# SECURITY OF QUANTUM KEY DISTRIBUTION
# WITH BIT AND BASIS DEPENDENT DETECTOR FLAWS

LARS LYDERSEN[a]      JOHANNES SKAAR

*Department of Electronics and Telecommunications, Norwegian University of Science and Technology*
*NO-7491 Trondheim, Norway*
and
*University Graduate Center, NO-2027 Kjeller, Norway*

We consider the security of the Bennett-Brassard 1984 (BB84) protocol for Quantum Key Distribution (QKD), in the presence of bit and basis dependent detector flaws. We suggest a powerful attack that can be used in systems with detector efficiency mismatch, even if the detector assignments are chosen randomly by Bob. A security proof is provided, valid for any basis dependent, possibly lossy, linear optical imperfections in the channel/receiver/detectors. The proof does not assume the so-called squashing detector model.

*Keywords*: Quantum cryptography, quantum key distribution, security proof, detection efficiency mismatch

*Communicated by*: H-K Lo & R Laflamme

## 1   Introduction

Quantum mechanics makes it possible to exchange a random bit string at a distance [1, 2, 3, 4]. In theory, the key distribution is secure, even if an eavesdropper Eve can do anything allowed by the currently known laws of nature [5, 6, 7, 8].

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved [5, 9, 10, 11]. However, a QKD system is relatively complex, and loopholes and imperfections exist that are not covered by existing security proofs. A security loophole can be dealt with in two different ways: Either you modify the implementation, or you increase the amount of privacy amplification [12] required to remove Eve's information about the key. The first approach, to modify the implementation, may often be done without decreasing the rate of which secret key can be generated. It may however increase the complexity of the implementation, which in turn may lead to new loopholes. The advantages of the second approach, to increase the amount of privacy amplification, are that the apparatus can be kept as simple as possible, and that existing implementations can be made secure with a software update. A drawback is clearly the reduced key rate, which is considered as a critical parameter in commercial QKD systems.

One of the imperfections to be considered in this paper, is called detector efficiency mismatch (DEM) [13]. If an apparatus has DEM, Eve can control the efficiencies of Bob's

---

[a]Email: lars.lydersen@iet.ntnu.no

detectors by choosing a parameter $t$ in some external domain. Examples of such domains can be the timing, polarization, or frequency of the photons [13, 14].

To be more concrete, consider DEM in the time-domain. In most QKD systems Bob's apparatus contains two single photon detectors to detect the incoming photons, one for each bit value. (Equivalently, two different detection windows of a single detector can be used for the two bit values (time-multiplexed detector).) Normally the detectors are gated in the time-domain to avoid high dark-counts. This means that electronic circuits are used to turn the detectors on and off, creating detection windows. Different optical path lengths, inaccuracies in the electronics, and finite precision in detector manufacturing may cause the detection windows of the two detectors to be slightly shifted, as seen in Fig. 1. The shift means that there exist times where the two detectors have different efficiencies.

Efficiency

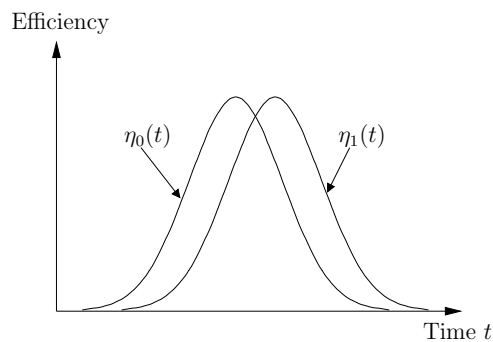$\eta_0(t)$     $\eta_1(t)$

Time $t$

Fig. 1. An example of mismatched efficiency curves for two detectors in the time-domain. The functions $\eta_0(t)$ and $\eta_1(t)$ are the efficiencies of detector 0 and 1, respectively. The parameter $t$ can be used to parametrize other domains as well.

Systems with DEM can be attacked with a faked-states attack [13]. The faked-states attack is an intercept-resend attack where Eve does not try to reconstruct the original state sent by Alice, but rather exploit the imperfections in Bob's apparatus to hide errors. The faked-states attack can be adapted to the Scarani-Acin-Ribordy-Gisin 2004 (SARG04), Ekert, and Differential Phase Shift Keying (DPSK) protocols, in addition to BB84 [15]. Another attack on systems with DEM is the time-shift attack [16]. In this attack Eve just selects the timing of each qubit randomly, thereby gaining information about the bit value when Bob announces which qubits were received and which were lost. The major advantage of the time-shift attack is that it does not introduce any quantum bit error rate (QBER). It has been demonstrated experimentally that the security of a commercially available QKD system can be compromised with a time-shift attack [17].

A frequently mentioned countermeasure for systems with DEM is called *four-state Bob* [18, 19, 13, 16]. In a phase-encoded QKD system, Bob chooses from four different phase settings $\{0, \pi/2, \pi, 3\pi/2\}$ instead of only two $\{0, \pi/2\}$. This will randomly assign the bit values 0 and 1 to the detectors (or the detection windows, in the case of one time-multiplexed detector) for each received state. Therefore Eve does not know which detector characteristics that corresponds to the 0 and 1 detectors.

However, as mentioned previously [13, 16] Eve may use a large laser pulse attack [20, 21,

22, 23] to read Bob's phase modulator settings. In a large pulse attack Eve uses a strong laser pulse to measure the reflections from either Alice's or Bob's apparatus. The setting of the phase modulator may give a signature on the reflections, enabling Eve to obtain the phase.

First assume that Eve is able to read Alice's modulator settings. Then Eve could obtain bit and/or basis information before the pulse enters Bob's apparatus, and therefore the security would be seriously compromised. Fortunately, Alice's implementation can easily be modified to avoid the large pulse attack. A setup with a coherent laser source contains an attenuator, and moving this to the end of the apparatus, as well as introducing an optical isolator, will put impossible requirements on Eve's laser [22]. In "plug-and-play" systems Alice already uses a detector to monitor the input of her setup. Therefore a large pulse attack can easily be revealed by monitoring the intensity of the input.

In a straightforward implementation of BB84, the phase modulator setting in Bob's setup only contains basis information. It usually poses no security threat if Eve reads the basis, as she will get it during the public discussion anyway. One only has to avoid that Eve receives the basis information before the pulse enters Bob's apparatus. This can be taken care of by placing a properly long coil of optical fiber at the entrance of Bob's setup.

