Adaptive Reconciliation for Experimental Continuous-Variable Quantum Key Distribution Over a Turbulent Free-Space Optical Channel

Kadir Gümüş[1,*], João dos Reis Frazão,[1], Vincent van Vliet[1], Sjoerd van der Heide[1], Menno van den Hout[1], Aaron Albores-Mejia[1,2], Thomas Bradley[1], and 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*

[*] *k.gumus@tue.nl*

Abstract: We experimentally demonstrate adaptive reconciliation for continuous-variable quantum key distribution over a turbulent free-space optical channel. Additionally, we propose a method for optimising the reconciliation efficiency, increasing secret key rates by up to 8.1%.

1. Introduction

In recent years, many exciting advancements have been made in the field of quantum computing, with expected improvements in the number of qubits [1]. Although these advancements will certainly carry great benefits, they also raise concerns about data security, as these quantum technologies may break current data security protocols. As a result, attention has shifted to protocols that remain unbreakable, even in a post-quantum world. One such protocol is continuous-variable quantum key distribution (CV-QKD), a method for securely sharing secret keys between two communicating parties, Alice and Bob, without a potential eavesdropper (Eve) recovering keys [2].

One of the channels considered for CV-QKD is the free-space optical (FSO) channel, as this would allow for wireless key sharing. The instability of the FSO channel caused by atmospheric turbulence is less of an issue for CV-QKD compared to classical communications, as the encoding occurs after transmission. Despite this, CV-QKD implementation for an FSO channel still poses a challenge, with different considerations and trade-offs to be made when compared to the optical fibre channel. Several experimental CV-QKD transmissions over FSO have already been demonstrated [3–5], however, the reconciliation is rarely analysed, often kept as a footnote.

In this paper, we demonstrate adaptive reconciliation for CV-QKD over an FSO channel with differing turbulence strengths. We show that the modulation format significantly impacts the reconciliation performance, and by choosing a high-dimensional reconciliation protocol, secret key rates (SKRs) can be increased by 122%. Finally, we propose a method for optimising the reconciliation efficiency, increasing SKR by an additional 8.1%.

2. Reverse Reconciliation

Reconciliation is a part of the CV-QKD protocol where Alice and Bob share bit strings which is employed for generating the secret keys. In this paper we will consider only reverse multi-dimensional reconciliation, as direct reconciliation is affected by the 3dB limit [2], and slice reconciliation performs worse than the multi-dimensional protocol in the regime we operate at [6]. An overview of reverse multi-dimensional reconciliation as described in [6] is given in Fig. 1. At the start of the reconciliation, Alice and Bob have the transmitted and measured quantum states $\mathbf{x}$ and $\mathbf{y}$, respectively. Bob generates a string of bits $\mathbf{s}$ using a quantum random number generator (QRNG) and encodes these bits using an error correction code with code rate R creating a codeword $\mathbf{c}$, which is modulated using $\mathbf{y}$ to obfuscate the values of the bits. Bob transmits the modulated message $\mathbf{m}$ to Alice over the classical channel, where it is demodulated before calculation of the log-likelihood ratios (LLR). These LLRs are employed in the decoder to get $\hat{\mathbf{s}}$, which is an estimate of $\mathbf{s}$. After decoding, Alice and Bob compare whether $\mathbf{s}$ and $\hat{\mathbf{s}}$ are the same with, for example, a hashing function. If the decoding has failed, a frame error has occurred and the frame is discarded, otherwise, the frame will be used during privacy amplification for key generation.

The SKR depends on the performance of the error correction codes used during reconciliation and is given by $\text{SKR} = (1-\text{FER})(\beta I_{AB} - \chi_{BE})$, where FER is the frame error rate, I_{AB} is the mutual information between $\mathbf{x}$ and $\mathbf{y}$, $\beta = \frac{R}{I_{AB}}$ is the reconciliation efficiency, and χ_{BE} is the Holevo information (Eve's information) [2]. Secret key exchange is possible when the SKR is positive, i.e., β is close to 1. There is a trade-off between β and the FER, as the FER increases as β increases, so good performing error correction is vital for providing high key rates.

