Secure gated detection scheme for quantum cryptography

Lars Lydersen,[1,2,*] Vadim Makarov,[1] and Johannes Skaar[1,2]

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

Several attacks have been proposed on quantum key distribution systems with gated single-photon detectors. The attacks involve triggering the detectors outside the center of the detector gate, and/or using bright illumination to exploit classical photodiode mode of the detectors. Hence a secure detection scheme requires two features: The detection events must take place in the middle of the gate, and the detector must be single-photon sensitive. Here we present a technique called *bit-mapped gating,* which is an elegant way to force the detections in the middle of the detector gate by coupling detection time and quantum bit error rate. We also discuss how to guarantee single-photon sensitivity by directly measuring detector parameters. Bit-mapped gating also provides a simple way to measure the detector blinding parameter in security proofs for quantum key distribution systems with detector efficiency mismatch, which up until now has remained a theoretical, unmeasurable quantity. Thus if single-photon sensitivity can be guaranteed within the gates, a detection scheme with bit-mapped gating satisfies the assumptions of the current security proofs.

I. INTRODUCTION

Quantum mechanics allows two parties, Alice and Bob, to grow a random, secret bit string at a distance [1–4]. In theory, the quantum key distribution (QKD) is secure, even if an eavesdropper Eve can do anything allowed by the currently known laws of nature [5–9].

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved [5,10–17]. Device-independent QKD tries to minimize the number of assumptions on the system, but unfortunately the few assumptions [2,18,19] in the security proofs seem to be too strict to allow useful implementations [20] with current technology [21].

Several security loopholes caused by imperfections have been identified, and attacks have been proposed and in some cases implemented [15,22–34]. With notable exceptions [22,23,27,30,33], most of the loopholes are caused by an insufficient model of the detectors.

While several detection schemes exist, most implementations use avalanche photodiodes (APDs) gated in the time domain to avoid a high rate of dark counts. Gated means that the APD is single-photon sensitive only when a photon is expected to arrive in a time window called the detector gate. Attacks on these detection schemes are based on exploiting the classical photodiode mode of the APD, or the detector response at the beginning and/or end of the detector gate.

In the attacks based on the classical photodiode mode of the APD, the detectors are triggered by bright pulses [28,31]. If necessary, the APDs can be kept in the classical photodiode mode, in a so-called blind state, using additional bright background illumination [28,29,31,34,35]. When the detectors are blind, they are not single-photon sensitive any more, but only respond to bright optical trigger pulses. In most gated systems, blinding is not necessary because the APDs are in the classical photodiode mode outside the gates. Therefore, in

the after-gate attack [36], the trigger pulses are simply placed after the gate.

Several attacks are based on detector efficiency mismatch (DEM) [24]. If Bob's apparatus has DEM, Eve can control the efficiencies of Bob's detectors individually, by choosing a parameter t in some external domain. Examples of such domains can be the timing, polarization, or frequency of the photons [14,24]. As an example, consider DEM in the time domain. Usually Bob's apparatus contains two single-photon detectors to detect the incoming photons, one for each bit value. Owing to different optical path lengths, inaccuracies in the electronics, and finite precision in detector manufacturing, the detection windows and hence the efficiency curves of the two detectors a and b are slightly shifted, as seen in Fig. 1(a). Several attacks exploit DEM [15,24,25] in various protocols [37], some of which are implementable with current technology. The time-shift attack [25] has been used to gain an information-theoretical advantage for Eve when applied to a commercially available QKD system [32]. In the experiment, Eve captured partial information about the key in 4% of her attempts, such that she could improve her search over possible keys.