However, if the DEM loophole is patched with four-state Bob, the large pulse attack is dangerous, because it may give Eve information about the detector assignments. Modifying Bob's setup to avoid large pulse attacks is not an easy task. The most practical solution seems to be a beam splitter or an optical circulator combined with an intensity detector [22]. Note that the key rate will suffer; the the input of Bob's setup is precious single photons. Also the setup gets more complex, which should be avoided as far as possible, to limit the number of "hidden surprises". It is therefore not obvious whether such modifications should be implemented, or whether the security should be regained with extra privacy amplification. Even though some systems implement four-state Bob, several of them lack countermeasures for a strong pulse attack on Bob's side. Therefore we will pursue the latter solution, i.e., we assume that Eve is able to read Bob's phase modulator setting after Bob's detection.

Security bounds state a unconditionally secure key rate, positive a range in some parameter(s). Ideally one should be able to prove the converse, namely that with the parameter(s) outside this range the QKD-system is provable insecure. Unfortunately this is not always simple. Usually there is a third range of the parameter(s) where it is not known whether the QKD-protocol is secure. For instance with perfect devices and one-way classical communication, the QKD-system is unconditionally secure for QBER < 11 % [8], and provable insecure for QBER > 14.6 % [24]. Until the gap is closed the security bounds represent a lower bound on the secure key rate, and the best known attacks represent an upper bound.

Fung et al. found a security bound for QKD systems with DEM [14]. QKD systems with four-state Bob is proved to be secure, provided Eve cannot read Bob's phase settings with a large pulse attack. The security proof assumes the so-called squashing model [11].

In this paper we first establish an upper bound for the secure key rate of QKD-system with DEM by presenting two powerful attacks, one of which even applies to implementations with four-state Bob (Section II). Then we will establish a lower bound for the secure key rate by providing a simple security proof of QKD systems with general, basis and bit dependent detector flaws (Section III), generalizing the proof by Fung et al. More precisely, any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver are covered

by the proof. For example, the proof covers mixing between all available optical modes, misalignments, mode-dependent losses, DEM, and any basis dependence of those effects. The proof is formulated for a decoy-state BB84 protocol and does not assume a squashing model. Finally, in Section IV we will examine some examples, including DEM, DEM with mode mixing, and DEM with misalignment.

## 2   Security analysis: upper bound

In this section we analyse two powerful attacks on systems with DEM. Such attacks are important because they establish a regime where QKD-systems with DEM is provable insecure. To analyze the attacks, for the moment we define $\eta = \max\{\min_t \eta_1(t)/\eta_0(t), \min_t \eta_0(t)/\eta_1(t)\} \in [0, 1]$, representing the smallest efficiency ratio available for both bit values. For individual attacks the secret key rate is given by [12, 25] (given one-way classical communication)

$$R = I(\alpha : \beta) - I(\alpha : \epsilon), \tag{1}$$

where $I(\cdot : \cdot)$ denotes mutual information and $\alpha$, $\beta$, and $\epsilon$ represent Alice's, Bob's and Eve's bits.

In the previous analysis of the faked-states attack [13], the attack was limited by the introduced QBER rather than Eve's insufficient knowledge about the key. By attacking only a fraction of the bits with the faked-states attack one can compromise the security for even higher values of $\eta$. The other fraction could be attacked with the time-shift attack [16] which introduces no QBER.

To tailor $E$, the QBER measured by Alice and Bob, the fraction $r$ attacked by the faked-states attack is given by

$$r = \frac{E}{E_{\text{fs}}} = E\frac{1 + 3\eta}{2\eta}, \tag{2}$$

where $E_{\text{fs}} = 2\eta/(1 + 3\eta)$ is the QBER introduced by the faked-states attack. The mutual information between Alice and Eve is given by

$$\begin{aligned} I(\alpha : \epsilon) &= rI(\alpha : \epsilon)_{\text{fs}} + (1 - r)I(\alpha : \epsilon)_{\text{ts}} \\ &= 1 - E - h(\frac{\eta}{1 + \eta})\left(1 - \frac{1 + 3\eta}{2\eta}E\right), \end{aligned} \tag{3}$$

where $r$ is given in (2) and $I(\alpha : \epsilon)_{\text{fs}} = 1 - E$ and $I(\alpha : \epsilon)_{\text{ts}} = 1 - h(\eta/(1 + \eta))$ denote the mutual information in the faked-states and the time-shift attack, respectively, as given in Refs [13, 16]. $h(\cdot)$ is the binary entropy function. Since Alice and Bob does not know how each bit is attacked, $I(\alpha : \beta)$ is simply given by $1 - h(E)$. The key rate (1) thus becomes

$$R = E + h(\frac{\eta}{1 + \eta})\left(1 - \frac{1 + 3\eta}{2\eta}E\right) - h(E). \tag{4}$$

Without considering DEM, Alice and Bob think that the key is secure when QBER $< 11\%$ (symmetric protocols with one-way classical communication [8]). Solving the equality $R = 0$, where $R$ is given by (4), and setting $E = 0.11$ gives $\eta = 0.215$.

The above combined attack is implementable with current technology. Up to $\eta = 0.160$ it represent an upper bound on the secure key rate (see Fig. 3). However with four-state Bob,

the attack is impossible since the faked-states attack requires knowledge of the bit-detector mapping before Bob receives the pulse.

For higher values of $\eta$ there exists an even more efficient attack. The optimal individual attack in the absence of imperfections is known [24]. Here Eve lets the qubit from Alice interact with a probe. After the basis is revealed, Eve's probe is in one of two non-orthogonal states [24]

$$|\xi_0\rangle = |0\rangle \tag{5a}$$

$$|\xi_1\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle, \tag{5b}$$

where $\varphi$ is related to the QBER by

$$\cos\varphi = 1 - 2E. \tag{6}$$

Eve has to separate between $|\xi_0\rangle$, corresponding to the bit value 0 at Alice, and $|\xi_1\rangle$, corresponding to the bit value 1. The two states occur with an *a priori* probability $1/2$.

In the presence of DEM, we improve the attack as follows: In addition to using a probe, Eve launches a time-shift attack. If Bob announces receipt, the probabilities of the two bit values is now $\{1/(1+\eta), \eta/(1+\eta)\}$ according to the time-shift attack [16]. Then after the public discussion, Eve has to separate between the states (5) with the *a priori* probabilities $\{1/(1+\eta), \eta/(1+\eta)\}$. The optimal measurement is projective [26], and the probability $p$ of Eve measuring the correct bit value is found to be

$$
\begin{aligned}
p = {}& \left(\frac{1}{1+\eta}\right)\cos^2\left[\frac{1}{2}\arctan\left(\frac{\sin 2\varphi}{\frac{1}{\eta} - \cos 2\varphi}\right)\right] \\
& + \left(\frac{\eta}{1+\eta}\right)\sin^2\left[\varphi + \frac{1}{2}\arctan\left(\frac{\sin 2\varphi}{\frac{1}{\eta} - \cos 2\varphi}\right)\right],
\end{aligned}
\tag{7}
$$

where $\varphi$ is related to the QBER as in Eq. (6).

