Finite-key analysis of loss-tolerant QKD based on random sampling theory

Phys. Rev. A 104, 012406 (2021)

Guillermo Currás-Lorenzo[1], Álvaro Navarrete[2], Margarida Pereira[2] and Kiyoshi Tamaki[3]

[1]School of Electronic and Electrical Engineering, University of Leeds, Leeds, United Kingdom
[2]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[3]Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

Motivation

To prove the security of QKD, the crucial step is typically to **bound** the **phase-error rate**.

Basis independent protocols ($\rho_Z = \rho_X$)

In BB84, the observed X-basis bit-error rate (e_X) provides a **random sample** for the Z-basis phase-error rate (e_{ph}). In the asymptotic regime, $e_X = e_{\text{ph}}$.

In the finite-key regime, obtaining a bound on e_{ph} is a **random sampling problem**. It can be solved using concentration inequalities for sums of **independent RVs** (e.g. **Chernoff bounds**)

Basis dependent protocols ($\rho_Z \neq \rho_X$)

This may be due to the **inherent design** of the protocol, or to **source flaws**.
In this case, **Eve can learn information** about Alice's **basis choice**.

The X-basis bit-error rate **no longer provides a random sample** for the Z-basis phase error rate.

Moreover, **under** a **coherent attack**, the **detection statistics** of a round can **depend on** the **basis choices** made in **other rounds**.

Difficult to apply concentration inequalities for independent RVs.

To deal with these correlations, security proofs typically use **Azuma's inequality** for sums of **dependent RVs**.
Problem: Less tight than Chernoff bounds → **Worse finite-key performance**.

Can we apply random sampling to basis-dependent protocols?

Loss-tolerant (LT) QKD

Proposed to deal with **imperfect sources** that suffer from **state preparation flaws** → **Basis dependent** protocol

Alice sends just **three states**. Their only assumption is that they are characterised and in the same qubit space.

Easy to implement experimentally, and in the asymptotic regime, can provide an al**most identical performance** to a **perfect BB84** protocol.

In the finite-key regime, previous security proofs used **Azuma's inequality**, which results in a significant **performance drop.**

Our work: Tighter finite-key security analysis based on random sampling theory.

Two steps:
1. Show an equivalence to a hypothetical scenario by assigning tags;
2. Apply a random sampling argument to the hypothetical scenario.

#2: Hypothetical scenario

Alice sends three states, ρ_{vir}, ρ_{pos}, and ρ_{neg}, satisfying

$$\rho_{\text{vir}} = |c_{\text{pos}}|\rho_{\text{pos}} - |c_{\text{neg}}|\rho_{\text{neg}}$$

In this scenario, the # of detections of ρ_{pos}, and ρ_{neg} can be directly observed, but the # of detections of ρ_{vir} cannot.

Using similar arguments as in Ref. [2], we show that **obtaining a bound** on the **# of detections of ρ_{vir}** can be reduced to a **random sampling problem** and solved using Chernoff bounds.

#1: Reduction to scenario in #2

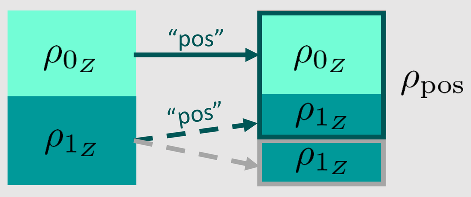
In the LT protocol, the **phase-error rate** can be **estimated** by considering the **detection statistics** of two "virtual" states, $\boldsymbol{\rho_{\text{vir}_0}}$ **and** $\boldsymbol{\rho_{\text{vir}_1}}$, which are not emitted in the actual protocol.

We show that, because they are in the same qubit space as the actual states, one can always **express them as an (operator-form) linear combination of the actual states**. Example:

$$\rho_{\text{vir}_1} = \underbrace{\rho_{0_Z} + \frac{1}{2}\rho_{1_Z}}_{\frac{3}{2}\rho_{\text{pos}}} - \underbrace{\frac{1}{2}\rho_{0_X}}_{\frac{1}{2}\rho_{\text{neg}}}$$

which is similar to the scenario in #2, but here Alice does not actually emit ρ_{pos}.

Solution: Alice probabilistically assigns a tag of pos to her emissions of $\boldsymbol{\rho_{0_Z}}$ and $\boldsymbol{\rho_{1_Z}}$, in such a way that the average state with a tag of pos is $\boldsymbol{\rho_{\text{pos}}}$.

