Experimental Demonstration of High Key Rate and Low Complexity CVQKD System with Local Local Oscillator

Shengjun Ren, Shuai Yang, Adrian Wonfor, Richard Penty and Ian White
Centre for photonic systems, University of Cambridge, CB3 0FA, UK
sr734@cam.ac.uk

Abstract: We experimentally demonstrate a 250MHz repetition rate Gaussian-modulated coherent-state CVQKD with local local oscillator implementation which is capable of realizing record 14.2 Mbps key generation in the asymptotic regime over 15km of optical fiber.
OCIS codes: (270.5565) Quantum communications; (270.5568) Quantum cryptography

1. Introduction

Quantum key distribution (QKD) allows unconditional information security between two authenticated users (Alice and Bob) [1]. Continuous Variable QKD (CVQKD) modulates both quadratures of the electromagnetic field with a random continuous data which can be extracted with coherent detection techniques [2] and be post-processed to distil secure keys. The Gaussian-modulated coherent-state (GMCS) protocol has been developed to offer security against malicious eavesdropping attacks [3]. More importantly, CVQKD systems have the benefit of compatibility with commercial off-the-shelf (COTS) telecom components. However, several obstacles have been identified in practical CVQKD systems, especially those associated with the transmitted local oscillator (TLO). These include insufficient LO intensity and the security weakness of being able to manipulate the LO [4]. As result, a second independent narrow linewidth laser of the same center wavelength, located at Bob to realize a fully protected local LO (LLO), has been proposed in [5-7], removing the requirement of LO transmission from Alice. In order to achieve a common phase reference between the two lasers and ensure secure key distillation, Alice shares low intensity reference pulses with Bob to recover the phase drift during transmission and uses a phase rotation scheme to correct for the quadrature measurements [8]. Researchers have proposed various LLO schemes and enhanced the performance up to 100MHz repetition rate [7]. To date the highest secure key rate to be predicted using the GMCS protocol is an asymptotic 3.14Mbps over 25km optical fiber at 50MHz repetition rate [9].

In this paper, we experimentally demonstrate a 250MHz repetition rate GMCS LLO-CVQKD implementation which, allows a record estimated asymptotic secure key rate of 14.2Mbps over a 15km optical fiber. The signal contamination from adjacent reference pulses is tracked and mitigated by real-time shot-noise calibration. We propose a new 'combined-optimization' technique based upon a comprehensive system-level noise model analysis, in which optimum modulation variance and reference pulse intensity are chosen to enhance the achievable key rate. Further, compared with the delay-line setup [9], the suppression of phase noise achieved by the short pulse interval enables a simple time-multiplexing signal-reference modulation and single heterodyne detection scheme with fewer components and less complex configuration. The system repetition rate and the intensity of reference pulses can easily be adjusted within a computer without any setup modification.

2. Experimental setup

Fig. 1 shows the experimental setup of our GMCS-LLO-CVQKD system realized using COTS optical communication components. In a commercial system it is clear that two laser sources will be used in Alice and Bob, however, for convenience in this laboratory demonstration we use a single laser (center wavelength of 1549.73nm and a linewidth Δv of 50 kHz) both in the transmitter and local oscillator in the receiver. The transmission distance of the CVQKD signals is significantly greater than the coherence length of the source laser, therefore the noise performance of the system is equivalent to one with a second laser at Bob, whose wavelength is controlled by a feedback loop. We note that the system has also been tested with a second laser at Bob and the experimental results are equivalent to those presented here. The output of the source laser is split by a 50:50 beam splitter (BS) and each arm contains an optical isolator to prevent back reflections. At Alice, a $LiNbO_3$ intensity modulator (AM1, iXblue) with high extinction ratio is used to transform the continuous wave (CW) light into 0.2ns pulses at a rate of 500MHz. This pulse train is modulated as interleaved signal and reference pulse trains, one delayed by 2ns relative to the other. In this setup, the signal amplitude is modulated by a second $LiNbO_3$ intensity modulator (AM2) and the phase is modulated by a cascaded pair of electro-optic phase modulators (PM1,PM2, iXbule). All modulation and synchronization signals originate from an arbitrary-waveform generator (AWG, Tektronix) and are then amplified by wideband RF amplifiers (AMP, iXblue). These amplified signals are then shifted to the appropriate bias voltage levels by bias-tees. In GMCS, the phase needs to be modulated between 0 to 2π . As the high modulation voltage swing required to provide a 0 - 2π

