A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution

Yue-Meng Chi\textsuperscript{1}, Bing Qi\textsuperscript{1}, Wen Zhu\textsuperscript{1}, Li Qian\textsuperscript{1,4}, Hoi-Kwong Lo\textsuperscript{1}, Sun-Hyun Youn\textsuperscript{2,3}, A I Lvovsky\textsuperscript{2} and Liang Tian\textsuperscript{1}

\textsuperscript{1} Center for Quantum Information and Quantum Control (CQIQC), Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada
\textsuperscript{2} Institute for Quantum Information Science, University of Calgary, Calgary, Alberta, T2N 1N4, Canada
\textsuperscript{3} Department of Physics, Chonnam National University, Gwangju 500-757, Korea
E-mail: l.qian@utoronto.ca

New Journal of Physics 13 (2011) 013003 (18pp)
Received 5 August 2010
Published 5 January 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/1/013003

Abstract. We discuss the excess noise contributions of a practical balanced homodyne detector (BHD) in Gaussian-modulated coherent-state (GMCS) quantum key distribution (QKD). We point out that the key generated from the original realistic model of GMCS QKD may not be secure. In our refined realistic model, we take into account excess noise due to the finite bandwidth of the homodyne detector and the fluctuation of the local oscillator (LO). A high-speed BHD suitable for GMCS QKD in the telecommunication wavelength region is built and experimentally tested. The 3 dB bandwidth of the BHD is found to be 104 MHz and its electronic noise level is 13 dB below the shot noise at an LO level of $8.5 \times 10^8$ photons per pulse. The secure key rate of a GMCS QKD experiment with this homodyne detector is expected to reach Mbits s\textsuperscript{-1} over a few kilometers.
## Contents

1. Introduction 2  
2. Gaussian-modulated coherent-state protocol 4  
3. Excess noise contributed by the balanced homodyne detector in a GMCS quantum key distribution 6  
   3.1. BHD electronic noise 6  
   3.2. Excess noise due to electrical pulse overlap 6  
   3.3. Excess noise contributed by local oscillator fluctuations 7  
4. Construction and performance 9  
   4.1. Schematic representation 9  
   4.2. Linearity 10  
   4.3. BHD bandwidth 11  
   4.4. Homodyne detector noise measurement in the time domain 12  
   4.5. Common mode rejection ratio 14  
   4.6. Excess noise evaluation and key rate simulation for a GMCS QKD experiment 14  
5. Conclusion 15  
Acknowledgments 17  
References 17  

### 1. Introduction

Quantum key distribution (QKD) based on Gaussian-modulated coherent-state (GMCS) protocol has attracted much attention [1]–[7]. Comparing with the BB84 QKD, the GMCS QKD presents several advantages. The coherent state required by GMCS QKD can be produced easily by a practical laser source, while the perfect single-photon source required by BB84 QKD is hard to obtain. Although improved BB84 protocols (such as decoy protocols [8]–[11]) are compatible with coherent laser sources, they do require single-photon detectors, which are expensive and have low efficiency. The homodyne detector in the GMCS QKD, on the other hand, can be constructed using high-efficiency PIN photodiodes [3]. The GMCS QKD also has the advantage of transmitting multiple bits per symbol [1, 12]. The security of the GMCS QKD was first proven against individual attacks with direct [13] or reverse [1, 14] reconciliation schemes. Security proofs were then given against general individual attacks [14] and general collective attacks [15]–[17]. To date, three groups have independently claimed that they have proved the unconditional security of GMCS QKD [18]–[20]. The secure key rate per pulse is the same in the three proofs.

Fiber-based GMCS QKD systems over a practical distance are challenging and only a few groups have demonstrated QKD experiments over tens of kilometers [6, 15, 21, 22]. Current repetition rates used in those GMCS QKD experiments are below 1 MHz, which in turn makes the GMCS QKD less competitive than the single-photon BB84 QKD operating at GHz repetition rates [24, 25]. The repetition rate of GMCS QKD is limited by a few factors: (i) the speed of the homodyne detector [6], (ii) the speed of the data acquisition system and (iii) the speed of the classical data processing algorithm [3]. The speed of data acquisition and classical data processing can be increased by hardware engineering and are not fundamental
limits in GMCS QKD. In this paper, we mostly focus on increasing the homodyne detector speed and analyzing various excess noise contributions introduced by a practical homodyne detector.

The balanced homodyne detection used in quantum measurement, proposed by Yuen and Chan [26], plays an important role in quantum optics [27]–[29] and quantum cryptography [1, 3, 6, 15, 22, 23]. In a balanced homodyne detector (BHD), the signal to be measured is mixed with a local oscillator (LO) at a beam splitter. The interference signals from the two output ports of the beam splitter are sent to two photodiodes followed by a subtraction operation, and then amplification may be applied. The output of a BHD can be made to be proportional to either the amplitude quadrature or the phase quadrature of the input signal depending on the relative phase between the signal and the LO. The output of the BHD can be captured in either frequency [30] or time domains [31]–[34]. For GMCS QKD, measurement in the time domain that is capable of resolving each individual pulse (representing a weak coherent state) is required in order to extract random key information [1]. This pulse-resolving requirement demands that the bandwidth of the detection system be significantly higher than the repetition rate of the QKD operation, which highlights the importance of developing high-bandwidth BHDs. Only very recently, high-speed InGaAs BHDs have been developed and used in quantum measurements [35].

