KEY RATE RELIABLE LOWER BOUND FOR BB84 PROTOCOL

Sebastiano Cocchi

October 13, 2021

Abstract

Following George u. a. (2021) and Winick u. a. (2018) papers, a key rate reliable lower bound for the standard four states BB84 protocol is calculated in condition of:

1. depolarizing channel;
2. efficiency mismatch at receiver detectors.

The simulation includes the announcement of the bases between A and B, the sifting phase and a key map that stores the choice of the bases of A and B in a classic register. The goal of the simulation is to minimize the relative entropy using a semidefinite program (SDP) before and after the application of a pinching channel. The result is a lower bound for the key rate.

Contents

1 Theory

Quantum key distribution (QKD) allow two distant parties, generally called Alice and Bob, to share a key with unconditional security. QKD protocols communicate upon a quantum channel and a classical channel.

Quantum channel is untrusted, public and unauthenticated so an eavesdropper, typically called Eve, can manipulate the message. Alice uses quantum channel to send qubits to Bob.

Classical channel is public and authenticated, so Alice and Bob recognize each other. Alice and Bob communicate via classical channel to perform error correction and privacy amplification in order to extract the key.

Source replacement scheme

In prepare and measure (P&M) schemes, Alice choose randomly the signal states $\{|\phi_i\rangle\}_{i=1}^N$ with probability p_i in which encode the key bits and sends to Bob the sequence through a quantum channel; Bob randomly choose a detection basis. In the entangled based (EB) schemes, a bipartite state ψ_{AB} is sent to Alice and to Bob; Both Alice and Bob choose randomly the measurement basis.

P&M schemes can be transposed into EB schemes using the so-called source-replacement scheme, since EB schemes are more natural to describe the joint system between Alice and Bob.

In the source-replacement scheme Alice creates the bipartite entangled state(Ferenczi und Lütkenhaus (2012))

$$|\psi\rangle = \sum_{i=1}^{N} \sqrt{p_i}\, |i\rangle_A \, |\phi_i\rangle_{A'},$$

where $\{|i\rangle\}_{i=1}^{N}$ is a basis of the Hilbert space $\mathcal{H}^N$. Alice keeps A and sends A' to Bob via quantum channel $\mathcal{E}_{AB}$ which transforms $A' \to B$. For example, if the channel introduces depolarization with a probability p on a qubit ρ,

$$\mathcal{E}_{AB}(\rho) = \sum_{i=1}^{4} E_i \rho E_i^\dagger \tag{1}$$

where, using the Pauli matrices $\{\sigma_i\}$, $E_1 = \sqrt{1 - \frac{3}{4}p}\,\mathbb{I}_2$, $E_2 = \sqrt{p/4}\sigma_x$, $E_3 = \sqrt{p/4}\sigma_y$ and $E_4 = \sqrt{p/4}\sigma_z$. The state shared between Alice and Bob is denoted by ρ_{AB}.

Post-prococessing

The post-processing phase can be divided into:

1. parameter estimation: Alice and Bob compute statistics on an announced random data set and agree if proceed or aborting the communication;
2. public string announcement: Alice and Bob choose part of their bits, respectively $\tilde{A}_i$ and $\tilde{B}_i$ and communicate it over the classical channel. Alice and Bob also keep private part of the key in the sequences $\bar{A}_j$ and $\bar{B}_j$;
3. sifting phase: using the public string, Alice and Bob agree only on qubits measured in the same basis;
4. key map: Alice performs a key map function able to extract a key based on her public and private sequence and Bob's public sequence;
5. error correction: using classical methods, Alice and Bob agree on a shorter, but correlated, key symbols. As proven by Shannon, this leakage is bounded by the mutual information $I(A:B) = H(A) + H(B) - H(AB) = 1 - leak_{EC}$ where H is the Shannon entropy.

Alice and Bob POVM $\{P_i^A\}$ and $\{P_j^B\}$ are the possibles measurements on the qubits, with outcomes

$$\mathrm{Tr}\Big[(P_i^A \otimes P_j^B)\rho_{AB}\Big] = p_{ij}. \tag{2}$$

As an anticipation, these p_{ij} defines the constraints of the SDP minimization. For P&M schemes there are additional constraints, due to the fact that Eve cannot gain any information about the system A, so

$$\mathrm{Tr}\Big[(\Theta_i^A \otimes \mathbb{I}^B)\rho_{AB}\Big] = \theta_i, \tag{3}$$

where $\{\Theta_i\}_{i=1}^{dim\mathcal{H}_A}$ is a complete set of hermitian operators of $\mathcal{H}_A$. For EB schemes the $\{p_{ij}\}$ constraints defines a set of possibles states

$$S^{EB} = \Big\{\rho_{AB} | \mathrm{Tr}\Big[(P_i^A \otimes P_j^B)\rho_{AB}\Big] = p_{ij}\Big\}$$

while for P&M schemes the constraints are $\{p_{ij}, \theta_i\}$ defining a set

$$S^{P\&M} = \Big\{\rho_{AB} | \mathrm{Tr}\Big[(P_i^A \otimes P_j^B)\rho_{AB}\Big] = p_{ij}, \mathrm{Tr}\Big[(\Theta_i^A \otimes \mathbb{I}^B)\rho_{AB}\Big] = \theta_i\Big\}.$$

To maintain a more general approach, I refer both to S^{EB} and S^{AB} with S.

