Composable finite size key generation in a polarization diverse continuous variable quantum key distribution system

Hou-Man Chin,[1,2,*] Ulrik L. Andersen,[1] and Tobias Gehring[1]

[1] *Center for Macroscopic Quantum States, bigQ, Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark*

[2] *Machine Learning in Photonic Systems, Department of Electrical and Photonic Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark*

[*] *homch@dtu.dk*

Abstract: We report on a polarization diverse continuous variable quantum key distribution system. Composable finite size key generation was assessed using 7.6×10^8 quantum states measured over 20 random states of polarization, secret key generation was achieved with 2×10^7 states. © 2023 The Author(s)

1. Introduction

Quantum key distribution (QKD) is a state-of-the-art technology, offering information theoretic security to protect our digital messages from attackers [1]. QKD uses the principles of quantum mechanics to establish cryptographic keys that are impervious to eavesdropping, even in the face of advanced computational threats [2, 3]. In this work we focus on continuous variable QKD because it can co-exist with classical signals within the same optical infrastructure easily, it can use standard electro-optical telecommunications components and it is very scalable to high symbol rates [4]. To deploy CVQKD systems into the real world with maximum efficiency, they must operate under the same conditions as telecommunication systems. One of these constraints is that the state of polarization (SOP) of the transmitter's (Alice) signal is unknown to the receiver (Bob), and for optimum performance, the SOP of Alice and Bob's lasers are matched. Typically in a lab environment, this is performed using manual optimization and a polarization controller [5]. For coherent telecommunication systems, the polarization diverse coherent receiver and digital signal processing (DSP) address this issue [6]. Similar capabilities are a necessity for real-world CVQKD implementations to reduce untrusted loss and thereby maximize the mutual information between Alice and Bob. This is also helpful in the information reconciliation (IR) process since it can assist in providing a consistent amount of mutual information.

In this work we use a modified constant modulus algorithm (CMA) in conjunction with a polarization diverse coherent balanced heterodyne receiver, to operate a single polarization CVQKD system in a completely free running system where the optical signal is the only connection between Alice and Bob. We measure the system's performance over 20 random states of polarization. Using this ensemble of measurements, we achieve secret key generation using as little as 2×10^7 exchanged quantum states.

2. Experimental setup

The experimental setup is as shown in Fig. 1. Quantum states are generated from the output of a quantum random generator, ostensibly at 20 Mbaud. The frequency response of both sets of balanced photodiodes are first whitened and gain matched such that the combined shot and electronic noise are equalized across the approximate quantum signal bandwidth. Two pilot tones and a quadrature phase shift keying (QPSK) signal (20 Mbaud) are frequency multiplexed with the quantum signal, and the composite signal was modulated onto the output of a fibre laser (specified 100 Hz linewidth) using a commercially available in-phase and quadrature modulator and a 1 Gsample/s arbitrary waveform generator (AWG). Alice's transmitted modulation variance was ≈ 0.8 photon number units (PNU). The optical signal is transmitted over 10 km of standard single mode fibre (SMF28). Bob detects her transmitted signal with a polarization diverse coherent balanced heterodyne detector with trusted efficiency of 53 %. The detector output is then captured by a digital storage oscilloscope (DSO) @ 1 Gsample/s. The measured signals were processed offline. A total of 3.8×10^8 symbols were measured across twenty randomly selected states of polarization for 7.6×10^8 quantum states, since a state is transmitted in both the in-phase and quadrature component of the symbol. Calibration for the shot noise was performed prior to each SOP measurement in a single shot manner [7].