In this paper, we develop a broadband BHD suitable for GMCS QKD operating at a repetition rate of tens of MHz. To predict its performance in GMCS QKD, we first analyze the excess noise contributed by this practical BHD. In the GMCS QKD, excess noise is defined in units of shot noise and includes all noises due to system imperfections and eavesdropping, which are above and beyond the vacuum noise associated with channel loss and losses in Bob’s system. It determines the maximum amount of information that could be obtained by Eve. In the original realistic model (ORM) proposed in previous GMCS QKD literature [1, 6, 15], the excess noise contributed by a BHD is the electronic noise of the BHD. This model does not consider the excess noise that originates from other imperfections in a practical BHD and is not conservative enough in estimating the information possibly leaked to Eve. In this paper, we refine the ORM that has been widely adopted to calculate key rates for practical GMCS QKD systems and identify two new noise sources of a practical homodyne detector: (i) the excess noise caused by the BHD electrical pulse overlap at the BHD output and (ii) the excess noise caused by LO fluctuation. Both of these noise contributions can be taken advantage of by Eve if they are not quantified. For example, Eve can control the arrival time of the signal and LO pulses, or change the LO intensity, to obtain partial information on the key. Under the refined realistic model (RRM), we quantify the various excess noise contributions from the broadband BHD we constructed. Based on our simulation using the experimentally determined excess noise of the BHD, secure GMCS QKD key rates using this BHD are predicted to reach Mbits s\(^{-1}\) over a few kilometers.

This paper is organized as follows. In section 2, we revisit GMCS QKD protocol, identify two new excess noise sources, and introduce the key generation rate formulae based on the RRM. In section 3, we analyze the excess noise contribution of a practical BHD. In section 4, we discuss practical issues in building a high-speed BHD, including different temporal responses of two photodiodes, appropriate pulse duration and the BHD linearity and construction of a high-speed HD in GMCS QKD. In section 5, we will report the performance of the BHD and predict the key rates by simulation.
2. Gaussian-modulated coherent-state protocol

The basic GMCS QKD protocol is as follows. Alice generates two random sets of continuous variables \( x \) and \( p \) with a Gaussian distribution that has a zero average. Alice then encodes random bits (key information) by modulating the amplitude quadrature \( \langle x \rangle \) and the phase quadrature \( \langle p \rangle \) of weak coherent states \( |x + ip\rangle \) (typically less than 100 photons in each pulse) with her Gaussian-distributed random variable sets \{\( x \), \( p \)\}. On the receiver’s side, Bob measures either the \( x \) or \( p \) quadrature of the weak coherent states randomly using homodyne detection. By repeating this procedure multiple times, Alice shares a set of correlated Gaussian variables (called the ‘raw key’) with Bob. By comparing a random sample of their raw key, they can evaluate parameters of QKD and the upper bound on Eve’s information. Finally, they can generate a secure key by performing reconciliation.

In the presence of individual attacks, one can estimate the information leaked to Eve from the amount of quadrature noise observed by Bob in excess of the standard quantum limit [1]. The most conservative estimation (the general model) assumes that all the excess noise is introduced by eavesdropping, whereas the ORM assumes that Eve cannot control the LO or take advantage of the excess noise generated within Bob’s system [1]. In the ORM, the excess noise has several contributions:

(i) Noise due to imperfection outside Bob’s system, denoted by \( \varepsilon_A \). This part of the noise can be controlled by Eve.

(ii) Noise from Bob’s system that is uncontrollable by Eve, called \( N_{Bob} \).

In [3, 15], (ii) refers to the homodyne detector noise \( (N_{hom}) \), while in [6, 21], it consists of both homodyne detector noise \( (N_{hom}) \) and the noise associated with the photon leakage from the LO to the signal \( (N_{leak}) \). In previous papers [3, 6, 15, 21], \( N_{hom} \) is regarded to consist of only the electronic noise (i.e. \( N_{hom} = N_{ele} \)). In this paper, we refine this realistic model and consider other imperfections of a practical BHD, and conclude that excess noise caused by a practical BHD \( (N_{hom}) \) could be divided into three parts: (i) electronic noise \( (N_{ele}) \), (ii) noise introduced by electrical pulse overlap due to the finite response time of the BHD \( (\varepsilon_{overlap}) \) and (iii) noise due to LO fluctuation in the presence of incomplete subtraction of a BHD \( (N_{LO}) \).

In [41], the need to monitor the intensity of the LO for security proofs in discrete QKD protocols embedded in continuous variables has been discussed. Here, we assume that in a GMCS QKD experiment, Alice and Bob can monitor LO and discard pulses with large intensity changes in LO; however, there is always a small measurement error due to imperfect measurement instruments. Consequently, Eve can take advantage of small LO fluctuations. Therefore, in this RRM, \( \varepsilon_{overlap} \) and \( N_{LO} \) generated by the BHD, as well as \( N_{leak} \) associated with leakage LO photons, are all considered controllable by Eve. \( N_{LO} \) is caused by imperfect subtraction of BHD in the presence of LO intensity fluctuations, while \( N_{leak} \) is due to the interference between the leakage photons and LO photons.

