Numerical Security Proof for Decoy-State BB84 and Measurement-Device-Independent QKD Resistant against Large Basis Misalignment

Wenyuan Wang,[1] and Norbert Lütkenhaus[1,*]

[1] *Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

[*] *email: lutkenhaus.office@uwaterloo.ca*

In this work, we **incorporate decoy-state analysis** into a well-established numerical framework for key rate calculation, and apply the numerical framework to **decoy-state BB84 and measurement-device-independent (MDI) QKD** protocols as examples. Additionally, we combine with these decoy-state protocols what is called ``**fine-grained statistics**", a variation of existing QKD protocols that makes use of originally discarded data to get better key rate. We show that such variations can grant protocols **resilience against any unknown and slowly changing rotation along one axis**, similar to reference-frame-independent QKD, but without the need for encoding physically in an additional rotation-invariant basis. Such an analysis can easily be applied to existing systems, or even data already recorded in previous experiments, to gain significantly higher key rate when considerable misalignment is present, extending the maximum distance for BB84 and MDI-QKD and reducing the need for manual alignment in an experiment.

Background

Numerical Framework:

In our group's previous works [1,2], a **numerical framework** capable of calculating the key rate of general QKD protocols with a **unified algorithm** was proposed. (*Also see **poster #227** on the framework.*)

A **QKD protocol** is described in a "prototypical" form containing:

- measurements (**POVMs**),
- public announcement and sifting (**Kraus operators**),
- retrieval of classical key bit (**Alice's key map**)
- **error-correction** and privacy amplification.

The key rate can be simply calculated from:

$$R = \min_{\rho \in S} f(\rho) - p_{pass} \times leak_{obs}^{EC}$$

where $f(\rho) = D(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho)))$ is the quantum relative entropy, and maps $\mathcal{G}$ and $\mathcal{Z}$ are defined by the Kraus operator and key map, respectively. The term $p_{pass} \times leak_{obs}^{EC}$ is the leaked information during error-correction.

This is an **optimization problem** of choosing quantum state ρ that minimizes the key rate, given the constraints $\rho \in S$ constructed from the **observed expectation values** $\{\boldsymbol{\gamma_k}\}$ of the POVMs $\{\Gamma_k\}$ in an actual experiment. Here

$$S = \{\rho \in H_+ | Tr(\Gamma_k \rho) = \gamma_k, \forall k\}$$

Decoy-State Analysis

In practice, phase-randomized **weak coherent pulse (WCP)** sources are often used for QKD, which emit mixtures of photon number states following a Poissonian distribution P_n^μ for intensity μ:

$$P_n^\mu = e^{-\mu} \mu^n / n!$$

Decoy-state analysis [3-5] is proposed to estimate the single-photon contribution among the statistics obtained from a WCP source, by observing that:

$$\gamma_\mu = \sum_{n=0}^{\infty} P_n^\mu \gamma_n$$

One can use several intensity settings μ to obtain a set of equations with γ_n as a set of variables, which form a **linear programming** (LP) problem, and the **single photon contribution $\boldsymbol{\gamma_1}$** can be upper/lower-bounded either numerically [6] or analytically [7].

$$\gamma_1^L \le \gamma_1 \le \gamma_1^U$$

Method

1. Incorporating Decoy-State Analysis

In this work, we apply the numerical framework to two important protocols, BB84 [8] and measurement-device-independent (MDI) QKD [9], in the case of using **WCP sources and a finite number of decoy states**.

Following the results of Ref. [10], importantly, **the state shared by Alice and Bob is block-diagonal** with respect to the number of photons n sent by Alice. The key rate can be lower-bounded by summing up the key rates from optimizing the conditional density matrices ρ_n of each subspace (for the photon number sent):

$$R = \sum_{n=0}^{\infty} P_n^\mu \min_{\rho_n \in S_n} f(\rho_n) - p_{pass} \times leak_{obs}^{EC} \ge P_1^\mu \min_{\rho_1 \in S_1} f(\rho_1) - p_{pass} \times leak_{obs}^{EC}$$

Here, we only care about the **single-photon-sent subspace**, $\min_{\rho_1 \in S_1} f(\rho_1)$.

