Quantum Science and Technology

RECEIVED
4 December 2016

REVISED
14 July 2017

ACCEPTED FOR PUBLICATION
3 August 2017

PUBLISHED
13 September 2017

PAPER

Secure detection in quantum key distribution by real-time calibration of receiver

Øystein Marøy[1], **Vadim Makarov**[2,3,4] **and Johannes Skaar**[1,5,6]

[1] Department of Electronic Systems, NTNU—Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[2] Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[3] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[4] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada
[5] Department of Technology Systems, University of Oslo, Box 70, NO-2027 Kjeller, Norway
[6] Author to whom any correspondence should be addressed.

E-mail: johannes.skaar@its.uio.no

Keywords: quantum key distribution, quantum cryptography, imperfect detector, detection efficiency, security proof

Abstract

The single-photon detectionefficiency of the detector unit is crucial for the security of common quantum key distribution protocols like Bennett-Brassard 1984 (BB84). A low value for the efficiency indicates a possible eavesdropping attack that exploits the photon receiver's imperfections. We present a method for estimating the detection efficiency, and calculate the corresponding secure key generation rate. The estimation is done by testing gated detectors using a randomly activated photon source inside the receiver unit. This estimate gives a secure rate for any detector with non-unity single-photon detection efficiency, both inherit or due to blinding. By adding extra optical components to the receiver, we make sure that the key is extracted from photon states for which our estimate is valid. The result is a quantum key distribution scheme that is secure against any attack that exploits detector imperfections.

1. Introduction

Quantum key distribution (QKD) [1, 2] is a method to distribute a secret key between two separate parties, commonly named Alice and Bob. In a QKD scheme, Alice and Bob share a quantum channel to distribute the key, as well as an authenticated classical channel for post processing. They also need a source to create a quantum signal, and a detector. An eavesdropper, Eve, is allowed full control over the quantum channel and may listen to the classical channel. Under these conditions, and under the assumption that Alice and Bob's equipment is flawless, QKD has been proven unconditionally secure [3, 4].

In the real world, equipment is imperfect. Security has been proven for certain general and specific imperfections [5–7]. However, for several different imperfections, attacks against QKD systems have been proposed [8–21]. Most of these studies experimentally demonstrated imperfection of a system component or subsystem that would allow an attack, but a couple experiments demonstrated successful eavesdropping of the key in a running system [14, 16]. Many realistic attacks, including the latter two, take advantage of imperfections in the detectors [8–10, 12–14, 16, 17, 21–25]. A secure setup requires Bob to measure the signal in a randomly chosen basis. Any differences in detection probability between the bases, in any domain (time, frequency, or modes), can be exploited by Eve [26, 27]. Such differences may either be inherent in the system itself or be forced upon the system by Eve, for example by blinding one of the detectors [12, 14].

Several solutions have been proposed to the problems caused by imperfect detectors. One option is to use a security proof which is valid for uncharacterized detectors [28]; however, then a positive QKD rate requires unrealistically high-detection efficiency in the system. A promising approach is the so-called measurement device-independent QKD [29], where a secure key is generated even with untrusted detectors at the expense of a somewhat more complicated system [30, 31]. Another more direct approach is to find countermeasures for each attack [32–34]. While convenient and practical, one cannot necessarily be sure that the countermeasures close all

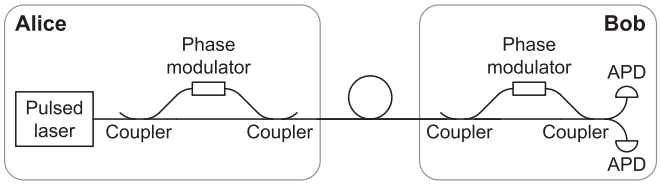

Figure 1. Alice and Bob's system for BB84 quantum key distribution.

types of attacks or just the already known attacks [35–37]. Also, the countermeasure itself often requires new components or modified setups, which in turn may open new loopholes.

In this article, we suggest an approach that secures the detector against all attacks as long as some reasonable assumptions are satisfied. This will be done by using the security proof in [38], where Bob's part of the system is characterized by a parameter η, which corresponds to the minimum probability that a non-vacuum signal incident to Bob is actually detected by him. Using an additional photon source, we can estimate η, and quantify the trustworthiness of the detectors. To make sure the assumptions for our proof are satisfied, we make some modifications to Bob's part of the system and use bit-mapped gating [39]. A secure key rate can then be calculated. Qualitatively, it can be said that the bit-mapped gating and the modifications to Bob takes care of detector efficiency mismatch type loopholes; our additional photon source takes care of attacks exploiting low single-photon detection efficiency, like the blinding attack.

For simplicity, we consider the special case of infinite key length (known as the asymptotic limit). Similarly, to the so-called device-independent QKD scenario, we assume that no information leaks out of Alice's and Bob's devices [40]. However, the result may be combined with imperfections in the source and with information leakage from the detectors, both as done in [38] and with decoy states [41–43].