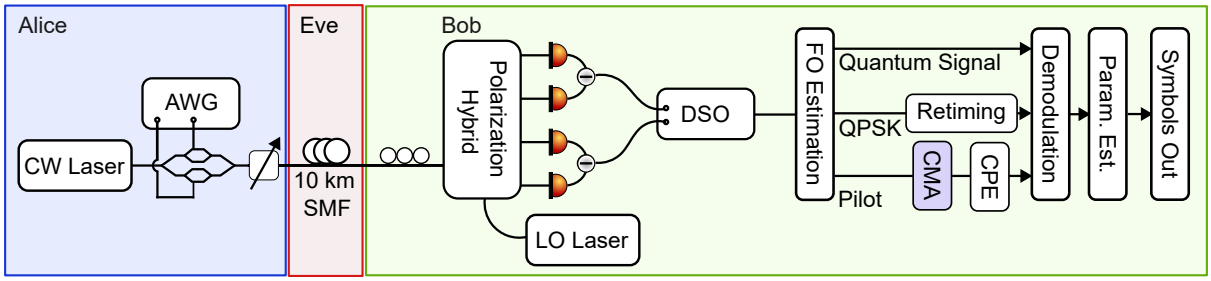
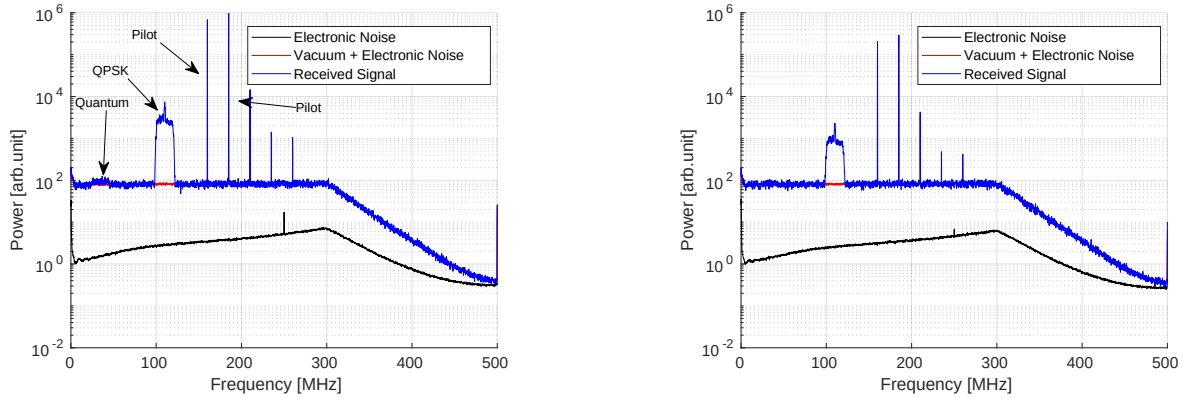


Fig. 1: Experimental setup



(a) X polarization

(b) Y polarization

Fig. 2: Example PSDs of received signals after frequency response whitening and gain equalization

2.1. *Digital signal processing*

Alice and Bob operate their respective transceivers in completely free running mode. Hence it is necessary to correct for various impairments digitally to successfully recover the quantum states. The frequency response of each set balanced photodiodes are whitened and gain matched, Fig. 2. Frequency offset estimation, compensation and synchronization is performed as per [8]. The CMA [6] was implemented with one tap and used on the pilot signal at 20 Mbaud. The CMA architecture was modified such that the taps $h_{xx}^2 + h_{xy}^2 = 1; h_{yx}^2 + h_{yy}^2 = 1$ to ensure SOP compensation performed on the quantum states is unitary. The convergence parameter was set to $\mu = 2^{-10}$. Carrier phase equalization was performed similar to [9] at symbol rate after frequency shifting a pilot tone to baseband. We note that though we implemented the entire CMA butterfly structure [6] to examine the mutual information left on the Y polarization, implementation could have been performed with half of it.

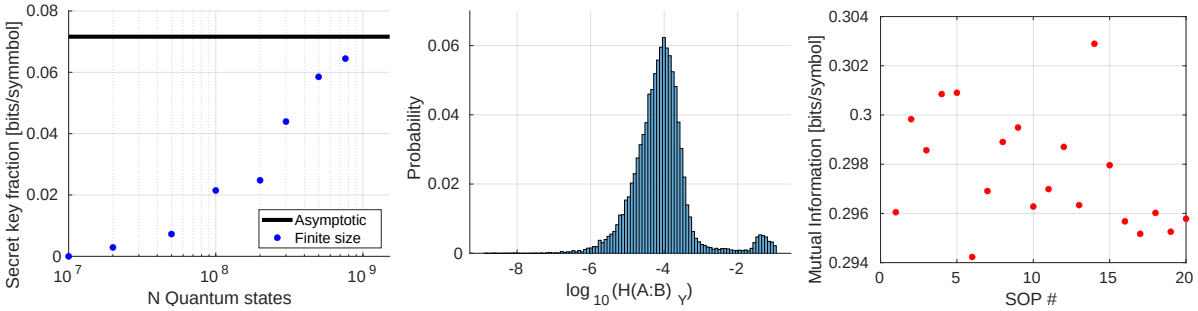
3. Results

Parameter estimation is performed on the demodulated quantum states and the secret key fraction (SKF) is calculated for the finite size regime, achieving composable security against collective attacks, [5] using