After each loophole has been identified, effort has been made to restore the security of the detection schemes. DEM is now included in the receiver model of several security proofs [14,15,17] as an efficiency mismatch or blinding parameter η, defined differently according to the generality of the proof. For arbitrary systems that can be described with linear optics [15],

$$\eta = \frac{\min_t\{\eta_a(t),\eta_b(t)\}}{\max_t\{\eta_a(t),\eta_b(t)\}},\qquad(1)$$

where $\eta_a(t)$ and $\eta_b(t)$ are the detection efficiencies of the two detectors. Here t labels the different optical modes; in the special case without mode coupling it labels the different temporal modes. An example is given in Fig. 1(a). In the most general case η is given by the lowest probability that a nonvacuum state incident to Bob is detected [17]. For either definition of η, there is an infinite number of modes involved

_____
*lars.lydersen@iet.ntnu.no

(a) Detector efficiency

(b) Optical bit mapping
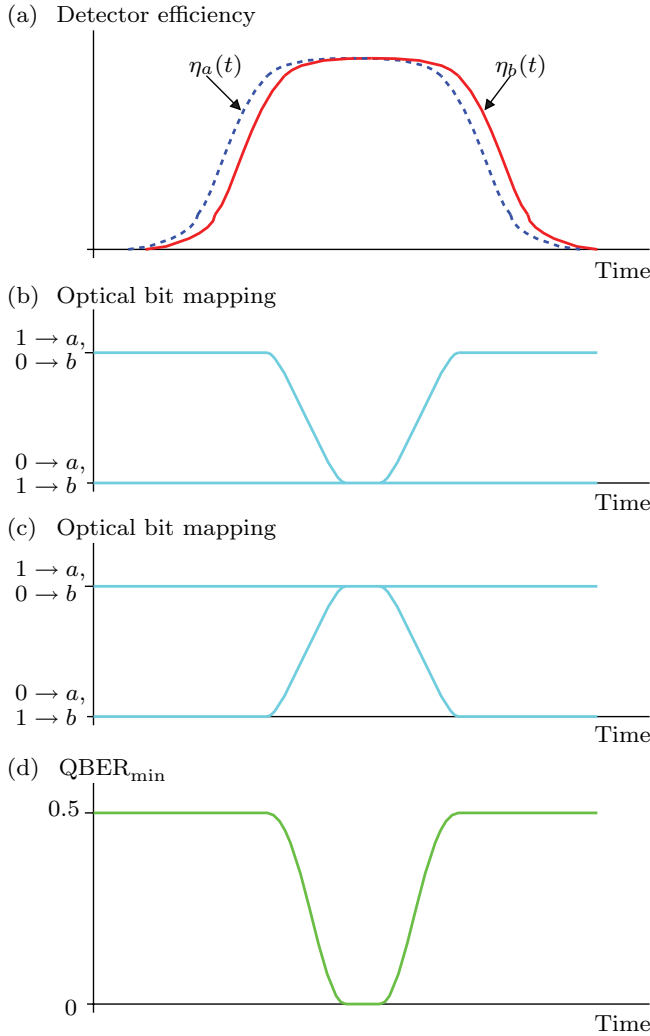
(c) Optical bit mapping

(d) QBER$_{\min}$

FIG. 1. (Color online) Bit-mapped gating. (a) Detector gates with DEM. $\eta_a(t)$ (blue, dashed) and $\eta_b(t)$ (red, solid) are the efficiencies of the two detectors a and b with respect to time t. (b),(c) Possible optical bit mapping (teal) when the software bit mapping is set to $a \to 0, b \to 1$ (b) and $a \to 1, b \to 0$ (c). In a phase-encoded system the two levels would correspond to 0 and π phase shift in one basis, and $\pi/2$ and $3\pi/2$ phase shift in the opposite basis. Note that software bit mapping and optical bit mapping coincide in the bit-mapped gate, which is well within the detector gates. (d) QBER$_{\min}(t)$ (green) as obtained from (8) with the bit-mapped gate shown in (b) and (c).

(all superpositions of temporal modes [15]), which makes the blinding parameter difficult to measure or bound in practice. For a given value of η, the secret key rate is given by [17]

$$R \geqslant -h(E) + \eta[1 - h(E)], \qquad (2)$$

where E is the quantum bit error rate (QBER) measured by Alice and Bob, and $h(\cdot)$ is the binary Shannon entropy function. Here we have assumed symmetry between the bases in the protocol; in addition, we have ignored any basis leakage from Alice and back reflection from Bob (the most general expression is given in the original reference [17]). Unfortunately, in practical systems the rate (2) will usually be zero, because $\eta \to 0$ owing to the edges of the detector gates. For the commercial QKD system subject to the time-shift

attack, $\eta < 0.01$ [estimated from the curves in Fig. 3 of Ref. [32] using Eq. (1)].

