Detector performance in long-distance quantum key distribution using superconducting nanowire single-photon detectors

Burm Baek*a, Lijun Mab, Alan Minkb, Xiao Tangb, and Sae Woo Nam*a

aNational Institute of Standards and Technology, 325 Broadway, Boulder, CO 80305, USA;
bNational Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899, USA

ABSTRACT

The recent advances in superconducting nanowire single-photon detector (SNSPD or SSPD) technology has enabled long distance quantum key distribution (QKD) over an optical fiber. We point out that the performance of SNSPDs play a crucial role in achieving a secure transmission distance of 100 km or longer. We analyze such an impact from a simplified model and use it to interpret results from our differential-phase-shift (DPS) QKD experiment. This allows us to discuss the optimization of the detection time window and the clock frequency given the detector characteristics such as dark count rate, detection efficiency, and timing jitter.

Keywords: quantum key distribution, superconducting nanowire single-photon detector, optical fiber, single photon detector, superconducting detector, cryptography

1. INTRODUCTION

QKD is a way to exchange a secure communication encryption key using quantum mechanics instead of mathematical complexity for the basis of security [1]. A single quantum (photon) is delivered to a receiver so that any attempt by an eavesdropper to extract information from the single quantum alters the quantum state of the photon resulting in the detectable increase of the quantum bit error rate (QBER). Since QKD is mostly done at a single photon level, the loss is the primary limitation in achieving a long-distance QKD.

Recently, QKD systems over an optical fiber using SNSPDs performed a remarkably because of their low level of dark counts and low timing jitter. SNSPDs have broad spectral responsivity that includes the telecommunication bands (1310/1550 nm) where optical fibers have the lowest loss [2,3]. Moreover, SNSPDs are capable of ungated operation for the detection of single photons at telecommunication wavelengths, and enable us to analyze the system performance in more detail by collecting all the detection events. Here, we address the issue of optimizing the detection time window to maximize the secret key rate.

NIST has applied SNSPD technology to various quantum optics experiments. In the NIST system SNSPDs are fiber-coupled, mounted on a compact closed-cycle cryostat, and continuously operated at around 3 K (Fig. 1(a)) [4]. Optical and electrical feedthroughs have low loss and the temperature fluctuation is passively suppressed. Using this multichannel SNSPD system, successful quantum key transmissions over long optical fibers (100 to 200 km) were achieved in different QKD architectures [5-7]. A simplified QKD system using attenuated laser and single-photon detectors is depicted in Fig. 1(b).

QBER limits the maximum distance for secure key generation and provides a simple measure for comparing detector performances in a long-distance QKD. In general, high detection efficiency (DE) increases the total key rate while low dark count rate ($R_d$) reduces the number of error bits. However, dark counts are not synchronous to signal pulses and can be blocked by setting a narrow detector gate time window resulting in a lower number of errors. On the other hand, the gate time should not be too short because the loss of the total key transmission rate becomes significant in the presence of detector time distribution (or jitter). This leads us to an optimization problem of the detection time window size, where the optimal time window depends on the goal of the system (high speed or long distance) and the details of the architecture in general. Nevertheless, the detector jitter usually expressed by its distribution full-width-half-maximum

*burm.baek@nist.gov; phone 1 303 497 4760; fax 1 303 497 3387
This is a work of the U. S. government and is not subject to U. S. copyright
(FWHM) gives a reasonable scale for the time window size. Here, we define a QBER measure = \(R_d \tau / \eta\) with detector jitter \(\tau\) in FWHM, and \(\eta\) in order to compare different kinds of single photon detectors. Table 1 shows the performances of four single photon detectors that are currently available at telecom wavelengths that have been used for QKD demonstrations [5,8-10]. In comparison with InGaAs APD and upconversion detector, SNSPD have a very low dark count rate, reducing the QBER measure of SSPD by two orders of magnitude at least, even though DEs and timing jitters vary by less than an order of magnitude. On the other hand, much lower timing jitter is the advantage leading to a better QBER measure in comparison with TES which was recently shown to have a very high DE [10,11]. It is not surprising that the previous QKD experiments using SSPDs achieved record-breaking long distances due to this advantage over other single photon detectors.

