bob's bit are equal if $\pi_a^g = 0$ and different if $\pi_a^g = 1$. Thereby the legitimate parties succeed in sharing a secret number.

The goal of a dishonest Eve is to try to learn this secret number without alarming the legitimate users. In the above situation, Eve wants to learn α or β but she also wants to announce an index g so that Alice and Bob do not notice the treachery. Indeed, Alice and Bob are careful, and can check whether the index g announced by Eve obeys the relation $\alpha+\beta = \pi_a^g \pmod 2$, as it should. To run this test, Alice and Bob could disclose their bits α and β publicly, and verify that indeed $\alpha+\beta = \pi_a^g \pmod 2$. To eavesdrop, Eve could try to perform the measurement given by the POVM $\{((\alpha', \beta'), |\alpha', \beta'\rangle_{+,\times}\,{}_{+,\times}\langle\alpha', \beta'|)\}$. Such measurement would allow Eve to learn Alice's bit if the chosen basis is $+$ or Bob's bit if the chosen basis is $\times$. However, it does not help Eve to give the correct index g, and she would fail the test with probability 0.5. The aim of this paper is to prove that there is no measurement that can provide information about the secret number while allowing Eve to pass the test.

So far, we have dealt with an ideal situation in which the legitimate users' source of light are perfect. Unfortunately, all practical implementations of quantum key distribution today use imperfect sources of light. Some sources emit a state which is always, or probabilistically, different from the single-photon state as required above. It is as well possible that the remaining degrees of freedom of the pulses are not perfectly independent of the choice of the polarisation state. Finally, some sources might be vulnerable to the Trojan Horse attacks. In these attacks, an enemy sends into the legitimate source a *probe* to read the settings of the source. If the probing is successful, the enemy does not even have to perform a measurement of the legitimate light pulse to get information about the chosen polarisation.

In this paper we deal with a family of imperfect sources satisfying the following requirements:

- The source succeeds, with non-zero probability, in emitting a single-photon pulse as indicated above and in countering a possible Trojan Horse attack. The other degrees of freedom of the pulse are independent of the choice of the polarisation.

- Suppose the source emits a sequence of light pulses with random and independent choice of polarisation for each pulse. Then each pulse (whether it is correctly emitted or not) is independent of the choices of polarisation for the other pulses. Likewise, the data Eve gets from a successful Trojan Horse attack on one pulse are independent of the choices of polarisation for the other pulses.

It is in practice hard to deal with the extra structure required to describe the imperfect signals and the Trojan probe, especially if one wants to describe them as quantum systems. To solve this technical issue, we adopt in this paper a pessimistic model in which the complete description of these quantum systems is provided *classically* to Eve (this idea was proposed in [30], [31], and [24]). That is, the density operator of the state of these extra quantum systems is given explicitly to Eve. In such a model, we can assume that the only quantum systems Eve receives are the correctly emitted single-photon quantum signals. Indeed, Eve can reconstruct the complete set of quantum signals from these single-photon pulses and the classical data about the remaining signals. This proves that the security following our pessimistic model implies the security of the protocol. This paper incorporates this idea and proves that the protocol is secure even if Eve is given the extra information provided by the imperfect signals.

We now give a formal description of the key distribution protocol.

4. The Protocol. We describe the quantum key distribution considered in this paper, and which was proposed in [5]. The protocol is designed to use classical error-reconciliation schemes like the interactive scheme proposed in [28]. Throughout the paper, all operations on binary numbers are made modulo 2. For any binary number x, $\neg x = 1 + x$.

Protocol setup. Alice and Bob specify:

- m, the length (in bits) of the private key to be generated.
- ε, the maximum threshold value for the error rate during the quantum transmission ($\varepsilon < \frac{1}{4}$).
- τ, a security constant such that $2\varepsilon/(1-\varepsilon) < 2\varepsilon/(1-\varepsilon) + \tau < 1$.
- p_L, the maximum threshold value for the proportion of leaked signals in the reconciled key.
- τ_L, a security constant such that $p_L < p_L + \tau_L < 1$.
- The security parameter r. It must be large enough so that Alice and Bob can find a binary matrix K of size $m \times r$ such that whenever one removes any $(p_L + \tau_L)r$ (or less) columns from K, the resulting matrix $\hat{K}$ obeys $\min_{\vec{x} \in \{0,1\}^m \setminus \vec{0}} (w(\vec{x}^T \hat{K})) \geq w_{\min}$ where $w_{\min} = (2\varepsilon/(1-\varepsilon) + \tau)\, r$. For any vector $\vec{y}$, $w(\vec{y})$ is the weight of $\vec{y}$, that is, the number of non-zero entries in $\vec{y}$. The problem of finding such matrices is a classical combinatorial one, closely related to the theory of linear error-correcting codes, and is not discussed in this proof. Nevertheless, the reader can refer to [15] and [24] for a technique proposed by Mayers to generate such matrices randomly, although more efficient techniques might exist.

- An error reconciliation scheme between Alice and Bob such that:
  — it tells, with high probability of correctness, whether more than εs errors are present in a string of s bits, where $s = \lfloor r/(1-\varepsilon) \rfloor$,
  — if there are less than εs errors in the string, the scheme corrects these errors, at least with high probability of success,
  — only positions of the errors are possibly disclosed publicly. In particular the scheme should disclose no information about parities of the reconciled string.

  The error reconciliation can be a probabilistic scheme for which an upper bound on the probability of failure can be specified by Alice and Bob. One can achieve such a task by first estimating the error rate on a small randomly chosen proportion of the string and then by using for instance the interactive error-reconciliation scheme proposed in [28]. In these processes, the exchanged parities or bits should be encrypted with the one-time pad method [9], [12]. This technique requires that Alice and Bob share beforehand a secret key for error-correction for the one-time pad encryption. According to Shannon's coding theorem, for asymptotic values of s, such probabilistic error-reconciliation is possible if Alice and Bob share a previously shared error-correction key of length
  $$q \geq sh(\varepsilon).$$
- n, the number of pairs of photons to be sent by the legitimate parties. A good choice for n is $\lceil r/(p_D(1-\varepsilon)/2 - \tau_S) \rceil$ where τ_S is a small but strictly positive constant and p_D is the probability that Eve detects the signals sent by Alice and Bob.
- An authentication algorithm [32] that ensures the authenticity of public communication, together with a previously shared authentication key.

The protocol requires that Alice and Bob share beforehand a secret random stream of bits that will be used as the keys for error-correction and authentication.

This stream of bits can be taken from a private key generated in a previous key distribution session. As no key distribution is perfect, it is conceivable that such a key is neither completely random nor private. However, in this paper, we adopt the simplifying assumption that the previously shared keys for error-correction and authentication have been generated with perfect randomness and privacy.

These previously shared secret bits must be discarded after use. The protocol is however expected to generate more secret bits than it consumes.

Quantum transmission.

- Alice's setup and Bob's setup perform the following tasks:
  1. Alice's setup returns a string of n choices of basis $\vec{a} \in \{+, \times\}^n$ and a string of n bits $\vec{\alpha} \in \{0, 1\}^n$. These bases and bits are picked randomly with independent and uniform distribution.
  2. Bob's setup returns a string of n choices of basis $\vec{b} \in \{+, \times\}^n$ and a string of n bits $\vec{\beta} \in \{0, 1\}^n$. These bases and bits are picked randomly with independent and uniform distribution, and independently of Alice's choices.
  3. Eve receives n signals from Alice and Bob's setups. These signals are classed in three categories: $\{1, \ldots, n\}$ is partitioned into three disjoint subsets V, N and L.
     — An index i in V corresponds to a *vacuum* instance in which Eve did not receive anything from at least one of Alice's or Bob's setups. That is, one of the setups has not emitted any photon and was not probed successfully by Eve.

— An index i in N corresponds to a *normal* instance in which Eve receives only a single photon in the polarisation state $|\alpha_i\rangle_{a_i}$ from Alice's setup and a single photon in the polarisation state $|\beta_i\rangle_{b_i}$ from Bob's setup. Eve did not succeed in probing any of the setups.
— An index i in L corresponds to a *leaking* instance in which: (1) one of the setups has been probed or emitted more than one photon and (2) the other setup has been probed or emitted at least one photon.

The partition (V, N, L) might not be known by Alice or Bob. Besides, the probability distribution for this partition can be arbitrary and influenced by Eve. The only constraints are that: (1) this partition is independent of $\vec{a}$, $\vec{b}$, $\vec{\alpha}$ and $\vec{\beta}$, (2) for any $i \in V \cup L$, the ith signal is independent of the jth bases and bits for any $j \neq i$ and (3) the setups perform a test that guarantees, at least with high probability, that the size of the leaked and reconciled set $L \cap R$ is smaller than $(\tau_L + p_L)r$.

- The n signals received by Eve are considered as constituting a single quantum system. Eve executes a measurement on this system and announces the *detected* subset D and a string $\vec{g} \in \{0, 1, 2, 3\}^d$, where $d = |D|$ is the size of D. Eve should choose $(D, \vec{g})$ so that: (1) D corresponds to the set of instances in which Eve received at least one photon from each setup and (2) for each index $i \in D$, g_i corresponds to the outcome of the Bell measurement on the pair formed by one of Alice's photons and one of Bob's photons in the ith signal. However, Eve need not be honest and could perform any general measurement she desires on all the signals considered as a single quantum system.

Sifting. We denote by $\vec{a} = (a_1, a_2, \ldots, a_n), \vec{b} = (b_1, b_2, \ldots, b_n), \vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$ the outcomes of the quantum transmission. For any vector $\vec{y} = (y_1, y_2, \ldots, y_n)$ in $\{0, 1\}^n$ or $\{+, \times\}^n$, and for any subset X of $\{1 \cdots n\}$, we denote by y_X the restriction of $\vec{y}$ on X.

Alice and Bob compare publicly their bases $\vec{a}$ and $\vec{b}$. We denote by $\vec{p}$ the vector in $\{0, 1\}^n$ such that for any $i \in \{1 \cdots n\}$, $p_i = 1$ if and only if $a_i = b_i$. If the number of indexes $i \in D$ such that $a_i = b_i$ is greater than, or equal to s (i.e. $w(\vec{p}_D) \geq s$), then the *sifted set* S is defined as the set of the first s such indexes. Otherwise the validation test is failed. The bit strings α_S and $\beta_S + \pi_{a_S}^{g_S}$ are usually referred to as the *sifted keys*. They should be identical if the Eve performed the Bell measurement exactly as described above.