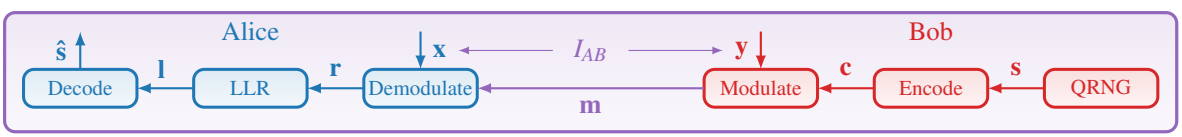

Fig. 1: An overview of the reverse multi-dimensional reconciliation protocol for CV-QKD.

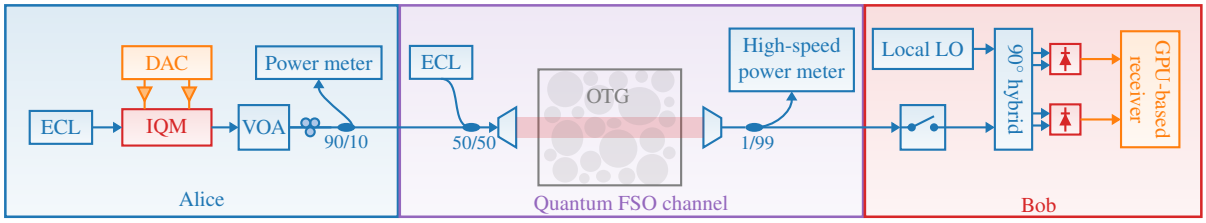

Fig. 2: The CV-QKD set-up for transmission over an FSO channel with an optical turbulence generator.

3. Experimental Set-up

The experimental set-up for the CV-QKD transmission is shown in Fig. 2. Alice employs a <100 kHz linewidth external cavity laser (ECL) at 1550 nm, a digital-to-analog (DAC) converter, and an optical modulator (IQM) to modulate probabilistically-shaped 256QAM (PS-256QAM) signals [7] at a symbol rate of 250 Mbaud. With a variable optical attenuator (VOA) and a power meter, the power of the signal is attenuated to an average of 7.44 shot noise units (SNU) (-69.2 dBm). The attenuated 1550 nm signal is combined with a second tone at 1528 nm and converted to free space using a collimator. The light traverses an optical turbulence generator (OTG) [8] which can mimic varying turbulence strengths. Afterwards, the light is coupled back to fiber using a collimator and a portion is split to a high-speed power meter for turbulence characterisation by fitting a combined log-normal pointing jitter distribution according to [9]. We measured four different turbulence strengths generated by the OTG, with scintillation index $\sigma_I = 0.001, 0.009, 0.01, 0.013$ and pointing jitter β_{jitter} = 123.8, 8.6, 3.0, 1.6 respectively, all classified as weak fluctuations [9].

The remaining 99% of light is directed to Bob's side. A local ECL is used as a local local oscillator (LLO) for the 90° optical hybrid, and the outputs are digitised. Digital signal processing is used for calibration and recovery of the quantum signal [10]. Parameter estimation, taking into account finite-size effects [11], is performed on each CV-QKD block and I_{AB}, the excess noise ξ_{Bob}, and χ_{BE} are estimated. Other relevant parameters for the system are a clearance of 10 dB, quantum efficiency η of 40%, CV-QKD block size of $6.8 \cdot 10^6$, average ξ_{Bob} of 0.0045 SNU, and an average transmittance T depending on the turbulence strength, ranging from 0.35 to 0.41.

