High-rate continuous-variable measurement-device-independent quantum key distribution

Adnan A.E. Hajomer,* Huy Q. Nguyen, and Tobias Gehring **

Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

**aaeha@dtu.dk, ** tobias.gehring@fysik.dtu.dk*

Abstract: We report the first continuous-variable measurement-device-independent QKD system generating secret keys at 5 MBaud without frequency and phase locking. We achieve this using a relay structure based on a polarization 90-degree optical hybrid and well-designed DSP.

1. Introduction

Quantum key distribution(QKD) is a secure means of distributing cryptographic keys based on the laws of quantum physics [1]. While QKD offers information-theoretic security in theory, the physical devices have practical imperfections which can result in side channels that can be exploited by an eavesdropper. For instance, various attacks on detectors have been reported as these are the most vulnerable part of QKD systems [2].

To cope with these side channels, measurement-device-independent QKD (MDI-QKD) has been proposed [3,4]. Here, the two communicating users (Alice and Bob) are connected by an untrusted third party, which performs a Bell-state measurement (BSM). This measurement acts as a correlator between Alice and Bob but does not reveal their symbol values. Thereby, MDI-QKD can eliminate all detector side-channel attacks.

A continuous variable (CV) MDI-QKD was first proposed [5], independently reproposed [6], and experimentally demonstrated [5, 7] achieving a higher secret key rate (per channel use) compared with its discrete variable counterpart. These demonstrations, however, required a complex frequency and optical phase locking system to perform CV-BSM, making the practical realization of CV-MDI-QKD quite challenging. Furthermore, both experiments used a quantum symbol rate of a few hundred kHz, limiting the achievable secret key rate.

Here, we report the first experimental CV-MDI-QKD system operating at a symbol rate of 5 Mbaud and without frequency and optical phase locking. Leveraging the concept of the polarization-based 90-degree hybrid [9], we develop a new relay structure, that enables the realization of CV-BSM without phase locking. Simultaneously, our system uses a continuous-wave laser with digital pulse shaping and digital time synchronization, and therefore, it does not require additional amplitude modulation for pulse carving or a delay line for time synchronization. Combining these technologies with quadrature remapping [7], we realize a practical and simple CV-MDI-QKD system, achieving a secret key rate of 0.12 bit per relay use, or correspondingly 600 kbit per second, over 2 dB loss corresponding to 10 km optical fiber channel (at the loss of 0.2 dB/km).

2. Basic concept and system

In the prepare-and-measure (PM) scheme of CV-MDI QKD protocol, Alice and Bob prepare coherent states $|\alpha\rangle$ and $|\beta\rangle$, respectively, whose amplitudes α and β are randomly drawn from a Gaussian distribution with zero mean and sufficiently large modulation variance in each quadrature. Then, Alice and Bob send their coherent states to the intermediate station (Relay) through two independent quantum channels, where a CV-BSM is performed by mixing the incoming signals at a balanced beam splitter followed by double homodyne detection. The output of the measurement (γ) is then sent to Alice and Bob via a classical public channel. With the knowledge of γ, either Alice or Bob infers the variable of the other party. Finally, Alice and Bob perform classical processing including parameter estimation, information reconciliation, and privacy amplification.

Figure 1 shows the schematic of our CV-MDI-QKD system. It consists of an optical layout and digital signal processing (DSP) pipeline for waveform generation and quantum symbols recovery. To prepare random coherent states, Alice and Bob drew random numbers at a rate of 5 MBaud from Gaussian distributions obtained by transforming the output of a vacuum-based quantum random number generator (QRNG) [8], forming the complex amplitude α and β of their coherent states. The quantum symbols were then upsampled to 1 GSample/s and pulse-shaped using a root-raised cosine filter with a roll-off of 0.2. To avoid the low-frequency noise of the transmitter,