modulation range [10] is not available from the available broadband amplifiers, two PMs (PM1 and PM2) are cascaded to provide the required phase modulation. The amplitude and phase of the signal pulses are randomly modulated with a two-dimensional zero-centered Gaussian distribution with an adjustable modulation variance $V_A N_o$ where N_o is the shot noise variance. The variance $V_A N_o$ is tuned by a variable optical attenuator (VOA). Reference pulses are modulated with a fixed intensity $E_{ref}^2 N_o$ and a constant zero phase. This enables the phase sharing scheme described in [8] to be used to correct for fast phase drift through reference pulses. A 50:50 BS placed at the output of Alice is used to monitor and optimize the V_A in real time. After that, the signal and reference pulses propagate through a 15km standard single mode fiber spool (3.0dB loss).

At Bob, the LO with a power of 13.5dBm provides a large shot to electronics noise ratio of 10. A polarization controller (PC) is applied to compensate the polarization drift during transmission and from environmental perturbations. In order to measure both X and P quadrature through heterodyne detection, both signal and reference pulses are fed into a 90-degree optical hybrid (Kylia) and detected by two shot-noise limited balanced homodyne detectors (BHD, Thorlabs). An oscilloscope (Keysight, DOSO254A) with a bandwidth of 2.5GHz is used to collect the quadrature information and the results are sent to a computer for $\sqrt{N_o}$ normalization. The real-time shot noise is determined by measuring the variance between the signal and reference pulses. Consequently, the effect of the photon leakage can be tracked and corrected correspondingly. Such a system configuration has significant advantages of low complexity and adjustment-flexibility.

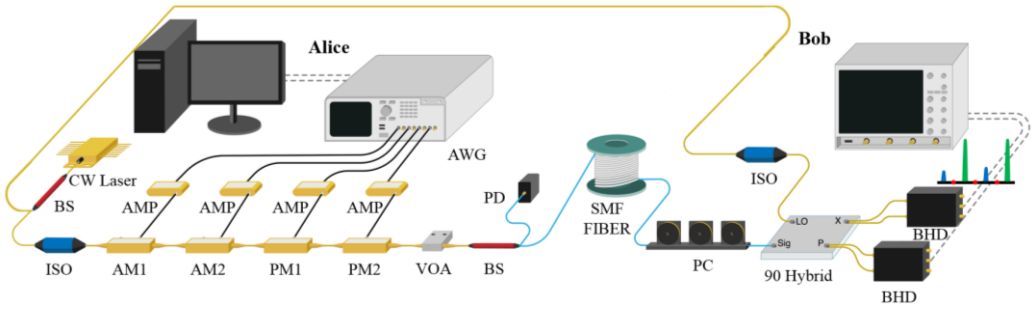

Fig. 1 Experiment setup. The SMF fiber length is 15km and all devices are listed above.

