Quantum Key Distribution with Characterized Source Defects

Shlok Nahar[1] and **Norbert Lütkenhaus**[1]

[1]Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo

Introduction

- Many protocols use phase randomised signals, for eg.- Weak Coherent Phase BB84. Driving the laser diodes far below the threshold usually randomises the phase. However, for higher repetition rates, the photons from the previous pulse might not all disappear from the laser cavity. These photons might seed the phase of the next laser pulse and cause phase memory in the form of coherences.
- Here, we investigate the impact of these partial coherences on the key rate.
- Previous work [1, 2] on source defects deals with generic source defects and Trojan horse attacks. As we make more assumptions and investigate only imperfections that arise as a result of partial coherences, we are able to tolerate larger imperfections than their work.

Our Contributions

- We provide a reduction of a general source with partial phase coherence motivated by a physical picture, and provide a reduction to a simplified source model.
- We derive analytical tools that allow us to analyze the secret key rates in a decoy state protocol approach for these sources using our numerical tool box.
- To demonstrate the power of our approach, we apply our tools to the 3-state protocol for which experimental realizations exists that measure the relevant source imperfection.

Simplified Model

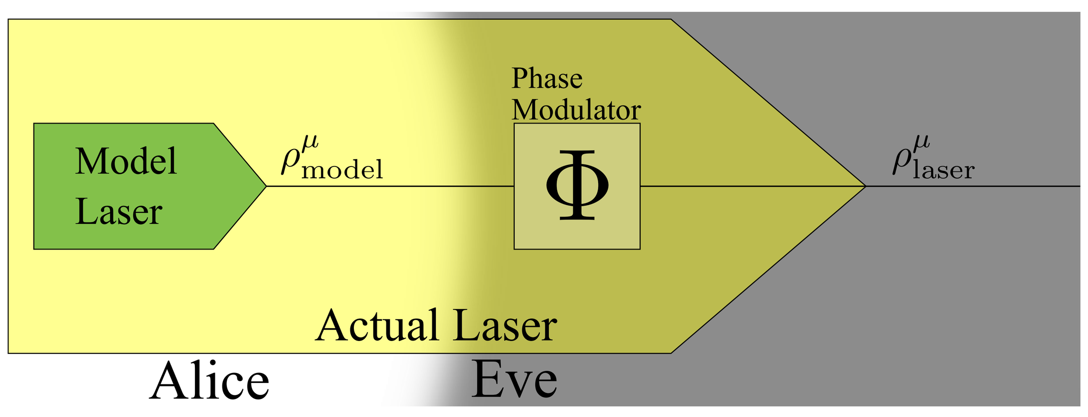
Actual Laser State

$$\rho^{\mu}_{\text{laser}} = \int d\phi_1 \ldots d\phi_n \, p(\phi_1 \ldots \phi_n) |\sqrt{\mu} e^{i\phi_1}\rangle\langle\sqrt{\mu} e^{i\phi_1}| \otimes \ldots \otimes |\sqrt{\mu} e^{i\phi_n}\rangle\langle\sqrt{\mu} e^{i\phi_n}|$$

Model Laser State

$$\rho^{\mu}_{\text{model}} = q \int d\phi \, \frac{1}{2\pi} |\sqrt{\mu} e^{i\phi}\rangle\langle\sqrt{\mu} e^{i\phi}|^{\otimes n} + (1-q)|\sqrt{\mu}\rangle\langle\sqrt{\mu}|^{\otimes n}$$

$q := \min_i \min_{\phi_i} 2\pi p(\phi_i|\phi_1 \ldots \phi_{i-1})$ is a parameter that must be experimentally characterised which represents the degree to which the states are fully phase randomised.



Thought setup for the actual laser source that produces $\rho^{\mu}_{\text{laser}}$.

$\rho^{\mu}_{\text{model}}$ lower bounds the key rate for the actual protocol using $\rho^{\mu}_{\text{laser}}$.

