Security of decoy-state QKD with faulty phase randomization

Guillermo Currás-Lorenzo and **Xoel Sixto**

in collaboration with **Shlok Nahar, Kiyoshi Tamaki, Norbert Lütkenhaus** and **Marcos Curty**

Introduction

Although the **standard BB84 protocol** assumes the emission of **single photons**, ideal **single-photon sources** remain **difficult**.

In practice: Phase-randomized attenuated laser pulses

→ Classical **mixture** of **photon-number states**

$$\rho_{\mathrm{PR}}^{\mu} = \int_0^{2\pi} \frac{d\theta}{2\pi} \left|\sqrt{\mu}e^{i\theta}\middle\rangle\middle\langle\sqrt{\mu}e^{i\theta}\right| = \sum_{n=0}^{\infty} p_{n|\mu} \left|n\middle\rangle\middle\langle n\right|$$

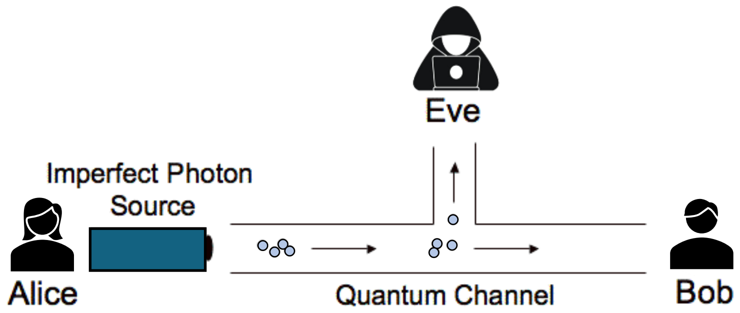
Phase-randomized weak coherent pulse (PR-WCP)

$p_{n|\mu} = e^{\mu}\mu^{n}/n!$ Poisson distribution

Since $\mu < 0.5$, most emissions have **zero** or **one photons**, but **some** have **multiple.**

PNS attack and decoy-state method

Problem: Multiphoton emissions are insecure
because of photon-number splitting attack[1].



Decoy-state method[2]

Emit pulses with **different intensities** → **Statistically characterize** the effect of the quantum channel on **single-photon states**

↓

bound Eve's information and **distill** a **secret key**

- **Same key-rate scaling** as with **ideal single-photon source**.
- **Most QKD implementations** and **commercial systems** use it.

[1] Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Phys. Rev. Lett. 85, 1330–1333 (2000).
[2] Lo, H.-K., Ma, X. & Chen, K. *Phys. Rev. Lett.* **94**, 230504 (2005); Wang, X.-B. *Phys. Rev. Lett.* **94**, 230503 (2005).

Imperfect phase randomization

Fundamental assumption

The **phase** of **each pulse** is **independent** and **uniformly random**

$$\rho_{\mathrm{PR}}^{\mu} = \int_0^{2\pi} \frac{d\theta}{2\pi} \left|\sqrt{\mu}e^{i\theta}\middle\rangle\middle\langle\sqrt{\mu}e^{i\theta}\right| = \sum_{n=0}^{\infty} p_{n|\mu} \, |n\rangle\langle n|$$

Two experimental approaches for phase randomization:

- **Passive:** Turn the laser on and off between pulses.
- **Active**: Modulate a random phase value into the pulse.

In practice, it may not be possible to satisfy this condition perfectly.

➡ **Existing proofs may not be able to guarantee the security of many QKD experiments and commercial systems.**

We have developed two security analyses that address this problem

Passive phase randomization

The laser is **turned on** and **off** between pulses via **gain switching**, **assuming** that the phases will be **completely random**.

However, **experiments**[1,2] have found **correlations** between the phases of consecutive pulses, especially when the sources are run at **high speeds**.