The public string announcement is represented by the following Kraus representation for Alice

$$K_a^A = \sum_{\bar{a}} \sqrt{P_{a,\bar{a}}^A}\, |a\rangle_{\tilde{A}} \, |\bar{a}\rangle_{\bar{A}}$$

and for Bob

$$K_b^B = \sum_{\bar{b}} \sqrt{P_{b,\bar{b}}^B}\, |b\rangle_{\tilde{B}} \, |\bar{b}\rangle_{\bar{B}}$$

where (a,b) are the public parts of Alice and Bob key and $\bar{a},\bar{b}$ are the private one. The two representations act on the system AB as completely positive and trace preserving (CPTP) map

$$\rho^1_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \sum_{a,b}(K_a^A \otimes K_b^B)\rho_{AB}(K_a^A \otimes K_b^B)^\dagger = \mathcal{A}(\rho_{AB}). \tag{4}$$

Then sifting phase is performed. Let $\mathbf{A}$ be the set of all announcements that are kept. Thus, post-selection can be seen as a projector

$$\Pi = \sum_{(a,b)\in\mathbf{A}} |a\rangle\langle a|_{\tilde{A}} \otimes |b\rangle\langle b|_{\tilde{B}} \to \rho^2_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \frac{\Pi\rho^1_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}}\Pi}{p_{pass}} \tag{5}$$

where $p_{pass} = \mathrm{Tr}[\rho_{AB}\Pi]$ gives the probability of passing the post-selection.

Alice chooses a key map, *i.e.* a function that, depending on Alice public and private parts $(a,\bar{a})$ and Bob announcement b, returns a value $g(a,\bar{a},b)$. The value of the key map can be thought to be stored in a classical register called R, so the key map operator is represented by an isometry

$$V = \sum_{a,\bar{a},b} |g(a,\bar{a},b)\rangle_R |a\rangle_{\tilde{A}} |\bar{a}\rangle_{\bar{A}} |b\rangle_{\tilde{B}} \to \rho^3_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} = V\rho^2_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}}V^\dagger. \tag{6}$$

If R contains J symbols, the register turns out to be a classical register after applying a pinching channel on $R \to Z^R$

$$\mathcal{Z}(\rho) = \sum_{j=1}^{J}(|j\rangle\langle j|_R \otimes \mathbb{I})\rho(|j\rangle\langle j|_R \otimes \mathbb{I}) \to \rho^4_{Z^RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \mathcal{Z}(\rho^3_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}}) \tag{7}$$

where the identity acts over all the other dimensions.

Reliable lower bound

Eve can use whatever strategy to extract as much information as possible from ρ_{AB}:

1. individual attacks, Eve acts on a single qubit and performs her treatment on it before the classical post-processing phase;

2. collective attacks, Eve performs measurements after the post-processing phase on all the qubits she has gained.

The simulation works under the assumption of identically and independently distributed (i.i.d.) collective attack, so it is possible to simulate only one qubit reducing drastically the dimension of the system.

The aim is to estimate the best attack Eve can do on ρ_{AB}. Following George u. a. (2021) and Winick u. a. (2018), the constraints of the problem are given by Alice and Bob POVM in (2) and (3).

The function to be minimized is the relative entropy $D(\rho||\sigma)$ (also called Kullback–Leibler divergence), which is a measure of how one probability distribution is different from a second. In particular, the simulation consider the divergence

$$f(\rho_{AB}) = D\left(\rho^3_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}}\middle|\middle|\rho^4_{Z^RA\tilde{A}\bar{A}B\tilde{B}\bar{B}}\right). \tag{8}$$

having defined the states as

$$\rho^3_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} = G(\rho_{AB}),$$
$$\rho^4_{Z^RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \mathcal{Z}(G(\rho_{AB}))$$

where the G map is defined by

$$G(\rho_{AB}) = V\Pi\mathcal{A}(\rho_{AB})\Pi V^\dagger$$

and $\mathcal{Z}$ map is defined in (7). The gradient of $f(\rho_{AB})$ is then

$$\nabla f(\rho)^T = G^\dagger(\log_2(G(\rho_{AB}))) - G^\dagger(\log_2(\mathcal{Z}(G(\rho_{AB}))))$$

If the post-selection process involves only a sifting and announcement phase, then the dimension reduces only to system AB without other registers. Suppose $\{Z_i^A\}$ is the Alice key map POVM, then (8) reduces to

$$f(\rho_{AB}) = D\left(\rho_{AB}\middle|\middle|\sum_i (Z_i^A \otimes \mathbb{I}_B)\rho_{AB}(Z_i^A \otimes \mathbb{I}_B)\right). \tag{9}$$