Since Eve has probability $p$ to have the same bit value as Alice, $I(\alpha:\epsilon)$ is simply $1 - h(p)$. $I(\alpha:\beta)$ is given by $1 - h(E)$. The key rate (1) for this improved optimal individual attack is thus

$$R = h(p) - h(E), \tag{8}$$

where $p$ is given by (7).

Without considering DEM, Alice and Bob think that the key is secure when QBER $< 11\%$. Solving the equality $R = 0$, where $R$ is given by (8), and setting $E = 0.11$ gives $\eta = 0.252$. In a commercial QKD system $\eta$ was found to be approximately 0.25 (see Fig. 3 in [17]) [b]. Therefore, this attack could be used to compromise the security of such QKD systems. Note that the attack does not require the bit-detector mapping until the post-processing step. Therefore systems patched with four-state Bob are vulnerable to the attack combined with a large pulse attack.

Note that the both attacks represent a substantial improvement compared to the previously published attacks which require $\eta < 0.066$ [13]. Fig. 3 shows the range of $E, \eta$ which compromises security, and compares the two attacks.

---

[b] Also note that the DEM found in this system is heavily asymmetric, and the attacks might be more powerful if optimized for asymmetric DEM.

## 3   Security analysis: lower bound

In this section we will prove the security of the BB84 protocol in the presence of bit and basis dependent detector flaws, and establish the secure key generation rate. We will prove the security in a general setting, lifting the so-called squashing model assumption. That is, Eve may send any multimode, photonic state, and Bob uses practical threshold detectors. Alice may use a single-photon source or phase-randomized faint laser pulses; in the latter case, Alice may use decoy states [27, 28, 29] to estimate photon-number dependent parameters. Alice's source is otherwise assumed perfect: It emits an incoherent mixture of photonic number states, randomly in logical modes "0" or "1", randomly in the $X$ or $Z$ bases, with no correlation between the bits, bases, and photon number statistics [30].

The state space accessible to Eve consists of the Fock space associated with all photonic modes supported by the channel. The channel and receiver is modeled as a basis-dependent quantum operation, $\mathcal{C}_Z$ and $\mathcal{C}_X$, in front of two threshold detectors. Here $Z$ and $X$ denote the bases chosen by Bob. Since reduced detector efficiencies can be absorbed into the quantum operations, we can let Bob's threshold detectors have perfect efficiency. Dark counts are attributed to Eve, and for double click events, Bob assigns a random value to his bit [9, 11].

In our security proof, the key condition of $\mathcal{C}_Z$ and $\mathcal{C}_X$ is that they are passive, in the sense of

$$|0\rangle \rightarrow |0\rangle, \tag{9}$$

where $|0\rangle$ denotes the vacuum state of all modes. In other words, vacuum incident to all modes gives vacuum out. This condition is rather general; it includes all linear and nonlinear optical transformations of the modes supported by the channel.

For simplicity, however, we will restrict ourselves to linear optical imperfections. Bob's two detectors may still have different efficiencies, depending on the time, frequency, and/or polarization of the incoming states. Moreover, there may be imperfections in the channel and Bob's receiver. This can be described as arbitrary, square matrices $C_Z$ and $C_X$, acting on the *channel modes* after Eve's intervention. The linear-optical property of $C_Z$ and $C_X$ is ensured from the fact that they are classical transformations (or transfer matrices) operating on the physical, photonic modes (e.g. temporal modes and polarization modes) rather than the total Fock space of the modes. Each mode can contain any photonic state such as number states or coherent states. Although $C_Z$ and $C_X$ have finite dimension, the associated, induced quantum operations $\mathcal{C}_Z$ and $\mathcal{C}_X$ operate on an infinite dimensional Fock space. We use the convention that Bob's basis selector is included in $C_X$ (see Subsection 4.1).

With singular value decomposition, we can write

$$C_Z = U_Z F_Z V_Z C, \tag{10}$$

where $U_Z$ and $V_Z$ are unitary operators, and $F_Z$ is a diagonal, positive matrix. In addition to the usual singular value decomposition, we have included an extra matrix factor $C$, governing losses and imperfections in the channel and/or receiver, independent of the basis chosen by Bob. The matrix $C$ may for example describe loss of the channel and time-dependent detector efficiencies common for the two detectors. The operator $C$ can be absorbed into Eve's attack, thus it never appears in the following analysis. The unitary operators $U_Z$ and $V_Z$ mix the modes together. For example, $V_Z$ is the result of sending the modes through a network

isomorphic to the type in [31]. The diagonal matrix $F_Z$ represents the different efficiencies of the two detectors (in addition to basis-dependent absorptions in the receiver), and satisfies

$$|F_Z|^2 = \mathrm{diag} \begin{bmatrix} \eta_{Z0}(t_1) & \eta_{Z1}(t_1) & \eta_{Z0}(t_2) & \eta_{Z1}(t_2) \dots \end{bmatrix}. \tag{11}$$

The parameters $t_j, j = 1, 2, \dots$ label different modes. For example, $t_j$ may correspond to different temporal modes. In the absence of $U_Z$ and $V_Z$, $\eta_{Z0}(t_j)$ and $\eta_{Z1}(t_j)$ can be viewed as the efficiencies of detector 0 and 1 in the $Z$-basis. Otherwise the efficiencies $\eta_{Z0}(t_j)$ and $\eta_{Z1}(t_j)$ do not necessarily correspond to the detectors 0 and 1, respectively, nor to detection time $t_j$. However, the notation is selected as in the special case for intuition. Note that $F_Z$ may be represented as a collection of beam splitters with transmittivities $\eta_{Z0}(t_1)$, $\eta_{Z1}(t_1)$, and so forth. Then each mode is incident to its own beam splitter, and the vacuum state is sent into the other input.