Error correction. Alice and Bob perform the error correction on their sifted keys α_S and $\beta_S + \pi_{a_S}^{g_S}$ as specified in the protocol setup. We define the *error set* E as the set of indexes in S in which an error is found, that is, $\alpha_i \neq \beta_i + \pi_{a_i}^{g_i}$. Likewise, we define the *error vector* $\vec{e}$ as the vector in $\{0, 1\}^s$ giving the positions of the errors ($\forall i \in S$, $e_i = 1$ if and only if $\alpha_i \neq \beta_i + \pi_{a_i}^{g_i}$). We denote by e the size of the set E, i.e. $e = |E| = w(\vec{e})$. The validation test is passed if $e < \varepsilon s$, otherwise it is failed. If the validation test is passed, then Alice and Bob define the *reconciled set* R as the set of the first r indexes $i \in S \backslash E$. (Note that $|S \backslash E| \geq r$ if the validation test is passed.) Therefore $|R| = r$ and $\forall i \in R$, $a_i = b_i$ and $\alpha_i = \beta_i + \pi_{a_i}^{g_i}$. Alice and Bob obtain, at least with high probability, an identical string of bits $\alpha_R \in \{0, 1\}^r$, called the *reconciled key*.

Privacy amplification. The private key is defined as:

1. $\vec{\kappa} = K\alpha_R$ if the validation test is passed.
2. An m-bit string $\vec{\kappa}$ picked randomly by Alice with uniform probability distribution each time the validation test is failed.

Authentication. If the validation test is passed, Alice and Bob authenticate all the exchanged classical messages. The protocol is successfully completed upon satisfactory authentication for both legitimate parties.

If successfully completed, the protocol generate m secret shared bits. It also consumes from a previously shared secret key $n_e \simeq sh(\varepsilon)$ bits for error-correction and n_a bits for authentication. The *net key creation rate* is defined as $(m - n_e - n_a)/r$. For large values of r, using the authentication algorithm proposed in [32], one obtains that n_a is negligible compared with r. Using Mayers' technique [15], one obtains the lower-bound

$$\frac{m}{r} \geq (1 - p_L)\left(1 - h\left(\frac{2\varepsilon}{(1-\varepsilon)(1-p_L)}\right)\right),$$

although this bound might not be tight. We therefore obtain the following lower bound for the net key creation rate for large values of r:

$$\frac{m - n_e - n_a}{r} \geq (1 - p_L)\left(1 - h\left(\frac{2\varepsilon}{(1-\varepsilon)(1-p_L)}\right)\right) - \frac{1}{1-\varepsilon}h(\varepsilon).$$

5. Privacy of the Protocol

PROPERTY 1. *The protocol described above offers perfect privacy*: *for any eavesdropping strategy chosen by Eve, the conditional entropy of the private key* $\vec{\kappa}$, *given Eve's view* $\boldsymbol{v}$, *is bounded from below by*

$$H(\vec{\kappa} \mid \boldsymbol{v}) \geq m - 2\left(m + \frac{1}{\ln 2}\right)\left(\theta(r) + 2\sqrt{\theta(r)}\right),$$

where

$$\theta(r) = 2^{-[1-h(1/2-(3/16)\tau)](\tau/2)r},$$

and where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ *is the Shannon binary entropy.*

6. Proof of the Privacy

6.1. *Notations*

Conventions. For any subset A of $\{1 \cdots n\}$, we denote by $\hat{A}$ the intersection $A \cap N$ where N is the normal set defined previously. We denote by $\check{A}$ the intersection $A \cap L$ where L is the leaked set.

For any vector $\vec{y}$, we denote by $\hat{y}$ the restriction of $\vec{y}$ on the normal set N. For any vector $\vec{y}$ and any subset X of $\{1 \cdots n\}$, $\hat{y}_X$ is the restriction of $\vec{y}$ on the intersection $\hat{X} = X \cap N$.

Likewise, for any vector $\vec{y}$, we denote by $\check{y}$ the restriction of $\vec{y}$ on the leaked set L.

Given the partition (V, N, L), we denote by $\hat{K}$ the matrix formed by removing columns of the matrix K corresponding to the indexes in $\check{R}$ (therefore $\hat{K}$ is an $m \times \hat{r}$ matrix). Likewise we denote by $\check{K}$ the matrix formed by removing columns of K corresponding to the indexes in $\hat{R}$.

For any vector $\vec{x}$ and any symbol A, $w(\vec{x})$ is the number of non-zero entries, and $w_A(\vec{x})$ is the number of entries with symbol A.

Classical data. We denote by $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e})$ the data that are publicly announced during the protocol. Recall that specifying $\vec{a}$ and $\vec{p}$ is equivalent to specifying $\vec{a}$ and $\vec{b}$.

We denote by $\mathcal{P}$ the set of all possible public announcements for which the validation test is passed. That is,

$$\mathcal{P} = \{P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e})\colon\ w(\vec{p}_D) \geq s \text{ and } e < \varepsilon s\}.$$

Finally, we denote by T the subset $S \backslash (E \cup R)$, and by t the size of T.

The size of the sets N, $\hat{S}$, $\hat{R}$ and $\hat{T}$ are denoted by $\hat{n}$, $\hat{s}$, $\hat{r}$ and $\hat{t}$, respectively.

More on Bell states. Given a basis $a \in \{+, \times\}$, and a Bell index $g \in \{0, 1, 2, 3\}$, we define the set X_a^g as the set of indexes of the two Bell states that have the parity π_a^g in basis a. For any subset A of $\hat{S}$, the notation $X_{a_A}^{g_A}$ stands for the Cartesian product $\{c_A \in \{0, 1, 2, 3\}^A\colon\ \forall i \in A, c_i \in X_{a_i}^{g_i}\}$. Given $\hat{R}$, $\hat{a}_R$ and $\hat{g}_R$, for any $\hat{c}_R \in X_{\hat{a}_R}^{\hat{g}_R}$, we define the binary vector $\vec{\gamma} \in \{0, 1\}^{\hat{r}}$ by: $\forall i \in \hat{R}$, $\gamma_i = \sigma_{\hat{a}_i}^{\hat{g}_i} + \sigma_{\hat{a}_i}^{\hat{c}_i}$. That is, $\gamma_i = 0$ if $\hat{c}_i = \hat{g}_i$, otherwise, $\gamma_i = 1$.

Given a basis $a \in \{+, \times\}$, and a Bell index $g \in \{0, 1, 2, 3\}$, we define the set Y_a^g as the set of indexes of the two Bell states that have parity $\neg\pi_a^g$ in basis a. As previously, $Y_{a_A}^{g_A}$ stands for the Cartesian product $\{c_A \in \{0, 1, 2, 3\}^A\colon\ \forall i \in A, c_i \in Y_{a_i}^{g_i}\}$.

6.2. *Dealing with Imperfect Sources and Signal Losses.* For a practical protocol, in most of the cases the detected set D is smaller than the union of the normal set N and the leaked set L. We assume in this paper that we always have $d \leq |N| + |L|$. We suppose that Eve has complete control of both channels connecting the source to Eve. To prove unconditional security of the protocol, we have to deal with the situation in which Eve has no technological limitation. In such a case, Eve would be lying if she declares a set D that is strictly smaller than $N \cup L$. We adopt the worst-case scenario in which the complete description of the signal is given classically to Eve for any signal in L at the time of its emission. In particular, for any $i \in L$, we assume that Eve knows $(a_i, \alpha_i, b_i, \beta_i)$ before she performs any measurement on the system. Therefore, for any $i \in L$, Eve can always announce the Bell index g_i that passes the test, if $i \in S$.

In comparison, for any $i \in V$, no measurement on the ith signal will help Eve find the correct Bell index to pass the test. Eve can only guess the correct index, and she has probability $1/2$ to give a correct guess. When the chosen bases (a_i, b_i) are known, Eve can perform a measurement on the signal to get Alice's or Bob's ith bit. Note that Eve can always perform the same strategy on any signal in N. We adopt the worst-case

scenario in which Eve gets a complete classical description of the quantum signal in V at the time of its emission. However, note that for signals in V, Eve does not receive anything from at least one source.

Therefore the best strategy for Eve is to announce a set D such that $L \subset D$ and $V \cap D = \emptyset$, while $|D|$ is big enough so that the validation test is passed. In the following part of the paper we assume that Eve follows this strategy regarding the choice of D and that Eve gets a complete description of signals in $L \cup V$. We also assume that Eve does not introduce any error in $L \cap S$ (since this can only increase the number of detected errors, without any compensation for Eve).

6.3. *Model of Measurements*. We have adopted the worst-case scenario in which the complete description of the signal is given classically to Eve for signals in $V \cup L$ at the time of their emission. We denote by $\boldsymbol{A}$ the random variable giving collectively the partition (V, N, L) and the complete description of the signals in $V \cup L$. In particular, $\boldsymbol{A}$ gives $\boldsymbol{L}$ and Alice's and Bob's data on $\boldsymbol{L}$: $(\check{\boldsymbol{a}}, \check{\boldsymbol{b}}, \check{\boldsymbol{\alpha}}, \check{\boldsymbol{\beta}})$. We denote by $\mathcal{A}$ the set of all possible values taken by the random variable $\boldsymbol{A}$. Given the classical data A and the quantum signals on N, Eve can reconstruct the entire sequence of quantum signals on $\{1 \cdots n\}$. Therefore we can assume that Eve gets A and receives only the quantum signals in N: this additional assumption has no consequence for the security of the protocol, as Eve is assumed to have no technological limitation. We have seen that Eve chooses the officially detected set D such that $L \subset D$ and $V \cap D = \emptyset$. We denote by $\mathcal{D}_A$ the set of all possible subsets $D \subset \{1 \cdots n\}$ obeying these conditions. Besides, we have assumed that Eve does not introduce any errors on L, i.e. Eve chooses $\vec{g}$ so that $\check{g}$ does not cause any detected error on $L \cap S$ (there are two choices for g_i for each $i \in L$ that does not cause error). We denote by G_A the set of all possible $\vec{g} \in \{0, 1\}^d$ that do not cause any error on L.