The secure bit rate can be increased with the clock frequency until neighboring bits start to overlap. Thus, precise setting of detection time window will be necessary to utilize the best performance of the detectors. SNSPDs can be operated continuously with no gating in contrast to InGaAs APDs, enabling such an optimization addressed by a simple data acquisition and post-processing. InGaAs APDs require high-frequency gating circuits of limited speed and accuracy. We develop a model to understand the impact of typical SNSPD characteristics on a QKD system in Section 2 in detail and show our DPS QKD experiment and its post-processing for optimizing the time window in Section 3.

Table 1. Performance measures in single photon detectors responsive at telecommunications wavelengths. The data are demonstrated parameters in QKD systems [5,8-10].

<table>
<thead>
<tr>
<th>Detector Type</th>
<th>DE</th>
<th>(R_d)</th>
<th>Timing jitter</th>
<th>QBER measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>InGaAs APD</td>
<td>10%</td>
<td>10 kHz</td>
<td>60 ps</td>
<td>6\times10^{-6}</td>
</tr>
<tr>
<td>Upconversion detector</td>
<td>9%</td>
<td>13 kHz</td>
<td>400 ps</td>
<td>6\times10^{-5}</td>
</tr>
<tr>
<td>SNSPD</td>
<td>1%</td>
<td>10 Hz</td>
<td>60 ps</td>
<td>6\times10^{-8}</td>
</tr>
<tr>
<td>TES</td>
<td>40%</td>
<td>3 Hz</td>
<td>100 ns</td>
<td>8\times10^{-7}</td>
</tr>
</tbody>
</table>

Fig. 1. (a) A photograph of NIST SNSPD system. (b) An illustrated example of a fiber-link QKD system. SPD: single photon detector.
2. ESTIMATION OF QKD PERFORMANCE

In this section, we develop a method to estimate the secure bit rate of DPS QKD to investigate the effects of DE, dark counts and the finite timing jitter of SNSPDs. This method could also be applied to other QKD protocols to estimate secure bit rate given the sifted bit rate and the error rate. A detection event by either of the two SNSPDs on the receiver side represents a qubit transmission with a value (0 or 1) depending on which detector clicks (Fig. 1(b)). We restrict our interest to the effect of the finite detector performance and perfect optics other than the loss in the optical fiber link. The basic idea starts with the SNSPDs and the time-interval analyzer dominating the detection time distribution, which is well approximated by Gaussian distribution. This makes a finite time window necessary in order to increase the transmission key rate, but also causes intersymbol interference (ISI), i.e., detection at a different time slot than prepared, especially in a high clock-frequency transmission (Fig. 2).

![Illustrated detection time distribution and time window settings for time-slot assignment. There exists an optimal time window between the two extremes for achieving the highest secret rate.](image)

We calculate the sifted bit rate and QBER at the first step; we require only these to estimate the secure bit rate eventually. Our detector performance is characterized by its DE \( \eta \), dark count rate \( R_d \), and timing jitter given by a probability distribution \( \rho(t) \). The optical fiber link loss is \( \eta_{\text{link}} \) and we assume zero insertion loss everywhere else. The photons are transmitted at a mean photon number per pulse \( \mu \) and a clock frequency \( f_{\text{clock}} \) (with period \( T = \frac{1}{f_{\text{clock}}} \)). \( w \) is the detection time window that we will vary.

