Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers

Bing Qi, Lei-Lei Huang, Li Qian, and Hoi-Kwong Lo
Center for Quantum Information and Quantum Control (CQIQC), Department of Physics and Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 3G4
(Received 23 September 2007; published 26 November 2007)

In this paper, we present a fully fiber-based one-way quantum-key-distribution (QKD) system implementing the Gaussian-modulated coherent-state (GMCS) protocol. The system employs a double Mach-Zehnder interferometer (MZI) configuration in which the weak quantum signal and the strong local oscillator (LO) go through the same fiber between Alice and Bob, and are separated into two paths inside Bob's terminal. To suppress the LO leakage into the signal path, which is an important contribution to the excess noise, we implemented a scheme combining polarization and frequency multiplexing, achieving an extinction ratio of 70 dB. To further minimize the system excess noise due to phase drift of the double MZI, we propose that, instead of employing phase feedback control, one simply let Alice remap her data by performing a rotation operation. We further present noise analysis both theoretically and experimentally. Our calculation shows that the combined polarization and frequency multiplexing scheme can achieve better stability in practice than the time-multiplexing scheme, because it allows one to use matched fiber lengths for the signal and the LO paths on both sides of the double MZI, greatly reducing the phase instability caused by unmatched fiber lengths. Our experimental noise analysis quantifies the three main contributions to the excess noise, which will be instructive to future studies of the GMCS QKD systems. Finally, we demonstrate, under the "realistic model" in which Eve cannot control the system within Bob's terminal, a secure key rate of 0.3bit/pulse over a 5km fiber link. This key rate is about two orders of magnitude higher than that of a practical Bennett-Brassard 1984 protocol QKD system.

DOI: 10.1103/PhysRevA.76.052323 PACS number(s): 03.67.Dd

I. INTRODUCTION

One important practical application of quantum information is quantum key distribution (QKD), whose unconditional security is based on the fundamental laws of quantum mechanics [1–4]. In principle, any eavesdropping attempts by a third party, Eve, will unavoidably introduce quantum disturbances and be caught by the legitimate users Alice and Bob.

Recently Gaussian-modulated coherent-state (GMCS) QKD protocol has drawn a lot of attention because of its potential high key rates, especially over short distances [5–9]. Compared with single photon QKD protocol [such as the Bennett-Brassard 1984 protocol (BB84) QKD [1]], GMCS QKD protocol has several distinctive advantages: First, the coherent state required in the GMCS QKD protocol can be easily produced by a practical laser source; whereas, a single photon source prescribed by the BB84 QKD is still unavailable. To use a weak coherent source in a single photon QKD system, special techniques, such as decoy states [10–12], are required to improve the secure key rate. Second, the homodyne detectors in the GMCS QKD protocol can be constructed using highly efficient PIN diodes, while the performance of the single photon QKD is limited by the low efficiency of today's single photon detector [13]. Third, in GMCS QKD, information is encoded on continuous variables. More than one bit of information could be transmitted by one pulse and thus yields a high key rate.

Recent interest has also been sparked by the fact that [5], with a "reverse reconciliation" protocol, GMCS QKD can tolerate high channel loss (>3 dB) on the condition that the excess noise (the noise above vacuum noise) is not too high (<0.5). We remark that the security analysis given by [5] is applicable to individual attacks only. The security of GMCS QKD protocol under the most general attack is still under investigation [9].

Despite its many advantages, the implementation of the GMCS QKD over a practical distance in fiber remains challenging, and only one other experimental demonstration has been reported so far [8]. The major experimental challenge lies in the reduction of the excess noise in a practical system. Here we study the performance of a fully fiber-based one-way GMCS QKD system over a 5 km span. The purpose of this study is not only to show that GMCS QKD can be operated over a practical distance, but also to investigate various sources of excess noise in a real system, and to offer practical solutions to reduce or eliminate some of the noise sources. Our experiment with a 5 km fiber demonstrates a secure rate of 0.3 bit/pulse under a "realistic model" in which we assume that Eve cannot control Bob's system. This key rate is about two orders of magnitude higher than that of a practical BB84 QKD system.

In early GMCS QKD experiments [5,6], to eliminate the leakage from the strong local oscillator to the weak quantum signal, the signal and the local oscillator were transmitted through separated channels. With this configuration, to achieve a low phase noise, the transmission distance could not be longer than a few meters. In [7], the authors studied the feasibility of a "go and return" configuration in GMCS QKD. Unfortunately, such a configuration is intrinsically vulnerable to "Trojan Horse" attack and its performance is compromised by the Rayleigh backscattering of the strong

local oscillator. A full implementation of the GMCS QKD over a practical distance has only been demonstrated very recently [8]. In [8], to reduce excess noise due to the leakage of the local oscillator, Mach-Zehnder interferometers (MZIs) with largely unbalanced path lengths were employed to separate the signal and the leakage in time domain (time multiplexing). However, it is quite challenging to stabilize a MZI with a large length unbalance in practice. In contrast, we introduce a polarization-frequency-multiplexing scheme to effectively suppress the leakage of the local oscillator with balanced MZI. Our theoretical analysis shows that the combined polarization- and frequency- multiplexing scheme can achieve better stability in practice than the time-multiplexing scheme, because it allows one to use matched fiber lengths for the signal and the local oscillator paths on both sides of the double MZI, greatly reducing the phase instability caused by unmatched fiber lengths.

This paper is organized as follows: Sec. II is a brief review of GMCS QKD protocol. In Sec. III, we discuss our experimental setup and summarize the experimental results. In Sec. IV, we present a detailed noise analysis and discuss noise control in a practical system. Section V is a brief conclusion.

II. GAUSSIAN-MODULATED COHERENT-STATE (GMCS) QKD PROTOCOL

The basic scheme of the GMCS QKD protocol is as follows [5]: Alice draws two random numbers X_A and P_A from a set of Gaussian random numbers (with a mean of zero and a variance of $V_A N_0$) and sends a coherent state $|X_A+iP_A\rangle$ to Bob. Here $N_0=1/4$ denotes the shot-noise variance [14]. In this paper, all variances are in shot-noise units. Bob randomly chooses to measure either the amplitude quadrature (X) or phase quadrature (P) with a phase modulator and a homodyne detector. After performing his measurement, Bob informs Alice which quadrature he actually measures for each pulse through an authenticated public channel. Alice drops the irrelevant data and only keeps the quadrature that Bob has measured. At this stage, Alice shares a set of correlated Gaussian variables (called the "raw key") with Bob. Alice and Bob then publicly compare a random sample of their raw key to evaluate the transmission efficiency of the quantum channel and the excess noise of the QKD system. Based on the above parameters, they can evaluate the mutual information I_{AB} and I_{BE}.