As noted in Ref. [15], one way of obtaining a better η would be to discard pulses near the edge of the detector gate. Then η could be calculated from (1) including only the modes t that are accepted as valid detections. However, this is highly nontrivial. The avalanche in an APD is a random process, and the jitter in the photon-timing resolution is of the same order of magnitude as the duration of the detector gate. A good photon-timing resolving detector still has 27-ps jitter [38]. Furthermore, the unavoidable difference in the acceptance windows for the different detectors will also contribute to DEM (one detector accepts clicks while the other discards them).

A frequently mentioned countermeasure for systems with DEM is called four-state Bob [24,25,39,40]. Then Bob uses a random detector–bit mapping, randomly assigning the bit values 0 and 1 to the detectors a,b for each gate. In a phase-encoded QKD system, this can be implemented by Bob choosing from four different phase settings $\{0, \pi/2, \pi, 3\pi/2\}$ instead of only two $\{0, \pi/2\}$. Then Eve does not know which detector characteristics correspond to which bit value. However, as mentioned previously [15,24,25], this patch does not close the loophole. Eve may use a Trojan-horse attack [22,23,41,42] to read Bob's phase modulator settings. While Alice's system is usually secured against the Trojan-horse attack by the optical attenuator at her entrance, this solution will not work for Bob's system because the attenuator would also absorb nearly all the single photons from Alice. Note also that the four-state Bob patch does not secure against the after-gate attack [36] nor any of the detector control attacks [31,35].

Here we present a novel way of securing Bob's receiver called bit-mapped gating (Sec. II). It secures the system against all kinds of pulses outside the central part of the detector gate in the Bennett-Brassard 1984 (BB84) and related protocols [1,43–45]. The technique is compatible with the existing security proofs [14,15,17] and makes it simple to find η. In general, it represents a useful concept, where parameters from characteristics of the QKD system are coupled to the parameters estimated by the protocol. In this case η becomes coupled to the QBER. Subsequently we analyze the security of bit-mapped gating (Sec. III), discuss how to characterize detectors, and how to implement a guarantee of single-photon sensitivity (Sec. IV). Finally we conclude (Sec. V).

II. BIT-MAPPED GATING

Let us start with two definitions. Software bit mapping determines how the signals from detectors a and b are mapped into the logical bits 0, 1. Similarly, optical bit mapping, which can be implemented by generalizing the basis selector, maps quantum states with bit values 0,1 (for instance, $|0\rangle, |1\rangle$ in the Z basis) to the detectors a,b. Note that if software bit mapping and optical bit mapping do not coincide, the bit value 0 sent by Alice will be detected as the bit value 1 by Bob.

Bit-mapped gating works as follows:

(1) Somewhere in between the detector gates, Bob randomly selects software bit mapping, assigning detectors a,b to bit values 0,1.

(2) Likewise, the basis is selected randomly between the *X* and *Z* basis, along with random optical bit mapping. Because this happens between the detector gates, jitter is not critical.

(3) Inside the detector gate, optical bit mapping is matched to software bit mapping. The period with matching optical and software bit mapping is the bit-mapped gate.

Note that optical bit mapping can be equal on both sides of the bit-mapped gate to minimize the need for random numbers. Figure 1 shows a typical time diagram.

As an example, consider a phase-encoded implementation of the BB84 protocol, where the basis selector at Bob is usually a phase modulator. The zero-phase shift corresponds to the *Z* basis and the $\pi/2$ phase shift corresponds to the *X* basis. Optical bit mapping can be selected by adding either 0 or π to the phase shift. Hence in this implementation the bit-mapped gating patch could be implemented as follows: Bob randomly selects software bit mapping somewhere between the gates. Furthermore, Bob selects a random basis, i.e., 0 or $\pi/2$ phase shift between the gates, and adds either 0 or π to the phase shift to apply the random optical bit mapping. During the gate, the software and optical bit mapping coincide.