3. Noise model analysis

Optimal performance requires a comprehensive noise analysis, especially for the excess noise that arises from the experimental imperfections and noise introduced by Eve's manipulation. All values are normalized to N_o. One of the most critical contributions to the excess noise in the LLO-CVQKD system is the phase noise, which contains two main contributions [11]: 1. the phase estimation error noise ξ_{esti} originating from the quantum uncertainty of the reference pulse at the detector as $\xi_{esti} = V_A(\chi_{tot} + 1)/E_{Ref}^2$ where χ_{tot} is the total noise; and 2. the drift noise ξ_{drift} resulting from the relative phase drift between the lasers at Alice and Bob; this can be calculated as $\xi_{drift} = 2\pi V_A (\Delta v_A + \Delta v_B)/f_{rep}$, where $\Delta v_A, \Delta v_B$ are the lasers' linewidths and f_{rep}=250 MHz is the data repetition rate. In addition to the phase noise, several other excess noise sources also cause a degradation in system performance. Firstly, the modulation noise ξ_{AM} due to the amplitude leakage on each optical pulses caused by amplitude modulator's (AM) finite dynamic range, which is approximated as $\xi_{AM} = E_{ref}^2 10^{-d_{AM}/10}$ where d_{AM} is the AM extinction ratio. Secondly, the ADC quantization noise appears in Bob's output measurements and its value is given by $\xi_{ADC} \geq E_{Ref}^2/(12 * 2^n)$. Other noise contributions, in our experimental setup, are deemed small enough to be included within the original system excess noise ξ_{ori}=0.01. The overall excess noise model can be described as: $\xi_e = \xi_{ori} + \xi_{esti} + \xi_{drift} + \xi_{AM} + \xi_{ADC}$.

4. Experimental results

From the above expressions, we find both V_A and E_{Ref}^2 critically influence the excess noise, and hence the system performance. Therefore, instead of optimizing system parameters individually, the combined-optimization method evaluates V_A and E_{Ref}^2 together and to validate our proposed method by experiment. The other parameters are identical to the values used in our experiment, shown in Fig. 2(a). Following the secret key rate derivation with heterodyne detection in [12], the theoretical key rate performance for varying V_A and E_{Ref}^2 is compared in Fig. 2(b). The peak key rate of 14.6Mbps occurs in simulation when V_A=3.1 and E_{Ref}^2=622. Any other parameter value choice away from the peak point reduces the key rate performance. In order to validate the theoretical optimization method, the simulation and experimental data for a range of reference pulse intensities with 15km optical fiber at V_A=3.1 are shown in Fig. 2(c). The excess noise (grey circles) measured using a block size of 10^7 data is a good fit to the derived noise model (blue line). The minimum excess noise in simulation is 0.0802 at E_{Ref}^2/V_A=221.

Distance L	15km
Block size	10^7
Quantum efficiency η	0.49
Electornics noise v_{el}	0.1
Attenunation factor α	0.2dB/km
Reconciliation efficiency β	96%

(a)

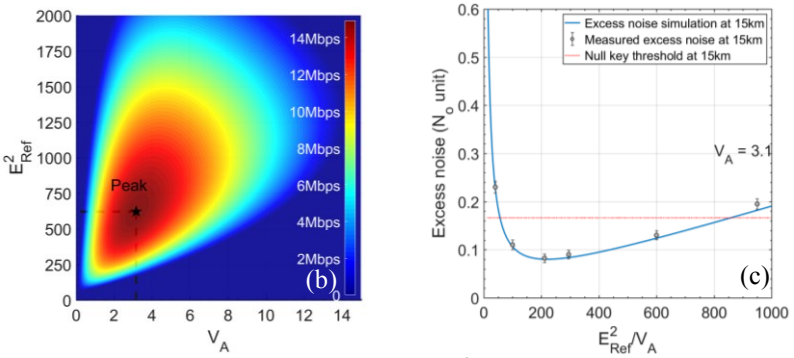

Fig 2. (a) Experimental paramters (b)The secret key rate analysis under different V_A = [0 15] and E^2_{Ref} = [0 2000] at L=15km. (b) Experimental validation of noise model and optimzation method by collecting excess noise at different E^2_{Ref} with fixed optimal V_A = 3.1 and L =15km.

