Towards a Finite Size Analysis of Decoy-State Quantum Key Distribution with Advantage Distillation

Philipp Kleinpaß, Jonas Treplin, Davide Orsucci

German Aerospace Center (DLR), Institute of Communications and Navigation

Abstract

Quantum Key Distribution (QKD) allows two legitimate parties, Alice and Bob, to share a secret key with information-theoretic security, ensuring that an eavesdropper, Eve, cannot obtain any information about the key. A QKD protocol is provably secure only when the Quantum Bit Error Rate (QBER) is below a certain threshold and, therefore, the presence of noise inherently limits the maximum transmission distance. Advantage Distillation (AD) is a classical post-processing technique that enhances QKD protocols by increasing the maximum acceptable QBER and, thus, allows extending the communication range. AD operates by post-selecting blocks of bits and extracting fewer but highly correlated bits between Alice and Bob, which exhibit a reduced QBER, thus lowering the amount of information that has to be disclosed during the information reconciliation step. In this study, we present a new analytical expression for the secure key rate. This will enable a finite-size secure key length analysis of the decoy state version of the BB84 protocol including AD post-processing.

Prepare and Measure Quantum Key Distribution

With one-way classical communication between Alice and Bob the secure key rate for any prepare and measure QKD protocol is given by [1]:

$$R_{\text{one-way}} = H(A|E) - H(A|B)$$

The key rate is lower bounded by the expression

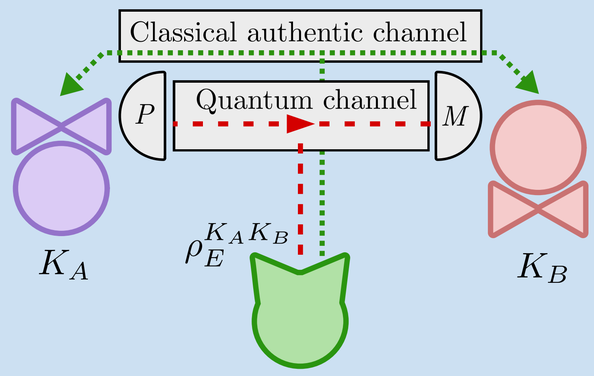
$$R_{\text{one-way}} \geq \min_{\phi_X,\phi_Y,\phi_Z} \left[1 - (1-\phi_Z)\, h\left(\frac{\phi_X+\phi_Y-\phi_Z}{2(1-\phi_Z)}\right) - \phi_Z\, h\left(\frac{\phi_X-\phi_Y+\phi_Z}{2\phi_Z}\right) - h(\phi_Z)\right]$$

where the minimisation is performed over the possible QBERs ϕ_X, ϕ_Y, ϕ_Z in the X, Y, Z bases that are compatible with parameter estimation.

In BB84 the value of ϕ_Y is never directly observed, hence it can only be bounded by $|\phi_X - \phi_Z| \leq \phi_Y \leq \phi_X + \phi_Z$. The minimisation can be carried out analytically, yielding

$$R_{\text{BB84}} \geq \min_{\phi_X,\phi_Z} [1 - h(\phi_X) - h(\phi_Z)] \qquad \text{with} \qquad \phi_Y = \phi_X + \phi_Z - 2\phi_X\phi_Z$$

For $\phi_X = \phi_Z = \phi$ the maximum tolerable QBER is $\phi \approx 11.0\%$ with one-way communication and $\phi \approx 18.7\%$ with two-way communication [2].



Classical Advantage Distillation

AD(*b*): advantage distillation protocol with block length *b* [3]

1. Alice and Bob partition their bit strings into blocks of b bits:
   - $(a_1, a_2, \ldots, a_b) \in \mathbb{Z}_2^b$ for Alice,
   - $(a'_1, a'_2, \ldots, a'_b) \in \mathbb{Z}_2^b$ for Bob.
2. Alice computes the parities $(a_1 \oplus a_2, \ldots, a_{b-1} \oplus a_b) \in \mathbb{Z}_2^{b-1}$ and sends them to Bob.
3. Bob computes the parities $(a'_1 \oplus a'_2, \ldots, a'_{b-1} \oplus a'_b) \in \mathbb{Z}_2^{b-1}$ and compares them with Alice's.
4. If any of the $b-1$ parities does not match:
   - The post-selection fails and all the b bits are discarded.
5. Else:
   - Alice keeps a_1 and Bob keeps a'_1 (discarding the other $b-1$ bits).

Properties of Advantage Distillation

- After post-selection either all of Bob's bits are correct $(a'_1, \ldots, a'_b) = (a_1, \ldots, a_b)$ or all of Bob's bits are incorrect $(a'_1, \ldots, a'_b) = (a_1 \oplus 1, \ldots, a_b \oplus 1)$.
- The success probability and the QBER on the post-selected bits are

$$p_{\text{succ}} = (1-\phi)^b + \phi^b \qquad \overline{\phi} = \frac{\phi^b}{(1-\phi)^b + \phi^b}$$

- Intuitively, in AD Alice and Bob exploit the authentic channel to post-select bits where the information they share is more than Eve's.
- Remarkably, Alice and Bob can establish a secure key even if Eve has more information about Alice's original key than Bob.