Decoy State

Standard Decoy	Our Analysis
Central Difference: Diagonal Basis	
• All intensities are diagonal in the same basis • $\rho^{\nu} = \sum_{n=0}^{\infty} p(n\|\nu)\|n\rangle\langle n\|$ • The key rate contribution comes from the single photon state $\|1\rangle\langle 1\|$	• Each intensity is diagonal in a different basis • $\rho^{\nu} = \sum_{n=0}^{\infty} p_{\nu}(n_{\nu})\|n_{\nu}\rangle\langle n_{\nu}\|$ • The key rate contribution comes from the state $\|1_{\mu}\rangle\langle 1_{\mu}\|$ for signal intensity μ
Preliminary Step: Diagonalise	
• We already know the eigenvalues/eigenvectors of the signal state $\rho^{\mu} = \sum_{n=0}^{\infty} p(n\|\mu)\|n\rangle\langle n\|$	• $\Pi_N \rho^{\mu} \Pi_N = \sum_{n'_{\mu}=0}^{N} p_{\mu}(n'_{\mu})\|n'_{\mu}\rangle\langle n'_{\mu}\|$ is easily diagonalisable and we can bound the deviation in eigenvalues/eigenvectors from the infinite state
Decoy State Goal: Infinite Optimisation	
Linear Program $\min / \max p(\det\|1)$ such that $p(\det\|\nu) = \sum_{n=0}^{\infty} p(\det\|n)p(n\|\nu) \; \forall \nu$ given $p(\det\|\nu)$	Semidefinite Program $\min / \max \mathrm{Tr}\left[\Gamma\Phi(\|1'_{\mu}\rangle\langle 1'_{\mu}\|)\right]$ such that $\mathrm{Tr}\left[\Gamma\Phi(\rho^{\nu})\right] = \mathrm{p}(\det\|\nu) \; \forall \nu$
Finite Loosening of Constraints	
$p(\det\|\nu) \geq \sum_{n=0}^{N} p(\det\|n)p(n\|\nu)$ $p(\det\|\nu) \leq \sum_{n=0}^{N} p(\det\|n)p(n\|\nu) + \sum_{n=N+1}^{\infty} p(n\|\nu)$	$\mathrm{Tr}\left[\Pi_M \Gamma \Pi_M \, \Phi(\Pi_N \rho^{\nu} \Pi_N)\right] \geq p(\det\|\nu) - \epsilon^L$ $\mathrm{Tr}\left[\Pi_M \Gamma \Pi_M \, \Phi(\Pi_N \rho^{\nu} \Pi_N)\right] \leq p(\det\|\nu) + \epsilon^U$

Our analysis is more general than the standard decoy state analysis as it can work for any arbitrary set of states.

We can now use these statistics with our numerical toolbox to find the key rate.

Numerical Key Rates

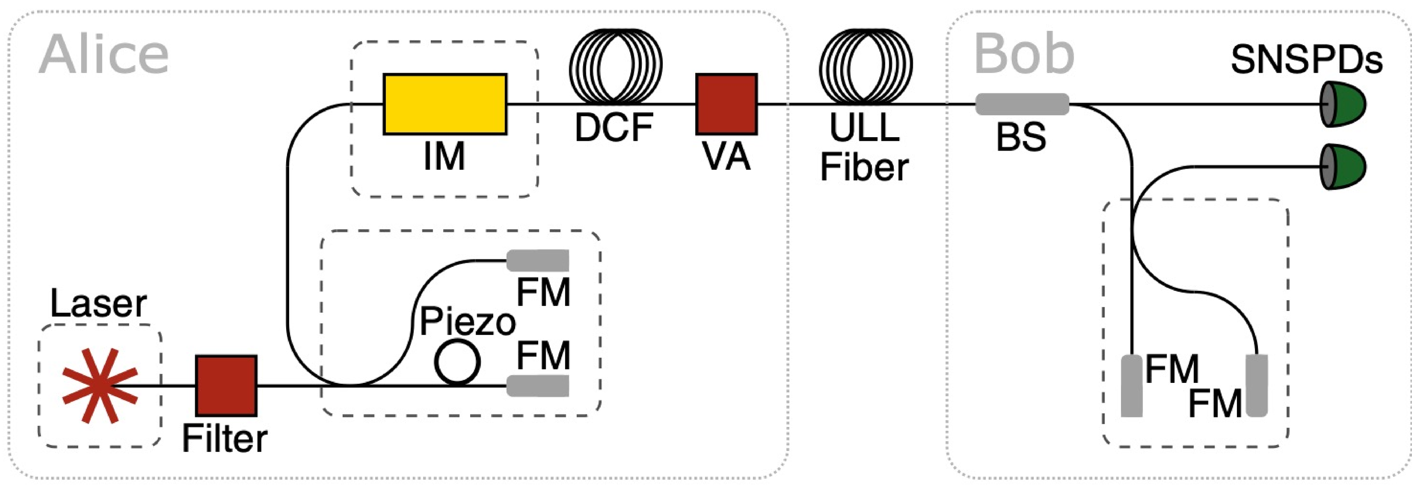
Computing the key rate can be reduced to solving an optimisation problem [3, 4]

$$\min f(\rho_{AB})$$
$$\text{such that } \mathrm{Tr}(\Gamma_i \rho_{AB}) = \gamma_i \, \forall i$$

where Γ_i are the different measurements that Alice and Bob perform on their joint system ρ_{AB} and γ_i are the statistics they observe for the respective measurements.