All states received and detected outside the bit-mapping gate cause random detection results (owing to the random optical and software bit mapping), and thus introduce a QBER of 50%. The measured QBER could be used to estimate the fraction of detections that must have occurred in the center of the gate (in Fig. 1: Close to zero QBER would mean that most detection events must have passed the basis selector, and thus hit the detector, in the middle of the gate). This can be used to limit the DEM, because considering only the modes in the center of the detector gate gives less DEM than considering all modes.

III. SECURITY ANALYSIS

The goal of this section is to derive an expression for the minimum QBER introduced by any state received by Bob, during the transition to and from the bit-mapped gate. Ideally, the minimum QBER is 0 inside the bit-mapped gate, and 1/2 outside the bit-mapped gate.

The input of Bob's detection system consists of many optical modes *t*, for instance, corresponding to different arrival times at Bob's system. Each mode *t* may contain a mixture of different number states. Note that Bob could have measured the photon number in each mode without disturbing the later measurement; thus it suffices to address specific number states. We use the usual assumption that each photon in a *n*-photon state is detected individually. Under these assumptions, we first calculate the minimum QBER caused by a single photon arriving in a single mode at Bob. Then, in the Appendix, we show that multiple photons in this mode, or photons in other modes, can only increase the minimum QBER.

Consider a single photon arriving at Bob in a given mode *t*. Because the BB84 protocol is symmetric with respect to the bit values and the bases, we may assume without loss of generality that Alice sent *Z*0 and that Bob measures in the *Z* basis. Outside the bit-mapped gate, Bob performs four different measurements depending on the software and optical bit mapping. For each measurement, Bob will obtain one out of

three measurement outcomes, bit 0, bit 1, or vacuum denoted by subscript v.

Let η_a, η_b be the efficiencies of the two detectors, $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|\theta^\perp\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$. During a bit-mapped gate, θ is varied from 0 to $\pi/2$. For each value of θ, Bob performs one out of the four measurements,

$$M_0 = \eta_a|0\rangle\langle 0|, \quad M_1 = \eta_b|1\rangle\langle 1|,$$
$$M_v = I - M_0 - M_1, \tag{3a}$$

$$M_0' = \eta_b|0\rangle\langle 0|, \quad M_1' = \eta_a|1\rangle\langle 1|,$$
$$M_v' = I - M_0' - M_1', \tag{3b}$$

$$M_0'' = \eta_a|\theta\rangle\langle\theta|, \quad M_1'' = \eta_b|\theta^\perp\rangle\langle\theta^\perp|,$$
$$M_v'' = I - M_0'' - M_1'', \tag{3c}$$

$$M_0''' = \eta_b|\theta\rangle\langle\theta|, \quad M_1''' = \eta_a|\theta^\perp\rangle\langle\theta^\perp|,$$
$$M_v''' = I - M_0''' - M_1'''. \tag{3d}$$

If Bob uses the four measurements with equal probabilities, the statistics will be given by using the measurement operators,

$$
\begin{aligned}
E_0 &= \tfrac{1}{4}(M_0 + M_0' + M_0'' + M_0''') \\
&= \tfrac{1}{4}(\eta_a + \eta_b)[(1 + \cos^2\theta)|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1| \\
&\quad + \sin\theta\cos\theta(|0\rangle\langle 1| + |1\rangle\langle 0|)], \tag{4a}
\end{aligned}
$$

$$
\begin{aligned}
E_1 &= \tfrac{1}{4}(M_1 + M_1' + M_1'' + M_1''') \\
&= \tfrac{1}{4}(\eta_a + \eta_b)[\sin^2\theta|0\rangle\langle 0| + (1 + \cos^2\theta)|1\rangle\langle 1| \\
&\quad - \sin\theta\cos\theta(|0\rangle\langle 1| + |1\rangle\langle 0|)], \tag{4b}
\end{aligned}
$$

$$
\begin{aligned}
E_v &= \tfrac{1}{4}(M_v + M_v' + M_v'' + M_v''') \\
&= \left(1 - \frac{\eta_a + \eta_b}{2}\right) I. \tag{4c}
\end{aligned}
$$