Quantum Advantage Distillation

In QKD, AD is applied only in the Z basis, while X and Y bases may be used for Parameter Estimation (PE). This can be interpreted as working with qubits having different QBERs:

$$\overline{\phi}_X = \frac{1}{2} - \frac{(1-\phi_Y-\phi_X)^b + (\phi_Y-\phi_X)^b}{2p_{\text{succ}}}$$
$$\overline{\phi}_Y = \frac{1}{2} - \frac{(1-\phi_Y-\phi_X)^b - (\phi_Y-\phi_X)^b}{2p_{\text{succ}}}$$
$$\overline{\phi}_Z = \frac{\phi_Z^b}{p_{\text{succ}}}$$

In the real protocol, parameter estimation has to be applied before AD. In BB84 only the X basis is employed for parameter estimation, while the Z basis is used for key generation.

AD corresponds to a BB84 protocol with the following measurements on virtual qubits:

	BB84		**BB84 + AD**		
	Key	PE	Parity	Key	PE
	$Z \otimes Z$	$X \otimes X$	$Z^{\otimes b}$	$Z \otimes I^{\otimes b-1}$	$X^{\otimes b}$
	$Z \otimes Z$	$X \otimes X$	$Z^{\otimes b}$	$Z \otimes I^{\otimes b-1}$	$X^{\otimes b}$

Here $\overline{Z} = Z \otimes I^{\otimes b-1}$ is the key-basis measurement and $\overline{X} = X^{\otimes b}$ is used for eavesdropper monitoring, analogously to Z and X measurements in standard BB84.

- $\overline{Z}$ and $\overline{X}$ are mutually unbiased
- $\overline{Z}$ and $\overline{X}$ commute with the parity measurements employed in AD post-selection
- $\overline{Z}_A \otimes \overline{Z}_B$ and $\overline{X}_A \otimes \overline{X}_B$ are associated to the QBER measurements, *conditioned on the AD post-selection succeeding*

Asymptotic Key Rate with AD

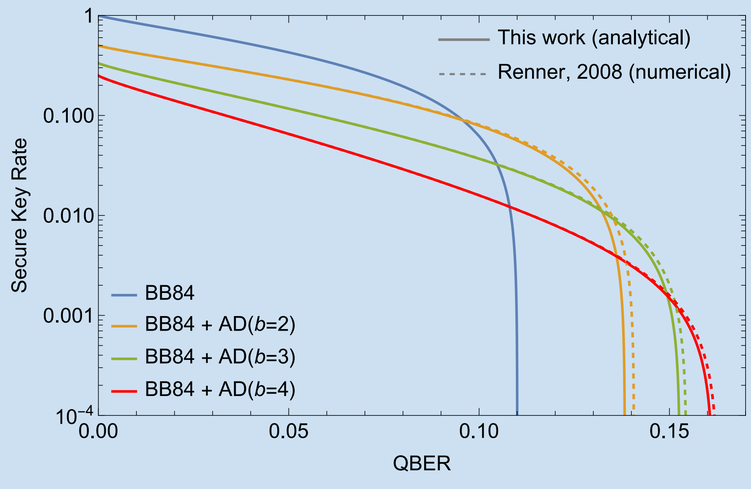
The secure key rate for BB84 + AD(b) can be expressed as:

$$R_{\text{AD}(b)} \geq \min_{\phi_X,\phi_Y,\phi_Z} \frac{p_{\text{succ}}}{b} [1 - h(\overline{\phi}_X) - h(\overline{\phi}_Z)]$$

The minimisation is performed on the QBERs prior to AD and can be carried out explicitly. In contrast to the standard BB84 case, the minimum is attained for the extreme value $\phi_Y = \phi_X + \phi_Z$, resulting in

$$R_{\text{AD}(b)} \geq \min_{\phi_X,\phi_Z} \frac{p_{\text{succ}}}{b} \left[1 - h\left(\frac{(1-\phi_Z)^b - (1-\phi_Z-2\phi_X)^b}{2p_{\text{succ}}}\right) - h\left(\frac{\phi_Z^b}{p_{\text{succ}}}\right)\right]$$

This yields a very good approximation of the achievable key rate:



This enables the analytical extension of the results to decoy state estimation and finite size key analysis – work in progress!

References

[1] Renato Renner. "Security of quantum key distribution." International Journal of Quantum Information 6.01 (2008).

[2] Daniel Gottesman and Hoi-Kwong Lo. "Proof of security of quantum key distribution with two-way classical communications." IEEE Trans. on Inf. Theory 49.2 (2003).

[3] Ueli M. Maurer. "Secret key agreement by public discussion from common information." IEEE Trans. on Inf. Theory 39.3 (1993).

Acknowledgements

This work was done within the project QuNET funded by the German Federal Ministry of Education and Research under the code 16KIS126.

Deutsches Zentrum für Luft- und Raumfahrt