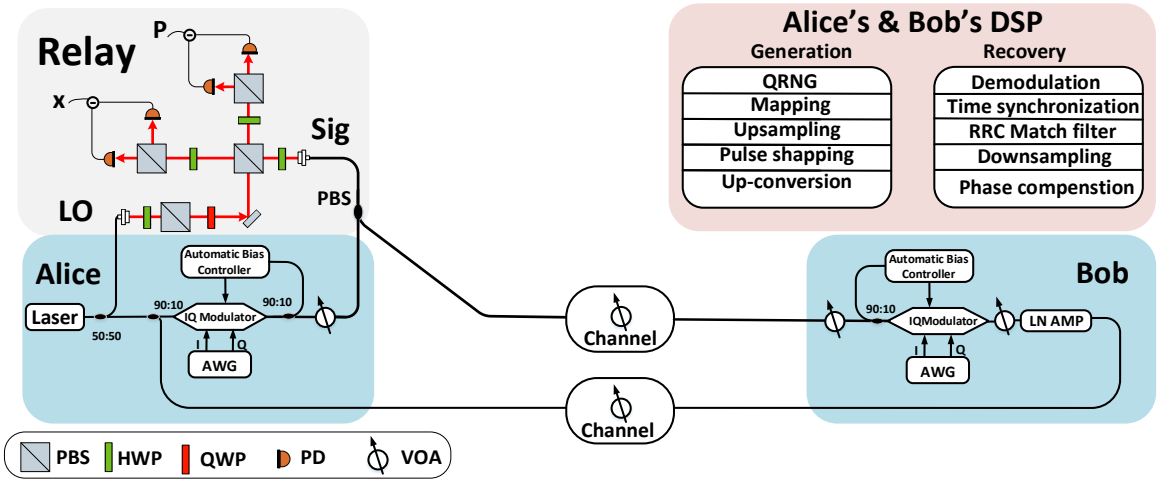

Fig. 1. CV-MDI-QKD system experimental setup and DPS pipeline. AWG: arbitrary waveform generator; PBS: polarization beam splitter; HWP: Half-wave plate; QWP: quarter-wave plate; PD: photodiode; VOA: variable optical attenuator.

the quantum signal was digitally up-converted to $\omega/2\pi$ =5 MHz, i.e. multiplied with $\cos(\omega t)$, for double sideband modulation. Finally, Alice and Bob uploaded their waveforms to dual-channel arbitrary waveform generators (AWGs) each with 16-bit resolution and a sampling rate of 1 GSample/s.

The transmitters of Alice and Bob were built from polarization maintaining fiber components. At Alice's station, a 1550 nm continuous-wave laser with a linewidth of $\approx$ 100 Hz was shared with the relay, as the optimal configuration of the CV-MDI protocol is asymmetric with the relay being at Alice [5]. To avoid frequency locking, a portion of Alice's laser of 1.9 mW was also sent to Bob through an independent fiber channel emulated by a variable optical attenuator (VOA) with a loss of 2 dB (corresponding to a 10 km fiber channel) and then amplified at Bob's station using a low noise amplifier (LN AMP). In each transmitter, an in-phase and quadrature (IQ) modulator driven by the AWG was used to prepare the ensemble of coherent states. The DC biases to these IQ modulators were controlled using commercial automatic bias controllers. To adjust the modulation variance of the coherent states two VOAs were used at Alice's and Bob's sides. At Bob's side the VOA was also used to simulate the fiber channel to the relay. As the relay is situated at Alice's station our implementation thus only requires a commonly available fiber pair.

At the relay, the incoming beams from Alice and Bob were overlapped at a fiber-based polarization beamsplitter (PBS). The signal was then free-space coupled into the polarization-based 90-degree hybrid, where the two quadratures (X and P) were detected simultaneously. This is possible because the local oscillator (LO) was prepared in circular polarization by means of a quarter wave-plate (QWP), while the signal was linearly polarized [9]. The hybrid was built from free-space bulk components with negligible losses to achieve high-efficiency CV-BSM. Two custom-made balanced detectors each with a bandwidth of 10 MHz and quantum efficiency of 99% were used. Considering the insertion loss and the visibility of the interference fringes, the total detection efficiency of the relay was 94 %. The output of the balanced detector was then digitized at a sampling rate of 1 GSample/s using an analog-to-digital converter (ADC), which was clock synchronized to Alice's and Bob's AWG using a 10 MHz external reference. The measurement time was divided into frames, each with 10^7 samples. Furthermore, the one-time shot noise calibration technique was used for system calibration [10].

After the relay broadcasting the output of CV-BSM, Alice's and Bob's DSP algorithms for quantum symbols recovery were applied. The steps are shown in Fig. 1. First, the relay output was downconverted to the baseband and low pass filtered. Temporal synchronization was achieved through the cross-correlation between Alice's and Bob's transmitted samples and the relay output. In contrast to one-way CVQKD, the propagation delay was compensated on the transmitted samples since each quantum channel had a different propagation delay. The synchronized samples were then matched filtered and downsampled to symbols. As one laser was shared between the communicating parties and the relay, Alice's and Bob's signals experienced a slow phase drift with respect to the LO. To compensate for this phase drift, Alice and Bob rotated their symbols to maximize the correlation as: $\hat{\alpha} = \arg\max_{\theta_1} Cov(\alpha\ \exp(j\theta_1), \gamma)$, $\hat{\beta} = \arg\max_{\theta_2} Cov(\beta\ \exp(j\theta_2), \gamma)$, where $Cov(.)$ denotes the covariance. Finally, Alice and Bob performed displacement operations [5] to correlate their symbols according to the CV-BSM output.