The resulting model is shown in Fig. 2a. In the model we have included an extra measurement, giving information to Eve whether the total state is equal to the vacuum $|0\rangle$. While this information actually comes from Bob, it is convenient to let Eve obtain this information from a separate measurement. Note that this extra vacuum measurement does not disturb Bob's measurement statistics for any basis choice.
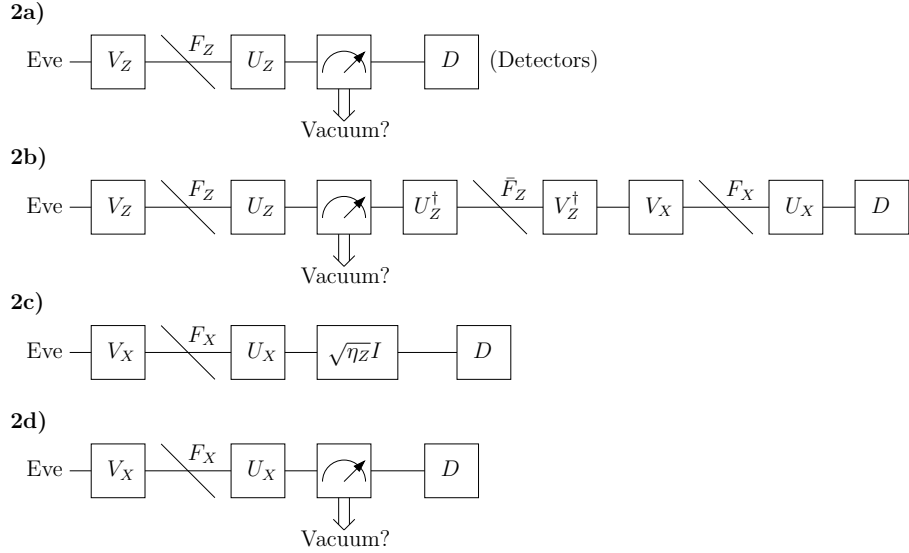


Fig. 2. a) Actual protocol. b) Estimation of Alice's virtual $X$-basis measurement. c) Simplification of Fig. 2b from Bob's point of view. d) Actual parameter estimation in the $X$-basis.

We will prove security using Koashi's argument [32, 33, 30] which we briefly summarize here. In the BB84-like actual protocol Alice generates a large number of bipartite states, where her part consists of a qubit which she measures randomly in the $X$- or $Z$-basis. The other part of the pairs is sent to Bob via Eve. Bob measures what he receives from Eve randomly in two different bases, which we will refer to as the "$X$-basis" or the "$Z$-basis". For example, for polarization encoding Bob's two measurements should ideally correspond to threshold detectors in horizontal/vertical or $\pm 45°$ polarization bases, with double clicks as

random assignment. Alice and Bob discard all events where they used incompatible basis. Further he publicly announces receipt if he receives something different from vacuum. Let $Q_X$ and $Q_Z$ be the fractions of non-vacuum results in each basis. Alice and Bob compare their $X$-basis measurement results to estimate $Q_X$ and the error rate $E_X$. The $N$ states measured in the $Z$-basis yield $NQ_Z$ non-vacuum results. For these $NQ_Z$ events Alice's measurement result is the raw key.

The required amount of privacy amplification can be found as follows: imagine a virtual experiment where Alice measures the qubits for the raw key in the $X$-basis instead of the $Z$-basis. Bob tries to predict the result of Alice's virtual $X$-basis measurement. Bob does not perform such a prediction in practice; thus in this prediction we may let Bob do everything permitted by quantum mechanics, as long as he does not alter the information given to Eve. Let $H_{\mathrm{virt}X}(A|B = \mu)$ denote the entropy of Alice's virtual $X$-basis measurement result, given measurement result $\mu$ in Bob's prediction. It turns out that $H_{\mathrm{virt}X}(A|B = \mu)$ can be bounded using $E_X$ and $Q_X$, so assume that $H_{\mathrm{virt}X}(A|B = \mu) \leq H$. Since the uncertainty about Alice $X$-measurement is less than $H$, the entropic uncertainty relation [34] suggests that any prediction (including Eves prediction) of the measurement result of Alice $Z$-basis measurement will have at least $NQ_Z - H$ entropy. Thus Alice can extract $NQ_Z - H$ bits of secret key. Rigorously, this rate is found by concertizing the privacy amplification procedure by universal hashing. Although Koashi's original proof is formulated with an obsolete security definition based on accessible information, the proof can easily be adapted to a composable security definition [35, 36, 37].

Bob must ensure that he has an identical raw key. Since it does not matter to Eve what Bob does (as long as he gives Eve the same information), he measures the bits for the raw key in the $Z$-basis. Alice and Bob compares a subset of the raw key to find the error rate $E_Z$ (consuming some of the raw key, but negliable in the asymptotic limit), and Alice sends Bob $NQ_Zh(E_Z)$ bits of error correcting information consuming $NQ_Zh(E_Z)$ bits of previously established secret key. In the asymptotic limit $N \to \infty$ the net secure key generation rate becomes

$$R_Z \geq 1 - \frac{H}{NQ_Z} - h(E_Z). \tag{12}$$

Note that $H$ is needed to ensure that Alice's key is secret, and this only requires $X$-basis parameters to be estimated by Alice and Bob. Thus there is no need to invoke the classicalization argument [7] regarding statistics of measurements involved in the simultaneous estimation of $E_X$ and $E_Z$.

For his prediction, Bob will use the virtual measurement in Fig. 2b. Bob first applies the unitary operator $U_Z^\dagger$, followed by the filter $\bar{F}_Z$, and the unitary operator $V_Z^\dagger$. Then he applies the operator $C_X = U_XF_XV_X$. Finally he performs an $X$-basis measurement. Note that we retain Eve's vacuum measurement and all components preceding it, so Eve obtains the identical information as in Fig. 2a. The matrix $\bar{F}_Z$ is diagonal, and is given by

$$\bar{F}_Z F_Z = \sqrt{\eta_Z}I, \tag{13}$$

where

$$\eta_Z = \min_{ij}\{\eta_{Zi}(t_j)\}. \tag{14}$$

Similarly to $F_Z$, the filter $\bar{F}_Z$ is implementable by beam splitters acting separately on each mode. The largest element of $|\bar{F}_Z|^2$ is 1, while the smallest element is $\eta_Z / \max_{ij}\{\eta_{Zi}(t_j)\}$.

To analyze how well Bob performs in his prediction, we will now simplify the system in Fig. 2b to determine Bob's measurement statistics. To do this, we introduce an extra vacuum measurement right before Bob's detectors, assuming nobody records the outcome. Clearly, Bob's measurement statistics are not altered by the presence of this extra measurement. The filter $U_X F_X V_X V_Z^\dagger \bar{F}_Z U_Z^\dagger$ obeys (9), being a linear optical transformation. As a result, we show in the appendix that the output state, after the extra vacuum measurement, is independent of the presence of Eve's vacuum measurement (i.e., the first vacuum measurement, after $U_Z$ in Fig. 2b). Thus, to estimate Bob's measurement statistics, we can remove Eve's vacuum measurement. We end up with the simplified system shown in Fig. 2c. Note that the simplified system is identical to the system in Fig. 2d, the actual protocol when Bob has chosen the $X$-basis, except for one thing: There is an extra, mode-independent absorption $\eta_Z$ in the channel. This fact will be used for estimating the performance of Bob's prediction.