We have **developed** a **security proof** that **takes into account** these **correlations**:

arXiv:2210.08183

Security of quantum key distribution with imperfect phase randomisation

The performance of quantum key distribution (QKD) is severely limited by multiphoton emissions, due to the photon-number-splitting attack. The most efficient solution, the decoy-state method, requires that the phases of all transmitted pulses are independent and uniformly random. In practice, however, these phases are often correlated, especially in high-speed systems, which opens a security loophole. Here, we address this pressing problem by providing a security proof for decoy-state QKD with correlated phases that offers key rates close to the ideal scenario. Our work paves the way towards high-performance secure QKD with practical laser sources, and may have applications beyond QKD.

[1] T. Kobayashi, A.Tomita, A. Okamoto, Physical Review A **90**, 032320 (2014);
[2] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, H. Zbinden, Applied Physics Letters **117**, 144003 (2020).

Assumptions of our proof

Our proof **does not require full characterization** of the phase probability distribution.
Only needs the following knowledge:

1 **Bound on maximum memory (i.e., correlation length)**

$$f(\phi_i|\phi_{i-1}...\phi_1) = f(\phi_i|\phi_{i-1}...\phi_{i-l_c})$$ for known l_c

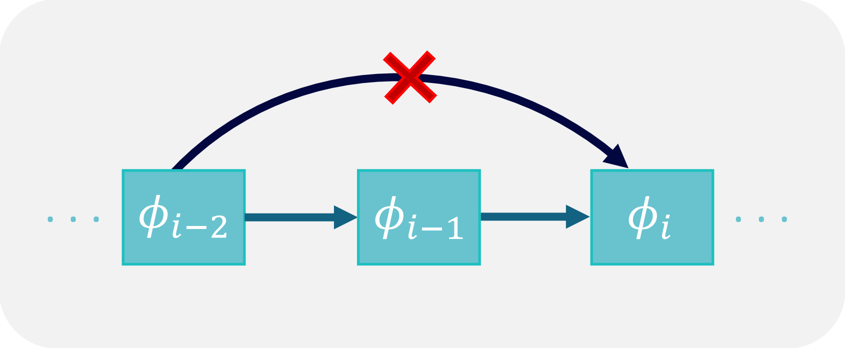
2 **Lower bound on conditional density function**

$$f(\phi_i|\phi_{i-l_c}...\phi_{i-1}\phi_{i+1}...\phi_{i+l_c}) \geq \frac{q}{2\pi},$$ for known q

$0 < q \leq 1$

Quantifies how close the conditional distribution is to ideal case (uniform), given all possible side information (previous and following phases).

E.g., if $l_c = 1$



Security proof (main idea)

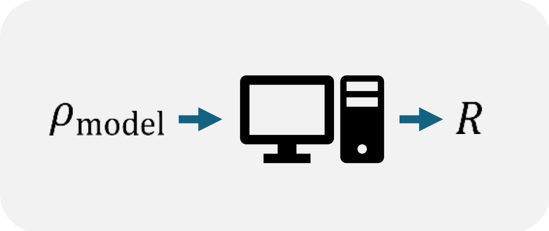
Objective: Show that the actual protocol is **equivalent** to a **scenario** in which Alice's source is **characterized and iid.**

KEY IDEA

Suppose that $\boldsymbol{\rho_{\text{global}} = \mathcal{E}(\rho_{\text{model}}^{\otimes N})}$, where $\boldsymbol{\rho_{\text{model}}}$ is known

➡ **We can assume that Alice generates $\boldsymbol{\rho_{\text{model}}^{\otimes N}}$ and $\boldsymbol{\mathcal{E}}$ is part of the channel**

We can finish the security proof using numerical methods based on semidefinite programming.



* This idea and some proof steps come from:
Nahar, S. MSc Thesis. (University of Waterloo, 2022)

Reduction to uncorrelated scenario (sketch for $l_c = 1$)

Step 1. Divide rounds into even and odd. Prove security independently for each sub-protocol. When proving security of e.g., even sub-protocol, assume that $\vec{\phi}_{\text{odd}} = \phi_1\phi_3$ ... is fixed.