2. Setup and security proof

We will consider the Bennett-Brassard 1984 (BB84) [1] protocol using a fiber-based setup with phase coding [44] and gated detectors. However, the ideas presented may also be adapted to free-space QKD [45], and to other encoding protocols. In phase-based QKD, the key is encoded into the phase difference between the two parts of a light pulse. Figure 1 shows a typical phase-based QKD system. The pulse is created at Alice's side. Using an unbalanced mach-Zehnder interferometer, she splits it and encodes her choice of bit and basis by introducing a relative phase shift between the two halves. Bob's part of the system, hereafter referred to as Bob, consists of a similar interferometer and two single-photon detectors.

Alice and Bob choose one of two bases for each pulse and each detection. These two bases are usually referred to as the z basis and x basis. In a practical setup, the pulses live in a large Hilbert space consisting of several Fock spaces, and the z and x bases do not correspond to the usual z and x bases in two-dimensional Hilbert space. They are just names for the two (possibly misaligned) bases that Alice and Bob specify. The key is created from the n pulses where the same basis is chosen by both Alice and Bob, and detection time corresponds to the pulse traveling the short arm of one interferometer and the long arm of the other. For these pulses interference between the two possible paths allows the bit value sent by Alice to be obtained by observing in which of the detectors the pulse arrives.

The choice of which basis to assign to each letter, x and z, is arbitrary. In fact, Alice and Bob may randomize this assignment for each pulse, creating a protocol that is symmetric between the bases. The system's average yield $\bar{q}$, which is the fraction of pulses that are detected by Bob, and $\bar{\delta}$, the average error rate for those pulses, are then both equal in the two bases[7]. The secure key generation rate extracted from $n\bar{q}$ bits received by Bob is given by [6]

$$R = 1 - h(\bar{\delta}) - \frac{H}{n\bar{q}} \tag{1}$$

in the asymptotic limit. The function $h(\cdot)$ is the binary Shannon entropy, and H is the amount of privacy amplification needed to remove Eve's knowledge of the key. If η is constant during the transmission, we have [38]

$$H = n(\bar{q} - \eta\bar{q}(1 - h(\bar{\delta}))). \tag{2}$$

[7] This symmetrization simplifies the analysis of the secret rate. In the case of a difference between yields, q_z and q_x, or error rates, δ_z and δ_x, between the bases of the unsymmetrized protocol, the symmetrization leads to a lower rate. However, such differences will generally be small and the impact on the secret rate insignificant.

Here, for simplicity, we have assumed that the source is perfect; the case with imperfections in the source can easily be covered by a small modification to (2) [38].

To find a valid numerical expression for the key generation rate, η needs to be lower bounded. The parameter η is, as in [38], interpreted as the minimum probability that a non-vacuum incident to the basis-dependent interferometer in Bob is detected. Thus, η is a parameter explicitly given by the state of Bob's system, while the yield q is dependent on both Bob's system and the incoming pulse. In a real QKD experiment, the state of Bob's system might change during key exchange. For example, the characteristics of the detectors may change as a result of bright illumination from Eve, as in the blinding attacks [12]. We will therefore consider η a variable parameter depending on the state of Bob's system. Before each individual qubit measurement, the system is characterized by the parameter η_i, which is the minimum probability that a non-vacuum signal is detected by Bob. The index i labels the different possible characteristics of Bob's system and $_{pi}$ is the probability that the system is in the state i. Note that η_i is independent of Bob's basis choice; it is the minimum over any possible configuration of Bob's system.

Because Eve may want to tune the yield q and error probability δ to correlate them with η_i, we need to index them by i as well. We note that Eve may control η_i, q_i, and δ_i. In the same way as $\bar{\delta}$ is the average error probability for those signals that are detected by Bob, we define $\bar{\eta}$ as the average value of η for those same detected signals. This is also in accordance with the security analyses in [38] [8]. According to these definitions, the parameters are subject to the relations

$$\sum_i p_i = 1, \tag{3a}$$

$$\sum_i p_i q_i = \bar{q}, \tag{3b}$$

$$\sum_i p_i q_i \eta_i = \bar{q}\bar{\eta}, \tag{3c}$$

$$\sum_i p_i q_i \delta_i = \bar{q}\bar{\delta}. \tag{3d}$$

Using random sampling to estimate $\bar{\delta}$, error correction can still be done by sacrificing $h(\bar{\delta})$ bits. The quantity H in (1) is now bounded by

$$\begin{aligned} H &\leqslant \max_{p_i,\eta_i,q_i,q_i,\delta_i} \sum_i (np_i q_i - np_i\eta_i q_i(1 - h(\delta_i))) \\ &= n\bar{q} - n\bar{\eta}\bar{q} + \max_{p_i,\eta_i,q_i,\delta_i} n\sum_i p_i\eta_i q_i h(\delta_i). \end{aligned} \tag{4}$$

