Quantum Information and Computation, Vol. 14, No. 3&4 (2014) 0217–0235
© Rinton Press

SECURITY OF HIGH SPEED QUANTUM KEY DISTRIBUTION WITH FINITE DETECTOR DEAD TIME

VIACHESLAV BURENKOV[a]
Department of Physics, University of Toronto
Toronto, Ontario, M5S 1A7, Canada

BING QI
Department of Electrical and Computer Engineering, University of Toronto
Toronto, Ontario, M5S 3G4, Canada

BEN FORTESCUE
Department of Physics, Southern Illinois University
Carbondale, Il 62901, USA

HOI-KWONG LO
Department of Physics, University of Toronto
Toronto, Ontario, M5S 1A7, Canada
and
Department of Electrical and Computer Engineering, University of Toronto
Toronto, Ontario, M5S 3G4, Canada

Received March 17, 2013
Revised July 6, 2013

The security of a high speed quantum key distribution system with finite detector dead time τ is analyzed. When the transmission rate becomes higher than the maximum count rate of the individual detectors ($1/\tau$), security issues affect the scheme for sifting bits. Analytical calculations and numerical simulations of the Bennett-Brassard BB84 protocol are performed. We study Rogers et al.'s scheme (further information is available in [D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu, and C. W. Clark, New J. Phys. **9**, 319 (2007)]) in the presence of an active eavesdropper Eve who has the power to perform an intercept-resend attack. It is shown that Rogers et al.'s scheme is no longer guaranteed to be secure. More specifically, Eve can induce a basis-dependent detection efficiency at the receiver's end. Modified key sifting schemes that are basis-independent and thus secure in the presence of dead time and an active eavesdropper are then introduced. We analyze and compare these secure sifting schemes for this active Eve scenario, and calculate and simulate their key generation rate. It is shown that the maximum key generation rate is $1/(2\tau)$ for passive basis selection, and $1/\tau$ for active basis selection. The security analysis for finite detector dead time is also extended to the decoy state BB84 protocol for one particular secure sifting scheme.

Keywords:

Communicated by: S Braunstein & K Moelmer

[a] viacheslav.burenkov@utoronto.ca

1 Introduction

Quantum key distribution (QKD) [1, 2] can be used to generate a secret key (random bit string) between two distant parties, Alice and Bob. This holds true even in the presence of a technologically-unbound eavesdropper, Eve. The security of the key is guaranteed by the laws of quantum mechanics; the process of measuring a quantum system generally disturbs it, thus allowing Alice and Bob to detect Eve's presence. For a review of QKD, see [3, 4, 5].

A commonly used protocol for QKD is the Bennett-Brassard 1984 (BB84) [1]. In BB84, Alice and Bob use two conjugate bases to encode the information. However, due to currently available technology, the BB84 protocol is typically performed with an attenuated laser source instead of a perfect single-photon source. It is therefore susceptible to the photon number splitting attack [6], which greatly limits its performance. In this attack, Eve can, in principle, identify and take advantage of the multi-photon pulses to gain information. However, it is possible to overcome this limitation by the use of decoy states [7, 8, 9], which can be sent to better characterize the channel, and as a result, significantly improve the secure key rate.

While the security of QKD has been proven to be unconditionally secure [10, 11, 12], it rests on the validity of certain assumptions about real-life devices. This includes correctly identifying and modelling the imperfections in these devices. A failure to take a certain real-life imperfection into account can completely compromise the security of the protocol.

As the length of the secret key needs to be as long as the message for secure one-time-pad encryption, the secret key generation rate is a crucial figure of merit. As such, there has been a lot of recent progress in experimental high speed QKD [13, 14]. It is generally true that increasing the transmission rate increases the secret key generation rate. However, since most realistic single photon detectors have a property called dead time—the time interval right after a detection, during which a detector recovers and cannot detect another incoming photon—certain security assumptions may be violated if transmission rates are increased inattentively. In this paper we consider the security of a high speed QKD system with finite detector dead time, in the regime where the transmission rate is so high that photons can arrive at Bob's detectors while one or more detectors are still recovering from previous detection events. This work builds on the earlier work by D. Rogers et al. [15]. Monte-Carlo simulations of the BB84 protocol were performed to extend the security analysis to include an active Eve capable of interfering with the signals.

In Sec. 2, we describe Bob's detection set-up and detector dead time model. In Sec. 3 we outline a sifting scheme proposed by Rogers et al. for secure operation in the passive Eve scenario. In Sec. 4, we show that this scheme is no longer guaranteed to be secure when Eve is able to perform an intercept-resend attack. The main reason of the potential insecurity of Rogers et al.'s scheme is that its detection efficiency is *basis-dependent*. In Sec. 5, we analyze sifting schemes that are basis-independent and thus secure in this active Eve scenario, and compare the sifted bit rate of these schemes. In Sec. 6, we move onto a practical scenario with an imperfect source and detector. In particular, we consider a standard phase randomized weak coherent state source and a standard threshold detector which is non-photon-number-resolving, and extend the analysis to the decoy-state BB84 protocol for one particular sifting scheme, (namely *SchemeDeactivate* introduced earlier in Sec. 5). Sec. 7 contains our concluding remarks.

2 System Model

We consider polarization encoded BB84 protocol, with a passive polarization detection set-up [3] shown in Fig. 1. There are two bases, basis 1 and basis 2, defined as follows:

1) Basis 1: Rectilinear (consisting of vertically and horizontally polarized photons) and

2) Basis 2: Diagonal (consisting of 45-degree and 135-degree polarized photons).

We will use this notation throughout the paper.

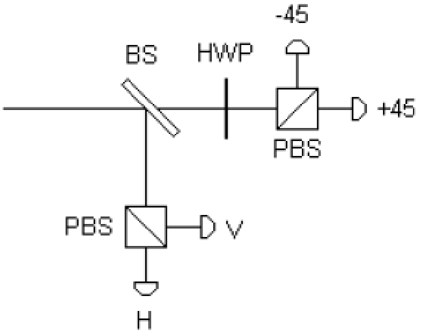

Fig. 1. Passive polarization detection optics. A 50-50 beam splitter (BS) performs basis selection and the combination of half waveplate (HWP) and polarizing beam splitters (PBS) perform the polarization measurement in two bases: basis 1 (V-H) and basis 2 (−45°, +45°).

The idealized gain η is given by the overall transmission and detection efficiency [16]:

$$\eta = t_{AB}\eta_{Bob} = t_{AB}t_{Bob}\eta_D \,, \tag{1}$$

where
t_{AB} = channel transmittance
η_{Bob} = efficiency of Bob's system
t_{Bob} = Bob's internal transmittance
η_D = detection efficiency.