Assuming Alice's modulation variance is V_A, the channel efficiency is G, and the total efficiency of Bob's device (including the optical losses and the efficiency of the homodyne detector) is η, I_{AB} and I_{BE} are determined by [5]

$$I_{AB}=\frac{1}{2}\log_2[(V+\chi)/(1+\chi)], \tag{1}$$

$$I_{BE}=\frac{1}{2}\log_2[(\eta G)^2(V+\chi)(V^{-1}+\chi)]. \tag{2}$$

Here, $V=V_A+1$ is the quadrature variance of the coherent state prepared by Alice. χ is the equivalent noise measured at the input, which can be separated into "vacuum noise" $\chi_{vac}=(1-\eta G)/\eta G$ (noise associated with the channel loss and detection efficiency of Bob's system) and "excess noise" ε (noise due to the imperfections in a nonideal QKD system) as follows:

$$\chi=\frac{1-\eta G}{\eta G}+\varepsilon. \tag{3}$$

Assuming a reverse reconciliation algorithm efficiency of β, the secure key rate is then given by [5]

$$\Delta I=\beta I_{AB}-I_{BE}. \tag{4}$$

Note, in Eq. (2), we assume that losses and noise in Bob's system can be controlled by the eavesdropper Eve. In practice, it may be reasonable to assume that Eve cannot control devices inside Bob's system. Under this "realistic model" [5], noise inside and outside of Bob's system are treated differently: while part of the excess noise (e.g., due to imperfections outside of Bob's system) might originate from Eve's attack, the noise contributed by Bob's devices is an intrinsic parameter of the QKD system of which Eve has no control. Thus it is useful to write the total excess noise ε as

$$\varepsilon=\varepsilon_A+\frac{N_{\mathrm{Bob}}}{\eta G}, \tag{5}$$

where ε_A denotes noise contribution from outside of Bob's system, and N_{Bob} denotes noise generated within Bob's system (measured at the output). ε_A and N_{Bob} can be determined separately.

From Eqs. (3) and (5), the equivalent input noise is

$$\chi=\frac{1-\eta G}{\eta G}+\varepsilon_A+\frac{N_{Bob}}{\eta G}. \tag{6}$$

Bob's quadrature variance is given by $V_B=\eta G(V+\chi)$, while the conditional variance under the "realistic model" is

$$V_{B|E}=\frac{\eta}{1-G+G(\varepsilon_A+V^{-1})}+(1-\eta)+N_{\mathrm{Bob}}. \tag{7}$$

From Eqs. (5)–(7), the mutual information I_{BE} is

$$I_{BE}=\frac{1}{2}\log_2\left[\frac{\eta G V_A+1+\eta G\varepsilon}{\eta/(1-G+G\varepsilon_A+GV^{-1})+1-\eta+N_{\mathrm{Bob}}}\right]. \tag{8}$$

Again, the secure key rate is determined by Eq. (4). Note that Eq. (8) is equivalent to Eq. (3) in [8].

III. GMCS-QKD EXPERIMENTAL SETUP AND EXPERIMENTAL RESULTS

In this section, we first present our experimental setup, followed by discussions on the technical challenges. Finally, we present our QKD experimental results.

A. Experimental setup

The schematic of our experimental setup is shown in Fig. 1. The laser source is a 1550 nm continuous-wave fiber laser

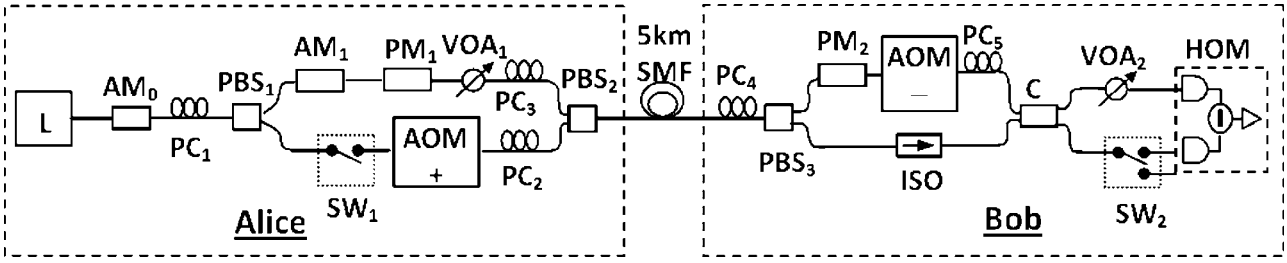

FIG. 1. The optical layout of our GMCS QKD system. L: 1550 nm CW fiber laser; PC_{1-5}: polarization controllers; PBS_{1-3}: polarization beam splitters or combiners; AM_{0-1}: amplitude modulators; PM_{1-2}: phase modulators; SW_{1-2}: optical switches; AOM+ (AOM−): upshift (downshift) acousto-optic modulator; VOA_{1-2}: variable optical attenuators; ISO: isolator; C: fiber coupler; HOM: homodyne detector.

(NP Photonics). Alice uses a $LiNbO_3$ amplitude modulator (AM_0) to generate 200 ns laser pulses at a repetition rate of 100 KHz. She then prepares a coherent state $|X_A+iP_A\rangle$ with the second amplitude modulator (AM_1) and a phase modulator (PM_1). AM_1 and PM_1 are driven by arbitrary waveform generators (AWG), which contain random amplitude and phase data produced from $\{X_A, P_A\}$. Alice sends Bob the quantum signal together with a strong local oscillator (LO) as the phase reference through a 5-km telecommunication fiber. On Bob's side, he randomly chooses to measure either X or P with his phase modulator (PM_2) and a homodyne detector. The phase modulator PM_2 is located in the reference path of Bob's MZI and is driven by a third AWG, which contains a binary random file for choosing X or P. The homodyne detector is constructed by a pair of photodiodes and a low noise charge sensitive amplifier, similar to the one described in Ref. [15]. Note, to reduce the noise due to multiple reflections of LO in Bob's system, a fiber isolator has been placed in the signal arm of Bob's MZI. The outputs of the homodyne detector are sampled by a 12-bit data acquisition card (NI, PCI-6115) at a sampling rate of 10 MS/s.

