Optical Wireless Communication Conference

Real-Time Bob in Continuous Variable Quantum Key Distribution over Free-Space Optical Link

João dos Reis Frazão[1*], Vincent van Vliet[1], Sjoerd van der Heide[1], Menno van den Hout[1], Alina Tomeeva[3] , Bas van der Wielen[3], Nourdin Kaai[3], John Reid[3], Daniele Raiteri[3], Aaron Albores-Mejía[1,2],Chigo Okonkwo[1,2]

[1]High-Capacity Optical Transmission Laboratory, Eindhoven University of Technology, The Netherlands
[2]CUbIQ Technologies, De Groene Loper 5, Eindhoven, The Netherlands
[3]Aircision, Building 12 High Tech Campus, Eindhoven, The Netherlands
* j.c.dos.reis.frazao@tue.nl

Introduction

Continuous variable quantum key distribution (CV-QKD) provides a quantum-secure solution for distributing secret random keys in optical wireless communication data centers. Leveraging weak coherent states, CV-QKD protocols utilize mature telecom technologies. Security relies on quantum mechanics for Gaussian and discrete modulation protocols [1,2]. We apply the analytical bound for asymptotic secret key ratio under arbitrary modulation [3], considering realistic trusted noise and finite size effects [4]. Several fiber-based CV-QKD experiments [5-8] achieved transmission over a channel with 2-20 dB loss and offline digital signal processing and post-processing. Free-space optical (FSO) CV-QKD was first demonstrated under realistic atmospheric conditions in [9]. Techniques like channel estimation, phase compensation, and noise suppression aim to enable real-world CV-QKD transmission over free space channels [10-12]. A 0.6 km free-space CV-QKD system operated in fog has been demonstrated in [13]. Robust FSO implementations resistant to polarization drift were developed [14], along with urban field trial [15]. In this paper, together with CUbIQ, Aircision and TU/e, a CV-QKD with real-time Bob was implemented in a free-space quantum channel.

Experimental set-up

The experimental free-space CV-QKD setup (Fig. 1) utilizes an offline transmitter (Alice) and real-time receiver (Bob) capable of operating in calibration and signal mode. Key system capabilities include <100 kHz External Cavity Lasers (ECLs), IQ optical modulation for probabilistic 64-QAM shaping [3], 250 Mbaud symbol rate with pilot symbols, and 2 GS/s ADC digitization at the receiver (Bob). Alice employs the ECL, offline DSP, and IQ modulator for shaped QAM with inserted pilot symbols. At the end of Alice, the light transitions to a collimated free space beam using a Thorlabs TC25APC-1550 collimator. A free space path of 3.7 meters is traversed, via two two-inch mirrors to fold the path on the optical table and ease alignment, before coupling back into a single mode fiber using a Thorlabs C280TMD-C focusing lens, with a total channel loss of 2.85 dB. Bob uses a local ECL as local oscillator into an optical hybrid, digitizes the outputs, and implements DSP

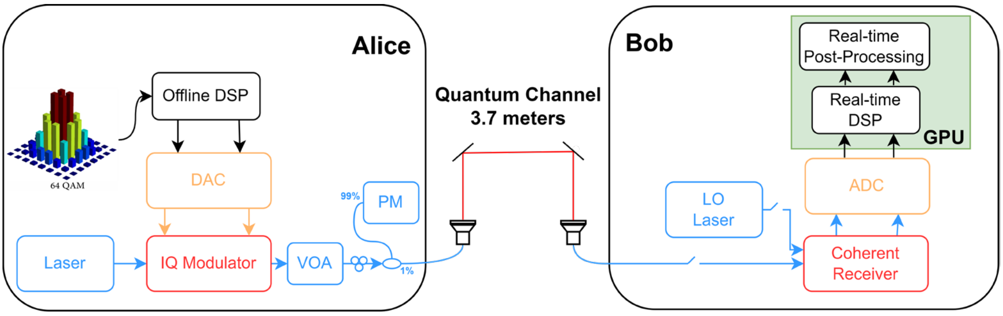

Fig. 1. Free space continuous variable quantum key distribution experimental set-up

for calibration and quantum signal recovery. DSP includes frequency off-set compensation, filtering, equalization, pilot-based phase recovery [16], and parameter estimation [17]. Real-time post-processing on a GPU evaluates security via excess noise and secret key ratio. Note that error correction and privacy amplification are implemented but not enabled because we have an offline transmitter. With a stable link, fixed channel loss is assumed. The setup demonstrates free-space CV-QKD with real-time reception. Adding Alice transmit power monitoring and polarization multiplexing could further enhance performance.