Due to $l_c = 1$, conditioned on $\vec{\phi}_{\text{odd}}$, the state of the even rounds is $\rho_{\text{even}} = \bigotimes_{i \text{ is even}} \rho_{\text{even}}^{(i)}$, where

$$\rho_{\text{even}}^{(i)} = \int_0^{2\pi} d\phi_i f(\phi_i|\vec{\phi}_{\text{odd}}) \, |\mu e^{i\phi_i}\rangle\langle\mu e^{i\phi_i}|$$

Step 2. Due to Ass. 2, $f(\phi_i|\vec{\phi}_{\text{odd}}) \geq q/2\pi$, so:

$$f(\phi_i|\vec{\phi}_{\text{odd}}) = \frac{q}{2\pi} + (1-q) f'(\phi_i|\vec{\phi}_{\text{odd}})$$ where $f'(\phi_i|\vec{\phi}_{\text{odd}}) \geq 0$ is a valid PDF

$$\downarrow$$

$$\rho_{\text{even}}^{(i)} = q \underbrace{\int_0^{2\pi} \frac{d\phi_i}{2\pi} \, |\mu e^{i\phi_i}\rangle\langle\mu e^{i\phi_i}|}_{\rho_{\text{PR}}^{\mu}} + (1-q) \int_0^{2\pi} f'(\phi_i|\vec{\phi}_{\text{odd}}) \, |\mu e^{i\phi_i}\rangle\langle\mu e^{i\phi_i}|$$

Reduction to uncorrelated scenario ($l_c = 1$)

Conditioned on $\vec{\phi}_{\mathrm{odd}}$, the state of the even rounds is $\rho_{\mathrm{even}} = \bigotimes_{i \text{ is even}} \rho_{\mathrm{even}}^{(i)}$, where

$$\rho_{\mathrm{even}}^{(i)} = q\rho_{\mathrm{PR}}^{\mu} + (1-q)\int_0^{2\pi} f'(\phi_i|\vec{\phi}_{\mathrm{odd}})\,|\mu e^{i\phi_i}\rangle\langle\mu e^{i\phi_i}|$$

Step 3. Define: $\rho_{\mathrm{model}} = q\,\rho_{\mathrm{PR}}^{\mu} + (1-q)\,|\sqrt{\mu}\rangle\langle\sqrt{\mu}|$

$\mathcal{E}_i$: Shifts the i-th phase according to the noise PDF $f'(\phi_i|\vec{\phi}_{\mathrm{odd}})$

Then, $\rho_{\mathrm{even}}^{(i)} = \mathcal{E}_i(\rho_{\mathrm{model}})$ ➔ $\boldsymbol{\rho_{\mathrm{even}} = \mathcal{E}\left(\rho_{\mathrm{model}}^{\otimes N/2}\right)}$.

➡ We can prove the security of the even sub-protocol assuming that Alice sends states like ρ_{model}. (Likewise for the odd sub-protocol)

The proof is **generalizable** to **any correlation length l_c**.