Eve gets the classical extra data A with probability $\mathrm{P}_{\boldsymbol{A}}(A)$. Given that $\boldsymbol{A} = A$, for any $(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}') \in \left(\{+, \times\}^{\hat{n}}\right)^2 \times \left(\{0, 1\}^{\hat{n}}\right)^2$, Alice and Bob choose the bases $\hat{a}'$, $\hat{b}'$ and the bitstreams $\hat{\alpha}'$, $\hat{\beta}'$ on the normal set N with probability $\mathrm{P}_{\hat{\boldsymbol{a}}\hat{\boldsymbol{b}}}(\hat{a}', \hat{b}')\mathrm{P}_{\hat{\alpha}\hat{\beta}}(\hat{\alpha}', \hat{\beta}') = (1/2^{\hat{n}})(1/2^{\hat{n}})\mathrm{P}_{\hat{\boldsymbol{a}}\hat{\boldsymbol{b}}}(\hat{a}', \hat{b}')$. Recall that $\boldsymbol{A}$ is indeed independent of $(\hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \hat{\boldsymbol{\alpha}}, \hat{\boldsymbol{\beta}})$.

Given that Eve got $\boldsymbol{A} = A$ and that Alice and Bob chose $(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}')$, then for any subset $D \in \mathcal{D}_A$ and $\vec{g} \in G_A$, the probability that Eve announces the set D and the string $\vec{g}$ reads

$$\mathrm{P}_{\boldsymbol{D}\vec{\boldsymbol{g}}|\boldsymbol{A}=A,\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(D, \vec{g}) = \mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A}|\hat{\alpha}', \hat{\beta}'\rangle_{\hat{a}'\hat{b}'\,\hat{a}'\hat{b}'}\langle\hat{\alpha}', \hat{\beta}'|\right], \tag{1}$$

where $\{F_{D\vec{g}|\boldsymbol{A}=A}\}_{D\in\mathcal{D}_A,\vec{g}\in G_A}$ is the positive operator-valued measure describing the general measurement Eve performs to find $\boldsymbol{D}$ and $\vec{\boldsymbol{g}}$, given that Eve found $\boldsymbol{A} = A$. We have $\sum_{D\in\mathcal{D}_A,\vec{g}\in G_A} F_{D\vec{g}|\boldsymbol{A}=A} = \mathbf{1}_N$, where $\mathbf{1}_N$ is the identity operator acting on the Hilbert space describing the signals in the normal set N. Recall indeed that Eve receives only the quantum signals in N.

After Eve announced D and $\vec{g}$, Alice and Bob announce publicly their bases $\vec{a}$, $\vec{b}$, and compute $\vec{p}$ and S. Then they run the error correction on S and find R, T and E, which are publicly announced. Let $\mathcal{P}_A$ be the set of all values for P that are compatible with A. (Remember that A gives Alice's and Bob's classical data on L and partially on V. The set $\mathcal{P}_A$ refers to the values for $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e})$ such that D, $\check{g}$, $\vec{a}_{V\cup L}$, $\vec{b}_{V\cup L}$

and $\vec{e}$ are compatible with A. In particular, $D \in \mathcal{D}_A$, $\vec{g} \in G_A$ and $\check{e} = \vec{0}$.) In knowledge of A and of these publicly announced values $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e}) \in \mathcal{P}_A$, Eve performs a second general measurement on the quantum system. This second measurement can of course be conditioned on $\boldsymbol{A}$ and $\boldsymbol{P}$. All these data Eve gets during the protocol are collectively denoted by v. We denote by $\mathcal{V}_{A,P}$ the set of views v that are compatible with Eve receiving the description A and the public announcement P.

Given that Eve got A and Alice and Bob chose $(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}')$ on the normal set N, the probability that $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e}) \in \mathcal{P}_A$ is announced publicly and that Eve finds $v \in \mathcal{V}_{A,P}$ reads

$$(2)\quad \mathrm{P}_{\boldsymbol{v}|\boldsymbol{A}=A,\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(v) = \delta_{\hat{a},\hat{a}'}\delta_{\hat{p},\neg(\hat{a}'+\hat{b}')}\delta_{\hat{e},\hat{\alpha}'_S+\hat{\beta}'_S+\pi^{\hat{g}_S}_{\hat{a}_S}} \mathrm{Tr}\left[|\chi_{v|AP}\rangle\langle\chi_{v|AP} \mid \hat{\alpha}', \hat{\beta}'\rangle_{\hat{a}\hat{b}\,\hat{a}\hat{b}}\langle\hat{\alpha}', \hat{\beta}'|\right],$$

where the POVM describing the general measurement Eve performs, given that $\boldsymbol{A} = A$, to find $\boldsymbol{P} \in \mathcal{P}_A$ and $\boldsymbol{v} \in \mathcal{V}_{A,P}$ is denoted by $\{|\chi_{v|AP}\rangle\langle\chi_{v|AP}|\}_{v\in\mathcal{V}_{A,P}}$ (we have assumed without loss of generality that these positive operators were of rank one). We have $\sum_{v\in\mathcal{V}_{A,P}} |\chi_{v|AP}\rangle\langle\chi_{v|AP}| = F_{D\vec{g}|\boldsymbol{A}=A}$.

The conditional probability, given $\boldsymbol{A} = A$, that Eve announces $P \in \mathcal{P}_A$ and gets the view $v \in \mathcal{V}_{A,P}$ is the sum over $(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}') \in \left(\{+, \times\}^{\hat{n}}\right)^2 \times \left(\{0, 1\}^{\hat{n}}\right)^2$ of the above conditional probability weighted with probability $\mathrm{P}_{\hat{\boldsymbol{a}}\hat{\boldsymbol{b}}\hat{\alpha}\hat{\beta}}(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}')$, that is,

$$\begin{aligned}\mathrm{P}_{\boldsymbol{v}|\boldsymbol{A}=A}(v) &= \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{\alpha}',\hat{\beta}':\\ \hat{e}=\hat{\alpha}'_S+\hat{\beta}'_S+\pi^{\hat{g}_S}_{\hat{a}_S}}} \mathrm{Tr}\left[|\chi_{v|AP}\rangle\langle\chi_{v|AP} \mid \hat{\alpha}', \hat{\beta}'\rangle_{\hat{a}\hat{b}\,\hat{a}\hat{b}}\langle\hat{\alpha}', \hat{\beta}'|\right] \\ &= \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R\in X^{\hat{g}_R}_{\hat{a}_R},\\ \hat{c}_T\in X^{\hat{g}_T}_{\hat{a}_T},\\ \hat{c}_E\in Y^{\hat{g}_E}_{\hat{a}_E}}} \langle\hat{c}|\chi_{v|AP}\rangle\langle\chi_{v|AP}|\hat{c}\rangle,\end{aligned}$$

where we have used the identities $|0, \pi^{g_i}_{a_i}\rangle_{a_i\,a_i}\langle 0, \pi^{g_i}_{a_i}| + |1, \neg\pi^{g_i}_{a_i}\rangle_{a_i\,a_i}\langle 1, \neg\pi^{g_i}_{a_i}| = \sum_{c\in X^{g_i}_{a_i}} |c\rangle\langle c|$ and $|0, \neg\pi^{g_i}_{a_i}\rangle_{a_i\,a_i}\langle 0, \neg\pi^{g_i}_{a_i}| + |1, \pi^{g_i}_{a_i}\rangle_{a_i\,a_i}\langle 1, \pi^{g_i}_{a_i}| = \sum_{c\in Y^{g_i}_{a_i}} |c\rangle\langle c|$ for any $i \in \hat{S}$. Naturally, the marginal probability that Eve gets A, announces $P \in \mathcal{P}_A$ and finds $v \in \mathcal{V}_{A,P}$ is $\mathrm{P}_{\boldsymbol{v}}(v) = \mathrm{P}_{\boldsymbol{A}}(A)\mathrm{P}_{\boldsymbol{v}|\boldsymbol{A}=A}(v)$.

The conditional probability, given $\boldsymbol{A} = A$, that $P \in \mathcal{P}_A$ is publicly announced, Eve gets the view $v \in \mathcal{V}_{A,P}$ and that Alice and Bob get the private key $\vec{\kappa}$ is the sum over $(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}') \in \left(\{+, \times\}^{\hat{n}}\right)^2 \times \left(\{0, 1\}^{\hat{n}}\right)^2$ of (2) weighted with the probability

$$\mathrm{P}_{\hat{\boldsymbol{a}}\hat{\boldsymbol{b}}\hat{\alpha}\hat{\beta}}(\hat{a}', \hat{b}', \hat{\alpha}', \hat{\beta}')\mathrm{P}_{\vec{\kappa}|\boldsymbol{v}=v,\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(\vec{\kappa}),$$

where $\mathrm{P}_{\vec{\kappa}|\boldsymbol{v}=v,\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(\vec{\kappa})$ is one if and only if $\check{\alpha}_R$, given by A and $\hat{\alpha}'_R$ yield the private key $\vec{\kappa}$, i.e. $\hat{K}\hat{\alpha}'_R = \tilde{\kappa}$ where $\tilde{\kappa}$ is a shorthand notation for $\vec{\kappa} + \check{K}\check{\alpha}_R$. Otherwise

this conditional probability is zero:

$$\begin{aligned}
\mathrm{P}_{\vec{\kappa}\boldsymbol{\nu}|\boldsymbol{A}=A}(\vec{\kappa},\nu) &= \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{\alpha}',\hat{\beta}':\\ \hat{e}=\hat{\alpha}'_S+\hat{\beta}'_S+\pi_{\hat{a}_S}^{\hat{g}_S}\\ \hat{K}\hat{\alpha}'_R=\tilde{\kappa}}} \mathrm{Tr}\left[|\chi_{\nu|AP}\rangle\langle\chi_{\nu|AP}\mid\hat{\alpha}',\hat{\beta}'\rangle_{\hat{a}\hat{b}\,\hat{a}\hat{b}}\langle\hat{\alpha}',\hat{\beta}'|\right]\\
&= \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c},\hat{c}'\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R,\hat{c}'_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T,\hat{c}'_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\hat{c}'_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \delta_{\hat{c}_{\bar{R}},\hat{c}'_{\bar{R}}}\langle\hat{c}'|\chi_{\nu|AP}\rangle\langle\chi_{\nu|AP}|\hat{c}\rangle\\
&\quad\times \sum_{\substack{\hat{\alpha}'_R\in\{0,1\}^{\hat{r}}\\ \hat{K}\hat{\alpha}'_R=\tilde{\kappa}}} \langle\hat{c}_R|\hat{\alpha}'_R,\hat{\alpha}'_R+\pi_{\hat{a}_R}^{\hat{g}_R}\rangle_{\hat{a}_R\,\hat{a}_R}\langle\hat{\alpha}'_R,\hat{\alpha}'_R+\pi_{\hat{a}_R}^{\hat{g}_R}|\hat{c}'_R\rangle.
\end{aligned}$$