To prove the security also for the multiphotonic case, we use the parameters $q_X^{(1)}$ and $e_X^{(1)}$ assumed known from the decoy state protocol. $q_X^{(1)}$ is the fraction of Bob's $X$-basis non-vacuum events that originate from single photons at Alice. $e_X^{(1)}$ is the QBER for single photon events in the $X$-basis (only single photons generate secure key). Consider the prediction in Fig. 2b-c. Let $NQ_Z$ be the number of states in the raw key. In a worst case, the number of detection events that originate from single photons at Alice, will be only $\eta_Z q_X^{(1)} Q_X N$, due to the filter $\sqrt{\eta_Z} I$ (note that $\eta_Z Q_X < Q_Z$). For each of these events Bob's entropic uncertainty about Alice's bit is (asymptotically) $h(e_X^{(1)*})$, where $e_X^{(1)*}$ is the associated error rate. We note that $e_X^{(1)*}$ is not measured in the actual protocol; it will rather be estimated below. For the events lost in the filter $\sqrt{\eta}_Z I$, Bob's entropic uncertainty about Alice's bit is 1, since he has no detection result. Summarizing, Bob's entropic uncertainty about Alice's $Q_Z N$ bits (corresponding to the number of detection events in Fig. 2a) is at most $H = Q_Z N - \eta_Z q_X^{(1)} Q_X N[1 - h(e_X^{(1)*})]$. In our analysis we have ignored the events associated with Alice sending the vacuum state [30]; their contribution will only give a marginally larger rate. From (12) the secure key rate becomes

$$R_Z = -h(E_Z) + \eta_Z q_X^{(1)} Q_X / Q_Z \left[1 - h(e_X^{(1)*})\right]. \tag{15}$$

It remains to bound the parameter $e_X^{(1)*}$, which is the QBER for single photon events in the estimation Fig. 2b-c. Recall that $e_X^{(1)}$ is the estimated QBER for single photon events in the $X$-basis, Fig. 2d. The only difference between the setup in Fig. 2c and Fig. 2d is the filter $\sqrt{\eta}_Z I$, which represent identical absorption in all modes. However, the removal of detection events by this filter is dependent on the photon number, so $e_X^{(1)*} \neq e_X^{(1)}$ in general.[c] To bound $e_X^{(1)*}$ we use the fact that the filter only alter the detection statistics by removing detection events. (An exception occurs for the few coincidence counts; these can be taken into account easily.) In a worst case,

$$e_X^{(1)*} \leq \frac{e_X^{(1)}}{\eta_Z(1 - e_X^{(1)}) + e_X^{(1)}} \leq e_X^{(1)}/\eta_Z. \tag{16}$$

---

[c]Note that although Alice send a single photon for a particular event, Eve may send any state.

Putting these results together, we obtain the secure key generation rate

$$R_Z \geq -h(E_Z) + \eta_Z q_X^{(1)} Q_X / Q_Z \left[ 1 - h(e_X^{(1)}/\eta_Z) \right]. \tag{17}$$

A similar result holds when Alice and Bob have chosen the $X$-basis in the actual protocol:

$$R_X \geq -h(E_X) + \eta_X q_Z^{(1)} Q_Z / Q_X \left[ 1 - h(e_Z^{(1)}/\eta_X) \right]. \tag{18}$$

Ineqs. (17) and (18) are valid for any basis and bit dependence of the channel and receiver/detectors, as long as the imperfections ($C_Z$ and $C_X$) can be described as possibly lossy, linear optical operators acting on the photonic modes.

To compare our result (17) to that of Ref. [14], we let Alice only send single photons. The rate then becomes

$$R \geq -h(E) + \eta[1 - h(E/\eta)], \tag{19}$$

where we have assumed symmetry between the bases, and therefore omitted the $Z$ and $X$ subscripts. The rate (19) coincides with the rate found in [14] (see Subsection 4.2 for a discussion on how to identify $\eta$). Note, however, that (19) is a stronger result in the sense that it applies to any basis-dependent linear optical imperfections, not only the case where $U_{Z,X} = I$, and $V_{Z,X}$ do not mix modes associated with different logical bits. Also it does not require the squashing model assumption.

Under the assumption that Eve only sends single photons, it is easy to realize that (16) can be replaced by $e_X^{(1)*} = e_X^{(1)}$. Then (19) is improved to

$$R \geq -h(E) + \eta[1 - h(E)]. \tag{20}$$

Fig. 3 shows the security bounds resulting from (19) and (20) when the right-hand side is set equal to zero.

## 4 Examples

### *4.1 DEM in the time-domain*

Consider the case where Bob's detectors have time-dependent efficiencies, as indicated in Fig. 1. We assume that the efficiencies are independent of the basis chosen by Bob ($F_X = F_Z$). The channel and receiver are otherwise assumed perfect, except for a background loss $C$. The background loss may be mode dependent, but independent of the basis chosen by Bob.

With these assumptions, we may take $C_Z = F_Z C$ and $C_X = F_X H C = F_Z H C$, where $H$ is a block-diagonal matrix consisting of $2 \times 2$ Hadamard matrices $H^{(2)}$, interchanging the bases $Z$ and $X$ for each time:

$$H = \text{diag} \begin{bmatrix} H^{(2)} & H^{(2)} & H^{(2)} & \dots \end{bmatrix}. \tag{21}$$

To maximize the secure key rate, as much as possible of the detector flaws should be absorbed into $C$. Therefore, we factorize

$$F_Z = FF', \tag{22}$$

where

$$F'^2 = \text{diag} \begin{bmatrix} \eta'(t_1) & \eta'(t_1) & \eta'(t_2) & \eta'(t_2) \dots \end{bmatrix}, \tag{23}$$
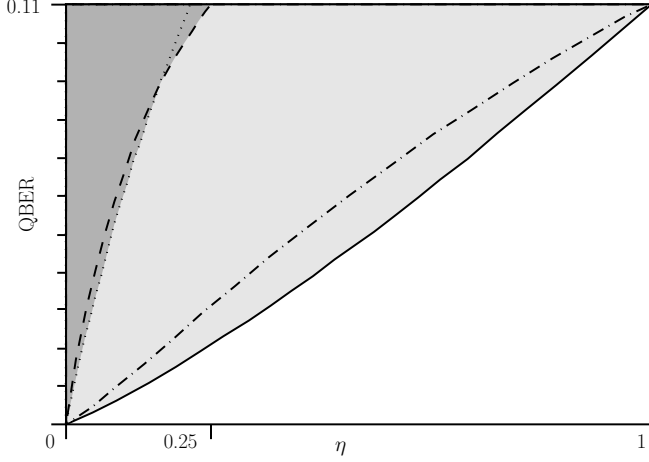
Fig. 3. Security bounds when Alice sends single photons ($q_Z^{(1)} = q_X^{(1)} = 1$), assuming symmetry between the bases. The bounds are found by setting the associated key generation rates equal to zero. Solid line: General security bound, as resulting from (19). Dash-dotted line: Security bound (20) assuming Eve sends single photons. Dashed line: The improvement of the optimal individual attack from Section 2, as resulting from (8). Dotted line: The combined attack from Section 2, as resulting from (4). For the attacks it is assumed that the DEM is equal for the two bit values. The dark grey region is proved to be insecure while the white region is proved to be secure with extra privacy amplification. The light grey region should be assumed insecure.