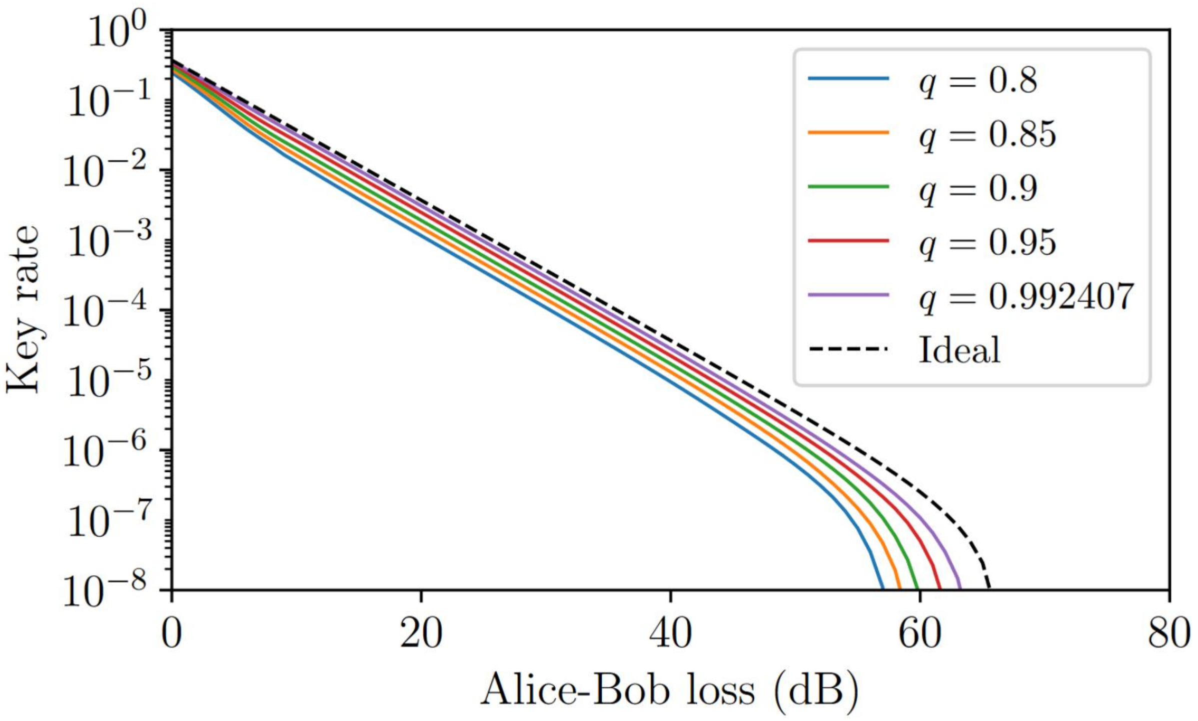
Results

We always prove security assuming that Alice generates $\rho_{\text{model}} = q\,\rho_{\text{PR}}^{\mu} + (1-q)\,|\sqrt{\mu}\rangle\langle\sqrt{\mu}|$

- **Asymptotic key rate only depends on q**

  i.e., how uniform the conditional distribution of each phase is given knowledge of all other phases.

- **We can obtain good key rates even when q is far from ideal!**



The value of q can be characterized using experimental data under reasonable[1] assumptions

(work is under way to develop more rigorous characterization tests – see poster by Alessandro Marcomini)

Using data from a recent 5 GHz experiment[2], we obtain $q = 0.992407$.

Decoy-state QKD with passive phase randomization is robust against correlations!

[1] T. Kobayashi, A.Tomita, A. Okamoto, Physical Review A **90**, 032320 (2014);

[2] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, H. Zbinden, Applied Physics Letters **117**, 144003 (2020).

Active phase randomization

In active phase randomization an **external phase modulator** driven by a **quantum random number generator** is used for phase randomization.

This approach is used in certain applications [1,2,3] like in chip-based QKD.

A security proof to account for **experimental imperfections** in an active setup is needed.

arXiv:2304.03562

Secret key rate bounds for quantum key distribution with non-uniform phase randomization

Xoel Sixto,[1,2,3,*] Guillermo Currás-Lorenzo,[4] Kiyoshi Tamaki,[4] and Marcos Curty[1,2,3]

[1] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[2] *Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[3] *atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[4] *Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*
(Dated: April 10, 2023)

Decoy-state quantum key distribution (QKD) is undoubtedly the most efficient solution to handle multi-photon signals emitted by laser sources, and provides the same secret key rate scaling as ideal single-photon sources. It requires, however, that the phase of each emitted pulse is uniformly random. This might be difficult to guarantee in practice, due to inevitable device imperfections and/or the use of an external phase modulator for phase randomization, which limits the possible selected phases to a finite set. Here, we investigate the security of decoy-state QKD with arbitrary, continuous or discrete, non-uniform phase randomization, and show that this technique is quite robust to deviations from the ideal uniformly random scenario. For this, we combine a novel parameter estimation technique based on semi-definite programming, with the use of basis mismatched events, to tightly estimate the parameters that determine the achievable secret key rate. In doing so, we demonstrate that our analysis can significantly outperform previous results that address more restricted scenarios.