There are two significant technical challenges in this double MZI scheme: First, the leakage (LE) of the strong LO (typically 10^8 photons/pulse) into the signal path has to be reduced effectively, particularly because the quantum signal is very weak (typically less than 100 photons/pulse). Ideally there should be no LE. The LO and the signal (Sig) are supposed to go through different arms in Bob's interferometer. For a nonideal system in our experiment, however, we expect that there will be some leakage LE to the same arm as the signal (see Fig. 2). If LE is in the same spatiotemporal mode and the same polarization state as the LO, it will interfere with LO and contribute to the excess noise. Second, the phase fluctuation introduced by the MZI, which is one of the major contributions to excess noise, has to be minimized. We discuss these issues in the next two subsections.

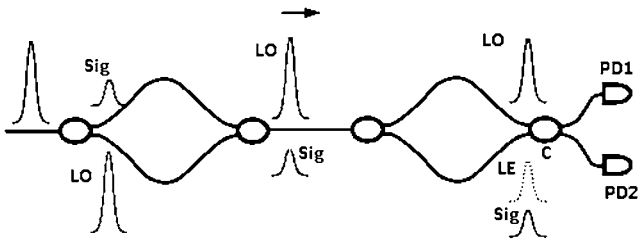

FIG. 2. The leakage of the local oscillator in the double Mach-Zehnder interferometer scheme: Sig—quantum signal; LO—local oscillator; LE—leakage of LO.

B. Reduce the leakage of the local oscillator

In a report by Lodewyck *et al.* [8], to reduce excess noise due to the leakage, LE is separated from LO in the time domain by using MZIs with largely unbalanced path lengths. Since LE and LO arrive at the fiber coupler (C in Fig. 1) at different times, they interfere with each other only weakly. Obviously, to minimize the overlap between LE and LO in the time domain, the required time delay should be much larger than the width of the laser pulse. This corresponds to a large length unbalance in the MZI (in Ref. [8], the length unbalance of MZI is 80 m). However, it is quite challenging to stabilize a MZI with such a large length unbalance in a practical system. The phase fluctuation of the unbalanced MZI may result in a dramatic increase in the excess noise.

In contrast, we employ polarization multiplexing combined with frequency multiplexing to minimize the leakage of the LO. Alice uses orthogonal polarization states for the quantum signal and the LO via a polarization beam splitter (PBS_1 in Fig. 1). On Bob's side, another polarization beam splitter (PBS_3 in Fig. 1) is used to separate the LO from the signal. This polarization-multiplexing scheme is expected to yield an extinction ratio of about 30 dB due to the imperfections of the PBSs. To further suppress the excess noise due to the leakage, we have introduced a frequency-multiplexing technique: a pair of acousto-optic modulators (AOM+ and AOM− in Fig. 1) are used to upshift and downshift the frequency of the LO by 55 MHz. As a result, the majority of LE can be filtered out since it has a different frequency from LO. Although in principle the phase of the LO will also be shifted by the AOM [16], since the driving frequency of the AOM (55 MHz) is much smaller than the laser frequency (200 THz), the phase noise contributed by the AOM is negligible.

The overall equivalent extinction ratio of this scheme has been determined experimentally to be around 70 dB, and the excess noise due to the leakage is about 0.02 (measured at the output; see details in Sec. IV).

C. Reduce phase fluctuation of the MZI

In both the GMCS QKD system and the phase coding BB84 QKD system, ideally, the phase difference between the

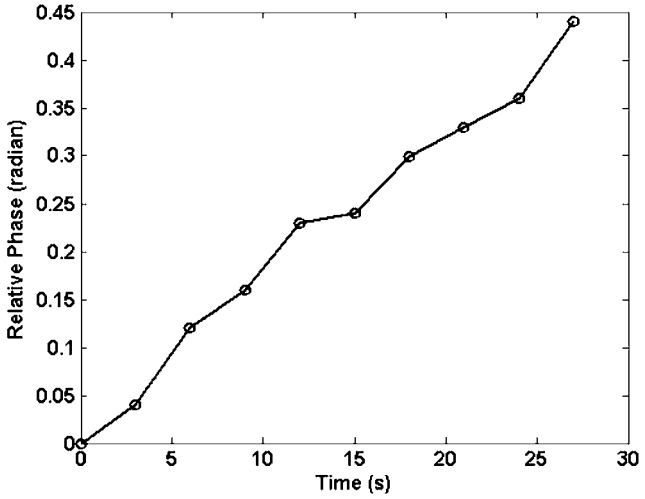

FIG. 3. The phase drift observed during QKD experiment without active phase stabilization. Each point in the curve is estimated from the QKD data in 40 ms. (Here, we assume the phase change in 40 ms is small enough to be neglected.) The total phase drift is about 0.016/s, or 6.4×10^{-4} in 40 ms.

quantum signal and the LO (phase reference) should be solely dependent on the phase information encoded by Alice. However, in practice, the zero point of the phase difference ϕ_0 (the phase difference when Alice encodes phase 0) will drift with time. The GMCS QKD protocol is more sensitive to this phase drift than the BB84 QKD protocol in the sense that a small phase drift would lower the secure key rate dramatically [17].

Under normal conditions, ϕ_0 drifts with time slowly. It is reasonable to assume that ϕ_0 is constant during one frame of QKD transmission (40 ms in our experiment). As shown in Fig. 3, the change of ϕ_0 measured during the QKD is 0.016/s, or 6.4×10^{-4} in 40 ms. The corresponding contribution to excess noise (with a modulation variance of 16.9) is about 7×10^{-6}, which is negligible. Alice and Bob can estimate the value of ϕ_0 in this transmission period by comparing a subset of their QKD data.

In the phase coding BB84 QKD system, knowing the value of ϕ_0 itself will not help Alice and Bob to lower the quantum bit error rate (QBER). To control the QBER due to the phase drift, a phase recalibration process is essential: Alice and Bob have to perform a phase feedback control to compensate this phase drift before they start the key transmission [18].

In contrast, in GMCS QKD, we propose a simpler way to remove the excess noise due to the phase drift ϕ_0: once Alice and Bob know the value of ϕ_0, instead of performing feedback phase control, Alice can simply modify her data to incorporate this phase drift. Specifically, during the classical communication stage, Bob announces a randomly selected subset of his measurement results. Alice can estimate ϕ_0 and other system parameters from Bob's measurement results and her original data. Then she maps her data $\{X_A, P_A\}$ into $\{X'_A, P'_A\}$ by performing

$$X'_A = X_A \cos\phi_0 + P_A \sin\phi_0, \tag{9}$$

$$P'_A = -X_A \sin\phi_0 + P_A \cos\phi_0. \tag{10}$$

Alice and Bob can produce a secure key from $\{X'_A, P'_A\}$ and $\{X_B, P_B\}$. The security analysis of GMCS QKD still holds.