Using the concavity of the binary entropy, we have, for any $\bar{q}$, $\bar{\eta}$ and $\bar{\delta} \leqslant \bar{\eta}/2$

$$\begin{aligned} \sum_i p_i q_i \eta_i h(\delta_i) &\leqslant \bar{q}\bar{\eta}\sum_i \frac{p_i q_i \eta_i}{\bar{q}\bar{\eta}} h(\delta_i) \\ &\leqslant \bar{q}\bar{\eta} h\left(\sum_i \frac{p_i q_i \delta_i \eta_i}{\bar{q}\bar{\eta}}\right) \\ &\leqslant \bar{q}\bar{\eta} h\left(\sum_i \frac{p_i q_i \delta_i}{\bar{q}\bar{\eta}}\right) \\ &\leqslant \bar{q}\bar{\eta} h\left(\frac{\bar{\delta}}{\bar{\eta}}\right). \end{aligned} \tag{5}$$

We therefore obtain

$$H \leqslant n\bar{q}\left(1 - \bar{\eta}\left(1 - h\left(\frac{\bar{\delta}}{\bar{\eta}}\right)\right)\right). \tag{6}$$

The bound (6) is tight, as the right-hand side is achieved if Eve controls the system as follows. For $np_1q_1 = n\bar{q}\bar{\eta}$ detected pulses, the system is in some state with $\eta_1 = 1$ and $\delta_1 = \bar{\delta}/\bar{\eta}$. For the remaining $n\bar{q}(1 - \bar{\eta})$ detected pulses, the system is in a state with $\eta_2 = 0$ and $\delta_2 = 0$. The key generation rate is bounded by

$$R \geqslant \bar{\eta}\left(1 - h\left(\frac{\bar{\delta}}{\bar{\eta}}\right)\right) - h(\bar{\delta}). \tag{7}$$

This rate is similar to the main result from [38], with the parameter η replaced by its average value and $q_x = q_z$. A main difference is the factor $1/\bar{\eta}$ inside the binary entropy function, which leads to a reduction of the rate. This is

[8] $\bar{\eta}$ could also have been defined as the average value of η over all incoming signals. This would change equations (3)–(7) and equation (11), but the main result equation (12) would be the same.

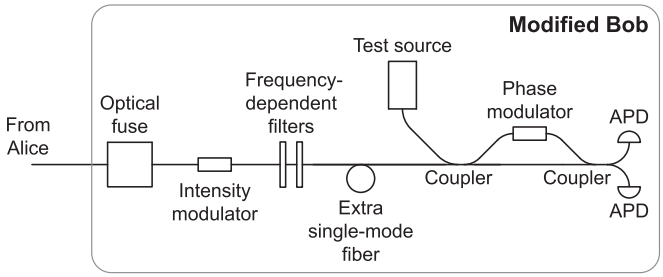

Figure 2. Bob's modified system including a test source.

due to Eve's ability to avoid introducing errors when the detectors are in a vulnerable state. On the other hand, in [38] η must be interpreted as a minimum value, which in many cases leads to zero rate.

3. Modifications to Bob

We now turn to find a lower bound for the average minimum detection probability $\bar{\eta}$. The main idea is to have a source inside Bob's setup to test detector sensitivities at random times. We will discuss Bob's parameter η as a function of frequency (i.e., wavelength of light), time or as a function of detailed field distributions. In this context, η is defined as the minimum detection probability of a non-vacuum state with the prescribed frequency, time or field distribution.

In general, the detection probability depends to some extent on the incoming photons frequency, polarization mode, phase and the time of arrival. These parameters may take infinitely many different values. Thus, it is unfeasible to find a lower bound for every state experimentally. Instead, we restrict the state space $\mathcal{T}$ of the incoming signals by modifying Bob. These modifications will make sure that any single-photon pulse in $\mathcal{T}$ will have almost the same detection probability. The modifications are all placed before the interferometer and Bob's basis choice. Any loss due to these components will then only contribute to a smaller yield q, and not to η. We can now estimate $\bar{\eta}$ from the detection rate q_T of test pulses in $\mathcal{T}$. The test pulses are generated by a source, fired at randomly chosen gates. The pulses are coupled into the fiber scheme before the interferometer. The modifications are shown in figure 2.

The first element in the modified Bob is an optical fuse. If Eve tries to send a pulse with higher power than a certain value P_0, this element will be destroyed and communication on the quantum channel will stop. This serves a dual purpose. Bounding the power of Eve's pulse is helpful in our security analysis. Also, deprived of the possibility of sending strong pulses, we may assume that Eve cannot radically change the behavior of the optical elements in Bob's system via laser damage [46, 47].

If some of Eve's pulses are let into Bob when we run the test pulses, our test results will be disturbed. We therefore want an element to deflect, extinguish or at least dampen Eve's pulses at these times. In combination with the optical fuse, this switch or modulator makes sure that Eve's pulses consist mainly of vacuum when we are sending test pulses. The disturbance of the test measurement statistics must be close to negligible. Note that this switch or modulator should not change the parameters q_i and δ_i in any other pulses from Eve, as this may give Eve some information about when we are sending test pulses.

Assumption 1. When we are sending a test pulse, any pulse from Eve will change the probability of a detection by at most ϵ_E.

To allow just a small bandwidth into Bob, we use a narrowpass filter that transmits light within a frequency range $\Omega = [\omega_0 - \omega_B, \omega_0 + \omega_B]$, and heavily attenuates all light outside it. In practice, such filter can be achieved by a combination of interference- and absorption-based optical filters. The central frequency of the filter, ω_0, is the same as the central frequency of Alice's pulse[9].