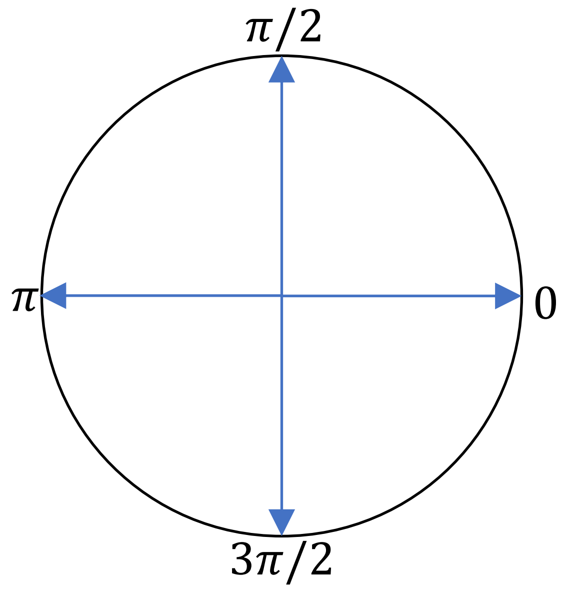
[1] Y. Zhao, B.Qi, H.-K. Lo, Applied Physics Letters **90** 044106 (2007).
[2] P. Sibon *et al*., Nature Communications **8** 13984 (2017).
[3] D. Bunandar *et al*., Physical Review X **8** 021009 (2018).

Generated states in an active scheme

Ideally: The **phase** of **each round** is **independently** and **uniformly random**.

$$\rho_{\mathrm{PR}}^{\mu} = \int_0^{2\pi} \frac{d\theta}{2\pi} \left|\sqrt{\mu}e^{i\theta}\middle\rangle\!\middle\langle\sqrt{\mu}e^{i\theta}\right| = \sum_{n=0}^{\infty} p_{n|\mu} \left|n\middle\rangle\!\middle\langle n\right|$$

In an ideal active scheme: The phase takes one of **N** possible **values** in $[0, 2\pi)$.
The states are **not** perfect **PR-WCP**.



Example for N=4.

The security of this scenario has been analyzed[4] .

However, that work assumes **evenly distributed phases,** but inevitable **imperfections** of the phase modulator and electronic noise might **invalidate this assumption**.

[4] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New Journal of Physics **17**, 053014 (2015).

Cases of interest

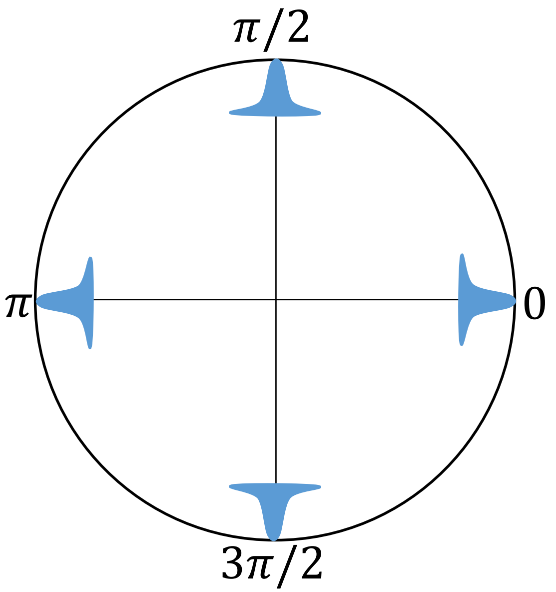
Realistically: In an **active** phase randomization **scheme**, the phase distribution follows a certain **PDF** $\boldsymbol{f(\theta)}$.