The above approach reduces the excess noise due to the slow drift of ϕ_0, but it does not solve the problem of fast variations in ϕ_0 resulting from instabilities in the MZIs. This instability is worse when the path lengths of the MZIs are not balanced. Fortunately, because we employ the combined polarization and frequency multiplexing instead of time multiplexing, we can use balanced MZIs. To further stabilize the MZIs, we carefully balance their path lengths and place each of them into an enclosure to minimize environmental noise.

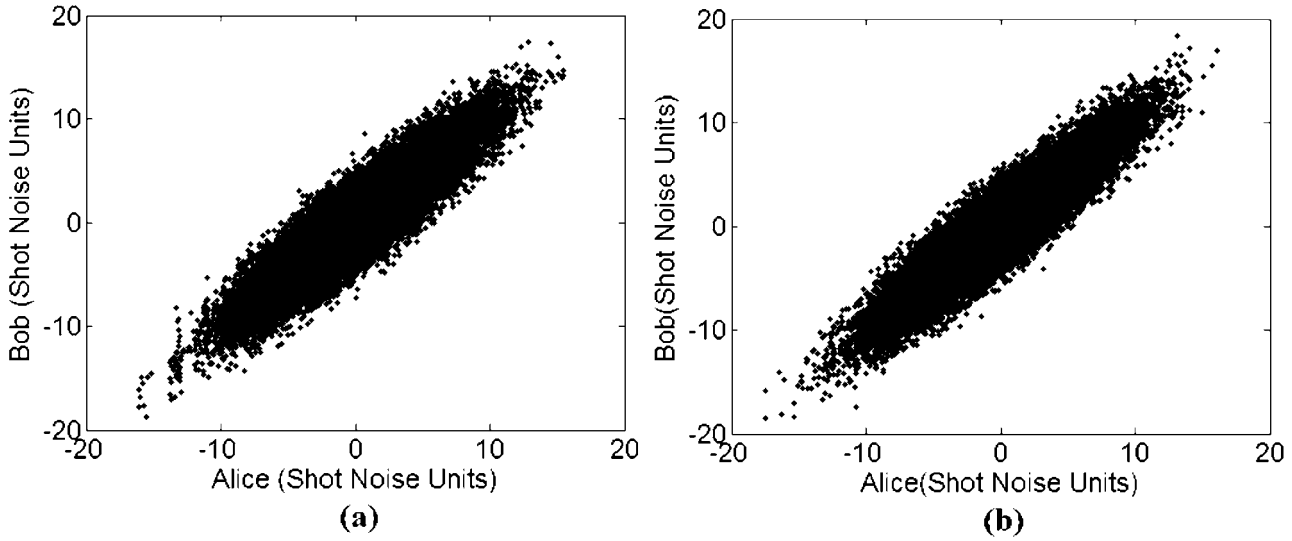

FIG. 4. (a) QKD experimental results (40 000 points). The equivalent input noise has been determined experimentally to be $\chi=2.25$, which includes vacuum noise $\chi_{vac}=2.00$ and excess noise $\varepsilon=0.25$. (b) Simulation results: assuming vacuum noise $\chi_{vac}=2.00$ and excess noise $\varepsilon=0$.

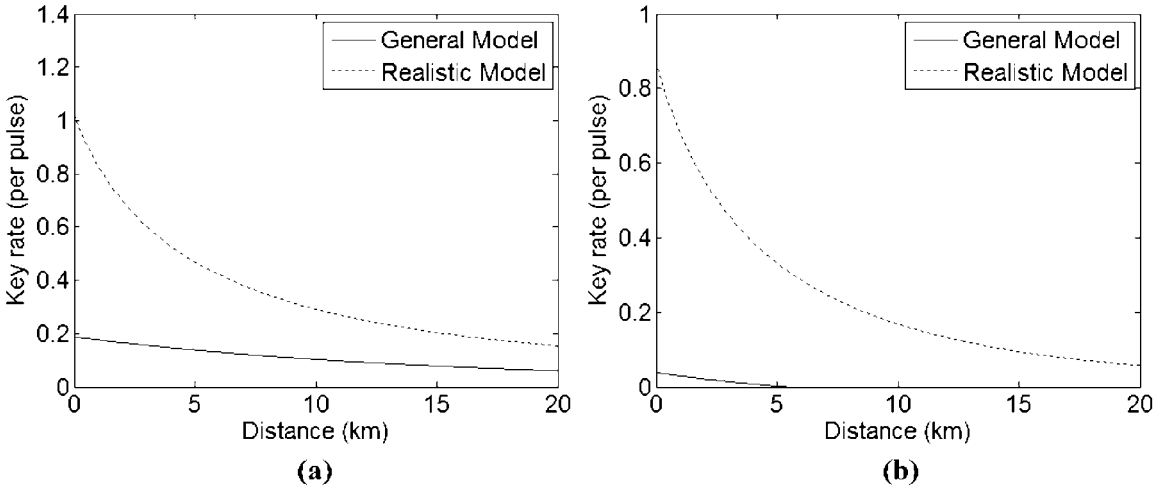

FIG. 5. Simulation results (a) $\beta=1$ and (b) $\beta=0.898$ [8].

D. Experimental results

We perform the QKD experiment with a strong LO (8×10^7photons/pulse) and a signal of modulation variance of 16.9. Data are transmitted by frames. Each frame contains 4000 points (Gaussian random numbers). Among them, Bob performs X quadrature measurements on 1980 points and P quadrature measurements on 2020 points. The same random patterns are used repeatedly in our experiment. The experimental results are shown in Fig. 4(a). The equivalent input noise has been determined experimentally to be $\chi=2.25$. For comparison, Fig. 4(b) shows the simulation results under the assumption of no excess noise.

The channel efficiency G and the total efficiency of Bob's device η have been calibrated carefully to be $G=0.758$ and $\eta=0.44$ (including optical loss in Bob's system 0.61 and the efficiency of the homodyne detector 0.72) [19]. Using Eqs. (1), (2), and (4) the secure key rate under the general model has been calculated to be 0 if we assume $\beta=0.898$ [8] or 0.13 bit/pulse if we assume $\beta=1$.