Experimental characterization and secure key rate estimation are shown in Fig.3. Here the excess noise measurements (red stars) are shown in Fig. 3(a), where each block has a size of 10^7 data and the measurement follows the standard procedures mentioned in [5,9]. ξ_e^{Fib}, the average excess noise when a 15km fiber is used was 0.0823 (red dashed line) in an asymptotic regime. According to the excess noise, thresholds shown as the solid lines in Fig. 3(a), a stable secret key rate generation in the asymptotic regime of greater than 10Mbps is predicted to be achieved. Fig. 3 (b) presents the simulation predictions of secret key rate with respect to transmission distances, together with that estimated from our experiment. The asymptotic theoretical key rate of our optimized model (blue dashed line) and excess noise thresholds (solid lines) shown in Fig. 3(a) are plotted respectively. For our system, the key rate is experimentally investigated under both a 15km optical fiber where a key rate of 14.2Mbps (red star) is predicted. For a 3dB equivalent attenuation loss an excess noise of ξ_e^{Att} = 0.0806 is achieved and a key rate of 14.5Mbps (grey circle) predicted. Considering the environmental perturbation, it is reasonable that the attenuation-only case gives a slightly better result. Although the performance is degraded if finite-size effects are considered, we have verified the feasibility of implementing a 10Mbps, low complexity LLO-CVQKD system over metropolitan area length scales.

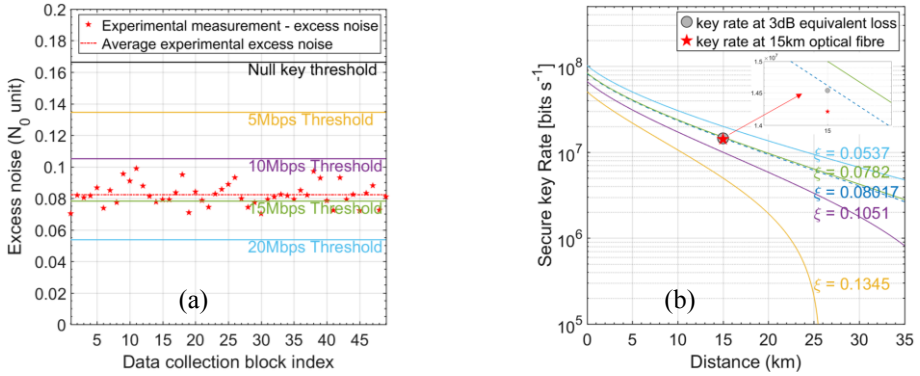

Fig 3(a) Experimental measurement of excess noise in the LLO CVQKD system.(b) the serect key rate performance as a function of transmission distance at simulation onbtained excess noise (dahsed line) and corresponding excess noise threshold (solid lines). Other parameters are: $V_A = 3.1$, $E^2_{Ref} = 622$, $\eta = 0.49$, $v_{el} = 0.1$, and $\beta = 0.96$. 3dB equivalent loss is achieved by VOA.

5. Conclusion

In this paper, a 250MHz, low complexity LLO-CVQKD system is proposed and a record asymptotic key rate of 14.2Mbpsover 15km optical fiber has been predicted. The real-time shot noise calibration and combined-optimization scheme are integrated through noise model analysis to achieve a stable low excess noise performance. It is expected that a higher repetition rate can be achieved or the transmission distance extended to 65km before the link fails. The excess noise also can be additionally reduced at the expense of additional system complexity.

The authors would like to acknowledge support from the Quantum Communication Hub through EPSRC UK National Quantum Technology Programme (UKNQTP) fund EP/M013472/1.

6. References

[1] H.-K. Lo et al., Nature Photon. 8(8), 595–604 (2014)
[2] F. Grosshans et al., Nature 421, 238–241 (2003).
[3] L. Leverrier et al., Phys. Rev. Lett. 110, 030502(2013)
[4] X.C. Ma et al., Phys. Rev. A 89, 032310. (2014)
[5] Q. Bing et al., Phys. Rev. X 5, 041009 (2015)
[6] S. Daniel et al., Phys. Rev. X 5, 041010(2015)
[7] H. Duan et al., Opt. Letters 40, 3695-3968 (2015)
[8] S.Ren et al., J. Opt. Soc. Am. B 36, B7-B15 (2019)
[9] T. Wang et al., Opt. Exp. 26, 2794-2806 (2018)
[10] photonics.ixblue.com
[11] A, Maire and R, Alleaume, Phys.Rev.A 95, 0.12316 (2017)
[12] S. Fossier et al., J. Phys. B: At. Mol. Opt. Phys. 42 114014(2009)