We have seen that the validation test is passed if and only if $|S|\geq s$ and $|E|<\varepsilon s$. The marginal probability that Eve passes the test is therefore the sum over $A\in\mathcal{A}$, $D\in\mathcal{D}_A$, $\vec{g}\in G_A$ and $(\hat{a}',\hat{b}',\hat{\alpha}',\hat{\beta}')\in\left(\{+,\times\}^{\hat{n}}\right)^2\times\left(\{0,1\}^{\hat{n}}\right)^2$ of (1) weighted with the probability

$$\mathrm{P}_{\boldsymbol{A}}(A)\mathrm{P}_{\hat{\boldsymbol{a}}\hat{\boldsymbol{b}}\hat{\alpha}\hat{\beta}}(\hat{a}',\hat{b}',\hat{\alpha}',\hat{\beta}')\mathrm{P}_{\mathbf{valid}|\boldsymbol{A}=A,\boldsymbol{D}=D,\vec{\boldsymbol{g}}=\vec{g},\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(\mathrm{true}),$$

where $\mathrm{P}_{\mathbf{valid}|\boldsymbol{A}=A,\boldsymbol{D}=D,\vec{\boldsymbol{g}}=\vec{g},\hat{\boldsymbol{a}}=\hat{a}',\hat{\boldsymbol{b}}=\hat{b}',\hat{\alpha}=\hat{\alpha}',\hat{\beta}=\hat{\beta}'}(\mathrm{true})$ is one if and only if:

- $w(\hat{p}'_D)+w(\check{p}_D)\geq s$ where $\check{p}_D$ is given by A and D (recall that $V\cap D=\emptyset$), and
- $w(\hat{\alpha}'_S+\hat{\beta}'_S+\pi_{\hat{a}'_{\hat{S}'}}^{\hat{g}_{\hat{S}'}})<\varepsilon s$ (recall that Eve does not introduce any error on L, and that $S\cap L=\emptyset$),

and zero otherwise. That is,

$$\begin{aligned}
\mathrm{P}_{\mathbf{valid}}(\mathrm{true}) &= \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{D\in\mathcal{D}_A}\sum_{\substack{\hat{a}',\hat{p}'\in\{0,1\}^{\hat{n}}\\ w(\hat{p}'_D)\geq s-w(\check{p}_D)}}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a}')\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}')\\
&\quad\times\sum_{\hat{\alpha}',\hat{\beta}'}\sum_{\substack{\vec{g}\in G_A:\\ w(\hat{\alpha}'_{S'}+\hat{\beta}'_{S'}+\pi_{\hat{a}'_{S'}}^{\hat{g}_{S'}})<\varepsilon s}}\mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A}|\hat{\alpha}',\hat{\beta}'\rangle_{\hat{a}'\hat{b}'\,\hat{a}'\hat{b}'}\langle\hat{\alpha}',\hat{\beta}'|\right]\\
&= \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p})\sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}}\langle\hat{c}|F_{D\vec{g}|\boldsymbol{A}=A}|\hat{c}\rangle.
\end{aligned}$$

6.4. *The Role of the Validation Test*

PROPERTY 2. *For any* $(A, D, \vec{p}, \vec{g}, \vec{e})$, *define the operator acting on the Hilbert space of the* $\hat{n}$ *pairs of photons by*

$$\Pi_{\hat{R}}^{\vec{g}} = \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ d(\hat{c}_R,\hat{g}_R)\geq w_{\min}/2}} |\hat{c}\rangle\langle\hat{c}| = \mathbf{1}_{N\cap\overline{R}} \otimes \sum_{\substack{\hat{c}_R\in\{0,1,2,3\}^{\hat{r}}:\\ d(\hat{c}_R,\hat{g}_R)\geq w_{\min}/2}} |\hat{c}_R\rangle\langle\hat{c}_R|.$$

Then for any $A \in \mathcal{A}$, *the following inequality holds*:

$$\sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}} \mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \langle\hat{c}|\Pi_{\hat{R}}^{\vec{g}} F_{D\vec{g}|\boldsymbol{A}=A} \Pi_{\hat{R}}^{\vec{g}}|\hat{c}\rangle \leq \theta(r),$$

where

$$\theta(r) = 2^{-[1-h(1/2-(3/16)\tau)](\tau/2)r}.$$

The property tells that $F_{D\vec{g}|\boldsymbol{A}=A}$ should be "close" to the honest operator corresponding to the Bell state measurement if Eve wants to pass the validation test with non-negligible probability.

PROOF. The expression above reads

$$\sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}} \mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \langle\hat{c}|\Pi_{\hat{R}}^{\vec{g}} F_{D\vec{g}|\boldsymbol{A}=A} \Pi_{\hat{R}}^{\vec{g}}|\hat{c}\rangle$$

$$= \sum_{D\in\mathcal{D}_A} \sum_{\hat{p}:\ w(\hat{p})\geq s-w(\check{p})} \sum_{\vec{g}\in G_A} \frac{1}{4^{\hat{n}}} \mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p})$$

$$\times \mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A} \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \Pi_{\hat{R}}^{\vec{g}} \sum_{\hat{a}} \mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} |\hat{c}\rangle\langle\hat{c}|\Pi_{\hat{R}}^{\vec{g}} \right].$$

For any $g \in \{0, 1, 2, 3\}$, let U_g be the unitary operator acting on the Hilbert space of a pair of photons defined on the Bell basis as follows:

$$\begin{aligned}
U_g|0\rangle &= |g\rangle \\
U_g|1\rangle &\text{ is the Bell state with parity } \pi_+^g \text{ and phase } \neg\sigma_+^g, \\
U_g|2\rangle &\text{ is the Bell state with parity } \neg\pi_+^g \text{ and phase } \sigma_+^g, \\
U_g|3\rangle &\text{ is the Bell state with parity } \neg\pi_+^g \text{ and phase } \neg\sigma_+^g.
\end{aligned}$$

Note that $(U_g)^{-1} = U_g$. Remarking further that

$$\begin{aligned}
X_+^g &= \{U_g|0\rangle, U_g|1\rangle\}, \\
X_\times^g &= \{U_g|0\rangle, U_g|2\rangle\}, \\
Y_+^g &= \{U_g|2\rangle, U_g|3\rangle\}, \\
Y_\times^g &= \{U_g|1\rangle, U_g|3\rangle\},
\end{aligned}$$

we have, for any $(A, D, \vec{p}, \vec{g})$,

$$\begin{aligned}
&\mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A} \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \Pi_{\hat{R}}^{\vec{g}} \sum_{\hat{a}} \mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}: \\ \hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R}, \\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T}, \\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} |\hat{c}\rangle\langle\hat{c}| \Pi_{\hat{R}}^{\vec{g}} \right] \\
&\quad = \mathrm{Tr}\left[U_{\hat{g}} F_{D\vec{g}|\boldsymbol{A}=A} U_{\hat{g}} \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \Pi_{\hat{R}} \left(\mathbf{1}_{N\cap\overline{S}} \otimes_{i\in\hat{E}} Y_i \otimes_{j\in\hat{T}} X_j \otimes_{k\in\hat{R}} X_k \right) \Pi_{\hat{R}} \right],
\end{aligned}$$

where

$$\Pi_{\hat{R}} = U_{\hat{g}} \Pi_{\hat{R}}^{\vec{g}} U_{\hat{g}} = \mathbf{1}_{N\cap\overline{R}} \otimes \sum_{\hat{c}_R:\ w(\hat{c}_R)\geq w_{\min}/2} |\hat{c}_R\rangle\langle\hat{c}_R|,$$

and

$$\begin{aligned}
X_i &= |0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| + \tfrac{1}{2}|2\rangle\langle 2|, \\
Y_i &= |3\rangle\langle 3| + \tfrac{1}{2}|1\rangle\langle 1| + \tfrac{1}{2}|2\rangle\langle 2|.
\end{aligned}$$

We are going to show that for any $(A, D, \vec{p})$, the eigenvalues of the non-negative Hermitian operator

$$Q_{A,D,\vec{p}} = \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \Pi_{\hat{R}} \left(\mathbf{1}_{N\cap\overline{S}} \otimes_{i\in\hat{E}} Y_i \otimes_{j\in\hat{T}} X_j \otimes_{k\in\hat{R}} X_k \right) \Pi_{\hat{R}}$$

$$= \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \mathbf{1}_{N\cap\bar{S}} \otimes_{i\in\hat{E}} Y_i \otimes_{j\in\hat{T}} X_j \otimes \left(\sum_{\substack{\hat{c}_R\in\{0,1,2\}^{\hat{r}}: \\ w(\hat{c}_R)\geq w_{\min}/2}} \frac{|\hat{c}_R\rangle\langle\hat{c}_R|}{2^{w_1(\hat{c}_R)+w_2(\hat{c}_R)}} \right)$$

are bounded from above by $\theta(r)$. The operator $Q_{A,D,\vec{p}}$ is diagonal in the Bell basis $|\hat{c}\rangle$. Given a vector $\hat{c} \in \{0, 1, 2, 3\}^{\hat{n}}$ and an error vector $\hat{e} \in \{0, 1\}^{\hat{s}}$, a necessary condition for the scalar

$$\langle\hat{c}|\Pi_{\hat{R}} \left(\mathbf{1}_{N\cap\overline{S}} \otimes_{i\in\hat{E}} Y_i \otimes_{j\in\hat{T}} X_j \otimes_{k\in\hat{R}} X_k \right) \Pi_{\hat{R}}|\hat{c}\rangle$$

to be non-zero is that, for all $i \in \hat{S}$,

- $\hat{e}_i = 0$ if $\hat{c}_i = 0$,
- $\hat{e}_i = 1$ if $\hat{c}_i = 3$, and
- $w_1(\hat{c}_S) + w_2(\hat{c}_S) \geq e - w_3(\hat{c}_S) + w_{\min}/2$ (otherwise $w(\hat{c}_R)$ is smaller than $w_{\min}/2$).