Assumption 2. For any pulse from Eve with frequencies outside the range Ω, the probability that at least one photon is transmitted through the filter and detected is smaller than q_ω [10].

[9] Another interesting idea is to use frequency-dependent phase modulation. Then frequencies different from ω_0 are detected by an increased error rate.

[10] Frequencies inside Ω will also be attenuated by this filter. However, as this loss is basis-independent, we can attribute it to Eve and it doesn't contribute to η.

The probability q_ω depends on the filter performance and the power P_0 needed to damage the optical fuse. For later use, let ζ_ω be the fraction of detection events that corresponds to photons outside Ω. Clearly, $\zeta_\omega \leqslant q_\omega/q$.

For states in Ω we make the following assumption.

Assumption 3. For any frequencies $\omega_1,\ \omega_2 \in \Omega, |\eta(\omega_1) - \eta(\omega_2)| \leqslant \epsilon_\Omega$.

When it comes to spatial modes, almost all incoming waves now have the same frequency. We can then insert a short length of single-mode fiber in front of the interferometer.

Assumption 4. At most $n\zeta_k$ of the pulses detected by Bob have another mode than the mode allowed in the single-mode fiber.

The parameter ζ_k depends on P_0 and the length of the single-mode fiber. We make sure that all of this fiber is inside Bob so Eve cannot easily access it.

Having made sure that virtually all signals entering Bob have the required frequency and mode, we now consider the timing of the signal. Because Eve controls the fiber between Alice and Bob, we must assume that she can control this timing. A gated detection scheme is thus needed, where the following assumption is satisfied.

Assumption 5. For any times $t_1,\ t_2$ inside the gate, $|\eta(t_1) - \eta(t_2)| \leqslant \epsilon_T$.

As long as this assumption holds true, we can fire our test pulse at any time inside a gate. Eve's advantage by choosing another part of the gate is limited by ϵ_T.

If Bob's system suffers from detector efficiency mismatch [8], η is not slowly varying at the beginning and the end of the gate. We would therefore like to discard pulses which arrive at these times. Due to jitter in the detector of the same order of magnitude as the detector gate length [48], it is impossible to recognize these events after detection. We therefore suggest to employ the technique of bit-mapped gating [39]. Any signal detected at the beginning and end of the gate will have a random value and contribute to the error rate δ. At least a fraction $(1 - 2\delta)$ of the detected signals must then have passed inside the inner gate, for which assumption 5 is valid. Another feature of bit-mapped gating is that the two detectors are randomly assigned to bit value 0 or 1 for each pulse. Thus, our setup is equivalent to a setup with one detector which measures whether the bit is 0 or 1. We therefore don't need to measure η for the two detectors seperately. Finally, we note that the detection probability drops to zero immediately after a detection. Although this violates assumption 5, it does not affect $\bar{\eta}$ as we can only have one detection per gate.

We also need to consider the number of photons in the pulse. We cannot test all possible states; however, for weak pulses detection probability increases with the number of photons in the pulse. Thus, the following assumption is natural.

Assumption 6. The detection probability is smaller for a single photon than for any multiphoton state.

The pulse arrives at Bob in two parts: the first gives detection if the photon travels in the long arm of the interferometer and the last gives detection if the photon travels the short arm. To some extent, η may depend on the phase, polarization or detailed shape of the two parts. However, due to assigning each detector to a random bit value for each pulse, such dependency should be small. Let the detailed field, including the polarization, be described by $\psi(t)$ as a function of time.

Assumption 7. For any two distributions $\psi_1(t)$ and $\psi_2(t)$, $|\eta_{\psi_1} - \eta_{\psi_2}| \leqslant \epsilon_I$.

4. Key generation rate with estimation of η

Because of the modifications to Bob most of the pulses entering the detectors are now in $\mathcal{T}$, Eve would like as many pulses as possible outside $\mathcal{T}$ because for these pulses she can construct states for which $\eta = 0$ without getting noticed. To get an upper bound on the fraction of pulses not in $\mathcal{T}$, we note that being outside of $\mathcal{T}$ in both frequency and mode dimensions further decreases the detection probability of these pulses. Therefore, Eve should send pulses which is outside $\mathcal{T}$ only in the dimension where the transmission probability is largest. In addition, some of the detected pulses might be outside $\mathcal{T}$ in the time dimension. With probability larger than

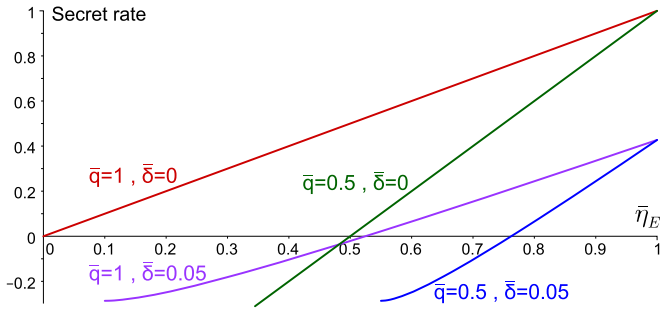

Figure 3. Key generation rate (equation (12)) as a function of estimated single-photon detection efficiency $\bar{\eta}_E$ for different values of the yield $\bar{q}$ and error rate $\bar{\delta}$.

$$1 - \zeta = 1 - 2\delta - \max\{\zeta_\omega, \zeta_k\}, \tag{8}$$

a detection event originates from a photon with frequency in Ω, arrival time in the gate and with the same mode as the test pulse.