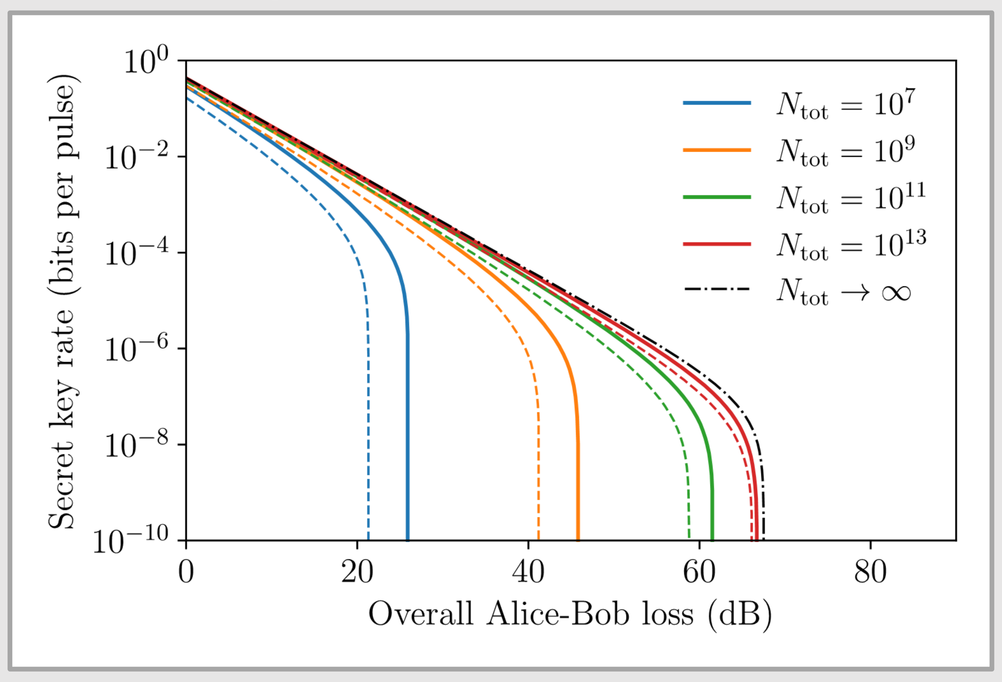


In general, we show that Alice can always assign random tags of pos and neg to her emissions, in such a way that the average state with a tag of pos (neg) is ρ_{pos} (ρ_{neg}).

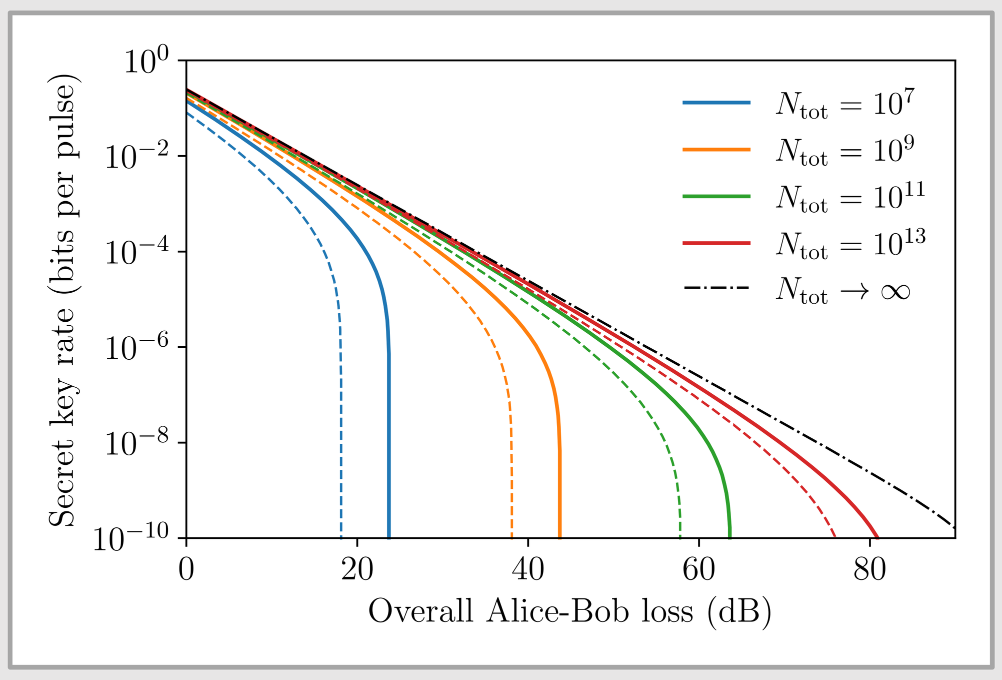
Thanks to this, we find an equivalence to the scenario in #2, allowing us to apply its random sampling argument to estimate the detection statistics of the virtual states, and thus the **phase-error rate**.

Results

Prepare-and-measure LT



Measurement-device-independent LT



solid – our work
dashed – previous work based on Azuma's inequality [1]

Conclusions

- Our work: finite-key security analysis of loss-tolerant QKD based on random sampling theory.
- Can be applied to the PM and MDI versions.
- Offers better results than the previous analysis based on Azuma's inequality.

References

[1] Mizutani, A., Curty, M., Lim, C. C. W., Imoto, N., & Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* 17, 093011 (2015).
[2] Maeda, K., Sasaki, T. & Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat Commun* 10, 3140 (2019).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662.