The channel transmittance can be expressed as:

$$t_{AB} = 10^{(-\alpha l/10)} \,, \tag{2}$$

where α is the loss coefficient in dB/km and l is the channel distance in km.

The list of assumptions about the QKD system is provided below.

Except for Sec. 6 and 7, the source is assumed to be a perfect single photon source. A number of randomly and uniformly chosen signals sent by Alice are erased to model the loss in the quantum channel. Fiber loss α is about 0.2 dB/km at the telecom wavelength of 1550 nm. As such, a typical loss for a 100 km length of fiber in current experiments is of the order of 20 dB.

The detector model is as follows. Except for Sec. 6 and 7, we assume that single photons arrive at Bob's detector unit. In Sec. 6 and 7, we will consider the practical case where both the source and the detector are imperfect. More concretely, the source may be a phase randomized weak coherent state and multi-photons may enter Bob's detectors. Specifically, we consider a standard *threshold detector* model where a detector can distinguish a vacuum from a non-vacuum signal, but cannot tell the difference between one photon and two or more photons. We assume detectors have a dead time τ. In Si-APDs, during the dead time, the bias voltage across the p-n junction is below the breakdown threshold and as such, another photon cannot be detected [17]. This limits their counting rate to $1/\tau$.

In our simplified model, we assume that an active detector will detect an incoming signal with some maximum constant detection efficiency η_D, which drops instantaneously to 0 after a detection event, and undergoes an instantaneous transition back to η_D after the dead time τ (see Fig. 2). Even though this model does not fully capture the behaviour of the detectors, it does capture the key feature of the detectors to highlight the dead time problem.

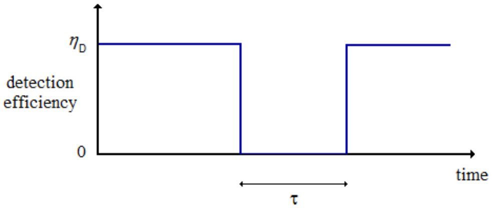

Fig. 2. Detection dead time model. The detector undergoes an instantaneous transition from some constant maximum value η_D to 0 % efficiency upon being hit by a photon and instantly back again after a dead time τ.

For Silicon SPADs the typical dead time is of the order of 100 *ns* [17], which is the value used in our simulations. All four detectors are assumed to have the same dead time. We further assume that a photon that strikes the detector while it is recovering does not extend the recovery time, nor has any effect whatsoever [18]. This makes individual detectors non-paralyzable systems [19]. Finally, it is assumed that there are no dark counts (except for Sec. 6 and 7) and the channel is noiseless.

3 Rogers et al.'s Scheme

In this section, it is assumed that Eve is passive. In other words, she does not interfere with the quantum signals but she can 'listen' to the classical channel so that she has full information about the classical transmission from Bob to Alice (bases used and time of detections) and Alice to Bob (which detections to sift).

Generally, as the transmission rate increases, the sifted key rate increases. However, since the detectors have a finite dead time τ, there comes a point where the transmission rate ρ (in terms of number of transmissions per second) is so high that it exceeds the maximum counting rate of the individual detectors ($1/\tau$), so that photons can arrive at Bob while one or more of his detectors are recovering from previous detection events. If two detection events occur in the same basis within one dead time window, they necessarily correspond to two *different* bits [20]. This leads to correlations in the sifted bit string, which is an obvious security flaw. Each 'closely-spaced' detection sequence can thus produce at most a single sifted bit.

Rogers et al. [15] proposed a sifting scheme with the goal of allowing the system to work in the high-speed regime without compromising the security of the key. The hope is that the key can be generated at a rate higher than $1/(2\tau)$ the maximum key rate achievable by deactivating all detectors upon any detector firing, as we will discuss in Sec. 5.

Rogers et al.'s scheme can be defined as follows. Each basis is treated individually; the status of the two detectors in the other basis is irrelevant. A basis is defined as *active* if *both* detectors in that basis are active at the expected photon arrival time. Otherwise, if either one, or both, of the detectors in that basis are dead, the basis is called *inactive*. $P_{0,0}$ is used to denote the probability of a basis being active. Only if a basis is active, the subsequent detection sequence in that basis will be accepted. The length of an accepted detection sequence can range anywhere from one (for a single detection) upwards (for overlapping detections within a basis). A bit can only be sifted from the sequence from a detection event for which Alice and Bob used the same basis. For each detection in the sequence, Alice and Bob will have used the same basis with probability of 0.5. Therefore, the probability of sifting the one possible bit from all the detections in a given sequence depends on whether Alice and Bob used the same basis at least once, and simply ranges from 0.5 (for a single detection) up to 1 (for a very long detection sequence).

It is useful to consider a quantity k, the number of transmission periods per dead time, defined by $k = \rho\tau$, where ρ is the transmission rate. The transition between the standard and the high-speed regimes occurs at $k = 1$, irrespective of channel loss. Rogers et al. [15] showed that the probability of a basis being active, and thus capable of sifting a bit, tends to zero as k (and the transmission rate) tend to infinity. This means that high-speed QKD systems are paralyzable counting systems. This phenomenon occurs from the collective behavior of a pair of detectors in a given basis which lock up.

Increasing the transmission rate tends to lock up the detectors in each basis, resulting in a long string of closely spaced detections which allow at most one bit to be sifted. This effect reduces and eventually outweighs the advantage of transmitting at a higher rate. The point where these balance gives rise to an optimum transmission rate that maximizes sifted bit rate production. Plotting the log of transmission rate vs sifted key rate shows a Bell-like curve. That is to say, the sifted key rate reaches a maximum value at the optimal transmission rate, after which further increases in transmission rate actually hinder sifted key production. This maximum key rate achievable with Rogers et al.'s scheme is considerably higher than $1/(2\tau)$, given approximately by $1.43/(2\tau)$ [15].

4 Problems with Rogers et al.'s Scheme with Active Eve

Rogers et al.'s paper [15] considers a purely passive Eve who can only 'listen'. Such an assumption is clearly not valid in any realistic setting where the channel is noisy and Eve can be active. We extend the analysis by introducing an Eve that can perform an intercept-resend attack.

The intercept-resend attack is a simple, yet effective, attack that involves Eve intercepting Alice's photons individually, measuring them in one of two bases used by Alice and Bob, and sending new photons to Bob according to the outcome of her measurement. Eve gains information at the cost of introducing quantum bit errors.