Note that $E_v \propto I$, so the detection probability is independent of the photon state ρ:

$$p_{\text{det}} = 1 - \text{Tr}[\rho E_v] = \frac{\eta_a + \eta_b}{2}. \tag{5}$$

The eigenvalues of operators E_0 and E_1 are given by $p_{\text{det}}(1 \pm \cos\theta)/2$. Thus the minimum and maximum probability of detecting bit values 0 and 1 for any single photon sent by Eve is given by

$$p_{0,\,\text{min}} = p_{1,\,\text{min}} = \frac{p_{\text{det}}}{2}(1 - \cos\theta), \tag{6}$$

$$p_{0,\,\text{max}} = p_{1,\,\text{max}} = \frac{p_{\text{det}}}{2}(1 + \cos\theta). \tag{7}$$

Because Alice sent *Z*0, the minimum QBER introduced by a single photon is given by

$$\text{QBER}_{\text{min}} = \frac{p_{1,\,\text{min}}}{p_{\text{det}}} = \frac{1}{2}(1 - \cos\theta). \tag{8}$$

As expected, for $\theta = \pi/2$, $\text{QBER}_{\text{min}} = 1/2$. For multiphotons, a random bit value is assigned to double clicks [10,16]. The Appendix shows that sending multiple photons can only increase the QBER caused by detection events. Hence Eq. (8) gives the minimum QBER for any photonic state sent by Eve.

The security proofs in Refs. [14,15,17] involve Bob predicting the results of Alice's virtual X-basis measurement. Because the prediction is not carried out in practice, Bob can perform any operation permitted by quantum mechanics. In the proofs Bob's prediction consists of a filter followed by an "X-basis" measurement. When nothing is known about the distribution of the detection events within the gate, the worst-case assumption is that all the detection events occur with maximum DEM. Therefore, the best filter we can construct can only guarantee that a fraction η of the inputs can successfully pass the filter.

With our patch, we may use the QBER to determine a lower bound for the number of detection events which must have occurred in the central part of the detector gate. Assuming that t labels temporal modes, consider the number of detection events that occurred in the range where $\mathrm{QBER_{min}} < E'$ (see Fig. 2). Here, E' is a threshold selected by Bob. Let η' be the blinding parameter for the modes for the range where $\mathrm{QBER_{min}} < E'$. It can be calculated from Eq. (1), but where t only runs over this range. If the measured QBER is equal to E, a fraction

$$f = \frac{E' - E}{E'} \qquad (9)$$

must have been detected in the modes where $\mathrm{QBER_{min}} < E'$. Note that increasing E' increases f, and may decrease η' (see Fig. 2). As will become apparent below, E' should be selected to maximize $f\eta'$.

For decoy protocols [43–45], E should be replaced with the QBER estimated for single-photon states. This improves the estimate of the fraction f, especially for large distances where the dark counts become a major part of the total QBER.

In the worst case, a fraction f experienced a reduced DEM η'. Therefore, the filters in the security proofs can be replaced as follows: The new filter discards pulses in the modes for which $\mathrm{QBER_{min}} > E'$. For the modes inside the bit-mapped gate, where $\mathrm{QBER_{min}} < E'$, the new filter reverts the quantum operation from the receiver in the opposite basis in the same way that the old filter reverted it for all modes, but now having a success rate η'. Because we can guarantee that a fraction f of the photons are in the bit-mapped gate, at least $f\eta'$ pulses will successfully pass the new filter. Therefore the parameter η in all the proofs [14,15,17] can be replaced with $f\eta'$, and the rate (2) becomes

$$R \geqslant -h(E) + f\eta'[1 - h(E)], \qquad (10)$$

when one assumes symmetry between the bases, and no source errors. Without symmetry between the bases, all parameters become basis dependent, and the rate is the sum of the rates in each basis.