Following an approach similar to that in [1], we will now present the GMCS QKD key rate formulae based on the RRM. The mutual information between Alice and Bob \( I_{AB} \) is determined by the Shannon entropy [36]. According to [1, 3],

\[
I_{AB} = \frac{1}{2} \log_2 \left[ \frac{(V + \chi)}{(1 + \chi)} \right],
\]

where

\[
\chi = \chi_{vac} + \varepsilon = \frac{1 - \eta G}{\eta G} + \varepsilon.
\]
Figure 1. Various noise terms in the ORM and RRM.

In equation (1), $V = V_A + 1$ is the quadrature variance of the coherent state prepared by Alice (1 is the shot noise of a coherent state) and $V_A$ is Alice’s modulation variance (variance of the $x$ or $p$ quadratures modulated by Alice). In equations (1) and (2), $\chi$ is the equivalent noise measured at the input$^5$, which is composed of the ‘vacuum noise’ $\chi_{\text{vac}}$ (noise associated with the channel loss and detection efficiency of Bob’s system) and ‘excess noise’ $\varepsilon$ (noise due to the imperfections in a non-ideal QKD system). $G$ is the channel efficiency (transmission), and $\eta$ is the total efficiency of Bob’s device (optical loss and detector efficiency).

We will now discuss the key rate formulae for the case of the RRM, which we defined earlier in this section. Under the RRM, the noise that can in principle be controlled by Eve ($\varepsilon_E$) includes: (i) $\varepsilon_A$ due to imperfections outside Bob’s system; (ii) $\varepsilon_{\text{overlap}}$ introduced by electrical pulse overlap due to the finite response time of the BHD; (iii) $N_{\text{LO}}$ due to LO fluctuations in the presence of incomplete subtraction of a BHD and (iv) $N_{\text{leak}}$ associated with the leakage from LO to signal. The excess noise that is out of Eve’s control ($N_{\text{Bob}}$) is the electronic noise from the homodyne detector ($N_{\text{ele}}$). Therefore, the total excess noise $\varepsilon$ can be written as [1]

$$\varepsilon = \varepsilon_E + N_{\text{Bob}}/\eta G,$$

where $\varepsilon_E = \varepsilon_A + \varepsilon_{\text{overlap}} + N_{\text{LO}}/\eta G + N_{\text{leak}}/\eta G$ and $N_{\text{Bob}} = N_{\text{ele}}$. $\varepsilon_A$ and $\varepsilon_{\text{overlap}}$ are referring to the input. $N_{\text{LO}}$, $N_{\text{leak}}$ and $N_{\text{ele}}$ are measured at the output. Noises measured at the output can be divided by $\eta G$ when converted to the input. Figure 1 summarizes the various noise terms considered in the ORM and the RRM. $N_{\text{leak}}$ is mostly determined by the design of the QKD system rather than by the BHD. Since our main goal is to study the excess noises contributed by the BHD, we simply assume $N_{\text{leak}} = 0$ in this paper.

From equations (2) and (3), the equivalent input noise is

$$\chi = \frac{1}{\eta G} - \varepsilon_A + \varepsilon_E + \frac{N_{\text{Bob}}}{\eta G}.$$

With a reverse reconciliation scheme, the mutual information shared by Bob and Eve under RRM is

$$I_{BE} = \frac{1}{2} \log_2 \left[ \frac{\eta GV_A + 1 + \eta G \varepsilon}{\eta/(1-G + G \varepsilon_E + G V^{-1}) + 1 - \eta + N_{\text{Bob}}} \right].$$

Equation (5) has the same form as that of the ORM, except that $\varepsilon_E$ in the original model includes only the $\varepsilon_A$ term.

$^5$ Although noise can have different origins and occur at various locations along the system, for the calculation expressed by equation (1), all noises are referring to the input. Therefore, noise added by a component at a particular point in the system is scaled according to the gain/loss of the channel up to that point.
If a reverse reconciliation algorithm [1] is adopted, the secure key rate per pulse is
\[ \Delta I = \beta I_{AB} - I_{BE}, \]  
where \( \beta \) is the reconciliation efficiency (\( \beta \leq 1 \)). In real QKD systems, \( \beta \) is 0.9 in [22] and 0.898 in [15]. If the laser repetition rate of the QKD experiment is \( R \) Hz, the secure key per second can be written as
\[ \Delta I_{\text{second}} = (\beta I_{AB} - I_{BE}) \times R. \]  

3. Excess noise contributed by the balanced homodyne detector in a GMCS quantum key distribution

As previously stated, excess noise represents the amount of information that could possibly be leaked to Eve in a GMCS QKD system and is important in estimating the amount of secure information.

In this section, we will evaluate various sources of the excess noise for a practical BHD.

3.1. BHD electronic noise

Electronic noise \( N_{\text{ele}} \) of a BHD is mainly contributed by the thermal noise of the electronic components and the amplifier [37]. Since the shot noise scales with LO power and electronic noise is independent of the LO power [38], by measuring the BHD noise as a function of the LO power when vacuum is sent to the signal port, we can quantify the electronic noise in units of shot noise. Electronic noise in a BHD has been discussed in [39].