To estimate the secure key rate under the "realistic model," we need to determine ε, ε_A, and N_{Bob}. From $\chi=2.25$, $G=0.758$, and $\eta=0.44$, we can determine $\varepsilon=0.25$ by using Eq. (3). Experimentally, as will be discussed in detail in Sec. IV A later, we have estimated $\varepsilon_A=0.056$. From Eq. (5), we can calculate $N_{\mathrm{Bob}}=0.065$ (see the details in Sec. IV). Using Eqs. (1), (8), and (4), the secure key rate under the realistic model has been calculated to be either 0.30 ($\beta=0.898$) or 0.43 ($\beta=1$). Table I summarizes our experimental results.

Using the parameters in Table I, we have performed numerical simulations under both the general model and the realistic model. Here we assume the quantum channel is telecommunication fiber with a loss of 0.21 dB/km. Figure 5(a) shows the result with a perfect reverse reconciliation algorithm ($\beta=1$). Figure 5(b) shows the result with a practical reverse reconciliation algorithm ($\beta=0.898$). As shown in Fig. 5, under the realistic model, the achievable secure key rate is significantly higher than that of a practical BB84 QKD.

IV. EXPERIMENTAL INVESTIGATION AND ANALYSIS ON EXCESS NOISE

To estimate the secure key rate under the realistic model, we have to separate ε into ε_A and N_{Bob} [see Eq. (8)]. In this section, we will discuss how to estimate ε_A and N_{Bob} in a practical GMCS QKD system and other practical issues.

A. Estimate ε_A

ε_A is the excess noise due to imperfections outside of Bob's system, which includes the phase noise of the laser source, imperfect amplitude and phase modulations, the phase noise of the interferometer, etc. To reduce the phase noise of MZIs, we carefully balance their path lengths and enclose them to minimize environmental noise. To reduce the excess noise due to the imperfect modulations, both the amplitude modulator and the phase modulator have been calibrated carefully before the QKD experiment. Nevertheless, Alice and Bob have to measure ε_A experimentally in order to apply the realistic model.

Following [6], we assume that ε_A is proportional to the modulation variance V_A and can be described by $\varepsilon_A=V_A\delta$. We have designed a procedure to determine the proportionality constant δ, by operating the system with a large modulation variance ($V_A\approx40\,000$) and a weak LO (10^5 photons/pulse, to reduce its leakage). Under this con-

TABLE I. QKD parameters and results (e: experimental result; c: calculated result).

V_A	G	η	χ	ε	ε_A	N_{Bob}	$R^{gen}_{\beta=1}$	$R^{gen}_{\beta=0.898}$	$R^{rea}_{\beta=1}$	$R^{rea}_{\beta=0.898}$
16.9(e)	0.758(e)	0.44(e)	2.25(e)	0.25(c)	0.056(e)	0.065(c)	0.13(c)	0(c)	0.43(c)	0.30(c)

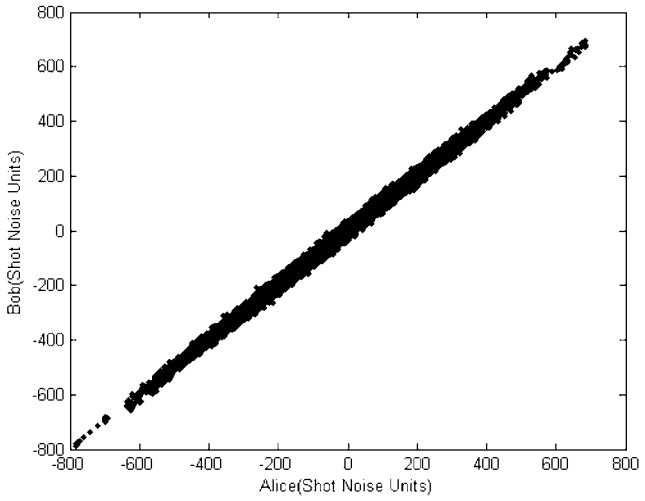

FIG. 6. Determine δ by using a high modulation variance $V_A \approx 40\,000$ and a weak LO (10^5 photons per pulse). The result is $\delta = 0.0033$ (40 000 points).

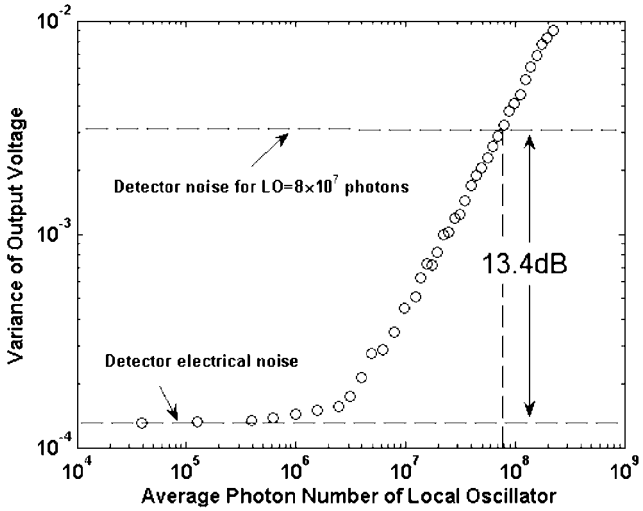

FIG. 7. Noise of the balanced homodyne detector. The electrical noise is independent of the photon number of the local oscillator while the shot noise is directly proportional to the photon number of the local oscillator. With a local oscillator of 8×10^7 photons/pulse, the electrical noise (the variance observed at a low photon number of the local oscillator) is about 13.4 dB below the shot noise.

dition, all other excess noises in Eq. (6) except ε_A are negligible, i.e., $\chi \simeq V_A\delta$. We can determine δ by normalizing the observed equivalent input noise χ to the modulation variance V_A.

Figure 6 shows the experimental results. The measured δ is 0.0033 (in another test with $V_A \approx 80\,000$, the measured δ is 0.0032). Therefore, for a modulation variance of $V_A = 16.9$, the expected excess noise component $\varepsilon_A = 0.056$.

B. Estimate N_{Bob}

In Secs. III D and IV A, we experimentally determined $\chi = 2.25$, $G = 0.758$, $\eta = 0.44$, and $\varepsilon_A = 0.056$. From these parameters, we can obtain $\varepsilon = 0.25$ by using Eq. (3), and obtain $N_{\mathrm{Bob}} = 0.065$ by using Eq. (5).