$$\rho^{\mu}_{[f(\theta)]} = \int_0^{2\pi} f(\theta)\hat{P}(|\sqrt{\mu}e^{i\theta}\rangle)d\theta = \sum_{n=0}^{\infty} p_{n|\mu,f(\theta)}\hat{P}(|\psi_{n,\mu,f(\theta)}\rangle)$$

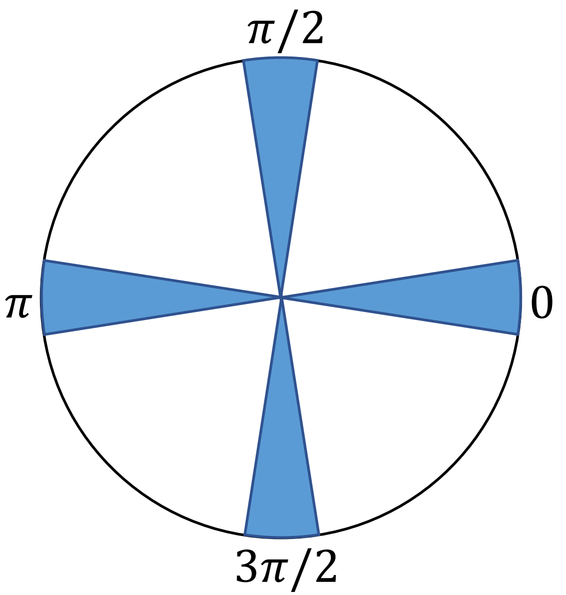
Where $\hat{P}(|\phi\rangle) = |\phi\rangle\langle\phi|$.

Our results are applicable for **any PDF** $\boldsymbol{f(\theta)}$. For simplicity we consider two cases:

Noisy discrete-phase randomization



Partially known $\boldsymbol{f(\theta)}$



Key ideas of the security proof

The previous security proof for passive randomization requires that $f(\theta)$ satisfies $\boldsymbol{f(\theta) \geq q > 0}$ for all θ, where q is a known **non-zero** parameter.

In the case of active phase randomization, only a discrete number of phases is selected, and therefore there might be many values of the phase such that $\boldsymbol{f(\theta) = 0}$.

Despite this, we can **adapt** the previous parameter estimation technique to the active scenario.

We also employ certain inequalities based on the **Bures distance** to evaluate the key rate in the partially known $f(\theta)$ case.