Eve has the ability to intercept any (or all) pulses, and resend one of Alice's states at will (also single photons), or none at all (blocking the signal). Eve is assumed to have a 4-detector set-up like Bob, but her detectors have infinitesimal dead time.

In what follows, we will show that Rogers et al.'s sifting scheme can no longer be considered secure with certainty. This is because Eve can force Bob's detection efficiency to be basis-dependent. To illustrate this, consider a simple attack by Eve that goes as follows. Eve blocks Alice's pulses $1, 2, \ldots, N$ (where N is a large number, which would depend on the channel loss). In their place, she sends N pulses all in the "vertical" polarization state. Summing over the corresponding detection events, the probability of basis 1 (rectilinear) being active is higher than the probability of basis 2 (diagonal) being active. When N is large enough we reach the stationary distribution.

Intuitively, the attack works as follows. If a photon is detected in basis 1 (rectilinear), it is necessarily the detector corresponding to the vertically polarized photon that clicks and becomes inactive for the duration of its dead time. The detector corresponding to the horizontally polarized photon never clicks, and is therefore always active. Upon recovery the "vertical" detector is ready to detect another photon, and thus the basis itself becomes active. In basis 2 (diagonal) however, the situation is quite different. An incoming vertically-polarized photon is equally likely to trigger and thus disable either detector in this basis. Thus both detectors in this basis click and recover. However, as time goes on the recovery of one detector would become randomized with respect to the other one. Therefore, we are more likely to have a situation where one detector is hit while the other is still recovering, so that the two detectors are clicking alternately, preventing the basis from becoming active. Our simulation (see below) confirms our intuition.

Although this specific attack can be easily detected by Alice and Bob in practice (because Eve's N "vertical" photons will cause a high error rate), notice that Eve may lower the error rate she introduces by performing the attack on only part of the signals. Here comes a key point: Eve's ability to introduce basis-dependent detection efficiency violates a fundamental assumption in security proofs [12, 21, 6, 22, 23]. Note that for repetition rate smaller than $1/\tau$, both bases are active with equal probability.

A simulation was carried out to test for basis dependence on Bob's side in the case of this simple attack, with finite detector dead times. Note that in this simulation Bob is only receiving vertically polarized photons. The probability $P_{0,0}$ of both detectors being active in each basis was calculated using Rogers et al.'s scheme for a large number of photons ($N = 5 \times 10^6$ photons). See Fig. 3.

The result is that basis 1 (rectilinear) is considerably more active than basis 2 (diagonal). Note that the ratio of $P_{0,0}$ for basis 2 to $P_{0,0}$ for basis 1 (equal to 0.67 in this case) approaches the theoretical value (discussed below) in the limit of large number of pulses. It is not a transient effect caused by detectors starting off in the active state. We have used the value of 3 dB for the channel loss, which has no special significance; the fundamental result is true for any value of loss, as well as the lossless case: Bob's detection efficiency is basis-dependent.

It is instructive to see how this basis dependence varies with k. We want to derive the dependence of $P_{0,0}$ on k for each basis. For basis 2, $P_{0,0}$ has already been derived in Eq. (8) of Ref. [15], and we quote the result here:

$$P_{0,0}(basis\ 2) = \left[1 + (2k')\left(\frac{2p}{1-2p}\right) + (k'^2 - k')\left(\frac{(2p)^2}{1-2p}\right)\right]^{-1}, \tag{3}$$

where p is the probability that a particular detector produces a sifted bit on a given clock

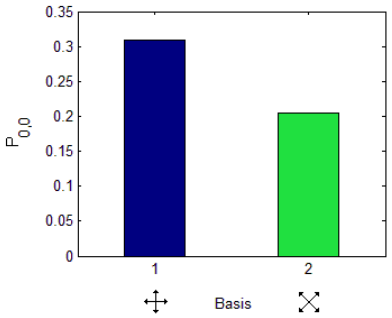

Fig. 3. A simple intercept-resend attack can force a basis dependence of detector efficiency. Normalized transmission rate $k = 10$, channel loss = 3 dB, detection efficiency $\eta_D = 100$ %, $N = 5 \times 10^6$ photons. The error estimate, taking into account the statistical fluctuations involved, would not be discernible on the scale that this figure is presented. In the low-speed regime both bases would be active 100 % of the (expected photon arrival) time.

cycle and k' is the number of transmission periods per dead time. More concretely, for BB84 with four detectors,

$$p = \frac{\eta}{8}\,, \tag{4}$$

where η is the idealized gain defined in Eq. (1), and the factor of 1/8 accounts for the correct basis choice (1/2) and the specific detector clicking (1/4). The definition of the normalized transmission rate used by Rogers et al. [15] is slightly different than in this paper. To account for this, Eq. (3) has to be adjusted by replacing k' with $k' = (k-1)$. Note that Eq. (3) applies only at integer values of k'.

In Ref. [15], Eq. (3) above was derived for the case where Eve is passive and thus, in each basis, Bob receives a random bit on average. Notice that, in our case Eve always sends a vertical photon. Nonetheless, for basis 2, Bob also receives a random bit. Therefore, the derivation in Ref. [15] carries over directly here.

To find $P_{0,0}$ for basis 1 we only need to find the probability of detector 1 being active, since detector 2 is always active. The basis, at any discrete point (expected photon arrival time), is either active or inactive. Let us assume for the moment that the detection system comprises only of basis 1. Then, the probability of a click given that the basis is active is given by the idealized gain for one basis η_1. Similarly, the probability of the basis remaining active is given by $1 - \eta_1$:

$$\begin{aligned} P(click|active) &= \eta_1 \\ P(no\ click|active) &= 1 - \eta_1\,. \end{aligned} \tag{5}$$

Once in an inactive state, the detection system will evolve in a unique way through a series of inactive states and take $(k-1)$ steps to return to the active state. From the active state, the system at the next step can either remain active (if photon is lost), or become inactive (if detector 1 is hit) and begin to recover.

We can therefore write the following equations that govern the evolution of the system in the *stationary* state, where P_a is the probability that the detection system is active and T_n is the probability that the system is inactive after n steps:

$$\begin{aligned} P_a &= T_{k-1} + P_a(1-\eta) \\ T_1 &= P_a\eta_1 \\ T_i &= T_{i-1} \end{aligned} \tag{6}$$

for $i = 2, ..., k-1$.