In this section, we will discuss the two main sources of N_{Bob}, namely, the electrical noise of the homodyne detector (N_{el}) and the noise associated with the leakage of LO (N_{leak}).

Since the electrical noise of the homodyne detector scales with its bandwidth, intuitively, a narrow bandwidth should be used to minimize the electrical noise. However, a narrow bandwidth would result in a wide pulse in time domain, which in turn reduces the achievable repetition rate of the QKD system. Therefore, a trade-off has to be made between the speed and the electrical noise.

We remark that this constraint on the noise and the speed of the homodyne detector could be relaxed by adopting the "dual-detector method" [20]: the legitimate receiver randomly uses either a fast but noisy detector or a quiet but slow detector to measure the incoming quantum signals. The measurement results from the quiet detector can be used to upper bound the eavesdropper's information, while the measurement results from the fast detector are used to generate a secure key.

Nevertheless, in our current setup, the bandwidth of the homodyne detector is about 1 MHz. The electrical noise is about 13.4 dB below the shot noise (with a LO of 8×10^7 photons/pulse), as shown in Fig. 7. The corresponding N_{el} is therefore 0.045.

The analysis of the excess noise associated with the leakage of LO is more complicated. Here, we estimate the order of magnitude of N_{leak} in both the time-multiplexing scheme and the polarization-frequency-multiplexing scheme by treating the leakage LE as a classical electromagnetic wave with a Gaussian shape [21]. More rigorous results could be acquired by solving this problem quantum mechanically.

Case 1. N_{leak} in the time-multiplexing scheme. In this scheme, MZIs with large unbalanced paths are employed to introduce a time delay between the LO and its leakage LE, as shown in Fig. 8. We denote the average photon number of the leakage as $\langle n_{le}\rangle$. Note that only part of LE—the part that is in the same spatiotemporal mode as the LO—will interfere with LO and contribute to the excess noise. We denote the average photon number of this "effective" leakage as $\langle n_{le}^e\rangle$.

The effective leakage $\langle n_{le}^e\rangle$ can be estimated from

$$\langle n_{le}^e\rangle = \alpha\langle n_{le}\rangle, \tag{11}$$

where α is the overlapping factor between LO and LE.

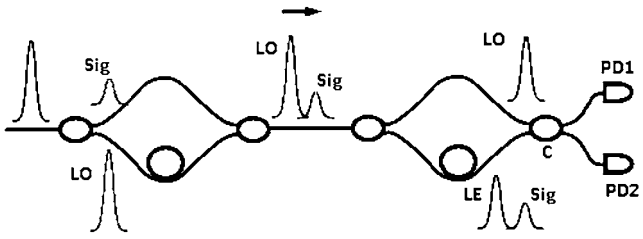

FIG. 8. The time-multiplexing scheme: Sig—quantum signal; LO—local oscillator; LE-—leakage of LO. Note Sig and LO arrive at the fiber coupler (c) at the same time, while LE has been delayed.

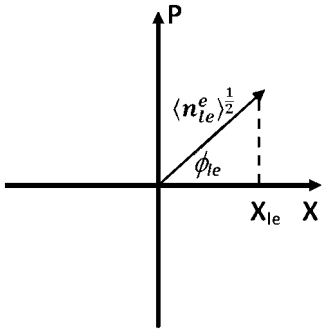

FIG. 9. The contribution of the effective leakage on X quadrature measurement.

Assuming a Gaussian pulse shape, the normalized electrical fields of LO and LE can be described by

$$E_{lo} = E_0 \exp\left(-\frac{(t-\Delta_t/2)^2}{2\sigma_t^2}\right)\exp(-i\omega_0 t), \tag{12}$$

$$E_{le} = E_0 \exp\left(-\frac{(t+\Delta_t/2)^2}{2\sigma_t^2}\right)\exp[-i(\omega_0 t+\phi_{le})]. \tag{13}$$

Here the normalizing factor is $E_0^2=\frac{1}{\sqrt{\pi}\sigma_t}$, Δ_t is the time delay between LO and LE, ϕ_{le} is the phase difference between LO and LE, and σ_t is related to the full width at half maximum (FWHM) σ_{FW} by $\sigma_t=\frac{\sigma_{FW}}{2\sqrt{\ln 2}}$.

The overlapping factor α can be calculated from

$$\alpha = \left|\int_{-\infty}^{\infty} E_{lo}^* E_{le} dt\right|^2 = \left[E_0^2\int_{-\infty}^{\infty}\exp\left(-\frac{t^2}{\sigma_t^2}\right)dt\right]^2 \exp\left(-\frac{\Delta_t^2}{2\sigma_t^2}\right)$$
$$= \exp\left(-\frac{\Delta_t^2}{2\sigma_t^2}\right). \tag{14}$$

Here we use the normalization relation $E_0^2\int_{-\infty}^{\infty}\exp\left(-\frac{t^2}{\sigma_t^2}\right)dt=1$.

If Bob chooses to measure the X quadrature, the contribution from the leakage is (see Fig. 9)

$$X_{le} = \sqrt{\langle n_{le}^e\rangle}\cos\phi_{le}. \tag{15}$$

Because of the large length unbalance required in this scheme, we assume that the relative phase ϕ_{le} randomly and rapidly changes in the range of $[0,2\pi]$. The corresponding excess noise (in shot-noise units) is

$$N_{leak} = 4\langle X_{le}^2\rangle = 4\langle n_{le}^e\rangle\langle(\cos\phi_{le})^2\rangle = 2\langle n_{le}^e\rangle. \tag{16}$$

Using Eqs. (11), (14), and (16), N_{leak} can be estimated by

$$N_{leak} = 2\langle n_{le}\rangle\exp\left(-\frac{\Delta_t^2}{2\sigma_t^2}\right). \tag{17}$$

From another point of view, the required time delay for a given N_{leak} can be estimated by

$$\Delta_t = \sqrt{2\ln\left(\frac{2\langle n_{le}\rangle}{N_{leak}}\right)}\sigma_t. \tag{18}$$

If a simple time-multiplexing scheme is adopted, and a 3 dB coupler is used in Bob's MZI, the leakage LE will be on the same order as LO. Assuming $\langle n_{le}\rangle=10^8$, $\sigma_t=60$ ns (corresponds to $\sigma_{FW}=100$ ns), to suppress the excess noise N_{leak} to below 0.02 (this is the N_{leak} observed in our polarization-frequency-multiplexing setup), the required time delay calculated from Eq. (18) is about 406 ns, which corresponds to a 81 m fiber length difference in the MZI.