Let $k = e - w_3(\hat{c}_S)$. Then there are $\binom{w_1(\hat{c}_S)+w_2(\hat{c}_S)}{k}$ vectors $\hat{e}$ of weight e obeying the above conditions provided that $0 \leq k < \varepsilon s - w_3(\hat{c}_S)$ and $k \leq w_1(\hat{c}_S) + w_2(\hat{c}_S) - w_{\min}/2$. Therefore,

$$\langle\hat{c}|Q_{A,D,\vec{p}}|\hat{c}\rangle \leq \frac{1}{2^{w_1(\hat{c}_S)+w_2(\hat{c}_S)}} \sum_{\substack{0\leq k<\varepsilon s-w_3(\hat{c}_S),\ \text{and} \\ k\leq w_1(\hat{c}_S)+w_2(\hat{c}_S)-w_{\min}/2}} \binom{w_1(\hat{c}_S) + w_2(\hat{c}_S)}{k}.$$

Now, $w_{\min}$ is either greater or smaller than $(w_1(\hat{c}_S) + w_2(\hat{c}_S))\,(1 + (\tau/2)(1 - \varepsilon))$.

- If $w_{\min} > (w_1(\hat{c}_S) + w_2(\hat{c}_S))\,(1 + (\tau/2)(1 - \varepsilon))$, then

$$w_1(\hat{c}_S) + w_2(\hat{c}_S) - \frac{w_{\min}}{2} < \frac{1}{2}\left(1 - \frac{\tau}{2}(1-\varepsilon) \right)(w_1(\hat{c}_S) + w_2(\hat{c}_S))$$

and

- if $w_{\min} \leq (w_1(\hat{c}_S) + w_2(\hat{c}_S))\left(1 + \frac{\tau}{2}(1 - \varepsilon)\right)$, then

$$\begin{aligned} \varepsilon s - w_3(\hat{c}_S) &\leq \frac{\varepsilon r}{1-\varepsilon} \\ &= \frac{w_{\min}}{2} - \frac{\tau}{2} r \\ &\leq \frac{1}{2}\left(1 - \frac{\tau}{2}(1-\varepsilon) \right)(w_1(\hat{c}_S) + w_2(\hat{c}_S)), \end{aligned}$$

where we have used $r \geq s(1 - \varepsilon)$ and $s \geq w_1(\hat{c}_S) + w_2(\hat{c}_S)$.

We thus derived that

$$\begin{aligned}\langle\hat{c}|Q_{A,D,\vec{p}}|\hat{c}\rangle &\leq \frac{1}{2^{w_1(\hat{c}_S)+w_2(\hat{c}_S)}} \sum_{0\leq k<\frac{1}{2}(1-(\tau/2)(1-\varepsilon))(w_1(\hat{c}_S)+w_2(\hat{c}_S))} \binom{w_1(\hat{c}_S)+w_2(\hat{c}_S)}{k} \\ &\leq 2^{-[1-h((1/2)(1-(\tau/2)(1-\varepsilon)))](w_1(\hat{c}_S)+w_2(\hat{c}_S))} \\ &\leq 2^{-[1-h(1/2-(3/16)\tau)](\tau/2)r} \\ &= \theta(r),\end{aligned}$$

where we have used the binomial inequality stating that $\sum_{0\leq k<pn}\binom{n}{k} \leq 2^{nh(p)}$ for any positive integer n and $0 \leq p < \frac{1}{2}$. In the last inequality we have used the inequalities $\varepsilon < \frac{1}{4}$ and $w_1(\hat{c}_S) + w_2(\hat{c}_S) \geq w_{\min}/2$ when the above scalar is non-zero. This entails that for any $(A, D, \vec{p}, \vec{g})$,

$$\begin{aligned}&\mathrm{Tr}\left[U_{\hat{g}} F_{D\vec{g}|\boldsymbol{A}=A} U_{\hat{g}} \sum_{\hat{e}:\ w(\hat{e})<\varepsilon s} \Pi_{\hat{R}} \left(\mathbf{1}_{N\cap\overline{S}} \otimes_{i\in\hat{E}} Y_i \otimes_{j\in\hat{T}} X_j \otimes_{k\in\hat{R}} X_k \right) \Pi_{\hat{R}} \right] \\ &\quad\leq \theta(r)\mathrm{Tr}\left[U_{\hat{g}} F_{D\vec{g}|\boldsymbol{A}=A} U_{\hat{g}} \right] \\ &\quad= \theta(r)\mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A} \right].\end{aligned}$$

Thus, for any $A \in \mathcal{A}$,

$$\begin{aligned}&\sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}} \mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a}) \mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}\in\{0,1,2,3\}^{\hat{n}}: \\ \hat{c}_R\in X^{\hat{g}_R}_{\hat{a}_R}, \\ \hat{c}_T\in X^{\hat{g}_T}_{\hat{a}_T}, \\ \hat{c}_E\in Y^{\hat{g}_E}_{\hat{a}_E}}} \langle\hat{c}|\Pi^{\vec{g}}_{\hat{R}} F_{D\vec{g}|\boldsymbol{A}=A} \Pi^{\vec{g}}_{\hat{R}}|\hat{c}\rangle \\ &\quad\leq \sum_{D\in\mathcal{D}_A} \sum_{\hat{p}:\ w(\hat{p})\geq s-w(\check{p})} \mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\vec{g}\in G_A} \frac{1}{4^{\hat{n}}} \theta(r)\,\mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A} \right] \\ &\quad\leq \sum_{D\in\mathcal{D}_A} \sum_{\vec{g}\in G_A} \frac{1}{4^{\hat{n}}} \theta(r)\,\mathrm{Tr}\left[F_{D\vec{g}|\boldsymbol{A}=A} \right] \\ &\quad= \frac{1}{4^{\hat{n}}} \theta(r)\,\mathrm{Tr}\left[\mathbf{1}_N\right] \\ &\quad= \theta(r)\end{aligned}$$

since the identity operator in the last trace acts on a Hilbert space of dimension $4^{\hat{n}}$. This concludes the proof. □

6.5. *Quasi-Independence of the Key and the View*

PROPERTY 3. *For any strategy chosen by Eve, the joint probability distribution of the private key* $\vec{\kappa}$ *and Eve's view* $\boldsymbol{\nu}$ *obeys the following inequality*:

$$\sum_{A\in\mathcal{A}} \mathrm{P}_{\boldsymbol{A}}(A) \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \sum_{v\in\mathcal{V}_{A,P}} \sum_{\vec{\kappa}\in\{0,1\}^m} \left| \mathrm{P}_{\vec{\kappa}\boldsymbol{\nu}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{\nu}}(v) \right| \leq 2\left(\theta(r) + 2\sqrt{\theta(r)}\right).$$

PROOF. For any $\vec{\kappa} \in \{0,1\}^m$, $A \in \mathcal{A}$, $P \in \mathcal{P}\cap\mathcal{P}_A$ and $v \in \mathcal{V}_{A,P}$, we have

$$\begin{aligned}
&\mathrm{P}_{\vec{\kappa}\boldsymbol{\nu}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{\nu}}(v) \\
&= \mathrm{P}_{\boldsymbol{A}}(A)\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c},\hat{c}'\in\{0,1,2,3\}^{\hat{n}}:\\ \hat{c}_R,\hat{c}'_R\in X_{\hat{a}_R}^{\hat{g}_R},\\ \hat{c}_T,\hat{c}'_T\in X_{\hat{a}_T}^{\hat{g}_T},\\ \hat{c}_E\hat{c}'_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \delta_{\hat{c}_{\hat{R}},\hat{c}'_{\hat{R}}} \langle\hat{c}'|\chi_{v|AP}\rangle\langle\chi_{v|AP}|\hat{c}\rangle d_{A,P,\vec{\kappa}}(\hat{c}_R, \hat{c}'_R),
\end{aligned}$$

where

$$d_{A,P,\vec{\kappa}}(\hat{c}_R, \hat{c}'_R) = \sum_{\hat{\alpha}_R:\ \hat{K}\hat{\alpha}_R=\tilde{\kappa}} \langle\hat{c}_R|\hat{\alpha}_R, \hat{\alpha}_R + \pi_{\hat{a}_R}^{\hat{g}_R}\rangle_{\hat{a}_R\,\hat{a}_R}\langle\hat{\alpha}_R, \hat{\alpha}_R + \pi_{\hat{a}_R}^{\hat{g}_R}|\hat{c}'_R\rangle - \frac{1}{2^m}\delta_{\hat{c}_R,\hat{c}'_R}.$$

At this point we use the following lemma:

LEMMA 1. *For any given* $A \in \mathcal{A}$, $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e}) \in \mathcal{P}_A$, *we have*

$$\begin{aligned}
&\forall \hat{c}_R,\ \hat{c}'_R \in X_{\hat{a}_R}^{\hat{g}_R}, \\
&\qquad \langle\hat{c}_R|\hat{\alpha}_R, \hat{\alpha}_R + \pi_{\hat{a}_R}^{\hat{g}_R}\rangle_{\hat{a}_R\,\hat{a}_R}\langle\hat{\alpha}_R, \hat{\alpha}_R + \pi_{\hat{a}_R}^{\hat{g}_R}|\hat{c}'_R\rangle = \frac{(-1)^{(\vec{\nu}+\hat{\alpha}_R)\cdot(\vec{\gamma}'+\vec{\gamma})}}{2^{\hat{r}}},
\end{aligned}$$

where given A, $P = (D, \vec{g}, \vec{a}, \vec{p}, \vec{e})$, $\vec{\nu}$ *is the binary vector in* $\{0,1\}^{\hat{r}}$ *defined by*: $\nu_i = 1$ *if and only if* $\hat{a}_i = \times$ *and* $\pi_{\hat{a}_i}^{\hat{g}_i} = 1$.