We only look at the detection events within the time window. We denote \( S \) as the probability that a detector triggered by a transmitted photon in the correct time bin is registered as a correct bit. Meanwhile, a photon could be detected accidentally in an adjacent time bin in the presence of the detection timing jitter (intersymbol interference or ISI) denoted by \( I \). The probability of errors due to dark counts is denoted by \( D \). These are usually much smaller than 1 and closely related to \( w \) and \( \rho(t) \) as:

\[
S = \mu \eta_{\text{link}} \eta \int_{-w/2}^{w/2} \rho(t)dt, \quad (1a)
\]

\[
I = \mu \eta_{\text{link}} \eta \int_{-w/2}^{w/2} \rho(t)dt, \quad (1b)
\]

\[
D = R_d w, \quad (1c)
\]

Within the time window \( w \) (i.e., \(-w/2 < t < w/2\)), we get a sifted bit if only one of the two detectors fires. Let \( p_s \) be the probability of the firing detector being the correct one with regard to the sender’s encoding. Then \( p_s = S + I + D \). The probability of error is \( p_e = I + D \).

Now the sifted bit rate \( R_{\text{sift}} \) and QBER \( e \) are calculated from \( p_s \) and \( p_e \):

\[
R_{\text{sift}} = f_{\text{clock}}(p_s + p_e), \quad (1d)
\]

\[
e = p_e/(p_s + p_e) \quad (1e)
\]

Using the accessible detector performance parameters and assuming perfect components otherwise, we calculated the sifted bit rate and QBER expected using SNSPDs in a DPS QKD system (Fig. 3). The key parameters are: wavelength =
1550 nm, clock frequency = 10 GHz, detection efficiency = 5\%, detection time jitter = 50 ps FWHM, and $R_d = 10$ Hz. Both the sifted bit rate and QBER increases with a wider detection time window. The sifted bit rate increases steeply at a narrow window range and becomes almost a constant when the window is significantly wider than the timing jitter. On the other hand, the steeper increase of QBER near the maximum window size is the effect of the ISI.

From ref. [12], we estimate the theoretical secure bit rate in a DPS QKD system as:

$$R_{\text{secure}} = R_{\text{shift}} \left\{ - (1 - 2\mu) \log_2 \left( 1 - e^2 - \frac{(1 - 6e)^2}{2} \right) + f(e)h(e) \right\}$$  \hfill (2)

$f(e)$: performance factor of the error correction algorithm
$h(e) = \text{binary entropy function} = - e \log_2 e - (1-e) \log_2 (1-e)$.

After the numerical integrations over the detection time window for the sifted bit rate and QBER, we get the estimated secure bit rate from (2) (Fig 4). As we expected, there exists an optimal time window size maximizing the secure bit rate at each distance. The initial increase is dominated by the increase of the transmission rate, which saturates with the window wider than the detector jitter. At a larger $w$, the increased error rate and saturating transmission rate together result in a reduction in the secure bit rate. At short distances, ISI is the dominant factor for the increased QBER while dark count rate becomes a limiting factor at long distances requiring narrower window sizes to obtain finite secure bit rates. In designing a QKD system, this gives an estimation of the achievable transmission distance with a proper consideration of the detection time window. This could be optimized further by varying the transmission frequency, but the optimization should be aimed at the specific application need.

Besides the time window optimization, DE and dark count rate of an SNSPD can be controlled by its bias current to optimize the QKD performance. An SNSPD shows a modest (almost linear) increase of DE with its bias current in contrast to an exponential increase of its dark count rate. This implies that reducing the bias current will suppress dark counts significantly with modest decrease in the secure key transmission rate as a tradeoff. For instance, an order of magnitude reduction in dark count rate with only a factor of two reduction in DE could compensate for 7 dB optical loss, which is equivalent to ~35 km-longer optical fiber at 1550 nm wavelength, although this would decrease the sifted key transmission rate by half. However, this optimization also depends on the specific application need: distance vs. secure key rate.
3. EXPERIMENT: DPS QKD AND THE TIME WINDOW OPTIMIZATION

We implemented a QKD system over standard single-mode optical fiber at 1310 nm using a DPS architecture and SNSPDs [13]. This wavelength is known for low loss, zero dispersion in standard single-mode optical fiber, and low Raman scattering from the C and L bands near 1550 nm. Also, QKD at 1310 nm can coexist with classical communications traffic at 1550 nm.