If time multiplexing and polarization multiplexing are combined to suppress the leakage, then the leakage LE will be three orders of magnitude lower than LO (assuming a 30 dB polarization extinction ratio). Using $\langle n_{le}\rangle=10^5$, $\sigma_t=60$ ns, and $N_{leak}=0.02$, the required time delay is about 340 ns, which corresponds to a 68m fiber length difference in MZI.

Based on the above calculations, we can see that although the excess noise due to leakage can be effectively reduced by employing this time multiplexing scheme, the required length unbalance is quite large. In practice, it is quite challenging to stabilize a MZI with such a large length unbalance. Without phase stabilization, the phase fluctuation of the unbalanced MZI will result in a dramatic increase in the excess noise.

Case 2. N_{leak} in the polarization-frequency-multiplexing scheme. If the laser pulse has an ideal Gaussian-shaped spectrum, the calculations in case 1 can be easily extended into frequency domain. Similar to Eq. (14), in the spectral domain, the overlapping factor α can be estimated from

$$\alpha = \exp\left(-\frac{\Delta_\nu^2}{2\sigma_\nu^2}\right), \tag{19}$$

where Δ_ν is the frequency difference between LO and LE, while σ_ν is the spectral width of the laser pulse.

For a 100 ns (FWHM) transform limited Gaussian pulse, its spectral width (FWHM) is about 4.4 MHz, or $\sigma_\nu \approx 2.64$ MHz. With a Δ_ν of 55 MHz, from Eq. (19), we would expect an extremely small α ($<10^{-90}$), which means the leakage contribution to the excess noise is negligible. Though in practice, the spectrum of a practical laser source does not have an ideal Gaussian shape: far from the peak wavelength, the spectral power density approaches a constant noise floor. The overlapping factor α is mainly determined by this noise floor.

Here, we estimate the order of magnitude of α from experimental data directly. Since we design MZIs with carefully balanced path lengths, in the period of one frame of transmission (40 ms), the phase difference between LO and LE has a constant average value $\phi_{le}^{(0)}$ with a small fluctuation term $\Delta\phi_{le}$,

$$\phi_{le} = \phi_{le}^{(0)} + \Delta\phi_{le}. \tag{20}$$

Consequently, the contributions of LE to Bob's measurement results are (see Fig. 9)

$$X_{le} = \sqrt{\langle n_{le}^e\rangle}\cos\phi_{le} = X_{le}^{(0)} + \Delta X_{le}, \tag{21}$$

$$P_{le} = \sqrt{\langle n_{le}^e\rangle}\sin\phi_{le} = P_{le}^{(0)} + \Delta P_{le}, \tag{22}$$

where

$$X_{le}^{(0)} = \sqrt{\langle n_{le}^e\rangle}\cos\phi_{le}^{(0)}, \tag{23}$$

$$P_{le}^{(0)} = \sqrt{\langle n_{le}^{e} \rangle} \sin \phi_{le}^{(0)}, \tag{24}$$

$$\Delta X_{le} \approx -\sqrt{\langle n_{le}^{e} \rangle} (\sin \phi_{le}^{(0)}) \Delta \phi_{le}, \tag{25}$$

$$\Delta P_{le} \approx \sqrt{\langle n_{le}^{e} \rangle} (\cos \phi_{le}^{(0)}) \Delta \phi_{le}. \tag{26}$$

Since $X_{le}^{(0)}$ and $P_{le}^{(0)}$ are constant in each frame, Bob can determine their values from his experimental results and remove their contributions by simply shifting his data. So $X_{le}^{(0)}$ and $P_{le}^{(0)}$ will not contribute to excess noise. In our QKD experiment, during the postprocessing stage, Bob calculates the dc component of his measurement results for each transmission frame, then simply subtracts this dc component from his original data.

In addition, the effective leakage $\langle n_{le}^{e} \rangle$ and $\phi_{le}^{(0)}$ can be estimated from experimentally obtained $X_{le}^{(0)}$ and $P_{le}^{(0)}$ as follows:

$$\langle n_{le}^{e} \rangle = (X_{le}^{(0)})^2 + (P_{le}^{(0)})^2, \tag{27}$$

$$\phi_{le}^{(0)} = \arctan\left(\frac{P_{le}^{(0)}}{X_{le}^{(0)}} \right). \tag{28}$$

During the QKD experiment, the average photon number of LO is around 8×10^7, while the $\langle n_{le}^{e} \rangle$ has been determined using Eq. (27) to be 6, indicating an overall equivalent extinction ratio of ~ 70 dB.

From Eqs. (25) and (26), the excess noise due to leakage N_{leak} is proportional to $\langle n_{le}^{e} \rangle$ and can be described by

$$N_{leak} = \langle n_{le}^{e} \rangle \gamma. \tag{29}$$

Let us estimate γ from experimental data: N_{Bob} has been determined to be 0.065 (Sec. IV B) and N_{el} has been determined to be 0.045 (Sec. IV B). Thus N_{leak} is about 0.02. Using $\langle n_{le}^{e} \rangle \approx 6$, we obtain γ to be on the order of 0.003. In Sec. IV A, we described ε_A as $V_A \delta$ and determined δ to be 0.0033. Since both γ and δ are associated with the phase noise of MZI's and the laser source, we expect these quantities to have the same order of magnitude, and indeed they do.

One major advantage of the polarization-frequency-multiplexing scheme is that balanced MZIs can be employed. Under the same conditions, the phase noise of balanced MZIs should be much lower than MZIs with large path length imbalance. The resulting improvements are twofold: first, a small phase fluctuation between LO and signal corresponds to a small excess noise ε_A. Second, a small phase fluctuation between LO and LE reduces the excess noise due to the leakage.

C. Other practical issues with GMCS QKD

As shown in Table I, under the realistic model, the achievable secure key rate of our system is significantly higher than that of a practical BB84 QKD over short distances. However, to achieve such a high key rate, the excess noises in the system need to be controlled effectively and the system parameters need to be determined with high accuracies.

Note in the BB84 QKD system with a single photon source, Eve's information is upper bounded by the QBER, which can be estimated by Alice and Bob from their QKD results directly. In practice, a moderate error on determining QBER will not change the secure key rate significantly [22].