3.2. Excess noise due to electrical pulse overlap

Ideally, the secure key rate of a GMCS QKD system is proportional to its operation rate. However, in practice, the BHD has a finite bandwidth. As the laser pulse repetition rate approaches the bandwidth of the BHD, we will expect a non-negligible overlap between adjacent electrical pulses at the output of the BHD. If the electrical pulses have overlap in the time domain, the measured quadrature value contains contributions from adjacent pulses.

We will estimate the amount of excess noise contributed by the electrical pulse overlap. The exact relation between the electrical pulse width \( \tau \) and the BHD bandwidth \( B \) depends on the electrical pulse shape. We have experimentally found that the relation \( \tau \sim 1/B \) is applicable to our homodyne detector. In this case, we can estimate the overlap by writing the following functions for two consecutive pulses: (a) \( e^{-t/(2R^2\tau^2)} \) and (b) \( e^{-t^2/2\tau^2} \), where \( R \) is the laser repetition rate and \( \tau \) is the Gaussian pulse width. If the quadrature value is determined by the peak of the measured electrical pulse, the contribution of pulse (a) to pulse (b) is \( e^{-B^2/2R^2} \). Since each pulse has two adjacent pulses, the excess noise contributed by the electrical pulses overlap (referring to the input) is
\[ \varepsilon_{\text{overlap}} = 2 V \times (e^{-B^2/2R^2})^2 = 2(V_A + 1) \times e^{-B^2/R^2}, \]  
where \( V_A \) is Alice’s modulation. We remark that the excess noise due to the overlap between adjacent pulses could be further reduced by deconvolution [34].

By decreasing this repetition rate, we can reduce the excess noise caused by the overlap. However, the GMCS QKD key rate per second will be reduced too. In figure 2, we simulate the
GMCS QKD secure key generation rate as a function of the laser repetition rate under the RRM. The bandwidth of the BHD is 100 MHz. The simulation parameters are from [6], $V_A = 16.9$, $G = 0.758$, $\eta = 0.44$, $\epsilon_A = 0.056$, $N_{\text{ele}} = 0.045$ and $\beta = 0.898$. In this simulation, $N_{\text{LO}} = N_{\text{leak}} = 0$.

3.3. Excess noise contributed by local oscillator fluctuations

One of the advantages of BHD is that ideally the fluctuations of LO will be canceled after the subtraction. However, in a practical BHD, the positive and negative pulses cannot be canceled completely due to several reasons, such as different quantum efficiencies of the two photodiodes, different temporal responses of the photodiodes and the subsequent electronic amplifiers, or different optical intensities of the two balanced beams. The difference can be partially compensated, for example by adjusting the losses and the relative delay of the two balanced arms; however, it cannot be completely canceled out. The remaining difference also varies with LO power. The consequence is that the fluctuation of the LO power will contribute to the excess noise.

The quadrature measurement corresponds to the time integrated electronic response of the detector. Neglecting the shot noise, this response equals

$$N_{\text{out}} = I_{\text{LO}}[G_1 t^2 - G_2 r^2],$$

where $I_{\text{LO}}$ is the number of photons in the LO pulse, $t$ is the beam splitter transmission coefficient, $r$ is the reflection coefficient and $G_{1,2}$ are the time integrated gains of the amplifiers associated with the two photodiodes. We assumed that the quantum efficiency of the

---

New Journal of Physics 13 (2011) 013003 (http://www.njp.org/)
photodiodes is 1 and the signal is in the vacuum state. Given that the variance in the number of photoelectrons in each photodiode due to the shot noise equals the number of incident photons, we obtain the output shot noise as
\[ \langle N_{\text{shot}}^2 \rangle = I_{\text{LO}}[G_1^2 t^2 + G_2^2 r^2]. \]  

If the relative fluctuation of the LO power is \( \sqrt{\langle \Delta I_{\text{LO}}^2 \rangle / I_{\text{LO}}} = f \), then the mean square fluctuation in the number of output photoelectrons is given, in units of shot noise, by
\[ N_{\text{LO}} = \frac{\langle \Delta N_{\text{out}}^2 \rangle}{\langle N_{\text{shot}}^2 \rangle} = I_{\text{LO}} f^2 \delta^2 \]  

with \( \delta = \frac{G_1 t^2 - G_2 r^2}{\sqrt{G_1^2 t^2 + G_2^2 r^2}}. \)

For a well-balanced detector, \( t^2 \approx r^2 \approx 1/2 \) and \( G_1 \approx G_2 \). In this case, the above expression can be written as \( \delta \approx \delta_{\text{opt}} + \delta_{\text{el}} \), where \( \delta_{\text{opt}} = t^2 - r^2 \) is the imbalance of the optical beam splitter, whereas \( \delta_{\text{el}} = (G_1 - G_2)/(G_1 + G_2) \) is the electronic characteristic of the balanced detector related to its common-mode rejection ratio (CMRR). In what follows, it is convenient to discuss \( N_{\text{LO}} \) in terms of generalized CMRR, which is measured in decibels and defined as
\[ \text{CMRR} = -20 \log_{10}(2\delta), \]  

i.e. includes both the optical and electronic components of the output signal fluctuation.