We also know that the system must be in *one* of these states at any point, and since there are a total of $(k-1)$ equally likely inactive states, we have

$$1 = P_a + (k-1)T_1 = P_a + (k-1)P_a\eta_1 \,,$$

which gives

$$P_a = \frac{1}{1+(k-1)\eta_1} \,. \tag{7}$$

However, there are two bases. Since only half of the photons that reach Bob will go to basis 1, we modify Eq. (7) by noting that $\eta_1 = (1/2)\eta$, where η is the idealized gain defined by Eq. (1). This gives the probability $P_{0,0}$ that basis 1 is active (and hence capable of sifting bits):

$$P_{0,0}(basis\ 1) = \frac{1}{1+0.5(k-1)\eta} \,. \tag{8}$$

We can now see how $P_{0,0}$ changes with k for the two different bases while Eve is doing the simple intercept-resend attack described above. Fig. 4 (a) shows both the results of Monte Carlo simulations and theoretical results (given by Eq. (3) and Eq. (8)) derived using Markov chain arguments. Note that the theoretical values apply only at integer values of k. Fig. 3 is a snapshot of Fig. 4 (a) for $k = 10$. It is also interesting to see how the ratio of $P_{0,0}$ for basis 2 to $P_0, 0$ for basis 1 varies with k, for the same values of η and p. See Fig. 4 (b).

Fig. 4 (a) and Fig. 4 (b) clearly show how detection efficiency becomes more basis-dependent with increasing k. The reason for the difference between the two bases is as follows. The two detectors' dead periods in basis 2 gradually move out of sync with respect to each other after a series of independent clicks and recoveries. The chance of basis 2 being active and capable of sifting bits drops as the detectors tend to recover at different times. It becomes increasingly unlikely to have both detectors recovering at about the same time for higher values of k. Basis 1 on the other hand never gets locked up and *always* sifts bit value 1 when (an active) detector 1 is hit. At $k = 1$ both bases are always active. As k increases, the % of time each basis is active drops as one would expect, but basis 2 suffers from the extra effect of detectors locking up, which is more prevalent for higher values of k.

We see that for Rogers et al.'s scheme detection efficiency is basis dependent:

$$P_{0,0}(basis\ 1) \neq P_{0,0}(basis\ 2) \,. \tag{9}$$

This contradicts security proof assumptions [12, 21, 6, 22, 23]. Therefore, the current sifting scheme is potentially no longer safe. Attacks attempting to exploit detection efficiency mismatch exist [24, 25, 26].

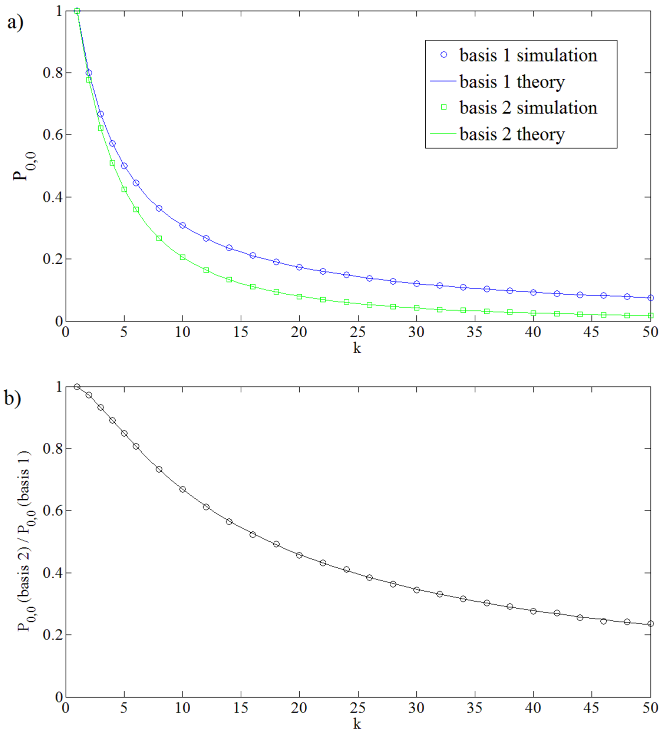

Fig. 4. (a)Basis dependence worsens with increasing k. Both bases become less active, but basis 2 becomes less active at a higher rate than basis 1. $\eta = 0.5$ (channel loss $= 3\ dB$), so that $p = 1/16$ (as defined in Eq. (4)), $N = 5 \times 10^6$ photons. The error bars for each point are smaller than the size of the marker. (b)Ratio of $P_{0,0}$ for basis 2 to $P_{0,0}$ for basis 1 decreases from 1 gradually to 0 with increasing k. The ratio of $P_{0,0}$ for basis 2 to $P_{0,0}$ for basis 1 drops gradually to 0 with increasing k from the initial value of 1 in the slow speed regime at $k = 1$.

5 Secure sifting schemes

We have investigated alternative sifting schemes to see if it is still possible to have secure operation for a finite dead time QKD system in the presence of the most general attack based on the dead time model we consider, assuming the original system without dead time is secure. Some of these are described below.

(i) **SchemeAllActive**
This is a purely software implementation and the scheme only sifts a bit if all four detectors are active. It removes the aforementioned basis dependence, and the sifted bit string is secure. It is simple to implement as the detectors are free-running.

(ii) **SchemeDeactivate** In this scheme, all detectors are actively disabled (or pulses actively blocked) for a period of time equal to or greater than the dead time, every time any one of the four detectors is hit [20]. This prevents any bit sifting unless all detectors are active. Again, the basis dependence is removed, and the scheme is secure. The maximum key rate achievable is $1/(2\tau)$; the factor of $1/\tau$ comes from the maximum count rate of the individual detectors, and the factor of $1/2$ comes from the fact Alice and Bob only use the right basis half the time. As this scheme involves the active disablement of all detectors, it requires an active component for its implementation.

(iii) **Scheme4state** This scheme [27, 28] is different from all other considered above in that it requires only *two* detectors. Consider the phase-encoded BB84 version of this design. (This is more practical compared to the polarization-encoded version of this design as high-speed phase modulators are readily available). Bob actively selects the measurement basis for each incoming pulse. In addition, he determines which of the two detectors represents which bit value (0 or 1) for each pulse, by randomly selecting the phase modulation from a set of *four* values (0, $\pi/2$, π, $3\pi/2$) instead of the usual two (0, $\pi/2$). A diagram representing the detection system is shown below in Fig. 5.

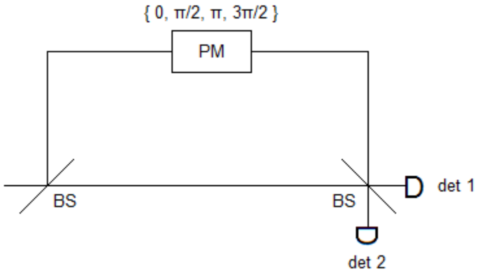

Fig. 5. Schematic diagram of the detection system for phase-encoded version of Scheme4state. BS = beamsplitter, PM = phase modulator, det 1 and det 2 = detectors 1 and 2.