If Bob's test pulse is a single-photon source, the minimum detection probability η_T of a single-photon state in $\mathcal{T}$ is bounded by the measured detection probability of the test pulse, q_T:

$$\eta_T \geqslant q_T - \epsilon_E - \epsilon_\Omega - \epsilon_T - \epsilon_I = q_T - \epsilon_{\text{tot}}. \tag{9}$$

Here, $\epsilon_{\text{tot}} = \epsilon_E + \epsilon_\Omega + \epsilon_T + \epsilon_I$. For states not in $\mathcal{T}$, we have no such bound. A lower bound for the estimated average minimum detection probability of single-photon states, $\bar{\eta}_E$, is then

$$\bar{\eta}_E \geqslant (1 - \zeta)\eta_T = (1 - \zeta)(q_T - \epsilon_{\text{tot}}). \tag{10}$$

We now need to take into account that the parameter $\bar{\eta}$ in equation (7) is the average value of η for those $n\bar{q}$ states which were detected. In the worst-case scenario, the remaining $n(1 - \bar{q})$ non-detected states have $\eta = 1$, such that

$$\bar{\eta}_E = \bar{q}\bar{\eta} + (1 - \bar{q}). \tag{11}$$

By combining (7) and (11), the expression for the key generation rate when using single photons as test pulses is found to be

$$R \geqslant \frac{\bar{q} + \bar{\eta}_E - 1}{\bar{q}}\left(1 - h\left(\frac{\bar{q}\bar{\delta}}{\bar{q} + \bar{\eta}_E - 1}\right)\right) - h(\bar{\delta}). \tag{12}$$

This is our main result, in addition to the corresponding expression when using a faint laser source to produce the test pulses (section 5.2). The main difference from the rate resulting from (1) and (2) is the dependence on the detection rate $\bar{q}$ and estimated detector parameter $\bar{\eta}_E$. This is due to the possibility that Eve forces detections when the detectors are in a vulnerable mode and no detections when the detectors are safe. Thus, the detectors need to be subject to random testing during key exchange. Any successful attempt from Eve to control the measurement results without introducing errors will show up as $\bar{\eta}_E < 1$ during testing. As seen in figure 3, as long as $\bar{q}$ remains high, positive key rate is still possible for small $\bar{\eta}_E$. Key gain is possible for $\bar{\eta}_E + \bar{q} \geqslant 1$ in an error-free protocol.

5. Key generation rate with practical equipment

When building Bob as described in figure 3, some parts are challenging to implement. In this section, we will consider certain solutions to these challenges.

5.1. Detectors with low efficiency

Commercially available detectors used in QKD operate with a detection efficiency substantially less than 1, with most avalanche photodiodes having detection efficiency in the 0.1 to 0.5 range [48–50]. This leads to the factor $(\bar{q} + \bar{\eta}_E - 1)$ being negative and (12) giving negative key rate. A practical solution to this is to assume that no matter what Eve does, she cannot improve the single-photon detection efficiency beyond some upper limit $\eta_{\max}$. This leads to some adjustments in the rate. In the third step of Inequality (5), we now get an extra factor $\eta_{\max}$ in

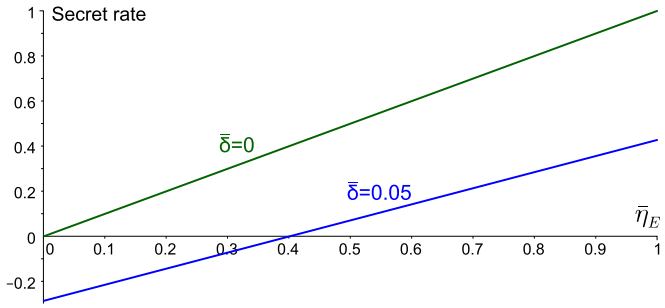

Figure 4. Key generation rate (equation (15)) as a function of estimated single-photon detection efficiency, $\bar{\eta}_E$, in the case where $\bar{\eta}_E$, is equal to the expected value $\eta_{\max}$. The rate is plotted for different error rates $\bar{\delta}$, and is valid for any yield $\bar{q}$.

the argument of the entropy function, $\bar{q}\bar{\eta}h\left(\sum_i \frac{p_i q_i \delta_i \eta_i}{\bar{q}\bar{\eta}}\right) \leqslant \bar{q}\bar{\eta}h\left(\sum_i \frac{p_i q_i \delta_i \eta_{\max}}{\bar{q}\bar{\eta}}\right)$. This factor carries over to equation (7) giving

$$R \geqslant \bar{\eta}\left(1 - h\left(\frac{\bar{\delta}\eta_{\max}}{\bar{\eta}}\right)\right) - h(\bar{\delta}). \tag{13}$$