The magnitude of \( N_{\text{LO}} \) can be estimated from the Taylor decomposition of the noise variance as a function of the LO power. The shot noise variance is proportional to the LO level, whereas \( N_{\text{LO}} \) depends on it quadratically [37]. We note that for determining \( N_{\text{LO}} \), only time-integrated response functions (over the bandwidth of the homodyne detector) of the photodetector–amplifier systems are relevant; faster varying differences in the time-dependent shapes of these functions play no role.

With the same GMCS QKD parameters as those used to produce figure 2, we simulate the GMCS QKD secure key rate as a function of the CMRR of the BHD in figure 3. When the
CMRR is lower than 55 dB (where the key rate is 90% of the maximum), the key rate drops quickly as the CMRR drops. To obtain a positive key rate, the CMRR of the BHD should be greater than \( \sim 44 \) dB. When the CMRR is greater than 55 dB, the secure key rate will not be significantly improved by increasing the CMRR since the other excess noise contribution (\( \varepsilon_A \)) is dominant.

4. Construction and performance

In this section, we will present our construction and test results of a high-speed BHD in the telecommunication wavelength region. We will also predict the excess noise and secure key rate when the BHD is used in a GMCS QKD experiment.

4.1. Schematic representation

Figure 4(a) shows a schematic representation of our balanced homodyne detection system. In the telecommunication wavelength region, the signal and the LO beams will interfere at a two-by-two fiber coupler with a splitting ratio of 50:50. A variable optical attenuator and a variable optical delay are placed in the output paths of the fiber coupler, for adjusting the losses and lengths of the two paths accurately. Two photodiodes detect the interference of the signal and the LO, which have to be precisely mode matched to each other. Finally, a subtraction of the photocurrents generated by the two photodiodes is performed and the differential signal...
is amplified. To avoid disturbances from the environment, we used an enclosure to isolate the system of figure 4(a).

In the electronic circuit shown in figure 4(b), two InGaAs photodiodes from Thorlabs (FGA04, 2 GHz bandwidth, quantum efficiencies: 90 and 93%) are reversely biased. The differential signal is amplified by two OPA847 operational amplifiers. The whole BHD circuit is built on a custom-designed printed circuit board. To minimize the parasitic capacitance, two photodiodes with short electrical contact legs are placed very close to each other.

4.2. Linearity

In GMCS QKD, continuous Gaussian random numbers encoded on each pulse by Alice have to be recovered by the balanced homodyne detection on Bob’s side. To ensure that the BHD output is proportional to the electric field quadrature of each pulse, the linearity of the BHD has to be guaranteed. In practice, the photodiode and electronic amplifiers can both have nonlinearities. A proper pulse width should be carefully chosen to guarantee that the photodiodes are working in their linear regions. In the test of the photodiode linearity, we send pulsed light to only one photodiode while blocking the other one. At a laser repetition rate of 10 MHz, we measure the output photocurrent generated by the photodiode (before it goes to the electronic amplifiers) at different incident optical powers using an oscilloscope. In figure 5, we compare the output electrical pulse peak current when (a) ~1 ps or (b) 50 ns laser pulse duration is used. We can see from figure 5(a) that the photodiodes saturate at a lower optical input photon number per pulse than that of (b). The difference in the saturation behavior of the two photodiodes (figure 5(a)) also leads to poorer matching of the photodiode responses when picosecond pulses are used, as compared to nanosecond pulses (figure 5(b)). In fact, the high peak power of the ~1 ps pulse (~18 W) saturates the photodiodes. In the case of 50 ns pulse as a source (figure 5(b)),

![Figure 5](http://www.njp.org/figure5.png)

**Figure 5.** Photodiode linearity test. The peak photocurrent as a function of the input photon number in each pulse, with (a) ~1 ps width laser as a source and (b) 50 ns width laser as a source, is displayed.
photodiodes are working in their linear regions (4% deviation) up to $10^9$ photons per pulse.

The linearity test of the electronic amplifiers is shown in figure 6. By sending positive or negative electrical pulses (50 ns width, 10 MHz repetition rate) to the amplifiers shown in figure 6(a), we measure the output electrical pulse peak voltage as a function of the input current. The trans-impedance gain is measured to be $22 \text{kV A}^{-1}$ in figure 6(b). The trans-impedance gains for the positive and negative pulses are almost equal, with less than 1% deviation from their linear fits.

4.3. BHD bandwidth

We first characterize the bandwidth of our BHD by sending a CW LO. In this case, the residual signal caused by different temporal responses of the photodiodes can be eliminated by adjusting the loss in one arm (figure 4(a)). Using an RF spectrum analyzer, the frequency spectrum of the BHD electronic output is measured and shown in figure 7. The trace (a) is the electronic noise and is measured when no optical signal is sent to the BHD. We can see that the 3 dB bandwidth of the BHD is 104 MHz. Trace (b) is measured when 6.64 mW CW LO is sent to the BHD. The noise includes electronic noise and shot noise. A noise spike $\sim 8$ dB at low frequency is visible in the plots. This low-frequency noise can be contributed by the imperfect cancellation due to finite CMRR of the relaxation oscillation carried by LO. Another contribution to the low-frequency noise is the $1/f$ noise common to all electric circuits. The latter is seen on both curves.
in figure 7. These very-low-frequency components are filtered out in practical applications of the BHD, and therefore they are not considered by the model.