The key problem is that we cannot directly obtain S_1 based on single photon statistics $\{\gamma_{1,k}\}$, but rather have to **estimate $\{\boldsymbol{\gamma_{1,k}}\}$ from decoy-state analysis**, from which we know each observable satisfies:

$$\gamma_{1,k} \in [\gamma_{1,k}^L, \gamma_{1,k}^U]$$

Each set of $\{\gamma_{1,k}\}$ corresponds to a bound S_1 for ρ_1. We can reformulate the problem as optimizing $\rho_1 \in S_1'$, where **$\boldsymbol{S_1'}$ is the union of all possible $\boldsymbol{S_1}$** for acceptable $\{\gamma_{1,k}\}$. Mathematically, this is simply:

$$S_1' = \{\rho_1 \in H_+ | \gamma_{1,k}^L \le Tr(\Gamma_k \rho_1) \le \gamma_{1,k}^U, \forall k\}$$

The final key rate (suppose signal intensity is μ) is written as:

$$R \ge P_1^\mu \min_{\rho_1 \in S_1'} f(\rho_1) - p_{pass} \times leak_{obs}^{EC}$$

From here we can see that the **decoy-state analysis functions like a "wrapper"**:

- the **linear program** generates bounds on the pseudo-statistics for single photons;
- the **numerical framework** accepts these statistics as if they are from single photon sources (only replacing equality constraints with inequalities).

2. Using Fine-Grained Statistics

Data used in security analysis

BB84

		Bob measures				
		H	V	+	-	∅
Alice sends	H	γ_{HH}	γ_{HV}	γ_{H+}	γ_{H-}	$\gamma_{H\varnothing}$
	V	γ_{VH}	γ_{VV}	γ_{V+}	γ_{V-}	$\gamma_{V\varnothing}$
	+	γ_{+H}	γ_{+V}	γ_{++}	γ_{+-}	$\gamma_{+\varnothing}$
	-	γ_{-H}	γ_{-V}	γ_{-+}	γ_{--}	$\gamma_{-\varnothing}$

MDI-QKD (partial)

		Bob sends			
		H	V	+	-
Alice sends	H	$\gamma_{HH}^{\Psi^+}$	$\gamma_{HV}^{\Psi^+}$	$\gamma_{H+}^{\Psi^+}$	$\gamma_{H-}^{\Psi^+}$
	V	$\gamma_{VH}^{\Psi^+}$	$\gamma_{VV}^{\Psi^+}$	$\gamma_{V+}^{\Psi^+}$	$\gamma_{V-}^{\Psi^+}$
	+	$\gamma_{+H}^{\Psi^+}$	$\gamma_{+V}^{\Psi^+}$	$\gamma_{++}^{\Psi^+}$	$\gamma_{+-}^{\Psi^+}$
	-	$\gamma_{-H}^{\Psi^+}$	$\gamma_{-V}^{\Psi^+}$	$\gamma_{-+}^{\Psi^+}$	$\gamma_{--}^{\Psi^+}$

(To be continued on upper-right)

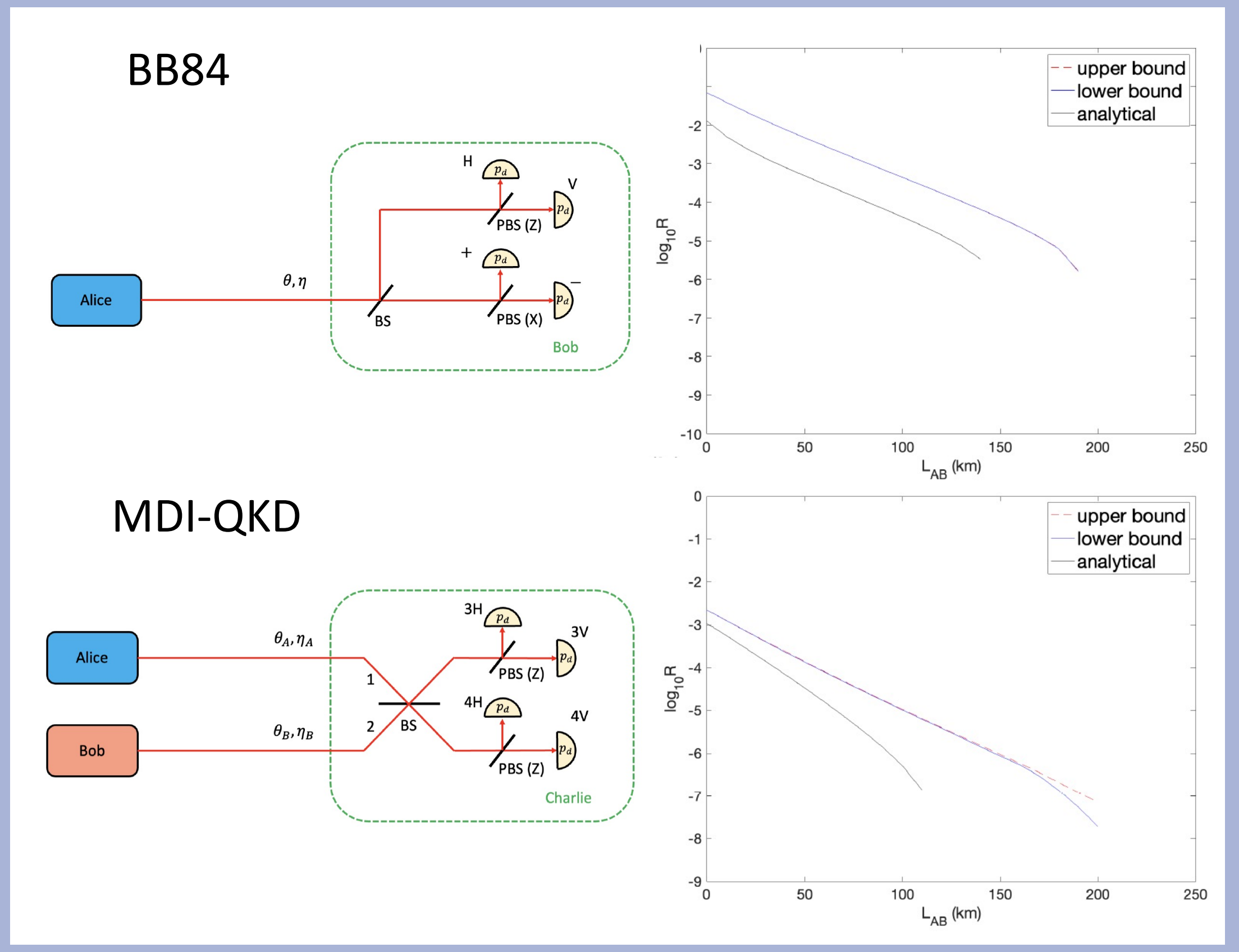
2. Using Fine-Grained Statistics (Continued)