However, there is a major challenge in GMCS QKD: to calculate the secure key rate under the realistic model, in addition to the total transmission efficiency (which is the product of G, η, and the gain of Bob's electrical amplifier) and the equivalent input noise χ (which can be determined from Bob's measurement results), Alice and Bob have to develop techniques to monitor other system parameters V_A, G, η, and ε_A with a high degree of accuracy in real time.

For example, among the total equivalent input noise $\chi = 2.25$, the contribution of vacuum noise (2.0) is much higher than that of the excess noise (0.25) [23]. To acquire a tight bound on ε_A from the experimentally measured equivalent input noise χ [see Eq. (6)], Bob has to determine the total efficiency ηG with an extremely high accuracy. Using Eq. (6) and parameters in Table I to achieve an accuracy of 0.01 in ε_A estimation, the required accuracy on ηG estimation is 0.1%.

To estimate ε_A accurately without referring to ηG, we have designed a separated calibration process (see Sec. IV A). Strictly speaking, this cannot be applied to the QKD experiment directly, since Eve may attack this calibration process and QKD process differently. We need to develop special techniques to estimate each system parameter accurately without compromising the security of the QKD system.

V. CONCLUSION

Gaussian-modulated coherent-state (GMCS) quantum key distribution (QKD) protocol has been proposed to achieve an efficient secure key distribution with standard telecommunication components. The performance of a practical GMCS QKD system is mainly determined by its excess noise. In this paper, we present a fully fiber GMCS-QKD system based on double Mach-Zehnder interferometer (MZI) scheme and build up a corresponding theoretical model for noise analysis. To effectively reduce the excess noise due to the leakage from the strong local oscillator to the weak quantum signal, we introduce a polarization-frequency-multiplexing scheme. To minimize the excess noise due to the phase drift of the MZI, instead of using phase feedback control, we propose that the sender simply remap her data by performing a rotating operation. The experiment with a 5 km fiber demonstrates a secure key rate of 0.3bit/pulse under the realistic model. This secure key rate is about two orders of magnitude higher than that of a practical BB84 QKD system.

We analyzed and quantified various sources of excess noise in a practical GMCS QKD system, and offered practical solutions to reduce or eliminate some of the noise sources. We believe, in order to achieve a high secure key rate in the real world, special techniques for estimating system parameters with high accuracies in real time (without compromising the security of the QKD system) are in demand. High speed GMCS QKD is also an important research direction for the future.

ACKNOWLEDGMENTS

We thank Ryan Bolen and Justin Chan for their work on the homodyne detector and Alexander Lvovsky for helpful discussions. Financial support from NSERC, CIFAR, CRC Program, CFI, OIT, MITACS, PREA, CIPI, and Quantum-Works are gratefully acknowledged. This research was supported by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and by the province of Ontario through MEDT.

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

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

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

[4] D. Mayers, J. ACM **48**, 351 (2001); H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); E. Biham *et al.*, *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC'00)* (ACM Press, New York, 2000), pp. 715–724; P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[5] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[6] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303(R) (2005).

[7] M. Legre, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **6**, 326 (2006).

[8] J. Lodewyck *et al.*, Phys. Rev. A **76**, 042305 (2007).

[9] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004); M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[10] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, in Proceedings of IEEE ISIT 2004 (IEEE, New York, 2004), p. 137; H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005);X.-B. Wang, *ibid.* **94**, 230503 (2005).

[11] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[12] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[13] We remark that new types of single photon detectors (SPDs), such as superconductor SPDs, could have high efficiency at telecommunication wavelength.

[14] R. Loudon, *The Quantum Theory of Light(e3)* (Oxford University Press, New York, 2003).

[15] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek, and S. Schiller, Opt. Lett. **26**, 1714 (2001).

[16] B. Qi, L.-L. Huang, H.-K. Lo, and L. Qian, Opt. Express **14**, 4264 (2006).

[17] Assume that the phase drift of MZI $\phi_0 \ll 1$. In the phase coding BB84 QKD, the resulting QBER is roughly equal to ϕ_0^2. In practice, a 1% error rate is acceptable (the secure bound on QBER is about 20% for two-way classical communication [D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003); H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002); K. S. Ranade and G. Alber, J. Phys. A **39**, 1701 (2006)] and corresponds to $\phi_0=0.1$). In GMCS QKD, Bob's measurement result of X quadrature becomes $X'=X\cos\phi_0+P\sin\phi_0$. If $\phi_0 \ll 1$ and its change during the time of one frame transmission (40 ms in our experiment) is negligible, the excess noise contributed by the phase drift can be estimated by $\langle (X'-X)^2\rangle \approx \langle P^2\rangle \phi_0^2 = V_A\phi_0^2$. With a modulation variance of $V_A=20$, a 0.1 phase drift will result in an excess noise of 0.2. Note that the secure bound (of excess noise) for a reverse reconciliation protocol is around 0.5 [5]. An excess noise of 0.2 would lower the secure key rate dramatically. In our system, numerical simulation shows that the secure key rate would drop from 0.3 bit/pulse to 0.1 bit/pulse.

[18] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, Opt. Lett. **30**, 2632 (2005).

[19] The channel efficiency G was calibrated by using a strong laser pulse and a power meter. To calibrate the total efficiency of Bob's device η, a strong laser was fed into Bob's system, while the output of the photodiode was measured with a calibrated transimpedance amplifier.

[20] B. Qi, Y. Zhao, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. A **75**, 052304 (2007).

[21] In this semiclassical picture, a coherent laser pulse can be treated as a classical electromagnetic wave plus the vacuum noise. Since we are estimating the excess noise (the noise above vacuum noise) here, we can treat the leakage LE classically.

[22] In BB84 QKD with a perfect single photon source, the secure key rate is given by $R=\frac{1}{2}Q_1[1-f(e_1)H_2(e_1)-H_2(e_1)]$. Here Q_1 is the overall gain. e_1 is the QBER. $f(x)$ is the bidirectional error correction efficiency and $H_2(x)$ is the binary entropy function. Assuming $e_1=3\%$ and $f(e_1)=1.22$, a 10% error on determining e_1 will result in a 3% change of the secure key rate, which is tolerable. In decoy QKD, the equation for calculating the secure key rate is more complicated. Nevertheless, as we showed in Ref. [11] moderate errors on determining system parameters are acceptable.

[23] This is illustrated in Fig. 4. Note the similarity between Fig. 4(a) (experimental results) and Fig. 4(b) (simulation result under the assumption of no excess noise).