All detections for which Alice and Bob's bases match are sifted. As such, as k goes to infinity, it achieves the highest sifted key rate of all the schemes, equal to $1/\tau$. The disadvantage is that the scheme involves more complicated modulation and requires extra random numbers.

With regard to security, as noted in Ref. [6, 23], the key point is to establish basis-independence of the detection efficiency. The three schemes listed here achieve this point. Specifically, in *SchemeAllActive*, Bob passively post-selects the detection events when the four detectors have the same efficiency. In *SchemeDeactivate*, Bob forces the four detectors to have the same efficiency by actively controlling their bias voltages. In *Scheme*4*state*, Bob randomly switches the role of each detector, thus averaging out the efficiency mismatch. Following [6, 23], we note that the three schemes listed above are indeed secure.

We want to compare the sifted key rate achievable by these different schemes. To derive the probability Pa of a detection system being active for both *SchemeDeactivate* and *Scheme*4*State*, we follow the procedure outlined in Sec. 4.

For *SchemeDeactivate*, an active detection system constitutes all four detectors being active. The moment any one of them fires, the detection system becomes *inactive*. $P_a(SchemeDeactivate)$ is therefore simply given by:

$$P_a(SchemeDeactivate) = \frac{1}{1+(k-1)\eta}\,, \tag{10}$$

where η is the gain, defined by the probability of a click on any of the detectors given that the detection system is active.

Only those detection events where Alice and Bob used the same bases will contribute to the sifted key, which means half of the total detection events for BB84. The sifted bit rate for *SchemeDeactivate* is therefore given by:

$$\begin{aligned} R(SchemeDeactivate) &= \frac{1}{2}(no.\ of\ clicks\ per\ second) \\ &= \frac{1}{2}\rho P_a(SchemeDeactivate)P(click|active) \\ &= \frac{1}{2}\rho P_a(SchemeDeactivate)\eta\,. \end{aligned} \tag{11}$$

Note that the idealized gain η is independently present in both the formula for P_a in Eq. (10) and the formula for the sifted bit rate R in Eq. (11). Once we have an expression for P_a, we still need to account for channel loss to calculate the sifted bit rate R. Consider the simple example where $\eta = 0$ (all signals lost), so that $P_a = 1$, and $R = 0$.

For *Scheme*4*State*, since all detections in which Alice and Bob choose the same basis are sifted, it is easiest to consider the two detectors *individually*. An active detection system consists of a specific detector being active. The situation is therefore completely analogous to the derivation in Sec. 4, and $P_a(Scheme4State)$ is simply given by:

$$P_a(Scheme4State) = \frac{1}{1+0.5(k-1)\eta}\,. \tag{12}$$

where η is the gain, defined by the probability of a click of a specific detector. The sifted bit rate for *Scheme*4*State* is given by combining the bit rate from each of these two detectors:

$$R(Scheme4State) = \frac{1}{2}\rho P_a(Scheme4State)\eta\,. \tag{13}$$

The factor of a half comes from three factors; 1/2 for Alice and Bob using the same basis in BB84, 1/2 to account for the photon hitting the correct one of the two detectors in an individual detection system, and finally a factor of 2 since there are effectively two independent detection systems. Again, we have to include the factor of η to account for channel loss when calculating the sifted bit rate.

The graph below (Fig. 6) shows the sifted key rate as a function of the transmission rate for the different schemes. The simulation results are based on the Monte Carlo method, while the theoretical formulas are derived above. Note that the theoretical values apply only at integer values of k.

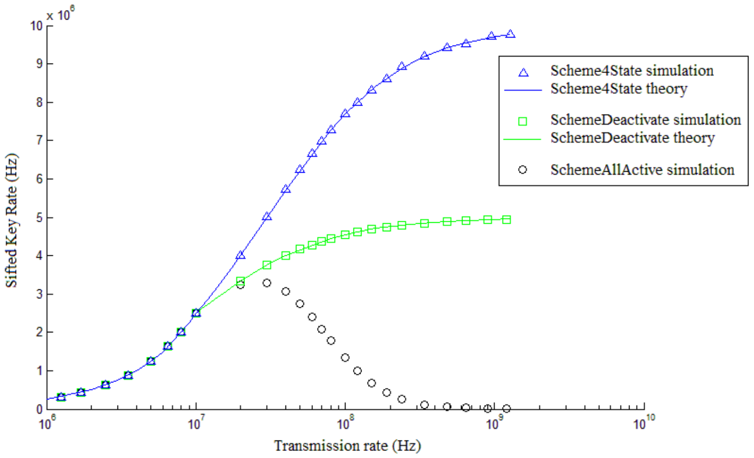

Fig. 6. Comparison of key rates for different sifting schemes. $\eta = 0.5$ (channel loss $= 3\ dB$), dead time $\tau = 100\ ns$, detection efficiency $\eta_D = 100\ \%$. The graph shows there is an optimum value for transmission for *SchemeAllActive* to achieve the maximum sifted key rate. *SchemeDeactivate* gives a higher key rate than *SchemeAllActive* for all values of k higher than 1. *Scheme4state* gives a higher key rate than *SchemeDeactivate* for all values of k higher than 1.

The graph shows that the three schemes are equivalent in the low-speed regime up to $k = 1$ ($10\ MHz$ on the graph since $\tau = 100\ ns$). *SchemeDeactivate* gives a higher key rate than *SchemeAllActive* for all values of k above 1. *Scheme4state* gives a higher key rate than *SchemeDeactivate* for all values of k above 1. The maximum key rate using *SchemeAllActive* is achieved by transmitting in the high-speed regime (at a value of k greater than 1), but not too much (exact value of k depends on the dead time and channel loss). Note that for *SchemeAllActive*, the sifted key rate represents a lower bound; we expect there to be a tighter lower bound since Eve cannot necessarily gain full information on the key.

SchemeDeactivate and *Scheme4state* do not have a peak transmission rate, but instead tend towards a constant value, given by $1/(2\tau)$ and $1/\tau$, respectively, as expected. There is no peak because in both cases the detectors do not get locked up and so the detection system is not paralyzable.