4.4. Homodyne detector noise measurement in the time domain

In GMCS QKD, each pulse is measured individually. To show that our BHD is suitable for QKD implementations, in the time domain, we first performed HD noise measurement at a pulse repetition rate of 10 MHz and obtained 12 dB shot noise to electronic noise ratio at an LO photon level of $8.2 \times 10^8$. We further increased the repetition rate to 32 MHz and will demonstrate our results here.

With a 16 ns width pulsed LO (5 ns edge time) at a repetition rate of 32 MHz, the total noise of each pulse is obtained by integrating the BHD output voltage over the pulse region. With an oscilloscope sampling rate of 20 G samples s$^{-1}$ and an integration time window of 20 ns in each cycle, each pulse quadrature is obtained from 400 sample points. Noise variance is obtained from 640 pulses. Figure 8 shows the BHD noise variance as a function of the LO photon number per pulse. The measured homodyne detector noise includes: (i) electronic noise $N_{\text{ele}}$, (ii) shot noise and (iii) noise associated with LO fluctuations $N_{\text{LO}}$. The square variances of the shot noise and $N_{\text{LO}}$ depend on the LO power linearly and quadratically, respectively. Note that $\varepsilon_{\text{overlap}}$ is neglected since it is much less than the shot noise when the signal is vacuum.

We distinguish the three types of noise by separating the quadratic LO-dependent ($N_{\text{LO}}$), the linear LO-dependent (shot noise) and LO-independent ($N_{\text{ele}}$) components of the BHD output signal. From the experimental results, the total variance of the BHD output signal (in $V^2$) can be written as $y = 8.0 \times 10^{-20} \cdot I_{\text{LO}}^2 + 7.0 \times 10^{-10} \cdot I_{\text{LO}} + 0.028$, where $I_{\text{LO}}$ is the LO photon number per pulse. The coefficient of determination is 0.999$^8$. The electronic noise $N_{\text{ele}}$ (in shot noise units) can be determined from the ratio between the third and second terms, which is $4.0 \times 10^7/I_{\text{LO}}$. We find that the shot noise to electronic noise ratio is 13 dB at an LO photon level

\[ y = 8.0 \times 10^{-20} \cdot I_{\text{LO}}^2 + 7.0 \times 10^{-10} \cdot I_{\text{LO}} + 0.028 \]

$^8$ If the measured HD noise is represented by $y'(i)$ and the fitting noise is represented by $y(i)$, where $i$ is the index for each LO level, the coefficient of determination is determined by $1 - \left(\sum_i[y'(i) - y(i)]^2/\sum_i[y'(i) - y']^2\right)$. 

New Journal of Physics 13 (2011) 013003 (http://www.njp.org/)
Figure 8. Total noise of the BHD as a function of the LO photon number per pulse.

of $8.5 \times 10^8$ per pulse. Similarly, $N_{LO}$ (in shot noise units) can be determined from the ratio of the first and second terms, which is $1.1 \times 10^{-10} \times I_{LO}$.

As a simple check of the randomness of the noise, we measure the correlation coefficient (CC) between adjacent sampling results. CC is defined as

$$CC = \frac{E(X(n)X(n+1)) - E(X(n))E(X(n+1))}{\sqrt{E(X(n)^2) - E^2(X(n))} \sqrt{E(X(n+1)^2) - E^2(X(n+1))}},$$

where $X(n)$ is the quadrature value of the $n$th pulse, and $E(X)$ represents the expectation value of $X$. At $3.4 \times 10^8$ LO photons per pulse, the CC between consecutive pulses is 0.051, which is comparable with other BHDs reported in [42] (0.04) and [43] (0.07). We can use the CC to determine the upper bound of the excess noise caused by electrical pulse overlap $\varepsilon_{\text{overlap}}$. In GMCS QKD, with the quadrature variance of the coherent state prepared by Alice, denoted by $V$, the excess noise due to the overlap between pulses will be $V \times CC^2 = (V_A + 1) \times CC^2$ (referring to the input). Assuming Alice’s modulation $V_A = 16.9$ [6] and that each pulse has two neighboring pulses, we derive the excess noise caused by BHD pulse overlap to be 0.044 referring to the input.

Assuming that we have a long sequence of pulse quadrature values $X_n$ measured by a BHD, if we consider that $X_n$ is contributed by the $(n-1)$th, $n$th and $(n+1)$th pulses, we can write the pulse quadrature to be $X_n = W_n + a W_{n-1} + a W_{n+1}$ ($a$ is a small number). The CC between consecutive pulses is $CC = E(X_nX_{n+1}) - E(X_n)E(X_{n+1})/\sqrt{E(X_n^2) - E^2(X_n)} \sqrt{E(X_{n+1}^2) - E^2(X_{n+1})}$. If we assume $E(W_n) = 0$, $E(W_nW_{n+2}) = 0$ (only consecutive pulse values have a non-zero expectation), $CC = a$. In GMCS QKD, the variance of Bob’s measurement of individual pulses will be contributed by the variances of its adjacent pulses. With the quadrature modulation of the coherent state prepared by Alice $V$, the excess noise due to the overlap between pulses $\varepsilon_{\text{overlap}}$ referring to the input will be $V \times CC^2$. 

New Journal of Physics 13 (2011) 013003 (http://www.njp.org/)
Figure 9. Noise spectrum at an LO power of 24.6 µW when (a) one photodiode is blocked or (b) both photodiodes are illuminated. Resolution bandwidth = 100 kHz.