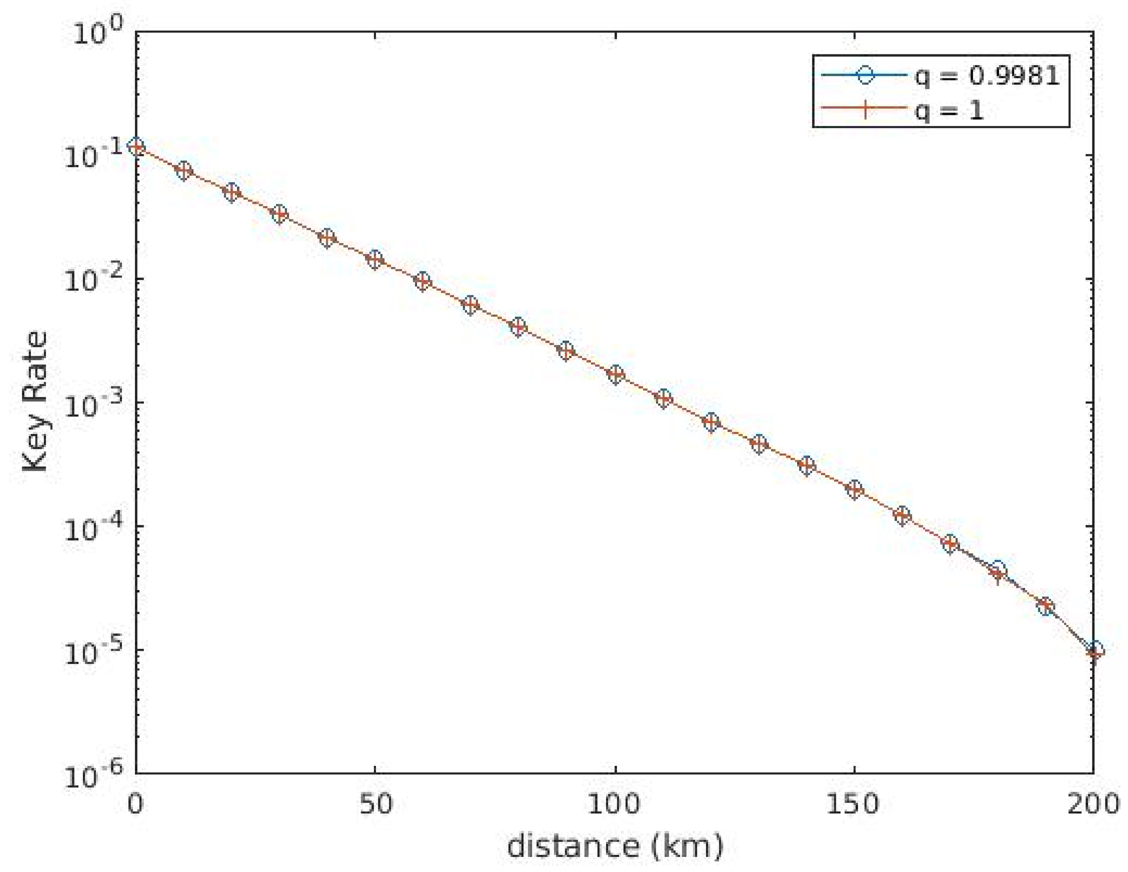
3-State Protocol

- The three-state protocol is simpler to implement than BB84 since it sends one less signal state and has fewer active elements.
- Recently, an optical implementation of the protocol was able to achieve key rates over 421 km of optical fiber [5]. This optical implementation uses high clock rates and the states were shown not to be fully phase-randomised. Assuming the laser state to be of the form shown in the simplified model, the experiment used an asymmetric Mach-Zehnder interferometer to check the coherences between consecutive laser pulses. The partial coherences were estimated to be $(1-q) = 0.0019$ [6].



Schematics of the experimental setup from [5].

Results



We found that upto 200 km partial coherences of the magnitude observed in the experiment [6] did not significantly affect key rates. This is in contrast to past results [2] that consider more general defects and thus predict key rates only under 40 km for defects of this magnitude.

Future Work

- Develop a good way to calculate q for an arbitrary phase distribution from experimental observations.
- Develop methods to deal with intensity correlations.
- Improve the numerical toolbox to get key rates past 200 km though practical applications would use distances upto 200 km that have been shown here.

References

[1] Álvaro Navarrete et al. "Practical Quantum Key Distribution That is Secure Against Side Channels". In: *Physical Review Applied* 15.3 (2021), p. 034072.

[2] Margarida Pereira et al. "Quantum key distribution with correlated sources". In: *Science Advances* 6.37 (2020), eaaz4487.

[3] Adam Winick, Norbert Lütkenhaus, and Patrick J Coles. "Reliable numerical key rates for quantum key distribution". In: *Quantum* 2 (2018), p. 77.

[4] Lütkenhaus Group. *QKD Software*. `http://www.openqkdsecurity.org/`. Aug. 2021.

[5] Alberto Boaron et al. "Secure quantum key distribution over 421 km of optical fiber". In: *Physical review letters* 121.19 (2018), p. 190502.

[6] Fadri Grünenfelder et al. "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution". In: *Applied Physics Letters* 117.14 (2020), p. 144003.