Additionally, we must make the following adjustment to equation (11):

$$\bar{\eta}_E = \bar{q}\bar{\eta} + (1 - \bar{q})\eta_{\max}, \tag{14}$$

Combining equations (13) and (14) gives a rate

$$R \geqslant \eta_{\max}\frac{\bar{q} + \frac{\bar{\eta}_E}{\eta_{\max}} - 1}{\bar{q}}\left(1 - h\left(\bar{\delta}\frac{\bar{q}}{\bar{q} + \frac{\bar{\eta}_E}{\eta_{\max}} - 1}\right)\right) - h(\bar{\delta}). \tag{15}$$

Note that the expression (15) simplifies to

$$R = \bar{\eta}_E(1 - h(\bar{\delta})) - h(\bar{\delta}) \tag{16}$$

for $\bar{\eta}_E = \eta_{\max}$, i.e. when the detector is working as well as we expect it to. This is the same rate as one gets if η is treated as a constant parameter [38]. This rate is depicted in figure 4 for different error rates $\bar{\delta}$. This shows that a detector with low single-photon efficiency is not a great security risk in itself, but is detrimental to the rate. A detector that shows a worse single-photon efficiency than expected indicates a possible attack from Eve and requires even more privacy amplification.

5.2. Estimation of η with a faint pulsed laser

While single photons sources are available [50] and have been used in some QKD experiments [51, 52], using a faint laser to produce the test pulse provides an easier setup. For a phase-randomized source with mean photon number μ, the produced state is

$$\rho_B = e^{-\mu}|0\rangle\langle 0| + \mu e^{-\mu}|1\rangle\langle 1| + (1 - e^{-\mu} - \mu e^{-\mu})\sigma_m, \tag{17}$$

with σ_m being all states with more than one photon. This changes the relationship (9) between the detection rate of the pulses q_T and the minimum single-photon detection probability η_T. We now have

$$q_T \leqslant e^{-\mu}d + \mu e^{-\mu}(\eta_T + \epsilon_{\text{tot}}) + (1 - e^{-\mu} - \mu e^{-\mu}), \tag{18}$$

or

$$\eta_T \geqslant 1 - \epsilon_{\text{tot}} + \frac{1 - d}{\mu} - \frac{1 - q_T}{\mu e^{-\mu}}. \tag{19}$$

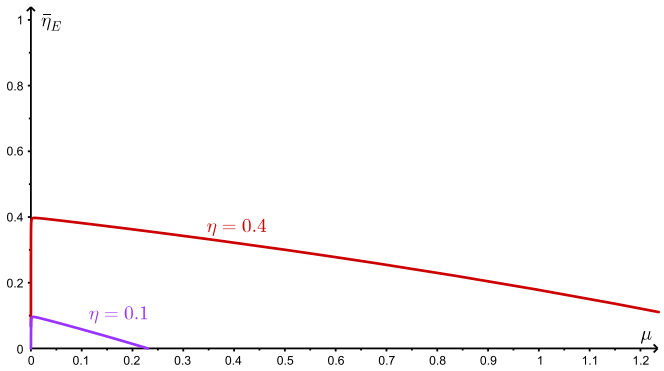

Figure 5. Estimated single-photon efficiency η_E as a function of mean photon number μ of for two different detectors: one with detection efficiency $\eta = 0.1$ and dark count rate $2 \cdot 10^{-5}$ (lower line) [53] and one with detection efficiency $\eta = 0.4$ and dark count rate $2 \cdot 10^{-5}$ (upper line).

In this case, the key generation rates given by (12) and (15) are still valid, but the limit for $\bar{\eta}_E$ in (10) is replaced with

$$\begin{aligned}\bar{\eta}_E &\geqslant (1-\zeta)\left(1-\epsilon_{\text{tot}}+\frac{1-d}{\mu}-\frac{1-q_T}{\mu e^{-\mu}}\right)\\ &= (1-\zeta)\left(\frac{q_T-d}{\mu}+q_T-\frac{\mu}{2}-\epsilon_{\text{tot}}\right)\\ &\quad+\mathcal{O}(\mu^2)+\mathcal{O}(\mu q_T).\end{aligned} \tag{20}$$

The dark count rate per gate per pair of detectors, d, can be upper bounded by turning off the test pulse while stopping Eve's pulses. As shown in figure 5, for a sufficiently small d, we can choose a small μ and obtain a result that is approximately the same as for a single-photon source. The lower line corresponds to a detector with $\eta = 0.1$, $d = 2 \cdot 10^{-5}$ as in [53]. The upper line shows a more sensitive detector with $\eta = 0.4$, $d = 2 \cdot 10^{-5}$. For both detectors, $\zeta = \epsilon_{\text{tot}} = 0$ is assumed for simplicity; for multiphoton states, each photon is assumed to be detected independently. We see that for both detectors, the method described in the previous subsection, using an estimate of η_{max}, is needed for positive rate. For the less sensitive detector, a very low μ is needed to approach the true value $\eta = 0.1$.