and $\eta'(t_j) = \max\{\eta_{Z0}(t_j), \eta_{Z1}(t_j)\}$. Noting that $F'$ and $H$ commute, we can absorb $F'$ into $C$. The remaining diagonal matrix $F$ then has the role of $F_Z$ (and $F_X$) in the security proof. The parameter $\eta_Z = \eta_X$ to substitute into the secure key generation rate (17) is therefore the minimum diagonal element of $|F|^2$:

$$\eta_Z = \min_t \min \left\{ \frac{\eta_{Z0}(t)}{\eta_{Z1}(t)}, \frac{\eta_{Z1}(t)}{\eta_{Z0}(t)} \right\}. \tag{24}$$

### 4.2   DEM and restricted mode mixing

Consider the case treated by Fung et al. [14], where there is no mixing between modes associated with different logical bits. Then $C_Z$ can be written in block diagonal form

$$C_Z = \begin{bmatrix} C_0 & 0 \\ 0 & C_1 \end{bmatrix} C, \tag{25}$$

provided we reorder the modes as in

$$|F_Z|^2 = \text{diag} \begin{bmatrix} \eta_{Z0}(t_1) & \eta_{Z0}(t_2) & \dots & \eta_{Z1}(t_1) & \eta_{Z1}(t_2) & \dots \end{bmatrix}, \tag{26}$$

to be compared to (11). As in Ref. [14] we assume basis independence in the sense

$$C_X = \begin{bmatrix} C_0 & 0 \\ 0 & C_1 \end{bmatrix} HC. \tag{27}$$

Here,

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ I & -I \end{bmatrix}, \tag{28}$$

with the present choice of mode order. We assume that $C_Z$ is nonsingular. (Otherwise, the secure key generation rate would be zero.)

We should associate as much as possible of the imperfections to the common channel operator $C$. Let the singular-value decomposition of $C_0 C_1^{-1}$ be $usv$, where $u$ and $v$ are unitary matrices, and $s$ is diagonal and positive. Let $\lambda^2$ be the maximum of $\max s$ and $\max s^{-1}$. Factorize

$$C_Z = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} \frac{1}{\lambda} \begin{bmatrix} s^{-1/2} u^\dagger C_0 & 0 \\ 0 & s^{1/2} v C_1 \end{bmatrix} C. \tag{29}$$

Defining

$$C' = \frac{1}{\lambda} \begin{bmatrix} s^{-1/2} u^\dagger C_0 & 0 \\ 0 & s^{1/2} v C_1 \end{bmatrix}, \tag{30}$$

and noting that $s^{-1/2} u^\dagger C_0 = s^{1/2} v C_1$, we have $C'H = HC'$. This gives

$$C_Z = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} C'C, \tag{31a}$$

$$C_X = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} HC'C. \tag{31b}$$

Similarly to the reasoning in Section III, Bob applies a virtual filter to transform $C_Z$ into an operator proportional to $C_X$. Applying

$$\frac{1}{\lambda} \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} H \frac{1}{\lambda} \begin{bmatrix} s^{-1/2} u^\dagger & 0 \\ 0 & s^{1/2} v \end{bmatrix},$$

the operator $C_Z$ is transformed into $C_X/\lambda^2$. Following Section III, $\sqrt{\eta} = 1/\lambda^2$. This gives

$$\sqrt{\eta} = \min(\min s, \min s^{-1}). \tag{32}$$

Equivalently, $\eta$ is the minimum value of the eigenvalues and inverse eigenvalues of $C_0 C_1^{-1} (C_0 C_1^{-1})^\dagger = C_0 (C_1^\dagger C_1)^{-1} C_0^\dagger$. This $\eta$ should be substituted into (17) to find the secure key generation rate.

The parameter $\eta$ can be measured as follows. For single photon input in a given superposition $\psi$ of logical "0" modes, the probability of a click in detector 0 is given by $\psi^\dagger C_0^\dagger C_0 \psi$. Similarly, we may use the identical superposition $\psi$ of "1" modes to find the detection probability of detector 1. Note that $\psi$ denotes a classical field vector, where each element corresponds to a separate mode. The parameter $\eta$ turns out to be equal to the minimum detection probability ratio

$$\eta = \min \left( \min_\psi \frac{\psi^\dagger C_0^\dagger C_0 \psi}{\psi^\dagger C_1^\dagger C_1 \psi}, \min_\psi \frac{\psi^\dagger C_1^\dagger C_1 \psi}{\psi^\dagger C_0^\dagger C_0 \psi} \right). \tag{33}$$

In other words, $\eta$ is given by the minimum efficiency mismatch ratio for all superpositions of input modes.

To see this, let $us^2 u^\dagger$ be the spectral decomposition of $C_0 (C_1^\dagger C_1)^{-1} C_0^\dagger$. Then we have

$C_0^{-1\dagger}(C_1^\dagger C_1)C_0^{-1} = us^{-2}u^\dagger$, and

$$
\begin{aligned}
\frac{\psi^\dagger C_1^\dagger C_1 \psi}{\psi^\dagger C_0^\dagger C_0 \psi} &= \frac{\psi'^\dagger C_0^{-1\dagger} C_1^\dagger C_1 C_0^{-1} \psi'}{\psi'^\dagger \psi'} \\
&= \frac{\psi'^\dagger u^\dagger s^{-2} u \psi'}{\psi'^\dagger \psi'} \\
&= s^{-2}.
\end{aligned}
\tag{34}
$$

Combining (32) and (34) gives the desired result.

### 4.3    DEM and misalignments

In addition to the detector efficiency mismatch in Subsection 4.1, suppose that Bob's detectors are misaligned. The misalignments may be dependent on Bob's choice of basis, and are described by unitary matrices $V_Z$ and $V_X$. This gives the channel operators $C_Z = F_Z V_Z C$ and $C_X = F_X V_X H C$. Assuming no coupling between different temporal modes (no multiple reflections), $V_Z$ and $V_X$ are block-diagonal matrices. For example,

$$
V_Z = \mathrm{diag}\left[V_1^{(2)} \quad V_2^{(2)} \quad V_3^{(2)} \quad \ldots\right],
\tag{35}
$$

where $V_j^{(2)}$ are unitary $2 \times 2$ matrices. Here we have used the same order of modes as in the original definition (11). Taking $F_X = F_Z$ and factorizing as in Subsection 4.1, we find that the parameter $\eta_Z = \eta_X$ again is given by (24). The secure key generation rate is then found from (17).