For the reverse reconciliation protocol, we use high-dimensional reconciliation, which is multi-dimensional reconciliation with dimensionality $d > 8$, with $d = 128$ as described in [6]. Although normally multi-dimensional reconciliation with $d = 8$ is chosen as it is less complex [6], we opted for higher d, as using PS-256QAM for the modulation of the quantum states significantly reduces the performance of the error correction. The unequal power of the transmitted quantum states makes it so that the virtual channel created during reconciliation does not exactly resemble the binary input additive white Gaussian noise (BI-AWGN) channel which the error correction codes are designed for [12]. As $d \to \infty$, the virtual channel converges to the BI-AWGN as the power of the transmitted quantum states gets averaged out, therefore a higher d improves the performance of the reconciliation.

We use a $R = 0.2$ expanded type-based protograph low-density parity check (TBP-LDPC) code [13] punctured to $R \approx 0.3$, the average I_{AB} of the system, for error correction. This code was chosen because it operates close to capacity, even after significantly changing the rate of the code after puncturing. To adapt the rate of the code during the reconciliation we use the *sp*-protocol described in [14]. We choose a blocklength $N \approx 10^5$ with a maximum of 500 decoding iterations. We randomly sample the parity check matrix according to the protograph, but remove all short cycles within the graph to ensure good error correction performance.

One additional improvement is on how to choose β. Normally, β is determined at a fixed value in order to optimise the average SKR of the system over all CV-QKD blocks. When I_{AB} changes, R is changed such that β stays consistent, which is a valid approach for CV-QKD transmission over fibre, as it tends to be a stable channel. However, in an FSO channel atmospheric turbulence causes additional time-dependent instabilities. As a result, the optimal β for each CV-QKD block changes, and it would make more sense to adaptively change β to optimise the SKR of each block. This adds no extra complexity to the system, as it can be implemented by using a β-FER look-up table during the parameter estimation phase, and picking the β-FER pair which maximises the SKR.

4. Results

In Fig. 3, the FER (left) and the SKR (middle) are shown for different β and d. For the FER we can see that using PS-256QAM for the modulation of the quantum states significantly impacts the error correction performance. Using the standard multi-dimensional protocol with $d = 8$, we lose 3.7% in reconciliation efficiency when compared to an ideal BI-AWGN channel, which is equivalent to when $d = \infty$, for a FER of 10%. Using higher dimensional reconciliation with $d = 128$ allows us to close to gap by 2.6%, with a gap of 1.1% to the ideal case. The SKR we obtained when using $d = 128$ is 122% higher when compared to $d = 8$, reducing the gap to BI-AWGN to 28%. Although using this higher dimensional reconciliation is more complex, simplified versions of this protocol exist [12], meaning that the bottleneck of the reconciliation is still the decoding on Alice's side.

In Fig. 3 (right) we also show the SKR for our β-optimisation method and compare it to using the same β for