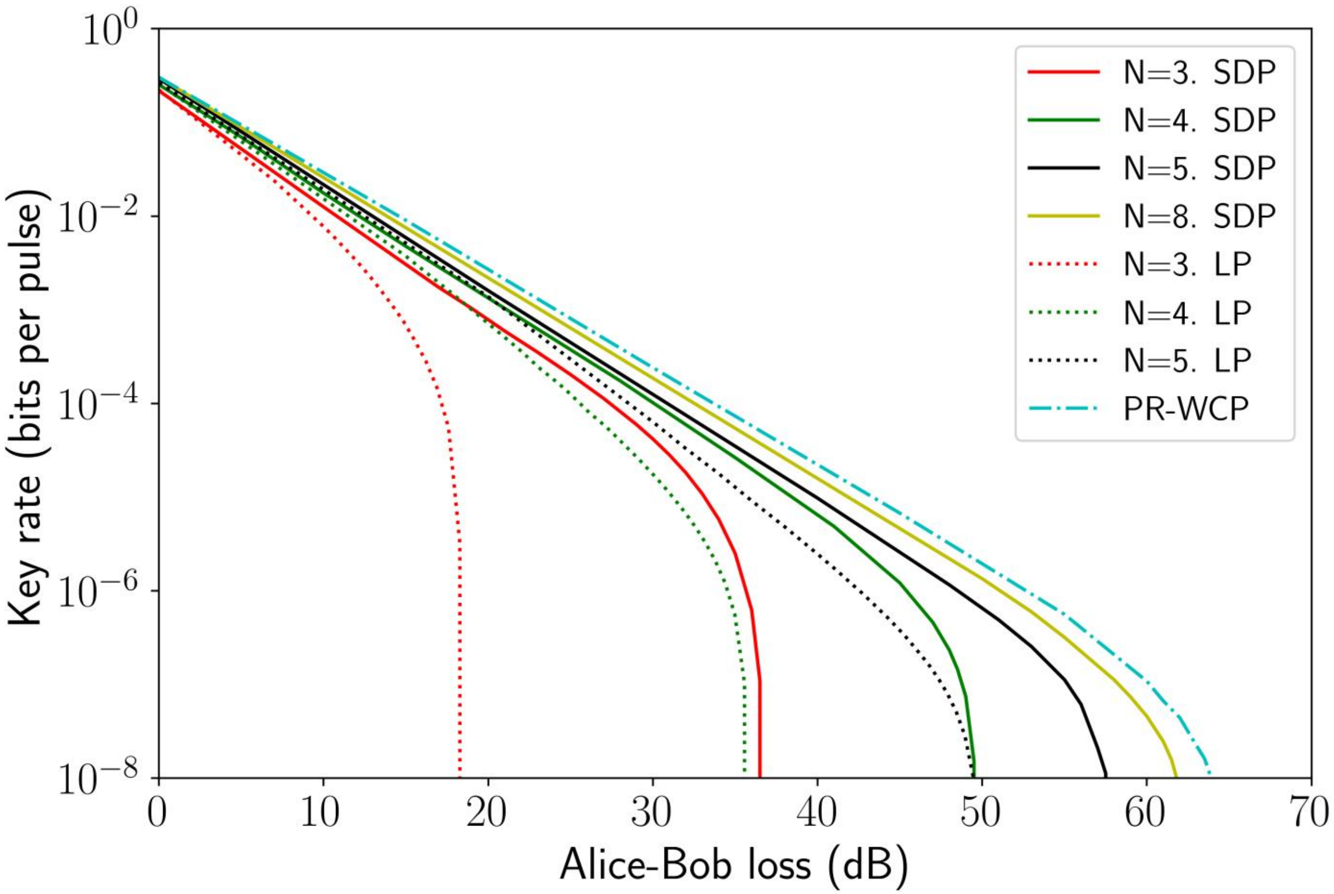
By combining a parameter estimation technique based on **SDP** with **basis mismatched events**, we significantly **improve the performance for the ideal discretization case**.

Results for ideal active phase randomization

For a standard channel model observed an **enhancement** of approximately **10 to 20 dB** in performance when compared to previous works[4].

Just with N=8 the performance is close to the ideal PR-WCP scenario.

The use of basis mismatched events yields a more noticeable improvement when N is low.