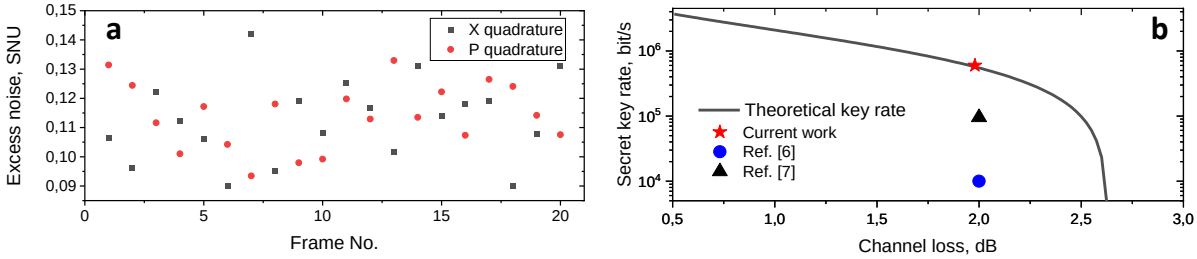

Fig. 2. Experimental results demonstrating our CV-MDI-QKD system performance. (a) Excess noise variance (in shot-noise units). (b) Experimental key rates and numerical simulations.

Table 1. Experimental parameters

symbol rate	V_{Alice}	V_{Bob}	ξ	η	τ_{Bob}
5 Mbaud	36 SNU	36 SNU	0.11 SNU	0.94 %	2 dB

3. Results

Table 1 summarizes the relevant parameters in our experiment. Alice and Bob prepared an ensemble of 4×10^6 coherent states, characterized by the modulation variance of V_{Alice} and V_{Bob}. As the modulation variance directly affects the excess noise ξ, our system operates at a modulation variance of 36 shot-noise units (SNU) to reduce the excess noise. Fig. 2(a) depicts the measured excess noise variance for 20 frames each with 2×10^5 symbols. The average excess noise of X and P quadratures is 0.11 SNU. The corresponding secret key rate is evaluated in the asymptotic regime according to [5]. Fig. 2(b) shows the secret key rate of the numerical simulation and experimental results. The black solid curve shows the numerical simulations calculated from experimental parameters. Considering the information reconciliation of 97% efficiency and Bob's channel loss τ_{Bob} of 2 dB, we achieved a secret key fraction of 0.12 bit per relay use which corresponds to 600 kbit secret key per second.

4. Discussion

In this work, we demonstrated the first simple and practical CV-MDI-QKD system, which is free of frequency and optical phase locking and operates at a 5 Mbaud symbol rate. This was enabled by means of a new relay structure leveraging the concept of a polarization-based 90-degree optical hybrid and DSP for CV-BSM. Compared to the previous demonstration [5, 7], our system improves the secret key rate by one order of magnitude, which boosts the secret key rate to 0.6 Mbps. This is six times higher than the record secret key bit per second [7]. However, the symbols rate can be further increased using a broadband balanced detector. Our demonstration could pave the way toward the practical adoption of CV-MDI-QKD to build high-rate quantum networks.

Acknowledgments This work was supported by the European Union's Horizon 2020 research and innovation programs through CiViQ (grant agreement no. 820466) and OPENQKD (grant agreement no. 857156) and from the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142).

References

1. S. Pirandola, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012 (2020).
2. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604 (2014).
3. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
4. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
5. S. Pirandola, *et al.*, "High-rate measurement-device-independent quantum cryptography," Nat. Photonics **9**, 397–402 (2015).
6. Z. Li, *et al.*, "Continuous-variable measurement-device-independent quantum key distribution," Phys. Rev. A **8**9, 052301 (2014).
7. Y. Tian *et al.*, "Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber," Optica **9**(5), 492–500 (2022).
8. T. Gehring, *et al.*, " Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side information," Nat. Commun. **12**, 1–11 (2021).
9. L. G. Kazovsky, "Phase- and polarization-diversity coherent optical techniques," J. Lightw. Technol., **7**(2), 279–292 (1989).
10. Y. Zhang *et al.*, "One-time shot-noise unit calibration method for continuous-variable quantum key distribution," Phys. Rev. Applied **13**(2), 024058 (2020).