- It is natural for the numerical framework to use the full set of data (including **cross-basis** events), i.e. **"fine-grained statistics*",** in the analysis: more data simply means adding more constraints to the same optimization and a tighter bound. This gives us **more information to characterize the channel**, such as one that contains misalignment.

- When converting raw detector data (e.g. 2^4 pattern for four detectors) to $\{\gamma_k\}$ corresponding to POVMs, **some coarse-graining** (binning) is still needed, either due to the use of a squashing model, or to simply reduce computational requirements. Such coarse-graining can be performed **arbitrarily before or after decoy-state analysis**.

* fine-grained statistics were applied to the numerical framework in [11], while the idea of using discarded data has been studied in multiple previous works [12,13], notably reference-frame-independent (RFI) QKD [13].

Simulation Results



Parameters: dark count rate is 10^{-6}, error-correction efficiency is assumed to be 1, and standard optical fibre of 0.2dB/km loss is used. Both protocols **only consider infinite data**.

For BB84, **a misalignment angle of 0.3 rad** (8.7% error) is assumed. The weaker decoy intensities are 0.02 and 0.001 while signal intensity is optimized at around 0.2-0.4.

For MDI-QKD, **misalignment angles of 0.15 rad each between Alice-Charlie and Bob-Charlie** (8.7% error between Alice and Bob) are assumed. Three intensity settings are fixed at [0.25,0.02,0.001].

- In both cases we observe **considerably higher rate in the presence of misalignment** when we utilize fine-grained statistics.

- Fine-grained statistics can **remove the effect of misalignment on privacy amplification**, but the increased **error-correction** will still cause key rate to decrease with misalignment.

- Like RFI-QKD, we need to assume **a slowly-changing angle and a rotation only along one axis**. However, our approach can be directly applied **to existing setup or data** without physically needing another basis for encoding.

[1] PJ Coles, EM Metodiev, and N Lütkenhaus. Nature Communications 7.1 (2016): 1-9.
[2] A Winick, N Lütkenhaus, and PJ Coles. Quantum 2 (2018): 77.
[3] WY Hwang, Physical Review Letters 91 (2003): 057901.
[4] HK Lo, X Ma, and K Chen. Physical Review Letters 94 (2005): 230504.
[5] XB Wang, Physical Review A 72 (2005): 012322.
[6] P Rice, and J Harrington. arXiv preprint arXiv: 0901.0013 (2008).
[7] X Ma, B Qi, Y Zhao, HK Lo, Physical Review A 72 (2005): 012326.
[8] CH Bennett, G Brassard. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984).
[9] HK Lo, M Curty, B Qi. Phys. Review Letters 108 (2012): 130503.
[10] NKH Li, and N Lütkenhaus. Physical Review Research 2 (2020): 043172.
[11] I George, J Lin, N Lütkenhaus. Physical Review Research 3 (2021): 013274.
[12] M Curty, M Lewenstein, and N Lütkenhaus. Physical Review Letters 92 (2004): 217903.
[13] A Laing, V Scarani, JG Rarity, JL O'Brien. Physical Review A 82 (2010): 012304.