If there is coupling between modes associated with different $t$'s (in addition to the misalignment), we must retain the general definition of $\eta_Z$ in (14). For unnormalized detection efficiencies, this definition can be rewritten

$$
\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max_{i,t}\{\eta_{Zi}(t)\}}.
\tag{36}
$$

Eq. (36) is obtained by absorbing the maximum detector efficiency $\max_{i,t}\{\eta_{Zi}(t)\}$ into $C$. Omitting the requirement $F_X = F_Z$, (36) must be rewritten as

$$
\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max\left(\max_{i,t}\{\eta_{Zi}(t)\}, \max_{i,t}\{\eta_{Xi}(t)\}\right)}.
\tag{37}
$$

### 4.4    Characterizing DEM of Bob's receiver

To estimate the secure key generation rate, Bob must characterize his receiver to find $\eta_Z$ and $\eta_X$ (or $\eta \equiv \min\{\eta_Z, \eta_X\}$). We note that rather different results are obtained dependent on whether or not there are coupling between different modes. For the case of DEM in the time-domain, since it is difficult to eliminate multiple reflections in Bob's receiver, a conservative approach is to use (37).

For the case with gated detectors, the efficiencies approach zero at the edges of the detection window. When there are coupling between different temporal modes, the resulting key generation rate will therefore be close to zero. Even if no such coupling is present, the key generation rate may approach zero, since at the edges of the detection window the efficiency

ratio may be very small. (Although the average detection probability at the edges may be small, Eve may compensate this by replacing the channel by a more transparent one, or by increasing the power of her pulses [13].) A possible solution may be that Bob monitors his input signal at all times, to ensure that Eve does not send photons outside the central part of the window. Then $\eta$ can be obtained by measuring the minimum and maximum detection efficiency for (superpositions of) modes with times inside this central part.

Such a measurement may be cumbersome due to many degrees of freedom of the possible inputs. Alternatively, one could specify the maximum possible amount of mode coupling in the system, and use this information to lower bound $\eta$. Suppose that the maximum (power) coupling from one mode $j$ to all other modes is $\delta$. Then the unitary matrix $V_Z$ satisfies $\sum_{i,i\neq j} |V_{ij}|^2 < \delta$ in addition to $\sum_i |V_{ij}|^2 = 1$, omitting the subscript $Z$ for clarity. Let $|f_j|^2$ be the $j$th diagonal element of $F_Z$. By measuring the detection efficiency when photons are incident to the $j$th mode, we obtain $\sum_i |V_{ij}|^2|f_i|^2 = |f_j|^2 + \sum_{i,i\neq j} |V_{ij}|^2 \left(|f_i|^2 - |f_j|^2\right)$. Hence, the elements $|f_j|^2$ can be found from the detection efficiency as a function of $j$ of the incident mode, up to an error $\left|\sum_{i,i\neq j} |V_{ij}|^2 \left(|f_i|^2 - |f_j|^2\right)\right| < \delta$. A lower bound of $\eta$ is therefore

$$\eta > \frac{\min_{t,\text{basis,bit}}(\text{detection efficiency}) - \delta}{\max_{t,\text{basis,bit}}(\text{detection efficiency}) + \delta}. \tag{38}$$

The required measurement is to obtain the detection efficiency as a function of $t$ and logical bit value for both bases. For detection efficiency mismatch in the time-domain the test pulses should be sufficiently short, in order to capture all details. An upper bound of the parameter $\delta$ may be estimated from the (worst case) multiple reflections and misalignment's that may happen in the system.

## 5   Discussion and conclusion

In this work we have proved the security of BB84 in the presence of any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver/detectors. The security proof thus covers a combination of several imperfections: Detection efficiency mismatch, misalignments, mixing between the modes, multiple reflections, and any basis dependence of those effects. Contrary to most previous security proofs, this proof does not require a squashing detector model.

A specific implementation of a QKD system may have several different imperfections. Ideally there should be a universal security proof with a set of parameters that cover all (worst case) imperfections and tolerances of the equipment. We have made a step towards this goal by describing generic imperfections at the detector, and by providing a compact proof, which may hopefully prove useful for an even more general description.

We have established an upper bound for the secure key rate by providing two powerful attacks. One of the attacks may be applied to systems even with the four-state Bob patch, and this demonstrates the seriousness of the detection efficiency loophole. This attack is based on a combination of an optimal individual attack, a time shift attack, and a large pulse attack. As a consequence of such types of attacks, the key generation rate may not increase substantially as a result of the four-state Bob patch. A possible countermeasure is to use the general bounds (17) and (18) for estimating the required amount of privacy amplification.

**Acknowledgements**

**References**

1. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: Public key distribution and coin tossing* in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, New York, Bangalore, India, pp. 175–179.
2. A. K. Ekert (1991), *Quantum cryptography based on bell theorem*, Phys. Rev. Lett., Vol. 67, pp. 661–663.
3. C. H. Bennett (1992), *Quantum cryptography using any 2 nonorthogonal states*, Phys. Rev. Lett., Vol. 68, pp. 3121–3124.
4. N. Gisin, G. G. Ribordy, W. Tittel and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys., Vol. 74, pp. 145–195.
5. D. Mayers (1996), *Advances in cryptology* in N. Koblitz, editor, *Proceedings of Crypto'96*, Vol. 1109, Springer, New York, pp. 343–357.
6. D. Mayers (2001), *Unconditional security in quantum cryptography*, J. Assoc. Comp. Mach., Vol. 48, pp. 351–406.
7. H.-K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, Vol. 283, pp. 2050–2056.
8. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., Vol. 85, pp. 441–444.
9. H. Inamori, N. Lütkenhaus and D. Mayers (2001), *Unconditional security of practical quantum key distribution*, e-print quant-ph/0107017.
10. M. Koashi and J. Preskill (2003), *Secure quantum key distribution with an uncharacterized source*, Phys. Rev. Lett., Vol. 90, 057902.
11. D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, Quant. Inf. Comp., Vol. 4, pp. 325–360.
12. I. Csiszàr and J. Körner (1978), *Broadcast channels with confidential messages*, IEEE Trans. Inf. Theory, Vol. 24, pp. 339–348.
13. V. Makarov, A. Anisimov and J. Skaar (2006), *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A, Vol. 74, 022313; Ibid. **78**, 019905 (2008).
14. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma (2009), *Security proof of quantum key distribution with detection efficiency mismatch*, Quant. Inf. Comp., Vol. 9, pp. 131–165.
15. V. Makarov and J. Skaar (2008), *Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols*, Quant. Inf. Comp., Vol. 8, 0622.
16. B. Qi, C. H. F. Fung, H.-K. Lo and X. F. Ma (2007), *Time-shift attack in practical quantum cryptosystems*, Quant. Inf. Comp., Vol. 7, pp. 73–82.
17. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo (2008), *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A, Vol. 78, 042333.
18. P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård and E. Polzik (2001), *Experimental quantum key distribution with proven security against realistic attacks*, J. Mod. Opt., Vol. 48, pp. 1921–1942.
19. M. LaGasse (2005), *Secure use of a single single-photon detector in a qkd system*, US patent application 20050190922.
20. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard and H. Zbinden (2000), *Fast and user-friendly quantum key distribution*, J. Mod. Opt., Vol. 47, pp. 517–531.
21. D. S. Bethune and W. P. Risk (2000), *An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light*, IEEE J. Quantum Electron., Vol. 36, pp. 340–347.