5.3. Testing without deflecting Alice/Eve

The element used to deflect/destroy Alice's pulse during testing must be able to change quickly between total transmittance and total absorbance or deflection. Constructing or finding such an element is challenging. As an alternative, testing can be done without deflecting Alice's pulse simply by coupling the test pulse into the line using a fiber optic coupler. Assumption 1 is then no longer valid. We can replace it with an assumption bounding the superlinearity [13] of the detector response.

Assumption 1a. Let q_T' be the actual detection probability under testing. Then $q_T' \leqslant q + q_T + \epsilon_S$, with q_T being the detection probability if Eve were totally disconnected and ϵ_S bounding the superlinearity of the detector.

The key generation rates given by (12) and (15) are valid in this approach also, with ϵ_S replacing ϵ_E and setting $q_T = q_T' - q$ in (9).

The validity of this assumption needs some further discussion. If a detector is blind for pulses below some threshold intensity and Eve sends pulses slightly below this threshold, clearly $q_T' > q + q_T$ could be possible. However, as long as the test pulse is weak ($\mu < 1$), the increase in detection probability by adding a test pulse to Eve's pulse should be small, especially because Eve won't be able to control the exact number of photons in her pulse reaching the detector due to losses in Bob. Therefore, ϵ_S might be considered small.

Security-wise, testing without deflecting Eve is possible, but for the secure key rate, such an approach seems disastrous. For positive key rate, $\bar{\eta}_E + q \geqslant 1$ is needed. The value we use for $\bar{\eta}_E$ is the lower bound given by (10). This bound is smaller than q_T. For positive rate, we therefore need $q + q_T > 1$, but this is impossible if we use $q_T = q_T' - q$. Thus, either some intensity modulation of Eve's pulse must be done during testing, or stricter assumptions upon the linear response of the detector are needed.

6. Discussion and conclusion

We proposed a method to estimate the average detection efficiency parameter $\bar{\eta}$. Given this parameter, QKD is secure for all imperfections in Bob, as long as no signals are emitted from him. Furthermore, information leakage from Alice and Bob can be taken into account by the approach in [38]. In this case, more work is needed to estimate the relevant parameters describing leakage. Alternatively, an approach to estimate leakage is proposed in [54, 55]. The proof of this approach is also based on Koashi's proof [6] which makes reconciling it with the proof in this article promising. Anyway, the introduction of new components in Bob must be considered in the estimation of information leakage.

When estimating η, the parameters in figure 3, ζ_ω, ϵ_Ω, ζ_k, ϵ_T, ϵ_I and ϵ_E, must be determined by Alice and Bob. If Eve can control these parameters, the assumptions of the security proof are not satisfied. The parameters ζ_ω, ϵ_Ω, ζ_k, ϵ_I and ϵ_E are controlled by the components in Bob, and can be estimated by testing these components. Their values are small in a proper setup, and conservative estimates will not affect the key generation rate considerably. We assume that the conservative estimates apply, unless irreversible and detectable damage is induced by Eve. Thus, these parameters do not need continuous monitoring like η. To keep ϵ_T small, a bit-mapped gated detection scheme [39] is necessary and sufficient.

The rate is strongly dependent on the yield $\bar{q}$ and estimated avreage detection efficiency $\bar{\eta}_E$. Realistically, the yield is less than the detection efficiency, which means that in practice, $\bar{\eta}_E \geqslant 1/2$ is needed for a positive key generation rate. The reason for this can be seen from the attack where Eve controls the system as described before equations (7) and (11). In this case, the bound for the secret key generation rate (12) is tight. Equality is attained by an attack where Eve controls both the incoming pulses and the single-photon detection efficiency. In the attack, $n\bar{q}(1-\bar{\eta})$ pulses are detected correctly while the detector is blind to single photons. The remaining $n\bar{q}\bar{\eta}$ detected pulses are detected, with some errors, while the detectors are sensitive to every single-photon pulse. The final $n(1-\bar{q})$ pulses are vacuum and the detector would have detected them if they were single photons. This attack shows why a decent detector with single-photon efficiency $\eta = 0.5$ can be considered insecure. If Eve controls η, she can e.g. increase it to unity for half of the pulses and let the detector be blind to single photons ($\eta = 0$) for the other half. In the instances when the detector is blind, she can send weak pulses as in the blinding attack [12] and get full knowledge of the key. In this case, we would still measure $\bar{\eta} = 0.5$.

To improve the rate, one needs to verify or assume that Eve does not control the system as described before equations (7) and (11). We describe one such possible assumption, assuming that Eve cannot increase the single-photon detection efficiency beyond some value $\eta_{\max}$ to fool the estimation procedure. This assumption seems reasonably safe, given that the setup prevents the use of laser damage [46, 47]. Under this assumption, as long as the estimated single photon η_E is close to $\eta_{\max}$, the key rate before error correction is the same as in QKD with perfect equipment multiplied by the single-photon detection efficiency. Key gain is therefore clearly possible, but non-unity single-photon detection efficiency is still a disadvantage with respect to the rate.