PROOF. We have just to show that, for any $i \in \hat{R}$ and any $\hat{c}_i, \hat{c}'_i \in X_{\hat{a}_i}^{\hat{g}_i}$,

$$\langle\hat{c}_i|\alpha_i, \hat{\alpha}_i + \pi_{\hat{a}_i}^{\hat{g}_i}\rangle_{\hat{a}_i\,\hat{a}_i}\langle\alpha_i, \hat{\alpha}_i + \pi_{\hat{a}_i}^{\hat{g}_i}|\hat{c}_i\rangle = \frac{(-1)^{(\nu_i+\hat{\alpha}_i)(\gamma_i'+\gamma_i)}}{2}.$$

Since $\hat{c}_i \in X_{\hat{a}_i}^{\hat{g}_i}$, we have:

$$|\hat{c}_i\rangle = (-1)^{\lambda_{\hat{a}_i}^{\hat{c}_i}}\left[\frac{|0, \pi_{\hat{a}_i}^{\hat{g}_i}\rangle_{\hat{a}_i} + (-1)^{\sigma_{\hat{a}_i}^{\hat{c}_i}}|1, \neg\pi_{\hat{a}_i}^{\hat{g}_i}\rangle_{\hat{a}_i}}{\sqrt{2}}\right]$$

and similarly for $|\hat{c}'_i\rangle$. Thus,

$$\begin{aligned}
&\langle \hat{c}_i \mid \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i}\rangle a_i\, a_i \langle \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i} \mid \hat{c}'_i\rangle \\
&= \frac{(-1)^{\lambda^{\hat{c}_i}_{\hat{a}_i}}}{\sqrt{2}} \left[{}_{\hat{a}_i}\langle 0, \pi^{\hat{g}_i}_{\hat{a}_i} \mid \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i}\rangle_{\hat{a}_i} + (-1)^{\sigma^{\hat{c}_i}_{\hat{a}_i}}\, {}_{\hat{a}_i}\langle 1, \neg\pi^{\hat{g}_i}_{\hat{a}_i} \mid \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i}\rangle_{\hat{a}_i} \right] \\
&\quad \times \frac{(-1)^{\lambda^{\hat{c}'_i}_{\hat{a}_i}}}{\sqrt{2}} \left[{}_{\hat{a}_i}\langle \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i} \mid 0, \pi^{\hat{g}_i}_{\hat{a}_i}\rangle_{\hat{a}_i} + (-1)^{\sigma^{\hat{c}'_i}_{\hat{a}_i}}\, {}_{\hat{a}_i}\langle \hat{\alpha}_i, \hat{\alpha}_i + \pi^{\hat{g}_i}_{\hat{a}_i} \mid 1, \neg\pi^{\hat{g}_i}_{\hat{a}_i}\rangle_{\hat{a}_i} \right] \\
&= \frac{(-1)^{\lambda^{\hat{c}_i}_{\hat{a}_i} + \lambda^{\hat{c}'_i}_{\hat{a}_i}}}{2} (-1)^{(\sigma^{\hat{c}_i}_{\hat{a}_i} + \sigma^{\hat{c}'_i}_{\hat{a}_i})\hat{\alpha}_i} \\
&= \frac{(-1)^{(\nu_i + \hat{\alpha}_i)(\gamma'_i + \gamma_i)}}{2},
\end{aligned}$$

which concludes the proof. □

Using this lemma, we get, for any $\hat{c}_R$ and $\hat{c}'_R$ in $X^{\hat{g}_R}_{\hat{a}_R}$,

$$d_{A,P,\vec{\kappa}}(\hat{c}_R, \hat{c}'_R) = \sum_{\hat{\alpha}_R:\ \hat{K}\hat{\alpha}_R = \tilde{\kappa}} \frac{(-1)^{(\vec{\nu} + \hat{\alpha}_R)\cdot(\vec{\gamma} + \vec{\gamma}')}}{2^{\hat{r}}} - \frac{1}{2^m}\delta_{\vec{\gamma},\vec{\gamma}'}.$$

Now the following vector spaces are defined:

- $\mathcal{G}$ is the set of all linear combinations over $\{0, 1\}$ of rows of $\hat{K}$. It is a vector space of dimension m.
- $\mathcal{S}$ is a subspace of $\{0, 1\}^{\hat{r}}$ that is supplement to the subspace $\mathcal{G}$, that is, $\mathcal{G} \oplus \mathcal{S} = \{0, 1\}^{\hat{r}}$. The dimension of $\mathcal{S}$ is $\hat{r} - m$.
- $\mathcal{K}$ is the set of all vectors $\vec{x} \in \{0, 1\}^{\hat{r}}$ such that $\hat{K}\vec{x} = \vec{0}$. The set $\mathcal{K}$ is a vector space of dimension $\hat{r} - m$, since the rows of $\hat{K}$ are linearly independent. We denote by $\{\vec{u}_1, \ldots, \vec{u}_{\hat{r}-m}\}$ a basis of $\mathcal{K}$.

Given a subspace F of $\{0, 1\}^{\hat{r}}$, we denote by $F^{\perp}$ the set of all vectors $\vec{x} \in \{0, 1\}^{\hat{r}}$ such that for all $\vec{y} \in F$, $\vec{x}\cdot\vec{y} = 0 \pmod 2$. Note that $\mathcal{K}^{\perp} = \mathcal{G}$. Since the rows of $\hat{K}$ are linearly independent, for any $\tilde{\kappa} \in \{0, 1\}^m$, there exists a vector $\vec{\theta}_{\tilde{\kappa}} \in \{0, 1\}^{\hat{r}}$ such that $\hat{K}\vec{\theta}_{\tilde{\kappa}} = \tilde{\kappa}$. It follows that $\hat{K}\hat{\alpha}_R = \tilde{\kappa}$ if and only if $\hat{\alpha}_R \in \vec{\theta}_{\tilde{\kappa}} + \mathcal{K}$. Thus following the techniques used in [15],

$$\begin{aligned}
\sum_{\substack{\hat{\alpha}_R \in \{0,1\}^{\hat{r}}: \\ \hat{K}\hat{\alpha}_R = \tilde{\kappa}}} (-1)^{(\vec{\nu} + \hat{\alpha}_R)\cdot(\vec{\gamma} + \vec{\gamma}')} &= \sum_{\hat{\alpha}_R \in \vec{\theta}_{\tilde{\kappa}} + \mathcal{K}} (-1)^{(\vec{\nu} + \hat{\alpha}_R)\cdot(\vec{\gamma} + \vec{\gamma}')} \\
&= (-1)^{(\vec{\nu} + \vec{\theta}_{\tilde{\kappa}})\cdot(\vec{\gamma} + \vec{\gamma}')} \prod_{i=1}^{\hat{r}-m} \left[1 + (-1)^{\vec{u}_i\cdot(\vec{\gamma} + \vec{\gamma}')} \right] \\
&= \begin{cases} (-1)^{(\vec{\nu} + \vec{\theta}_{\tilde{\kappa}})\cdot(\vec{\gamma} + \vec{\gamma}')} 2^{\hat{r}-m} & \text{if} \quad \vec{\gamma} + \vec{\gamma}' \in \mathcal{K}^{\perp} = \mathcal{G}, \\ 0 & \text{if} \quad \vec{\gamma} + \vec{\gamma}' \notin \mathcal{G}. \end{cases}
\end{aligned}$$

One obtains therefore that

$$\mathrm{P}_{\vec{\kappa}\boldsymbol{v}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)$$
$$= \mathrm{P}_{\boldsymbol{A}}(A)\frac{1}{2^m}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}_{\vec{R}}: \\ \hat{c}_T \in X_{\hat{a}_T}^{\hat{g}_T} \\ \hat{c}_E \in Y_{\hat{a}_E}^{\hat{g}_E}}} (U_{v\vec{\kappa}\hat{c}_{\vec{R}}} + V_{v\vec{\kappa}\hat{c}_{\vec{R}}})^{\dagger}\Delta(U_{v\vec{\kappa}\hat{c}_{\vec{R}}} + V_{v\vec{\kappa}\hat{c}_{\vec{R}}}),$$

where $U_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ and $V_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ are complex vectors of dimension $2^{\hat{r}}$ and Δ is a $2^{\hat{r}} \times 2^{\hat{r}}$ complex matrix, whose entries are indexed by $\vec{\gamma} \in \{0, 1\}^{\hat{r}}$. The $\vec{\gamma}$th entry of $U_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ and $V_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ are

$$\left(U_{v\vec{\kappa}\hat{c}_{\vec{R}}}\right)_{\vec{\gamma}} = \begin{cases} (-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{\gamma}}\langle\chi_{v|AP}|\hat{c}\rangle & \text{if} \quad w(\vec{\gamma}) < w_{\min}/2, \\ 0 & \text{if} \quad w(\vec{\gamma}) \geq w_{\min}/2, \end{cases}$$

$$\left(V_{v\vec{\kappa}\hat{c}_{\vec{R}}}\right)_{\vec{\gamma}} = \begin{cases} 0 & \text{if} \quad w(\vec{\gamma}) < w_{\min}/2, \\ (-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{\gamma}}\langle\chi_{v|AP}|\hat{c}\rangle & \text{if} \quad w(\vec{\gamma}) \geq w_{\min}/2, \end{cases}$$

where $\hat{c}$ is given by $\hat{c}_{\vec{R}}$, $\hat{a}_R$, $\hat{g}_R$ and $\vec{\gamma}$. The $(\vec{\gamma}, \vec{\gamma}')$th entry of Δ is

$$(\Delta)_{\vec{\gamma},\vec{\gamma}'} = \begin{cases} 1 & \text{if} \quad \vec{\gamma} + \vec{\gamma}' \in \mathcal{G}\backslash\{\vec{0}\}, \\ 0 & \text{if} \quad \vec{\gamma} + \vec{\gamma}' \notin \mathcal{G}\backslash\{\vec{0}\}. \end{cases}$$

This implies $U_{v\vec{\kappa}\hat{c}_{\vec{R}}}^{\dagger}\Delta U_{v\vec{\kappa}\hat{c}_{\vec{R}}} = 0$, since $w(\vec{\gamma}) < w_{\min}/2$ and $w(\vec{\gamma}') < w_{\min}/2$ imply that $w(\vec{\gamma} + \vec{\gamma}') < w_{\min}$, that is, $\vec{\gamma} + \vec{\gamma}' \notin \mathcal{G}\backslash\{\vec{0}\}$.