22. A. Vakhitov, V. Makarov and D. R. Hjelme (2001), *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography*, J. Mod. Opt., Vol. 48, pp. 2023–2038.

23. N. Gisin, S. Fasel, B. Kraus, H. Zbinden and G. Ribordy (2006), *Trojan-horse attacks on quantum-key-distribution systems*, Phys. Rev. A, Vol. 73, 022320.

24. C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu and A. Peres (1997), *Optimal eavesdropping in quantum cryptography .1. information bound and optimal strategy*, Phys. Rev. A, Vol. 56, pp. 1163–1172.

25. U. M. Maurer (1993), *Secret key agreement by public discussion from common information*, IEEE Trans. Inf. Theory, Vol. 39, pp. 733–742.

26. L. B. Levitin (1995), *Optimal quantum measurements for two pure and mixed states* in V. P. Belavkin,O. Hirota and R. L. Hudson, editors, *Quantum Communications and Measurement*, Plenum Press, New York, pp. 439–448.

27. W. Y. Hwang (2003), *Quantum key distribution with high loss: Toward global secure communication*, Phys. Rev. Lett., Vol. 91, 057901.

28. X.-B. Wang (2005), *Beating the photon-number-splitting attack in practical quantum cryptography*, Phys. Rev. Lett., Vol. 94, 230503.

29. H.-K. Lo, X. F. Ma and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., Vol. 94, 230504.

30. M. Koashi (2006), *Efficient quantum key distribution with practical sources and detectors*, e-print quant-ph/0609180v1.

31. M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani (1994), *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett., Vol. 73, pp. 58–61.

32. M. Koashi (2005), *Simple security proof of quantum key distribution via uncertainty principle*, e-print quant-ph/05051080v1.

33. M. Koashi (2006), *Simple security proof of quantum key distribution via uncertainty principle*, J. of Phys. Conference Series, Vol. 36, 98.

34. H. Maassen and J. B. M. Uffink (1988), *Generalized entropic uncertainty relations*, Phys. Rev. Lett., Vol. 60, pp. 1103–1106.

35. R. Renner and R. Koenig (2005), *Universally composable privacy amplification against quantum adversaries* in J. Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005*, Vol. 3378 of *LNCS*, Springer Verlag, Berlin, pp. 407–425, also available at http://arxiv.org/abs/quant-ph/0403133.

36. M. Ben-Or, M. Horodecki, D. Leung, D. Mayers and J. Oppenheim (2005), *The universal composable security of quantum key distribution* in *Second Theory of Cryptography Conference*, Vol. 3378 of *Lecture Notes in Computer Science*, Springer, New York, pp. 386–406.

37. H.-K. Lo and J. Preskill (2007), *Security of quantum key distribution using weak coherent states with nonrandom phases*, Quant. Inf. Comp., Vol. 7, pp. 431–458.

## Appendix A Properties of vacuum measurement

Let $\{|n\rangle\}$ be an orthonormal basis for a state space of interest. We refer to the state $|0\rangle$ as the "vacuum state of all modes", although it could in principle be any fixed, pure state. A vacuum measurement is a projective measurement with projectors $P = |0\rangle\langle 0|$ and $I - P$. We claim that if $\mathcal{F}$ is any quantum operation satisfying (9), i.e.,

$$\mathcal{F}(|0\rangle\langle 0|) = |0\rangle\langle 0|, \tag{A.1}$$

the presence of a vacuum measurement before $\mathcal{F}$ does not change the statistics and output state of a vacuum measurement after $\mathcal{F}$, see Fig. A.1.

This result can be proved by using the fact that any quantum operation can be viewed as a unitary transformation on an extended state space, with a standard state $|0\rangle_{\mathrm{aux}}$ as auxiliary
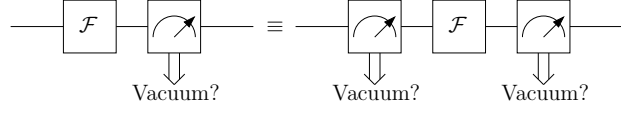
Fig. A.1. The statistics and output state of the vacuum measurement after $\mathcal{F}$ is not changed by the introduction of a vacuum measurement before $\mathcal{F}$.

input. Due to (A.1), we can assume that the unitary transformation transforms

$$|0\rangle \otimes |0\rangle_{\text{aux}} \rightarrow |0\rangle \otimes |0\rangle_{\text{aux}}, \tag{A.2}$$

with no loss of generality.

Consider the right-hand side of the identity (Fig. A.1). Let $P_{\text{aux}} = |0\rangle_{\text{aux}}\langle 0|_{\text{aux}}$. A vacuum measurement at the input can now be described as a projective measurement with $P \otimes P_{\text{aux}}$ and $I - P \otimes P_{\text{aux}}$, since the auxiliary input is fixed at $|0\rangle_{\text{aux}}$. Clearly, it does not matter if we measure the auxiliary output with projectors $P_{\text{aux}}$ and $I - P_{\text{aux}}$. In total, the extended measurement at the output is described by projectors $P \otimes P_{\text{aux}}$, $P \otimes (I - P_{\text{aux}})$, $(I - P) \otimes P_{\text{aux}}$, and $(I - P) \otimes (I - P_{\text{aux}})$. Transforming the projector $P \otimes P_{\text{aux}}$ backwards, we find that the corresponding projector at the input is $P \otimes P_{\text{aux}}$. In other words, the extended vacuum measurement at the output contains the vacuum measurement at the input, so the latter is redundant.