Let us see how bit-mapped gating could improve the secure key rate for the commercial QKD system in Ref. [32]. For this system, $\eta < 0.01$. In the same experiment, the QBER is measured to be 5.68%. Assuming $E' = 0.45$ and $\eta' = 0.9$, $f\eta'$ becomes 0.79, thus a substantial improvement. In fact, the rate obtained from Eq. (2) without the patch is 0, while the rate obtained from Eq. (10) is 0.227, so clearly the patch can be used to resecure an insecure implementation.

IV. DETECTOR DESIGN AND CHARACTERIZATION

When designing Bob's system, one should ensure that the bit-mapped gate is well within the detector gate, i.e., that the detector efficiencies are approximately equal within the bit-mapped gate. Then, it should be possible to measure or bound the detector efficiencies and the basis selector response $\theta(t)$ in the temporal domain. In a phase-encoded system this would correspond to measuring the detector efficiencies and the phase modulation as a function of time [46], over the range of wavelengths and polarizations accepted by Bob. With this data, the minimum QBER as a function of time can be calculated from (8), and a diagram similar to Fig. 2 can be obtained. After selecting an appropriate limit E', η' can be calculated by (1) but where t runs only over the modes where $\mathrm{QBER_{min}} < E'$, and not over all available modes.

In general, there might be coupling between the different temporal modes owing to misalignments and multiple reflections [14,15]. The bit-mapped gate ensures that the pulse passed the basis selector inside the temporal detector gate, but does not guarantee the actual detection time. For example, a pulse could pass in the center of the bit-mapped gate, but afterwards take a multiple reflection path such that it hits the detector outside the detector gate. This can be handled by characterizing the worst-case mode coupling as described previously [15]. Let δ be the worst-case (power) coupling of modes inside the bit-mapped gate to outside the gate. This will typically be the worst-case multiple-reflection path after the basis selector, and should be boundable from component characteristics. Then, the parameter δ can be
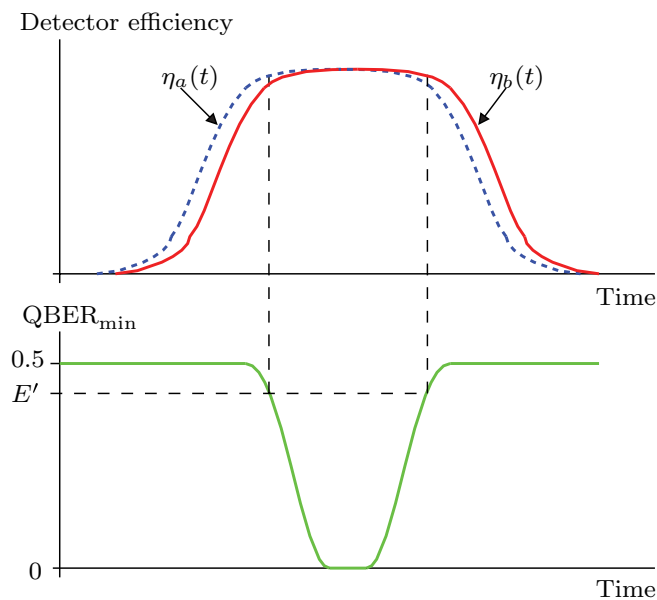

FIG. 2. (Color online) Curves (a) and (d) from Fig. 1. The dashed line shows how a threshold E' can be used to limit the range of modes t used to calculate or bound η'.

interpreted as

$$\delta = \frac{\text{\# pulses that hits the detector outside the gate}}{\text{\# pulses sent into the gate}}. \quad (11)$$

In the worst case, δ of the f detection events might have happened outside the central part of the detector gate; thus one must let $f \rightarrow f(1 - \delta)$.