The system is depicted in Fig. 5. On the Alice side, a 2.5 GHz pulse train is produced from a 1310 nm continuous-wave (CW) laser by an electro-optic amplitude modulator (AM). Random bit data are encoded in the pulses by a pattern generator and a phase modulator (PM) and attenuated to emit 0.1 photon per pulse. The receiver (Bob) uses a 1-bit-delayed Michelson interferometer (MI) to passively decode the qubits so that only one of the SNSPDs clicks depending on the differential phase of successive photon pulses encoded by the PM. Detection times measured relative to the (electrical) sync pulses by time-interval analyzers (TIAs) provide the time slot information of the qubits. We performed key rate measurements over fiber links of various lengths.

![Fig. 5. A diagram of our DPS QKD experimental setup. LD: laser diode, AM: amplitude modulator, PM: phase modulator, VOA: variable optical attenuator, MI: Michelson interferometer, TIA: time-interval analyzer.](image-url)
Fig. 6 is a histogram of arrival times over 25 clock periods at a short transmission distance of a (repeated) pseudo-random bit stream. The SNSPDs were operated in an ungated mode such that we can continuously take data and analyze them in different ways. We observe that the detection events have a Gaussian distribution with a FWHM ~130 ps contributed mostly by the timing electronics, source jitter, and SNSPD jitter. Assigning a time slot to each detection event is done by setting a time window around the center of a slot as explained in the previous section to see the effects of competing properties (mostly timing jitter and dark counts).

Fig. 7 shows the sifted bit rate and QBER as a function of the time window size. The sifted bit rate is dominated by the detection time distribution and obviously fits well to the model. The trend of the QBER increasing with the time window size agrees with the calculation, but it has more structure which cannot be explained by our simple model considering only detector performances (or with small variations considering the imbalance of two detectors and the finite interferometer visibility). We believe that the drift in the interferometer caused the deviation.

Using (2), the secure bit rate for various time windows was estimated and plotted in Fig. 8(a). The optimal time window for the highest secure bit rate was obtained at 140 to 200 ps varying with the fiber link loss (dependent on the
transmission distance) and resulted in the enhancement by ~30% compared with the results at a full time window width given by 1/(clock frequency). The exponential decrease in the secure bit rate with the distance is observed as expected from the associated optical loss and the sifted bit rate (Fig. 8(b)). The optimal time window size becomes smaller as the transmission distance is increased. This is because the reduction in the dark count rate dominating QBER becomes the biggest factor in reducing QBER in spite of the cost of a reduced sifted bit rate. On the other hand, the experimental data have a discrepancy against the calculated prediction despite the qualitative agreement. This comes from the difference in the QBER from the experiment and the calculation shown on Fig 7(b). Nevertheless, it is obvious that this optimization of the detection time window is essential to evaluate QKD system performance properly, especially in long distance transmission. The enhancement of the secure bit rate compared with that obtained with the full time window width amounts to ~130% consistently at different distances.

Fig. 8. (a) Secure bit rate vs time window size. The circles are the estimation from the rates obtained by the DPS QKD experiment done for a 50 km-long fiber link. The solid curve is a fit by the calculation described in Section 2. (b) Secure bit rates vs distance at optimal time windows (circle) and at a maximum time window (square). The line is a linear fit to the data obtained by setting the optimal time windows.

4. SUMMARY

SNSPD technology promises the best performance in QKD owing to its ultra-low dark count rate and high timing resolution. In particular, it is capable of ungated operation due to an ultra-low dark count rate and afterpulsing probability, enabling the characterization of the QKD system performance with no modification of the system. We analyzed the impact of the SNSPD performance which could be used for a first-step system design when the analytic expression for the secure bit rate is known. Our DPS QKD experiment was used to demonstrate the time window optimization necessary at the final step of maximizing QKD performance. We anticipate this thorough understanding of the detector performance effect on QKD and its systematic assessment would be used for design and characterization of QKD system using SNSPDs in future.

REFERENCES