Implementation of the modified Bob's setup is relatively simple in principle. However, it is challenging to find a sufficiently fast element for deflecting Eve's pulses during testing. Without it, a stricter assumption on the behavior of the detector is needed and the rate suffers. The single-photon source in Bob can be replaced by a faint laser similar to the one in Alice, as long as Bob's dark count rate is sufficiently small.

The setup and method described here can be an important step towards practical secure QKD. Security is no stronger than the weakest link. Because QKD is unconditionally secure with perfect equipment, the implementation is where Eve has had the best opportunities for attack. Our method gives secure key generation under realistic and testable assumptions.

Acknowledgments

ØM and JS thank the University Graduate Center, NO-2027 Kjeller, Norway, for providing a workplace.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE International Conf. on Computers, Systems, and Signal Processing (Bangalore, India)* (New York: IEEE Press) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Mayers D 1996 *Proc. of Crypto'96* vol 1109 ed N Koblitz (New York: Springer) pp 343–57
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[6] Koashi M 2009 *New J. Phys.* **11** 045018
[7] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J.* D **41** 599
[8] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
Makarov V, Anisimov A and Skaar J 2008 *Phys. Rev.* A **78** 019905

[9] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388
[10] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[11] Xu F, Qi B and Lo H-K 2010 *New J. Phys.* **12** 113026
[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686
[13] Lydersen L, Jain N, Wittmann C, Marøy Ø, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev.* A **84** 032320
[14] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[15] Li H-W *et al* 2011 *Phys. Rev.* A **84** 062308
[16] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
[17] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
[18] Sun S-H, Jiang M-S and Liang L-M 2011 *Phys. Rev.* A **83** 062331
[19] Jiang M-S, Sun S-H, Li C-Y and Liang L-M 2012 *Phys. Rev.* A **86** 032310
[20] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[21] Sajeed S, Chaiwongkhot P, Bourgoin J-P, Jennewein T, Lütkenhaus N and Makarov V 2015 *Phys. Rev.* A **91** 062301
[22] Lydersen L, Akhlaghi M K, Majedi A H, Skaar J and Makarov V 2011 *New J. Phys.* **13** 113042
[23] Tanner M G, Makarov V and Hadfield R H 2014 *Opt. Express* **22** 6734
[24] Kurtsiefer C, Zarda P, Mayer S and Weinfurter H 2001 *J. Mod. Opt.* **48** 2039
[25] Meda A, Degiovanni I P, Tosi A, Yuan Z L, Brida G and Genovese M 2017 *Light Sci. Appl.* **6** e16261 accepted article preview
[26] Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 *Quantum Inf. Comput.* **9** 131
[27] Lydersen L and Skaar J 2010 *Quantum Inf. Comput.* **10** 0060
[28] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[29] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[30] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[31] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[32] Yuan Z L, Dynes J F and Shields A J 2010 *Nat. Photonics* **4** 800
[33] Yuan Z L, Dynes J F and Shields A J 2011 *Appl. Phys. Lett.* **98** 231104
[34] Lim C C W, Walenta N, Legré M, Gisin N and Zbinden H 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 6601305
[35] Lydersen L, Wiechers C, Wittmann C, Elser D, Makarov V and Skaar J 2010 *Nat. Photonics* **4** 801
[36] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Appl. Phys. Lett.* **99** 196101
[37] Huang A, Sajeed S, Chaiwongkhot P, Soucarros M, Legré M and Makarov V 2016 *IEEE J. Quant. Electron* **52** 1
[38] Marøy Ø, Lydersen L and Skaar J 2010 *Phys. Rev.* A **82** 032337
[39] Lydersen L, Makarov V and Skaar J 2011c *Phys. Rev.* A **83** 032306
[40] Pironio S, Acin A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[41] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[42] Lo H-K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[43] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[44] Townsend P, Rarity J and Tapster P 1993 *Electron. Lett.* **29** 634
[45] Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev. Lett.* **81** 3283
[46] Bugge A N, Sauge S, Ghazali A M M, Skaar J, Lydersen L and Makarov V 2014 *Phys. Rev. Lett.* **112** 070503
[47] Makarov V, Bourgoin J-P, Chaiwongkhot P, Gagné M, Jennewein T, Kaiser S, Kashyap R, Legré M, Minshull C and Sajeed S 2016 *Phys. Rev.* A **94** 030302
[48] Cova S, Ghioni M, Lotito A, Rech I and Zappa F 2004 *J. Mod. Opt.* **51** 1267
[49] Hadfield R H 2009 *Nat. Photonics* **3** 696
[50] Eisaman M D, Fan J, Migdall A and Polyakov S V 2011 *Rev. Sci. Instrum.* **82** 071101
[51] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J-P and Grangier P 2002 *Phys. Rev. Lett.* **89** 187901
[52] Alléaume R, Treussart F, Messin G, Dumeige Y, Roch J-F, Beveratos A, Brouri-Tualle R, Poizat J-P and Grangier P 2004 *New J. Phys.* **6** 92
[53] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[54] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z and Shields A J 2015 *Phys. Rev.* X **5** 031030
[55] Tamaki K, Curty M and Lucamarini M 2016 *New J. Phys.* **18** 065008