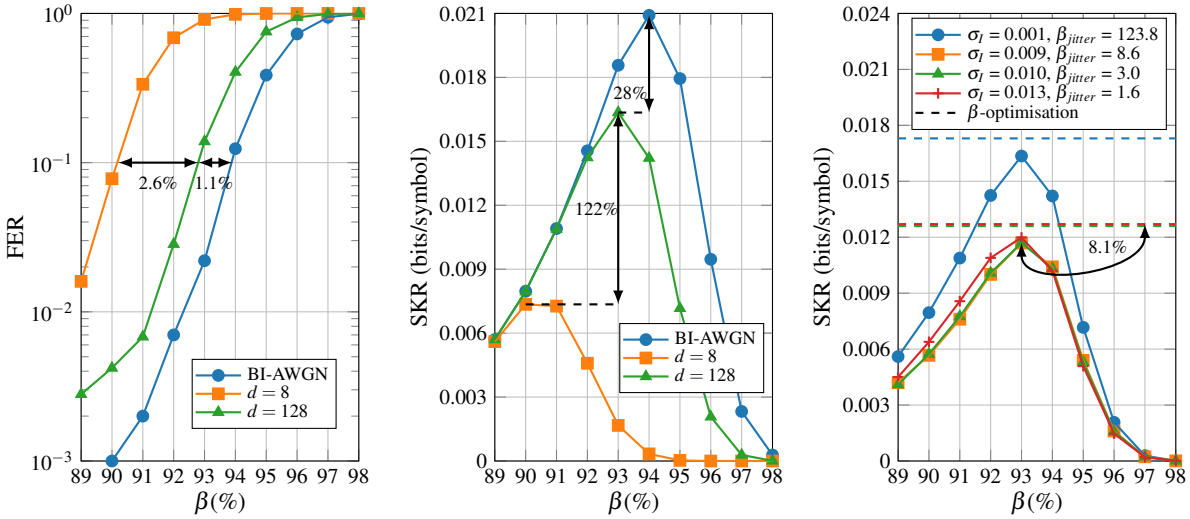

Fig. 3: Left: The FER of the $R = \frac{1}{5}$ expanded TBP-LDPC code when punctured to $R = 0.3$ for different d compared to the BI-AWGN channel. Middle: The SKR of the $R = \frac{1}{5}$ expanded TBP-LDPC code when punctured to $R = 0.3$ for different d compared to the BI-AWGN channel for the FSO channel with $\sigma_I = 0.001$ and $\beta_{jitter} = 123.8$. Right: The SKR for our CV-QKD set-up for different β compared to β-optimisation (dashed line) for different turbulence settings.

each CV-QKD block for FSO channels with different amounts of turbulence. The maximum SKR when using the same β for each CV-QKD block is achieved at a β around 93% for all turbulence settings. As expected, the SKR is highest for the case where there is almost no turbulence. Between the other turbulence settings the SKR does not change significantly because of random fluctuations of ξ_{Bob} during our measurements. When using our β optimisation method (SKRs shown with dashed line), we can get up to 8.1% higher SKR when compared to sticking to only one value for β. This gain is dependent on the specifications of the CV-QKD system, but considering that β-optimisation adds no additional complexity, while always increasing the SKR, it is always worth implementing.

5. Conclusion

In this work we have demonstrated adaptive reconciliation for an experimental CV-QKD transmission over an FSO channel. We have shown that when using PS-256QAM for modulating the quantum states, it is worth considering using higher dimensional reconciliation to improve the SKR by up to 122%. Finally, we proposed a method for optimising the reconciliation efficiency during parameter estimation, increasing the SKR by up to 8.1%.

This work was supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL KAT-2 programme on Quantum Communications and PhotonDelta GrowthFunds Programme on Photonics.

References

1. L. Gyongyosi and S. Imre, "A survey on quantum computing technology," Comput. Sci. Rev. **31** (2019).
2. F. Laudenbach *et al.*, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," Adv. Quantum Technol. **1** (2018).
3. A. Rani *et al.*, "Free space continuous variable quantum key distribution with discrete phases," Phys. Open **17** (2023).
4. S.-Y. Shen *et al.*, "Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment," Phys. Rev. A **100** (2019).
5. S. Wang *et al.*, "Feasibility of continuous-variable quantum key distribution through fog," Opt. Lett. **46** (2021).
6. A. Leverrier *et al.*, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77** (2008).
7. A. Denys *et al.*, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum **5** (2021).
8. V. van Vliet, "Optical turbulence generator for lab-based experimental studies of atmospheric turbulence in vertical optical communication links," Master's thesis, TU/e (2022).
9. K. Kiasaleh, "On the probability density function of signal intensity in free-space optical communications systems impaired by pointing jitter and turbulence," Opt. Eng. **33** (1994).
10. S. van der Heide *et al.*, "Receiver noise stability calibration for CV-QKD," Proc. OFC 2023 (2023).
11. P. Jouguet *et al.*, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86** (2012).
12. P. Jouguet *et al.*, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84** (2011).
13. K. Gümüş and L. Schmalen, "Low rate protograph-based LDPC codes for continuous variable quantum key distribution," Proc. ISWCS 2021 (2021).
14. X. Wang *et al.*, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," arXiv preprint arXiv:1703.04916 (2017).