Results

The free-space CV-QKD experiment uses a number of fixed variables and assumptions in order to calculate the security parameters (Fig. 2a). The variable optical attenuator (VOA) at the transmitter output was swept to optimize modulation variance (variable related to Alice output power: Va) for lowest excess noise and highest secret key ratio while maintaining digital signal processing stability (Fig. 2b). The peak average secret key ratio of 0.054 bits/symbol occurred at Va = 4 shot-noise units (SNU). With the VOA fixed for Va = 4 SNU, a 300 s measurement showed an average excess noise of 0.00536 SNU and secret key ratio of 0.0561 bits/symbol (Fig. 3a). The spacing between captures does not represent the signal and calibration modes, but instead the number of blocks analyzed to calculate each average. For the Va sweep and fixed Va a number of 20 and 95 blocks were used to average the results, respectively. The upward and downward line in between each point represents the minimum and maximum value for each average.

a)

Parameter	Va range	Va fix
Modulation	64-QAM	
Loss	2.85 dB	
Clearance	10 dB	
η	40%	
β	95%	
FER	10%	
Block	2621440	
Va	2-6 SNU	4 SNU
ξ_B	0.008 SNU	0.0056 SNU
Secret Key Rate	2 Mbps	4.2 Mbps

b)

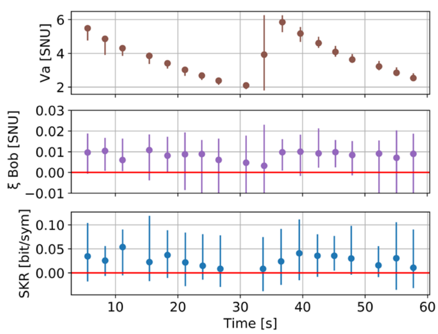

Fig. 2. a) Table: CV-QKD parameters, where η is quantum efficiency, β is reconciliation efficiency and FER is frame error rate b) Real-time SKR and ξ_B with Va range of 2-6 SNU

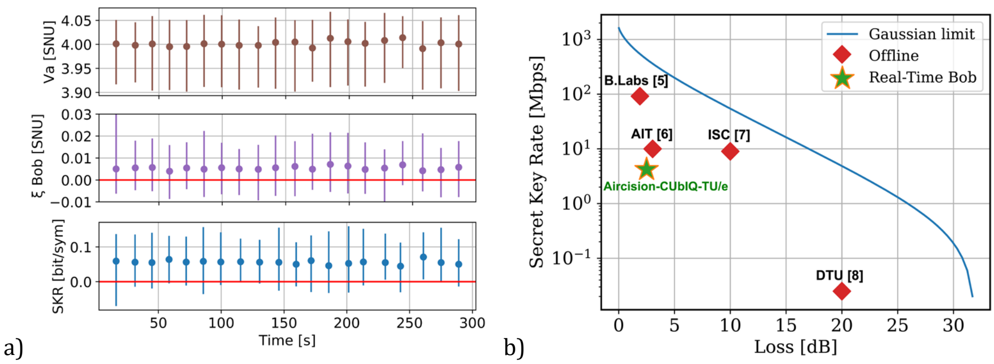

Fig. 3. a) Real-time SKR and ξ_B with fixed Va of 4 SNU b) Performance comparison with state-of-the-art CV-QKD implementations in fiber quantum channels

Considering the pilot tones, calibration, and parameter estimation results, the average secret key rate was 4.2 Mbps. Negative excess noise arose from random fluctuations of thermal and shot noise. Compared to leading fiber-based CV-QKD demonstrations, our free-space implementation with real-time reception has smaller block sizes and limiting performance due to finite-size effects (Fig. 3b). Still, this initial free-space experiment shows promising secret key rates. Further optimization of modulation variance, block sizes, and inclusion of dual-polarization transmission could improve performance. The results highlight the potential of CV-QKD in free-space links.

Conclusion

We demonstrate a practical CV-QKD implementation with a secret key rate of 4.2 Mbps in a free space quantum channel. We successfully implemented a real-time Bob, with an free-space link with 2.85 dB loss. This work paves the way to better understand quantum channel effects, in real-time quantum key distribution, by designing future experiments with beam wandering and atmospheric effects (turbulence and fog). Making it an attractive security solution in optical wireless communication for data centers.

References

[1] F. Grosshans, et al., Phys. Rev. Lett., 88(5):057902, 2002

[2] A. Leverrier, tel-00451021, 2009(Thesis)

[3] A.Denys, et al., Quantum, 5:540 2021.

[4] P. Jouguet, et al., Phys. Rev. A, 86(3):032309, 2012

[5] F. Roumestan, tel-03880444v2, 2022(Thesis)

[6] F. Honz, et al., ECOC, 2022

[7] Pan, Yan, et al., Optics Letters, vol. 47, no. 13, 2022, p. 3307.

[8] A. Hajomer, et al., QCrypt, 2023 (poster 113).

[9] D. Elser, et al., New J. Phys. 11(4), 045014 (2009).

[10] S. Wang, et al., Opt. Express 28(8), 10737–10745 (2020).

[11] S. Wang, et al., Opt. Lett. 45(21), 5921–5924 (2020).

[12] G. Chai, et al., New J. Phys. 22(10), 103009 (2020).

[13] S. Wang, et al., Opt. Lett. 46(23), 5858–5861 (2021).

[14] Rani, et al., Physics Open, 17, 100162.

[15] Shen, et al., *Phys. Rev. A*, 100(1):012325, 2019

[16] S. van der Heide, et al., *OFC*, 2023

[17] Kleis S, et al., Opt Lett. 2017