6 Decoy State BB84

So far we have considered a single photon source on Alice's side. Now we move onto a practical scenario with an imperfect source and an imperfect detector. As mentioned in the Introduction, here we consider a standard phase randomized weak coherent state source and threshold detector model in which a detector can tell a vacuum from a non-vacuum signal, but cannot tell the difference between one photon and two or more photons. In this section, for simplicity, we will only consider one particular secure sifting scheme, namely, $SchemeDeactivate$.

Single photon sources are not yet practical for high speed QKD. So, weak coherent pulses (WCP) are often used. Using WCP as the source drastically reduces performance of BB84 due to multi-photon events which are susceptible to the *photon number splitting* attack [6].This has led to the development of the *decoy state* method [7, 8, 9], which allows for efficient performance even with an attenuated laser as the source. Since decoy state is now a standard technique in QKD, we find it helpful to make the connection to this important subject in our paper.

In decoy state BB84, Alice uses more than one photon number distribution. One of these photon number distributions is optimized for the key rate. These events, called *signals*, constitute most of the pulses sent by Alice. She also sends events, called *decoys*, created with different linearly independent photon number distributions. Since Alice knows which events belong to each distribution, Alice and Bob can measure the gains (overall probability of a photon detection event for incoming pulses) for each distribution independently. This linear set of equations is used to ultimately calculate a lower bound on the key rate. Crucially, Eve must not be able to distinguish between n-photon events arising from different distributions.

Decoy state BB84 is now commonly used in practice after the initial experiments a few years ago [29, 30, 31, 32, 33]. It is interesting to analyze the security and performance of decoy state BB84 in the framework of finite detector dead time.

We now allow multi-photon signals to be received by Bob, as this is the realistic scenario in real experiments. Nonetheless, we still make the assumption that signals that strike the detector while it is recovering, regardless of whether they are single photons or multi-photons, do not extend the recovery time, nor have any effect whatsoever. This is a standard but rather strong assumption. We will discuss the practical validity of this assumption in the Conclusion section.

To mitigate the effects of dead time we consider using $SchemeDeactivate$. The security of the scheme also applies when Bob receives multi-photon pulses, as given by the squash model of the single photon detector for the BB84 protocol [34, 35, 36, 37].

In Sec. 5, we derived the probability $P_a(SchemeDeactivate)$ that a detection system is active for $SchemeDeactivate$ (all four detectors are active), and hence capable of sifting bits. It is given by Eq. (10). This derivation assumes a perfect source and detectors with no false counts. We can now adjust this to account for WCP source with μ being the average photon number per pulse, and other imperfections such as background rate Y_0 (including dark counts and stray light).

Let us for the moment ignore the effects of dead time and consider standard decoy state protocols. We will return to the subject of dead time later. It is useful to define the following quantities [16]. The single-photon gain Q_1 (the joint probability that Bob's detector clicks, and that the triggering event was a single-photon) is given by

$$Q_1 = Y_1 \mu \mathrm{e}^{-\mu} \,, \tag{14}$$

where μ is the average photon number per pulse and Y_1 is the single-photon yield (the conditional probability of a detection at Bob's side given that Alice sends a single-photon state), given by

$$Y_1 \cong Y_0 + \eta \,, \tag{15}$$

where Y_0 is the background count rate.

The overall gain Q_μ (overall detection probability summed over all individual gains) is given by

$$Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta\mu} \,. \tag{16}$$

The overall quantum bit error rate (QBER) E_μ is given by

$$E_\mu = \frac{e_0 Y_0 + e_{det}(1 - \mathrm{e}^{-\eta\mu})}{Q_\mu} \,, \tag{17}$$

where e_0 is the error rate of the background (taken to be 0.5) and e_{det} is the probability that a photon triggered an erroneous detector (caused by e.g. optical misalignment).

The single-photon error rate e_1 (error rate conditioned on single-photon events) is given by

$$e_1 = \frac{e_0 Y_0 + e_{det}\eta}{Y_1} \,. \tag{18}$$

Let us now return to the subject of dead time. We can now modify Eq. (10) by replacing η with Q_μ, to account for WCP source and background rate Y_0:

$$P_a^{decoy}(SchemeDeactivate) = \frac{1}{1 + (k-1)Q_\mu} \,. \tag{19}$$

Note that $P_a^{decoy}(SchemeDeactivate)$ goes to 0 as k goes to infinity. Provided that we consider the asymptotic limit of an infinitely long key and the case where the fraction of states used as decoys is negligible, we can use the following method to calculate the secure key rate of decoy BB84 with finite detector dead time:

1) Calculate the naïve key rate R_n by assuming dead time $\tau = 0$,

2) Calculate the actual key rate R by simply multiplying the naïve rate by $P_a^{decoy}(SchemeDeactivate)$:

$$R = P_a^{decoy}(SchemeDeactivate) R_n \,. \tag{20}$$

The naïve secure key rate R_n (in the asymptotic limit of an infinitely long key and without dead time) is given by [16]:

$$R_n = q\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu) H_2(E_\mu)\} \,, \tag{21}$$

where q depends on the implementation (taken to be 0.5 for the BB84 protocol due to the fact that Alice and Bob use different bases half the time), $f(x)$ is the bi-directional error correction inefficiency (taken to be 1.22) and $H_2(x) = x \log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

The actual secure rate (per bit) with dead time is therefore given by:

$$R = P_a^{decoy}(SchemeDeactivate)q\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu)\}\,. \qquad (22)$$

Together with ‘GYS’ parameters from an experiment in Ref. [38], we can calculate the lower bound on the actual secure key rate using Eq. (22) above. Note that in the actual GYS experiment [38] the standard BB84 protocol was used with InGaAs avalanche photodiodes operating in gated mode, while the transmission rate was just 2 MHz, so dead time effects were not significant. The value of μ is taken to be optimized for the given parameters. All the simulation parameters are summarized in Table 1.

Table 1. Key parameters used in the simulation.

τ (ns)	μ	α (dB/km)	l	e_{det}	Y_0	e_0	η_{Bob}	f
100 ns	0.48	0.21	50 km	0.033	1.7×10^{-6}	0.5	0.045	1.22

Fig. 7 shows how the transmission rate affects the secure key rate both for standard decoy BB84 (without dead time effects), and decoy BB84 with dead time effects accounted for with $SchemeDeactivate$.