$$s_n^{\varepsilon_h+\varepsilon_s+\varepsilon_{IR}} \geq H_{min}^{\varepsilon_s}(\bar{Y}|E) - \text{leak}_{IR}(n, \varepsilon_{IR}) + 2\log_2(\sqrt{2}\varepsilon_h), \tag{1}$$

where s_n is the SKF, $H_{min}^{\varepsilon_s}(\bar{Y}|E)$ is the conditional ε_s-smooth min-entropy of Bob's measured quantum states $\bar{Y}$ conditioned on Eve's quantum state. leak_{IR} is the information leaked through the reconciliation process (IR). ε_h is a security parameter characterizing the hashing function, ε_{IR} describes the failure probability of the correctness test after IR, ε_s is a smoothing parameter. $H(\bar{Y})$ is the Shannon entropy, $I(Y;E)$ is the Holevo information extracted by Eve, all $\varepsilon = 10^{-10}$ except $\varepsilon_{IR} = 10^{-12}$. The reconciliation efficiency is assumed to be 95% and a IR success rate of 100%.

The achieved SKF is shown in Fig. 3a, 7.6×10^8 quantum states were exchanged between Alice and Bob over 20 SOPs, we estimate the achievable secret key fraction over an increasing amount of quantum states as required for finite size key generation regime [5]. The results of which are seen in Fig. 3a, we see that positive secret key fraction (0.003 bits/symbol) was achieved for 2×10^7 states. Using all of the measured states, a SKF of 0.064 bits/symbol is achieved compared to the asymptotic SKF of 0.074 bits/symbol. Fig. 3b shows the probability distribution of the amount of mutual information left on the polarization that is not used for secret key generation,



(a) Composable finite size secret key fraction achieved with respect to number of exchanged states

(b) Probability distribution function of mutual information left on Y polarization not used for secret key generation

(c) Average mutual information per SOP after polarization correction

Fig. 3

equating to 10^{-4} bits/symbol, which is essentially untrusted loss. The slight increase in probability towards 10^{-1} bits/symbol is due to the symbols where the CMA is still converging since the measurements were taken in blocks of 1.6 Msymbols and the CMA is initialized per block. The mutual information per measured SOP is shown in Fig. 3c, in no particular order of SOP, of which the mean is 0.298 bits/symbol with a standard deviation of 0.0023 bits/symbol, demonstrating excellent consistency across measurements.

4. Conclusions

In this work, we investigate a CVQKD transmission system implementing a polarzation diverse balanced heterodyne architecture, operating in a completely free running regime. A digital signal processing chain using a modified CMA, and previously published retiming and phase compensation was used to retrieve the transmitted quantum states. A total of 7.6×10^8 states were measured across 20 randomized states of polarization to form an ensemble of quantum states for parameter estimation. We achieve a positive composable finite size regime secret key fraction of 0.003 bits/symbol using 2×10^7 quantum states exchanged between Alice and Bob. Using all measured states, we achieve 0.064 bits/symbol, compared to the asymptotic SKF of 0.074 bits/symbol.

5. Acknowledgements

The authors acknowledge support from Innovation Fund Denmark (CryptQ project #0175-00018A), and the DNRF Center for Macroscopic Quantum States (bigQ, DNRF142), and DCC [10]. This project was funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733.

References

1. S. Pirandola et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012, 2020.
2. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134. Ieee, 1994.
3. F. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
4. A. A. Hajomer et al. Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver. *arXiv preprint arXiv:2305.19642*, 2023.
5. N. Jain et al. Practical continuous-variable quantum key distribution with composable security. *Nature Communications*, 13(1), 2022.
6. M. S. Faruk and S. J. Savory. Digital Signal Processing for Coherent Transceivers Employing Multilevel Formats. *Journal of Lightwave Technology*, 35(5):1125–1141, 2017.
7. Y. Zhang et al. One-time shot-noise unit calibration method for continuous-variable quantum key distribution. *Physical Review Applied*, 13(2):024058, 2020.
8. H. M. Chin et al. Digital synchronization for continuous-variable quantum key distribution. *Quantum Science and Technology*, 7(4), 2022.
9. H.-M. Chin et al. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *npj Quantum Information*, 7(1), Feb 2021.
10. DTU Computing Center. DTU Computing Center resources, 2021.