The matrix Δ is Hermitian, of eigenvalues $2^m - 1$ and -1. There are $2^{\hat{r}-m}$ eigenvectors $\vec{v}_{\vec{x}}$ ($\vec{x} \in \mathcal{S}$) associated with the eigenvalue $2^m - 1$. The $\vec{\gamma}$th entry of $\vec{v}_{\vec{x}}$ is

$$(\vec{v}_{\vec{x}})_{\vec{\gamma}} = \begin{cases} 1 & \text{if} \quad \vec{\gamma} + \vec{x} \in \mathcal{G}, \\ 0 & \text{if} \quad \vec{\gamma} + \vec{x} \notin \mathcal{G}. \end{cases}$$

There are $2^{\hat{r}-m}(2^m - 1)$ eigenvectors $\vec{w}_{\vec{x},\vec{\sigma}}$ ($\vec{x} \in \mathcal{S}, \vec{\sigma} \in \{0, 1\}^m\backslash\{\vec{0}\}$) associated with the eigenvalue -1. The $\vec{\gamma}$th entry of $\vec{w}_{\vec{x},\vec{\sigma}}$ is

$$\left(\vec{w}_{\vec{x},\vec{\sigma}}\right)_{\vec{\gamma}} = \begin{cases} (-1)^{\vec{\omega}_{\vec{\gamma}+\vec{x}}\cdot\vec{\sigma}} & \text{if} \quad \vec{\gamma} + \vec{x} \in \mathcal{G}, \\ 0 & \text{if} \quad \vec{\gamma} + \vec{x} \notin \mathcal{G}, \end{cases}$$

where for any $\vec{y} \in \mathcal{G}$, $\vec{\omega}_{\vec{y}}$ is the unique vector in $\{0, 1\}^m$ such that $\hat{K}^T\vec{\omega}_{\vec{y}} = \vec{y}$. Note that for any $\vec{\gamma} \in \{0, 1\}^{\hat{r}}$, there is a unique $(\vec{x}, \vec{y}) \in \mathcal{S} \times \mathcal{G}$ such that $\vec{\gamma} = \vec{x} + \vec{y}$, and that

$$\mathbf{1}_{\vec{\gamma}} = \frac{1}{2^m}\left(\vec{v}_x + \sum_{\vec{\sigma}\in\{0,1\}^m\backslash\{\vec{0}\}} (-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{\sigma}}\,\vec{w}_{\vec{x},\vec{\sigma}}\right),$$

where $\mathbf{1}_{\vec{\gamma}}$ is the canonical vector with entry 1 at position $\vec{\gamma}$ and 0 everywhere else. We can express the vectors $U_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ and $V_{v\vec{\kappa}\hat{c}_{\vec{R}}}$ as linear combinations of these eigenvectors:

$$\begin{aligned} U_{v\vec{\kappa}\hat{c}_{\vec{R}}} &= \sum_{\vec{x}\in\mathcal{S}}(-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{x}}\varphi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}}\vec{v}_{\vec{x}} + \sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\sigma}\neq\vec{0}}(-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{x}}\varphi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}+\vec{\sigma}}\vec{w}_{\vec{x},\vec{\sigma}}, \\ V_{v\vec{\kappa}\hat{c}_{\vec{R}}} &= \sum_{\vec{x}\in\mathcal{S}}(-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{x}}\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}}\vec{v}_{\vec{x}} + \sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\sigma}\neq\vec{0}}(-1)^{(\vec{v}+\vec{\theta}_{\vec{\kappa}})\cdot\vec{x}}\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}+\vec{\sigma}}\vec{w}_{\vec{x},\vec{\sigma}}, \end{aligned}$$

where for any $\vec{z}\in\{0,1\}^m$,

$$\begin{aligned} \varphi_{v,\hat{c}_{\vec{R}},\vec{x},\vec{z}} &= \sum_{\vec{y}\in\mathcal{G}:\ w(\vec{x}+\vec{y})<w_{\min}/2}(-1)^{\vec{v}\cdot\vec{y}}\frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|AP}\mid\hat{c}\rangle, \\ \psi_{v,\hat{c}_{\vec{R}},\vec{x},\vec{z}} &= \sum_{\vec{y}\in\mathcal{G}:\ w(\vec{x}+\vec{y})\geq w_{\min}/2}(-1)^{\vec{v}\cdot\vec{y}}\frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|AP}\mid\hat{c}\rangle. \end{aligned}$$

In deriving the above formulae, we used the identity $\vec{\theta}_{\tilde{\kappa}}\cdot\vec{y}=\vec{\omega}_{\vec{y}}\cdot\tilde{\kappa}\pmod 2$ for any $\vec{y}\in\mathcal{G}$ and $\tilde{\kappa}\in\{0,1\}^m$. It follows that for any $\hat{c}_R$, v and $\vec{\kappa}$,

$$\begin{aligned} V^{\dagger}_{v\vec{\kappa}\hat{c}_{\vec{R}}}\Delta V_{v\vec{\kappa}\hat{c}_{\vec{R}}} &= \sum_{\vec{x}\in\mathcal{S}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}}|^2(2^m-1)\|\vec{v}_{\vec{x}}\|^2 - \sum_{\substack{\vec{x}\in\mathcal{S}\\ \vec{\sigma}\neq\vec{0}}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}+\vec{\sigma}}|^2\|\vec{w}_{\vec{x},\vec{\sigma}}\|^2 \\ &= 2^m\left[(2^m-1)\sum_{\vec{x}\in\mathcal{S}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}}|^2 - \sum_{\substack{\vec{x}\in\mathcal{S}\\ \vec{\sigma}\neq\vec{0}}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}+\vec{\sigma}}|^2\right], \end{aligned}$$

thus for any $\hat{c}_R$ and v,

$$\begin{aligned} &\sum_{\vec{\kappa}\in\{0,1\}^m}\left|V^{\dagger}_{v\vec{\kappa}\hat{c}_{\vec{R}}}\Delta V_{v\vec{\kappa}\hat{c}_{\vec{R}}}\right| \\ &\qquad\leq 2^m\sum_{\vec{x}\in\mathcal{S}}\left[(2^m-1)\sum_{\vec{\kappa}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}}|^2 + \sum_{\vec{\sigma}\neq\vec{0},\vec{\kappa}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\tilde{\kappa}+\vec{\sigma}}|^2\right] \\ &\qquad= 2^{m+1}(2^m-1)\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}|\psi_{v,\hat{c}_{\vec{R}},\vec{x},\vec{\kappa}}|^2. \end{aligned}$$

as $\tilde{\kappa}=\vec{\kappa}+\check{K}\check{\alpha}_R$ where $\check{K}\check{\alpha}_R$ is a constant vector for a given v. Similarly, we have

$$\sum_{\vec{\kappa}\in\{0,1\}^m}\left|U^{\dagger}_{v\vec{\kappa}\hat{c}_{\vec{R}}}\Delta V_{v\vec{\kappa}\hat{c}_{\vec{R}}}\right| \leq 2^{m+1}(2^m-1)\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}|\varphi^*_{v,\hat{c}_{\vec{R}},\vec{x},\vec{\kappa}}\psi_{v,\hat{c}_{\vec{R}},\vec{x},\vec{\kappa}}|.$$

Now,

$$\begin{aligned}
&\sum_{A\in\mathcal{A}}\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\vec{\kappa}\boldsymbol{v}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v)\right| \\
&\qquad\le \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\frac{1}{2^m}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \\
&\qquad\quad\times\sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{s}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{s}_E}}}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{\kappa}\in\{0,1\}^m}\left[|V^{\dagger}_{v\vec{\kappa}\hat{c}_{\bar{R}}}\Delta V_{v\vec{\kappa}\hat{c}_{\bar{R}}}|+2|U^{\dagger}_{v\vec{\kappa}\hat{c}_{\bar{R}}}\Delta V_{v\vec{\kappa}\hat{c}_{\bar{R}}}|\right] \\
&\qquad\le 2(2^m-1)\sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \\
&\qquad\quad\times\sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{s}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{s}_E}}}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\left[|\psi_{v,\hat{c}_{\bar{R}},\vec{x},\vec{\kappa}}|^2+2|\,\varphi^{*}_{v,\hat{c}_{\bar{R}},\vec{x},\vec{\kappa}}\psi_{v,\hat{c}_{\bar{R}},\vec{x},\vec{\kappa}}|\right] \\
&\qquad\le 2(2^m-1)(\eta+2\sqrt{\eta}\sqrt{\xi}),
\end{aligned}$$

where we used the Schwartz inequality, and where

$$\eta = \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{s}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{s}_E}}}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p})|\psi_{v,\hat{c}_{\bar{R}},\vec{x},\vec{\kappa}}|^2,$$

$$\xi = \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{s}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{s}_E}}}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p})|\varphi_{v,\hat{c}_{\bar{R}},\vec{x},\vec{\kappa}}|^2.$$

We derive an upper-bound on η and ξ. We have

$$\begin{aligned}
\eta &= \sum_{A\in\mathcal{A}}\mathrm{P}_{\boldsymbol{A}}(A)\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \\
&\quad\times\sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{s}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{s}_E}}}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\substack{\vec{x}\in\mathcal{S},\,\vec{y},\vec{y}'\in\mathcal{G}\\ w(\vec{x}+\vec{y})\ge w_{\min}/2\\ w(\vec{x}+\vec{y}')\ge w_{\min}/2}}\sum_{\vec{\kappa}}(-1)^{\vec{v}\cdot(\vec{y}+\vec{y}')}\frac{(-1)^{\vec{\omega}_{\vec{y}+\vec{y}'}\cdot\vec{\kappa}}}{2^{2m}}\langle\hat{c}'\mid\chi_{v|AP}\rangle\langle\chi_{v|AP}\mid\hat{c}\rangle
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2^m}\sum_{A\in\mathcal{A}} \mathrm{P}_{\boldsymbol{A}}(A) \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \\
&\quad\times \sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \sum_{\substack{\vec{x}\in\mathcal{S}\\ \vec{y}\in\mathcal{G}\\ w(\vec{x}+\vec{y})\geq w_{\min}/2}} \sum_{v\in\mathcal{V}_{A,P}} \langle\hat{c} \mid \chi_{v|AP}\rangle\langle\chi_{v|AP} \mid \hat{c}\rangle \\
&= \frac{1}{2^m}\sum_{A\in\mathcal{A}} \mathrm{P}_{\boldsymbol{A}}(A) \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \sum_{\substack{\vec{\gamma}\in\{0,1\}^{\hat{r}}\\ w(\vec{\gamma})\geq w_{\min}/2}} \langle\hat{c}|F_{D\vec{g}|\boldsymbol{A}=A}|\hat{c}\rangle \\
&= \frac{1}{2^m}\sum_{A\in\mathcal{A}} \mathrm{P}_{\boldsymbol{A}}(A) \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \sum_{\hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R}} \langle\hat{c}|\Pi_{\hat{R}}^{\vec{g}}F_{D\vec{g}|\boldsymbol{A}=A}\Pi_{\hat{R}}^{\vec{g}}|\hat{c}\rangle \\
&\leq \frac{1}{2^m}\theta(r),
\end{aligned}
$$