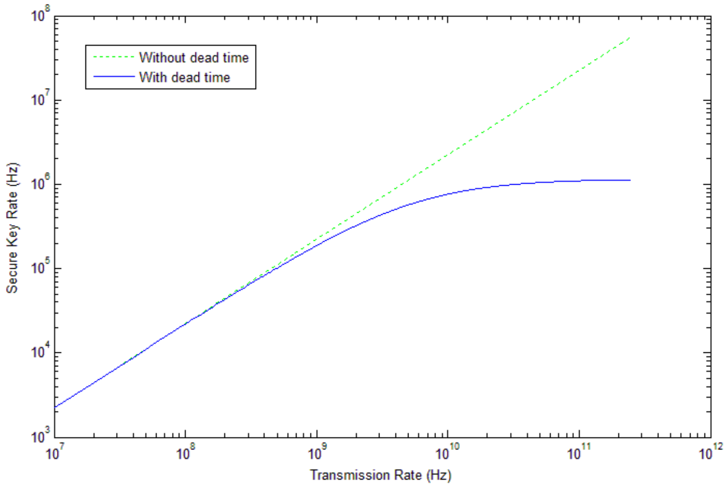

Fig. 7. Graph showing how increasing the transmission rate affects the secure key rate. The dashed green line shows the nave rate relation for standard decoy BB84, without any dead time effects taken into account. The solid blue line shows the actual secure key rate achievable taking dead time effects into account using $SchemeDeactivate$.

At lower transmission rates, the two schemes yield the same secure key rate which scales linearly with transmission rate as expected. The two start to deviate as dead time effects become important. The secure key rate (per second) with $SchemeDeactivate$ (solid blue line) levels off as expected, and is given by:

$$R = \rho P_a^{decoy}(SchemeDeactivate)R_n\,, \qquad (23)$$

where ρ is the transmission rate. As ρ goes to infinity, the secure key rate R approaches the limiting value of $R_n/\tau Q_\mu$.

It should be noted that working with transmission rates of the order of 100 GHz might be problematic. While this high-speed phase modulation is already possible technologically (and QKD with clock rates of 10 GHz has been demonstrated [39]), the timing jitter of current detectors would be a limiting factor for the possible transmission rate. Even a small 50 ps jitter would limit the rate to approximately 10 GHz.

7 Conclusions

Security concerns associated with detector dead times for QKD systems operating at transmission rates higher than the maximum count rates of detectors $(1/\tau)$ can limit the production rate of sifted bits. Rogers et al. [15] have proposed a sifting scheme incorporating these dead time effects that is secure in the case where Eve is completely passive. Monte-Carlo simulations of a BB84-type QKD system with finite detector dead times were performed and extended to include an active eavesdropper, capable of interfering with the quantum channel. It was shown that the sifting scheme proposed in Rogers et al.'s paper [15] is susceptible to intercept-resend attacks by Eve and is no longer guaranteed to be secure because Eve is able to induce basis-dependent detector efficiency. The importance of detectors' dead periods going out of sync with each other and thus being incapable of sifting bits was highlighted. Modified sifting schemes (*SchemeAllActive*, *SchemeDeactivate* and *Scheme*4*State*) were analyzed and compared. It was shown that a modified sifting scheme that is secure which sifts a bit only when all four detectors are active (*SchemeAllActive*) is worse in terms of maximum sifted key rate than a scheme in which all four detectors are disabled when any one of them fires (*SchemeDeactivate*). The advantage of *SchemeAllActive* is that it does not require any active components. The four-state scheme (*Scheme*4*State*) with two detectors still achieves the highest key rate $(1/\tau)$ but requires more complicated modulation and extra random numbers.

The security analysis was extended to the decoy-state BB84 protocol for SchemeDeactivate, and the secure key generation rate analyzed in the context of finite detector dead time.

As detectors and detection techniques improve, detector dead time is expected to be significantly reduced. Commercial Si-based products can achieve a dead time of 45 ns around 800 nm [40]. A dead time of just 1.93 ns has recently been reported with InGaAs detectors [41]. However, the dead time problem is still important to consider as the dead time could also be due to electronics in components such as the time interval analyzer (TIA) [42]. The effect of detector dead time on the security of the differential phase shift protocol [43] has also been analyzed [44].

While the dead time recovery model in Fig. 2 may not fully describe the behaviour of the detectors, it captures the key feature to highlight the dead time problem. This work can therefore be considered as a step towards incorporating the effect of detector dead times into the security analysis of high-speed QKD systems. Note also that *Scheme*4*State* works independently of the shape of the recovery curve in Fig. 2. Nonetheless, *Scheme*4*State* is still vulnerable to other types of detector loopholes such as the blinding attack [45] discussed below.

Future directions could include a more realistic detector dead time model, including a gradual recovery to maximum efficiency, dark counts and afterpulsing. The dead time of different detectors would also not be the same in practice. Eve's ability to control the dead time to her advantage could open up new avenues for attack.

In Sec. 6, we made the assumption that signals striking a detection unit while it is recovering will not extend its dead time and do not have any effect whatsoever. Whether this assumption is violated in practice is still an open question. The work by Makarov's group [45] suggests that the assumption may be violated by Eve using a strong pulse to gain some control over the detectors, although this appears not be the case as discussed in Ref. [46] if the detectors are operated correctly. See also the reply to Ref. [46] by Makarov's group [47]. The conclusive investigation of this question is outside the scope of our work. In addition, it is possible to monitor the large pulse at Bob's side [48] as a counter-measure.

The important lesson here is the need to check carefully the operations of components of a QKD system (in this case the detection system) and make sure that it is properly described by the security model. In a more general context, quantum hacking has attracted widespread recent interest in the quantum cryptography community. In addition to time-shift attack [26] and blinding attack [45], a phase remapping attack has been recently proposed [49] and experimentally demonstrated [50]. The ultimate solution could be the recently proposed Measurement-Device-Independent (MDI) QKD, which removes the possibility of all detector side-channel attacks [51].

Acknowledgements

Support of the funding agencies CIFAR, CIPI, Connaught, CRC, MITACS, NSERC, QuantumWorks and the University of Toronto is gratefully acknowledged. BF acknowledges funding from a PIMS postdoctoral fellowship and iCORE.

References

1. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* volume **175** Bangalore, India, 1984.
2. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Physical review letters* **67**(6):661–663, 1991.
3. Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, *Reviews of modern physics* **74**(1):145–195, 2002.
4. H.-K. Lo and Y. Zhao, Quantum cryptography, *Enc. of Complexity and Systems Science (New York, Springer)* **8**:7265–89, 2009.
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Reviews of Modern Physics* **81**(3):1301, 2009.
6. Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, Security of quantum key distribution with imperfect devices, *Quant. Inf. & Comput.*, **5**:325–360, 2004.
7. Won-Young Hwang, Quantum key distribution with high loss: Toward global secure communication, *Physical Review Letters* **91**(5):057901, 2003.
8. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy state quantum key distribution, *Physical Review Letters* **94**(23):230504, 2005.
9. Xiang-Bin Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Physical review letters* **94**(23):230503, 2005.