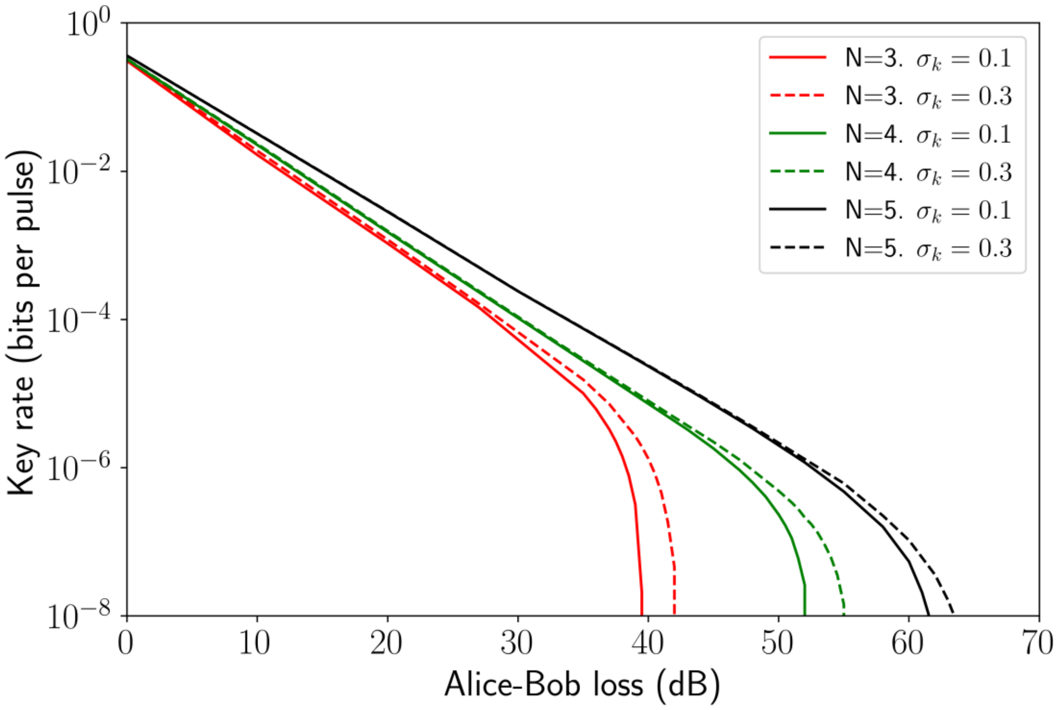


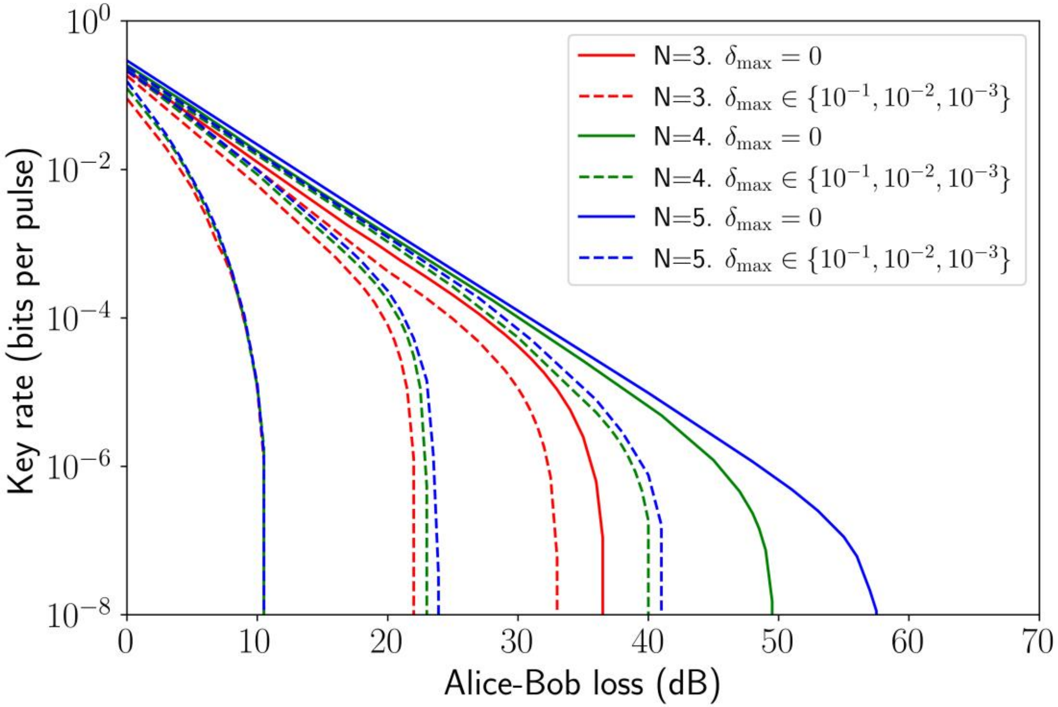
Results for realistic active phase randomization

For the **noisy** scenario we assume that each pulse follows a Gaussian distribution around the selected discrete value.

1. The performance **increases** with the **standard deviation**.

2. Our analysis is applicable regardless of the exact PDF.





When the PDF is not fully characterized the performance **drops** significantly

Characterizing the PDF of an active configuration is a **very relevant experimental task**.

THANK YOU FOR YOUR ATTENTION!