4.5. Common mode rejection ratio

To quantify the subtraction capability of the BHD, we measure the generalized CMRR. In the frequency domain, we obtain the CMRR by measuring the spectral power difference at the repetition rate of 32 MHz in two cases: (a) one photodiode is blocked and the other is illuminated, (b) both photodiodes are illuminated. To avoid saturation in case (a), the LO intensity was reduced to a very low level (24.6 µW). The spectral noise for both cases is shown in figure 9. The CMRR is obtained to be 46.0 dB.

4.6. Excess noise evaluation and key rate simulation for a GMCS QKD experiment

Under this RRM, we identify new excess noise sources of a practical BHD. Various sources of excess noise contributed by this BHD are summarized in table 1. Given this practical BHD, we can also optimize operation parameters based on the RRM. In figure 10, we simulate the key rate per pulse as a function of the LO level. The key rate under the RRM will reach the
### Table 1. Excess noise contributions by the BHD (in the shot noise unit).

$I_{LO}$ indicates the LO photon number per pulse.

|                          | Referring to the input | Referring to the output |
|--------------------------|------------------------|-------------------------|
| $N_{ele}$                | $4.0 \times 10^7/\eta GI_{LO}$ | $4.0 \times 10^7/I_{LO}$ |
| $\varepsilon_{overlap}$ | 0.044                  | 0.044 $\times \eta G$   |
| $N_{LO}$                 | $1.1 \times 10^{-10} \cdot I_{LO}/\eta G$ | $1.1 \times 10^{-10} \cdot I_{LO}$ |

Figure 10. Optimization of LO photon number under the RRM. The simulation parameters are from table 1 and [6], $G = 0.758$, $V_A = 16.9$, $\eta = 0.44$, $\varepsilon_A = 0.056$ and $\beta = 0.898$.

maximum at an LO photon number of $1.3 \times 10^8$ per pulse, because there is a tradeoff between $N_{LO}$ (increasing with the LO level) and $N_{ele}$ (decreasing with the LO level relatively to the shot noise).

In figure 11, we simulate the secure key rate of GMCS QKD using this BHD under the RRM by choosing the optimal LO level for each transmission distance. With this high-speed BHD allowing a repetition rate of tens of MHz, the secure key generation rate of GMCS QKD can be improved by one to two orders of magnitude compared to current systems operating at a 500 kHz repetition rate in [15] (with a key rate of 2 kbits s$^{-1}$ over 25 km fiber) and in [22] (with a key rate of 8 kbits s$^{-1}$ over 3 dB loss channel), and at 100 kHz in reference [21] (with a key rate of 5 kbits s$^{-1}$ over 20 km fiber). From the key rate simulation in figure 11, we expect to achieve a few Mbits s$^{-1}$ over a short distance in future GMCS QKD under the RRM.

### 5. Conclusion

In conclusion, we have analyzed the excess noise contributed by a practical BHD and refined the realistic model. The electronic noise $N_{ele}$, the excess noise due to electrical pulse overlap $\varepsilon_{overlap}$...
Table 2. A comparison between high-speed BHDs.

| Wavelength (nm) | 1064 | 800 | 786 | 1550 |
|----------------|------|-----|-----|------|
| Bandwidth (MHz) | ~250 | ~70 | ~82 | ~100 |
| CMRR (dB)       | 45   | 61.8| 42  | 46.0 |
| Shot-noise-to-electronic-noise ratio (dB) | 7.5 | 12 | – | 13 |

Figure 11. QKD secure key rate under the RRM as a function of the transmission distance when the repetition rate is 32 MHz based on the performance of our BHD. The simulation parameters are from table 1 and [6], $V_A = 16.9$, $\eta = 0.44$, $\varepsilon_A = 0.056$, and $\beta = 0.898$. Fiber loss is 0.21 dB km$^{-1}$. For each distance, the LO level is chosen to maximize the secure key rate. No secure key rate can be generated beyond 20 km due to the excess noise.

and the excess noise caused by LO fluctuations in the presence of incomplete subtraction $N_{LO}$ are three excess noise sources for a practical BHD. We remark that in the ORM, $N_{LO}$, $\varepsilon_{overlap}$ and $N_{leak}$ are not characterized. Depending on the actual calibration process of the BHD, Alice and Bob following the ORM may either overestimate or underestimate the intrinsic noise of the BHD itself, which in turn will either introduce potential loopholes or lower the secure key rate. Implementing attacks with current technology to GMCS QKD will be an interesting research direction to explore.

We also developed a high-speed BHD with a 104 MHz bandwidth in the telecommunication wavelength region. A comparison of the specifications between our BHD and other high-speed BHDs is shown in table 2. We achieved a shot-noise-to-electronic-noise ratio of 13 dB in the time domain at a pulse repetition rate of 32 MHz. The BHD has a high CMRR of 46.0 dB. Various sources of excess noise introduced by this practical BHD are identified, and their contributions to the excess noise are evaluated. Based on our experimental characterization of
the BHD, we have shown for the first time that the key generation rate of GMCS QKD experiments using such a BHD is expected to reach a few Mbits s\(^{-1}\) under the RRM. This represents more than an order of magnitude improvement over the key rate achievable with existing GMCS QKD systems.