10. Dominic Mayers, Unconditional security in quantum cryptography, *J. ACM* **48**(3):351–406, May 2001.
11. Hoi-Kwong Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**(5410):2050–2056, 1999.
12. Peter W Shor and John Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Physical Review Letters* **85**(2):441–444, 2000.
13. Qiang Zhang, Hiroki Takesue, Toshimori Honjo, Kai Wen, Toru Hirohata, Motohiro Suyama, Yoshihiro Takiguchi, Hidehiko Kamada, Yasuhiro Tokura, Osamu Tadanaga, et al, Megabits secure key rate quantum key distribution, *New Journal of Physics* **11**(4):045010, 2009.
14. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, *Opt. Express* **16**(23):18790–18979, Nov 2008.
15. Daniel J Rogers, Joshua C Bienfang, Anastase Nakassis, Hai Xu, and Charles W Clark, Detector dead-time effects and paralyzability in high-speed quantum key distribution, *New Journal of Physics* **9**(9):319, 2007.
16. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, Practical decoy state for quantum key distribution, *Physical Review A* **72**(1):012326, 2005.
17. Massimo Ghioni, Andrea Giudice, Sergio Cova, and Franco Zappa, High-rate quantum key distribution at short wavelength: Performance analysis and evaluation of silicon single photon avalanche diodes, *Journal of Modern Optics* **50**(14):2251–2269, 2003.
18. M. Höbel and J. Ricka, Dead-time and afterpulsing correction in multiphoton timing with nonideal detectors, *Review of Scientific Instruments* **65**(7):2326–2336, 1994.
19. G. F. Knoll, *Radiation Detection and Measurement*, New York, Wiley, 1979.
20. Hai Xu, Lijun Ma, Joshua C. Bienfang, and Xiao Tang, Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems, In *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies*, page JTuH3. Optical Society of America, 2006.
21. Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers, Unconditional security of practical quantum key distribution, *The European Physical Journal D* **41**(3):599–627, 2007.
22. Masato Koashi, Unconditional security of quantum key distribution and the uncertainty principle, In *Journal of Physics: Conference Series*, volume **36** page 98, IOP Publishing, 2006.
23. C. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, *Quantum Information & Computation* **9**(1):131–165, 2009.
24. Vadim Makarov, Andrey Anisimov, and Johannes Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Physical Review A* **74**(2):022313, 2006.
25. Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma, Time-shift attack in practical quantum cryptosystems, *Quantum Information and Computation*, **7**:073–082, 2007.
26. Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Physical Review A* **78**(4):042333, 2008.
27. Peter Moller Nielsen, Christian Schori, Jens Lykke Sorensen, Louis Salvail, Ivan Damgard, and Eugene Polzik, Experimental quantum key distribution with proven security against realistic attacks, *Journal of Modern Optics* **48**(13):1921–1942, 2001.
28. Michael LaGasse, Secure use of a single single-photon detector in a QKD system, *US patent application 20050190922*, 2005.
29. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian, Experimental quantum key distribution with decoy states, *Phys. Rev. Lett.* **96**:070502, Feb 2006.
30. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian, Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber, In *Information Theory, 2006 IEEE International Symposium on*, pages 2094–2098, IEEE, 2006.
31. Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter, Experimental demonstration of free-space decoy-state quantum

key distribution over 144 km, *Phys. Rev. Lett.* **98**:010504, 2007.

32. Danna Rosenberg, Jim W. Harrington, Patrick R. Rice, Philip A. Hiskett, Charles G. Peterson, Richard J. Hughes, Adriana E. Lita, Sae Woo Nam, and Jane E. Nordholt, Long-distance decoy-state quantum key distribution in optical fiber, *Phys. Rev. Lett.* **98**:010503, 2007.
33. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security, *Opt. Express* **15**(13):8465–8471, 2007.
34. Normand J Beaudry, Tobias Moroder, and Norbert Lütkenhaus, Squashing models for optical measurements in quantum communication, *Physical review letters* **101**(9):093601, 2008.
35. Toyohiro Tsurumaru and Kiyoshi Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, *Phys. Rev. A* **78**:032302, 2008.
36. Chi-Hang Fred Fung, H. F. Chau, and Hoi-Kwong Lo, Universal squash model for optical communications using linear optics and threshold detectors, *Phys. Rev. A* **84**:020303, 2011.
37. Masato Koashi, Yoritoshi Adachi, Takashi Yamamoto, and Nobuyuki Imoto, Security of entanglement-based quantum key distribution with practical detectors, *arXiv:0804.0891 [quant-ph]*, 2008.
38. C Gobby, ZL Yuan, and AJ Shields, Quantum key distribution over 122 km of standard telecom fiber, *Applied Physics Letters* **84**(19):3762–3764, 2004.
39. Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H Hadfield, Toshimori Honjo, Kiyoshi Tamaki, and Yoshihisa Yamamoto, Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nature photonics* **1**(6):343–348, 2007.
40. http://www.idquantique.com/scientific-instrumentation/id100-series-single-photon.html.
41. AR Dixon, JF Dynes, ZL Yuan, AW Sharpe, AJ Bennett, and AJ Shields, Ultrashort dead time of photon-counting ingaas avalanche photodiodes, *Applied Physics Letters* **94**(23):231113–231113, 2009.
42. Y. Zhao (private communication).
43. Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, Differential phase shift quantum key distribution, *Phys. Rev. Lett.* **89**:037902, 2002.
44. Marcos Curty, Kiyoshi Tamaki, and Tobias Moroder, Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks, *Phys. Rev. A* **77**:052321, 2008.
45. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature photonics* **4**(10):686–689, 2010.
46. Z.L. Yuan, J.F. Dynes, and A.J. Shields, Avoiding the blinding attack in QKD, *Nature Photonics* **4**(12):800–801, 2010.
47. Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nature photonics* **4**(10):686–689, 2010.
48. Nicolas Gisin, S Fasel, B Kraus, H Zbinden, and G Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Physical Review A* **73**(2):022320, 2006.
49. Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo, Phase-remapping attack in practical quantum-key-distribution systems, *Physical Review A* **75**(3):032314, 2007.
50. Feihu Xu, Bing Qi, and Hoi-Kwong Lo, Experimental demonstration of phase remapping attack in a practical quantum key distribution system, *New Journal of Physics* **12**(11):113026, 2010.
51. H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Physical Review Letters* **108**(13):130503, 2012.