Finally one must guarantee that the detectors are not blind within the gate [31], and fulfill the assumptions in Sec. III during the transition of the optical bit mapping. Note that the transition ends when there is no longer any correlation between software bit mapping and optical bit mapping. If a significant correlation exists also after the detector gate, it could be exploited in the after-gate attack [36].

Although it is tempting to place an optical watchdog detector at the entrance of Bob, the absence of bright illumination does not necessarily mean that the detectors are single-photon sensitive. For instance, owing to the thermal inertia of the APD, it can remain blind for a long time after the bright illumination is turned off [35].

A cheap way to guarantee single-photon sensitivity is to monitor all detector parameters [29], such as APD bias voltage, current, and temperature. It seems difficult to monitor the temperature of the APD chip [35], but monitoring the bias voltage and current should make it possible to predict the heat generated by the APD, and thus prevent thermal blinding [35].

The ultimate way of guaranteeing single-photon sensitivity is to measure it directly. This can be done by placing a calibrated light source inside Bob that emits faint pulses at random times [34] (see Fig. 3). Then the absence of detection events caused by this source would indicate that the detector
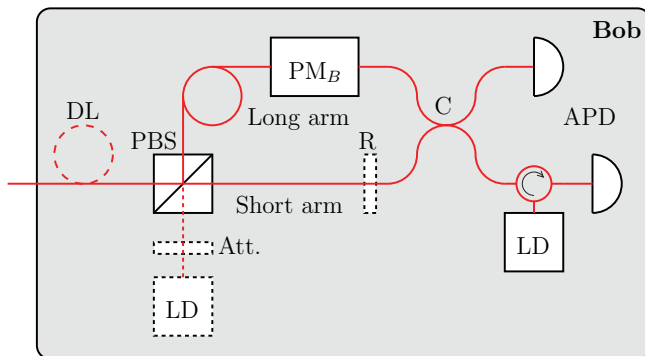

FIG. 3. (Color online) A calibrated light source inside Bob. The figure shows the Bob module in a plug-and-play system [4,47–49], which has two possible implementations of the calibrated light source: either a separate attenuated laser diode (LD) at a suitable place, or in the case of send-return systems where Bob already contains a laser diode, a weakly reflective element (R) to reflect some light back into the APDs. In one-way systems [3,50], Bob does not normally contain any light source, therefore a separate laser diode would be the only option. A short delay line (DL, delay > gate period/2) at Bob's input guarantees that Eve cannot interfere with the detector operation based on whether the source is activated or not. PBS: polarizing beam splitter; Att.: optical attenuator; PM: phase modulator; 50 : 50 fiber-optic coupler.

is blind. Further, a calibrated light source inside Bob could be useful in more ways, for instance, to characterize and calibrate detector performance in deployed systems.

The patch could cause a minor reduction in QKD performance compared to running an (insecure) system without the patch. In particular, the detector gates might have to be longer to contain the basis-selector gate. This would increase the dark count rate, and thus limit the maximum transmission distance. A calibrated light source inside Bob would also cause a minor reduction in the performance because the gates used for testing the detector sensitivity likely cannot be used to extract the secret key. However, both these effects are minor, and are easily justified by the restoration of security.

V. DISCUSSION AND CONCLUSION

In this work, we have presented a technique called "bit-mapped gating" to secure gated single-photon detectors in QKD systems. It is based on a general concept where hardware imperfections are coupled to the parameters estimated by the protocol. Bit-mapped gating causes all detection events outside the central part of the detector gate to cause high QBER.

Bit-mapped gating is compatible with the current security proofs for QKD systems with detector efficiency mismatch [14,15,17]. In particular, it provides a simple way of measuring the detector blinding parameter. A secure gated detection scheme is obtained if bit-mapped gating is combined with detectors guaranteed to be single-photon sensitive.

ACKNOWLEDGMENT

APPENDIX: MINIMUM QBER FOR MULTIPHOTONS

Here we prove that the minimum QBER can only increase when the number of photons sent to Bob is increased. As noted previously, we use the usual assumption that each photon in a n-photon state is detected individually. This means that each photon hits a separate set of detectors, and then the detection results are merged to give the detection results of threshold detectors.