using the result of the previous section. Similarly,

$$
\begin{aligned}
\xi &= \frac{1}{2^m}\sum_{A\in\mathcal{A}} \mathrm{P}_{\boldsymbol{A}}(A) \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \frac{1}{4^{\hat{n}}}\mathrm{P}_{\hat{\boldsymbol{a}}}(\hat{a})\mathrm{P}_{\hat{\boldsymbol{p}}}(\hat{p}) \\
&\quad\times \sum_{\substack{\hat{c}_{\bar{R}}:\\ \hat{c}_T\in X_{\hat{a}_T}^{\hat{g}_T}\\ \hat{c}_E\in Y_{\hat{a}_E}^{\hat{g}_E}}} \sum_{\substack{\hat{c}_R\in X_{\hat{a}_R}^{\hat{g}_R}:\\ d(\hat{c}_R,\hat{g}_R)<w_{\min}/2}} \langle\hat{c}|F_{D\vec{g}|\boldsymbol{A}=A}|\hat{c}\rangle \\
&\leq \frac{1}{2^m}\mathrm{P}_{\mathbf{valid}}(\mathrm{true}) \\
&\leq \frac{1}{2^m}.
\end{aligned}
$$

Consequently,

$$
\sum_{A\in\mathcal{A}}\sum_{P\in\mathcal{P}\cap\mathcal{P}_A}\sum_{v\in\mathcal{V}_{A,P}}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\vec{\kappa}\boldsymbol{\nu}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\boldsymbol{\nu}}(v)\right| \leq 2\left(\theta(r)+2\sqrt{\theta(r)}\right),
$$

which concludes our proof. □

6.6. *Bound on the Conditional Entropy.* We conclude the proof of privacy by using the following property from classical information theory.

PROPERTY 4. *Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two discrete random variables taking values in the sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. Let μ be a non-negative real number. If the following inequality is satisfied,*

$$\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \left| \mathrm{P}_{\boldsymbol{xy}}(x,\, y) - \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y) \right| \leq \mu,$$

then the conditional entropy of $\boldsymbol{x}$ given $\boldsymbol{y}$ is lower-bounded by

$$H(\boldsymbol{x} \mid \boldsymbol{y}) \geq (1-\mu)\log_2|\mathcal{X}| - \frac{1}{\ln 2}\mu.$$

PROOF. The hypothesis implies that there exist a set of real numbers $\eta_{x,y}$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that

$$\mathrm{P}_{\boldsymbol{xy}}(x,\, y) = \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)(1+\eta_{x,y})$$

($\eta_{x,y}$ is assigned the value zero if $\mathrm{P}_{\boldsymbol{y}}(y) = 0$), obeying the inequality

$$\sum_{x\in\mathcal{X},y\in\mathcal{Y}} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)|\eta_{x,y}| \leq \mu.$$

Note that for all x and y, we have $-1 \leq \eta_{x,y} \leq |\mathcal{X}| - 1$. Now,

$$\begin{aligned}
H(\boldsymbol{x} \mid \boldsymbol{y}) \;&=\; -\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}:\ \mathrm{P}_{\boldsymbol{xy}}(x,y)>0} \mathrm{P}_{\boldsymbol{xy}}(x,\, y)\log_2 \mathrm{P}_{\boldsymbol{x}|\boldsymbol{y}=y}(x) \\
&=\; \log_2|\mathcal{X}| - \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}:\ \eta_{x,y}>-1} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)\underbrace{\log_2(1+\eta_{x,y})}_{\leq|\eta_{x,y}|/\ln 2} \\
&\quad - \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}:\ \eta_{x,y}>-1} \frac{1}{|\mathcal{X}|}\mathrm{P}_{\boldsymbol{y}}(y)\eta_{x,y}\log_2 \underbrace{(1+\eta_{x,y})}_{\leq|\mathcal{X}|} \\
&\geq\; \log_2|\mathcal{X}| - \frac{\mu}{\ln 2} - \mu\log_2|\mathcal{X}|,
\end{aligned}$$

which concludes the proof. □

The probability distribution of the private key and the view obeys the following inequality:

$$\begin{aligned}
&\sum_{\substack{\vec{\kappa}\in\{0,1\}^m,\\ v\in\mathcal{V}}} \left| \mathrm{P}_{\vec{\kappa}\boldsymbol{v}}(\vec{\kappa},\, v) - \frac{1}{2^m}\mathrm{P}_{\boldsymbol{v}}(v) \right| \\
&\qquad \leq \sum_{A\in\mathcal{A}} \sum_{P\in\mathcal{P}\cap\mathcal{P}_A} \sum_{v\in\mathcal{V}_{A,P}} \sum_{\vec{\kappa}\in\{0,1\}^m} \left| \mathrm{P}_{\vec{\kappa}\boldsymbol{v}}(\vec{\kappa},\, v) - \frac{\mathrm{P}_{\boldsymbol{v}}(v)}{2^m} \right| \\
&\qquad \leq\; 2(\theta(r) + 2\sqrt{\theta(r)}),
\end{aligned}$$

where we have used the fact that the key is randomly chosen by Alice with uniform probability distribution if the validation test is not passed. Applying the above property for the random variables $\vec{\boldsymbol{\kappa}}$ and $\boldsymbol{\nu}$, we obtain

$$H(\vec{\boldsymbol{\kappa}} \mid \boldsymbol{\nu}) \geq m - 2\left(m + \frac{1}{\ln 2}\right)\left(\theta(r) + 2\sqrt{\theta(r)}\right),$$

which concludes the proof of privacy. □

7. Discussion. In this paper we have obtained the security of a quantum key distribution protocol in which the legitimate parties can use imperfect photon sources. We considered a protocol using only two conjugate bases for the polarisation encoding of single photons. However, the proof can be adapted to a protocol using three conjugate bases instead [33], using the techniques in [34]. Given a certain error-rate during the quantum transmission, the resulting key creation rate would be slightly increased.

The protocol we have considered requires the existence of a third party able to perform efficient and faithful Bell measurements. This requirement is not practical with current technology. However, should new techniques for Bell measurement and photon detection/storage become available, one could imagine relayed networks as described in [5]. On the other hand, if technology to achieve efficient and faithful Bell measurement is not available, the present proof still has practical relevance as one can derive from it the security of a realistic BB84 protocol [23].

Finally, the protocol we have considered uses two-way public communication for key distillation. One might adapt its security proof for protocols using other key distillation techniques using two-way public communication. It would be particularly interesting to study how a scheme like advantage distillation [35], [36] could modify the key creation rate one can achieve against enemies with unlimited computational resource.

Acknowledgement. The author thanks Hans Briegel, Artur Ekert, Nicolas Gisin, Patrick Hayden, Hoi-Kwong Lo, Norbert Lütkenhaus, Dominic Mayers, Michele Mosca, Luke Rallan, Peter Shor and Vlatko Vedral for interesting discussions and helpful comments.

References

[1] C. H. Bennett and G. Brassard. Quantum cryptography, public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, 1984.

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121, 1992.

[3] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661, 1991.

[4] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557, 1992.

[5] E. Biham, B. Huttner, and T. Mor. Quantum cryptographic network based on quantum memories. *Phys. Rev. A*, 54(4):2651, 1996.

[6] B. Huttner and A. Ekert. Information gain in quantum eavesdropping. *J. Mod. Opt.*, 41(12):2455, 1994.
[7] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Phys. Rev. A*, 56(2):1163, 1997.
[8] B. Slutsky, R. Rao, P.-C. Sun, and Y. Fainman. Security of quantum cryptography against individual attacks. *Phys. Rev. A*, 57(4):2383, 1998.
[9] N. Lütkenhaus. Security against eavesdropping in quantum cryptography. *Phys. Rev. A*, 54(1):97, 1996.
[10] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996.
[11] J. I. Cirac and N. Gisin. Coherent eavesdropping strategies for the 4 state quantum cryptography protocol. *Phys. Lett. A*, 229(1):1, 1997.
[12] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59(5):3301, 1999.
[13] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.
[14] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology—Proceedings of Crypto* '96, page 343, 1996.
[15] D. Mayers. Unconditional security in quantum cryptography. quant-ph/9802025, 1998.
[16] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050, 1999.
[17] H.-K. Lo. A simple proof of the unconditional security of quantum key distribution. quant-ph/9904091, 1999.
[18] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution. quant-ph/9912053, 1999.
[19] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441, 2000.
[20] M. Ben-Or. Manuscript in preparation.
[21] H. Aschauer and H. Briegel. Private entanglement over arbitrary distances, even using noisy apparatus. quant-ph/0008051, 2000.
[22] H. Inamori. Security of EPR-based quantum key distribution. quant-ph/0008064, 2000.
[23] H. Inamori. Security of practical BB84 quantum key distribution. *Algorithmica*, this issue, pp. 366–371.
[24] H. Inamori, N. Lütkenhaus, and D. Mayers. Security of practical quantum key distribution. Manuscript in preparation. Submitted to *Quantum Information and Computation*.
[25] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Tech. J*, 28:656, 1949.
[26] D. Welsh. *Codes and Cryptography*. Clarendon Press, Oxford, 1988.
[27] D. Stinson. *Cryptography*: *Theory and Practice*. CRC Press, Boca Raton, FL, 1995.
[28] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology, Eurocrypt* '93 *Proceedings*, page 410, 1993.
[29] A. Peres. *Quantum Theory*: *Concepts and Methods*. Kluwer, Dordrecht, 1995.
[30] N. Lütkenhaus. Security of quantum cryptography with realistic sources. *Acta Phys. Slovaca*, 49:549, 1999.
[31] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.
[32] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *J. Comput. System Sci.*, 22:265, 1981.
[33] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018, 1998.
[34] H. Inamori. Security of EPR-based quantum key distribution using three bases. quant-ph/0008076, 2000.
[35] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory*, 39(3):733, 1993.
[36] N. Gisin and S. Wolf. Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols. *Phys. Rev. Lett.*, 83:4200, 1999.