Acknowledgments

We thank CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, OIT and QuantumWorks for financial support.

References

[1] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N and Grangier P 2003 Nature 421 238
[2] Namiki R and Hirano T 2004 Phys. Rev. Lett. 92 117901
[3] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 Phys. Rev. A 72 050303
[4] Legré M, Zbinden H and Gisin N 2006 Quantum Inf. Comput. 6 326
[5] Heid M and Lütkenhaus N 2007 Phys. Rev. A 76 022313
[6] Qi B, Huang L L, Qian L and Lo H K 2007 Phys. Rev. A 76 052323
[7] Lo H K and Zhao Y 2009 Encyclopedia Complexity Syst. Sci. 8 7265
[8] Hwang W Y 2003 Phys. Rev. Lett. 91 057901
  Lo H K 2004 Proc. IEEE ISIT 2004 p 137
  Lo H K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
  Wang X B 2005 Phys. Rev. Lett. 94 230503
[9] Ma X, Qi B, Zhao Y and Lo H K 2005 Phys. Rev. A 72 012326
  Wang X B 2005 Phys. Rev. A 72 012322
[10] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 Phys. Rev. Lett. 96 070502
[11] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 Proc. IEEE Int. Symp. on Information Theory (IEEE, 2006) pp 2094–8
[12] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[13] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
[14] Grosshans F and Cerf N J 2004 Phys. Rev. Lett. 92 047905
[15] Lodewyck J et al 2007 Phys. Rev. A 76 042305
[16] Navascues M, Grosshans F and Acin A 2006 Phys. Rev. Lett. 97 190502
[17] Garcia-Patron R and Cerf N J 2006 Phys. Rev. Lett. 97 190503
[18] Renner R and Cirac J I 2009 Phys. Rev. Lett. 102 110504
[19] Leverrier A, Karpov E, Grangier P and Cerf N J 2009 New J. Phys. 11 115009
[20] Zhao Y B, Han Z F and Guo G C 2008 Apply current exponential de Finetti theorem to realistic quantum key distribution arXiv:0809.2683v2
[21] Qi B, Huang L L, Chi Y M, Qian L and Lo H K 2008 Oral presentation at CELO/QELS 2008, paper QWE1
  Qi B, Huang L L, Chi Y M, Qian L and Lo H K 2008 SPIE Optics and Photonics (San Diego, CA) pp 10–14
[22] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 New J. Phys. 11 045023
[23] Xuan Q D, Zhang Z and Voss P L 2009 Opt. Express 17 24244
[24] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Opt. Express 16 18790
[25] Zhang Q et al 2009 New J. Phys. 11 045010
[26] Yuen H P and Chan V W S 1983 Opt. Lett. 8 177
[27] Slusher R E, Hollberg L W, Yurke B, Mertz J C and Valley J F 1985 Phys. Rev. Lett. 55 2409

New Journal of Physics 13 (2011) 013003 (http://www.njp.org/)
[28] Breitenbach G, Scheiller S and Mlynek J 1997 *Nature* **387** 471
[29] Vasilyev M, Choi S K, Kumar P and D’Ariano G M 2000 *Phys. Rev. Lett.* **84** 2354
[30] Vasilyev M, Choi S K, Kumar P and D’Ariano G M 1998 *Opt. Lett.* **23** 1393
[31] Smithey D T, Beck M, Raymer M G and Faridani A 1993 *Phys. Rev. Lett.* **70** 1244
[32] Smithey D T, Beck M, Belsley M and Raymer M G 1999 *Phys. Rev. Lett.* **69** 2650
[33] Hansen H, Aichele T, Hettich C, Lodahl P, Lvovsky A I, Mlynek J and Schiller S 2001 *Opt. Lett.* **26** 1430
[34] Huisman S R, Jain N, Babichev S A, Vewinger F, Zhang A N, Youn S H and Lvovsky A I 2009 *Opt. Lett.* **34** 2739
[35] Heurs M, Webb J G, Dunlop A E, Harb C C, Ralph T C and Huntington E H 2010 *Phys. Rev. A* **81** 032325
[36] Shannon C 1948 *Bell Syst. Tech. J.* **27** 379
[37] Bachor H and Ralph T C 2004 *A Guide to Experiment in Quantum Optics* (New York: Wiley)
[38] Lvovsky A I and Raymer M G 2009 *Rev. Mod. Phys.* **81** 299
[39] Appel J, Hoffman D, Figueroa E and Lvovsky A I 2007 *Phys. Rev. A* **75** 035802
[40] Raymer M G, Cooper J, Carmichael H J, Beck M and Smithey D T 1995 *J. Opt. Soc. Am. B* **12** 1801
[41] Häseler H, Moroder T and Lütkenhaus N 2008 *Phys. Rev. A* **77** 032303
[42] Okubo R, Hirano M, Zhang Y and Hirano T 2008 *Opt. Lett.* **33** 1458
[43] Haderka O, Michalek V, Urbas V and Jezek M 2009 *Appl. Opt.* **48** 2884
[44] Zavatta A, Bellini M, Ramazza P L, Marin F and Arecchi F T 2002 *J. Opt. Soc. Am. B* **19** 1189

*New Journal of Physics* **13** (2011) 013003 (http://www.njp.org/)