Let us first consider the case where Bob receives a large number of two-photon states. Let the two photons within the states be labeled 1 and 2. Individually, each of the two photons would have caused the minimum QBER Q_1 and Q_2 [as found from Eq. (8)]. Again we assume that Alice sends the bit value 0, without loss of generality. For two-photon states there will be three cases of detected events: either only photon 1 is detected, only photon 2 is detected, or both photons are detected (in our model, this latter possibility corresponds to the case where both sets of detectors register a click). Let there be n_1 events where only photon 1 was detected, n_2 events where only photon 2 was detected, and c events where both photons were detected. For photon i, out of the $n_i = n_{i,0} + n_{i,1}$ events, $n_{i,0}$ and $n_{i,1}$ were detected as the bit value 0 and 1, respectively. Likewise, out of the $c = c_{i,0} + c_{i,1}$ events where both photons are detected,

$c_{i,0}$ and $c_{i,1}$ were detected as the bit value 0 and 1 for photon i (remember that in the model each photon hits a separate set of detectors).

When only one of the photons is detected, the situation is identical to the single-photon case treated in Sec. III. Hence states such that $Q_i = n_{i,1}/n_i$ give the lowest possible QBER. For the events where both photons are detected, the detections can have any correlation, but for each photon $c_{i,1} \geqslant cQ_i$, because Q_i represents the lowest fraction of the bit value 1 possible, regardless of the correlation with any other photon. The total QBER Q can be found from merging the detections from the two sets of detectors. Double clicks are assigned a random bit value [10,16], therefore half of the double clicks

get the bit value 1. This gives the total QBER,

$$
\begin{aligned}
Q &= \frac{n_{1,1} + n_{2,1} + \frac{1}{2}(c_{1,1} + c_{2,1})}{n_1 + n_2 + c} \\
&\geqslant \frac{Q_1\left(n_1 + \frac{c}{2}\right) + Q_2\left(n_2 + \frac{c}{2}\right)}{n_1 + n_2 + c} \\
&\geqslant \min(Q_1, Q_2). \qquad (A1)
\end{aligned}
$$

By repeating the argument above, but replacing the detection of photon 1 with the detection of N photons, it is easy to see that $Q \geqslant \min(Q_N, Q_{N+1})$. Hence, by induction, any detection event caused by more than one photon can only cause a higher QBER than the single-photon case.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] D. Mayers, in *Proceedings of Crypto'96*, edited by N. Koblitz (Springer, New York, 1996), Vol. 1109, pp. 343–357.

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[10] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[11] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[12] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).

[13] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).

[14] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).

[15] L. Lydersen and J. Skaar, Quantum Inf. Comput. **10**, 60 (2010).

[16] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[17] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[18] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[19] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[20] There exists at least one proposal for implementing device-independent QKD [51]. The implementation looks challenging and leads to a much lower secret key rate than the rate in conventional systems.

[21] V. Scarani and C. Kurtsiefer, e-print arXiv:0906.4547v1.

[22] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

[23] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[24] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).

[25] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[26] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[27] Chi-Hang Fred Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).

[28] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, e-print arXiv:0809.3408.

[29] V. Makarov, New J. Phys. **11**, 065003 (2009).

[30] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).

[31] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[32] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[33] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[34] I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, e-print arXiv:1011.0105.

[35] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[36] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[37] V. Makarov and J. Skaar, Quantum Inf. Comput. **8**, 622 (2008).

[38] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[39] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, J. Mod. Opt. **48**, 1921 (2001).

[40] M. J. LaGasse, US Patent application 20,050,190,922 (2005).

[41] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).

[42] D. S. Bethune and W. P. Risk, IEEE J. Quantum Electron. **36**, 340 (2000).

[43] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[44] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[45] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[46] If the phase modulator response differs depending on the software bit mapping and basis choice, it should simply be bounded.

[47] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[48] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. **33**, 586 (1997).

[49] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).

[50] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).

[51] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).