The key rate is

$$\begin{aligned} K =& p_{pass} \cdot \min_{\rho_{AB}} \Big(H(Z^R|E\tilde{A}\tilde{B}) \Big) - p_{pass} \cdot leak^{EC} = \\ =& \min_{\rho_{AB} \in S^m} D\left(G(\rho_{AB}) \| \mathcal{Z}(G(\rho_{AB}))\right) - leak^{EC} \\ =& \min_{\rho_{AB}\rho_{AB} \in S^m} f(\rho_{AB}) - leak^{EC} \end{aligned} \tag{10}$$

where Z^R is the classical register shared by Alice and Bob, and $E\tilde{A}\tilde{B}$ is the portion of the system where Eve has complete access without any disturbance on A and B.

Quantum relative entropy is a convex function, thus $f(\rho)$ is a convex function in ρ and can be minimized using a semidefinite program (SDP). Due to computer imprecision, the algorithm may exit before reaching the true lower bound. Thus, the problem is converted to its dual in order to find the upper bound. Then, the strategy is to split the algorithm into two steps: a primal problem and a dual problem.

The primal problem with m variables is defined as

$$\begin{aligned} \min_{X \in S^m} :& \langle C, X \rangle_{S^m} \\ \text{subject to :}& \langle A_i, X \rangle_{S^n} = b_i, \quad i = 1, \ldots, m \\ & X \geq 0. \end{aligned} \tag{11}$$

The dual of this problem is

$$\begin{aligned} \max_{y \in \mathbb{R}^n} :& \sum_i b_i y_i \\ \text{subject to :}& \sum_i A_i y_i \leq C. \end{aligned} \tag{12}$$

These two steps have two different scopes:

step 1 : estimation of the optimal attack Eve can apply to the qubits which gives an upper bound on the key rate;

step 2 : study the inverse problem finding the reliable lower bound.

Let's see in details the step 1 algorithm:

Algorithm 1

```
Result: near optimal attack
Parameters: $\epsilon > 0$, $\rho_0 \in S$, $maxIteration \in \mathbb{N}$ and $i = 0$
    1. compute $\Delta\rho = \arg\min_{\delta\rho} \mathrm{Tr}[\delta\rho \nabla f(\rho_i)]$.
       subject to $\Delta\rho + \rho_i \in S$, $\mathrm{Tr}[\Delta\rho] = 0$ and hermiticity $\Delta\rho = (\Delta\rho)^\dagger$;
    2. if $\mathrm{Tr}[\Delta\rho \nabla f(\rho_i)] < \epsilon$ then go to step 2
    3. find $\lambda \in [0,1]$ that minimizes $f(\rho_i + \lambda\Delta\rho_i)$;
    4. set $\rho_i \to \rho_i + \lambda\Delta\rho$;
    5. set $i \to i + 1$;
    6. if $i > maxIteration$ then go to step 2
       .
```

I want to stress the fact that this method does not depend on the state shared by AB. Indeed, the initial density operator ρ_0 can be written as

$$\rho_0 = \sum_{j=1}^{j} \tilde{p}_l \tilde{\Gamma}_l + \sum_{k=1}^{dim\mathcal{H}^2_{AB}-j} \omega_k \Omega_k$$

where $\{\tilde{\Gamma}_l\}_{l=1}^{j} \cup \{\tilde{\Omega}_k\}_{k=1}^{dim\mathcal{H}^2_{AB}-j}$ is complete set of hermitian operators for the system AB. The first sector of this basis, $\{\tilde{\Gamma}_l\}_{l=1}^{j}$, is an orthonormal set of $j < m$ hermitian operators which is created applying the Gram-Schmidt process to $\{\Gamma_j\}_{j=1}^{m}$, which are the m operators generating the constraints in (2) and (3); $\{\Omega_k\}_{k=1}^{dim\mathcal{H}^2_{AB}-j}$ are used to complete the basis.

In step 2, the reliable lower bound is found as a maximization problem. Relative entropy is a highly non-linear function, so it may be difficult to find the dual problem; A solution can be computing the dual of the linearization of the original problem SDP, which reads

$$\max_{\vec{z}\in S^*(\rho)} \vec{z}\cdot\vec{\gamma}, \quad S^*(\rho) = \{z \in \mathbb{R} | \sum_{i=1}^{m} z_i \Gamma_i \leq \nabla f(\rho)\}$$

where $\vec{\gamma} = \{\gamma_1, \ldots, \gamma_m\}$ are the m-constraints of the SDP. Finally, the reliable lower bound for the key rate is

$$\beta(\rho) = f(\rho) - \mathrm{Tr}[\rho \nabla f(\rho)] + \max_{\vec{z}\in S^*(\rho)} \vec{z}\cdot\vec{\gamma},$$

in which is present the result $f(\rho)$ of the step 1.

2 Code development

My simulation is performed on a BB84 protocol, which is a QKD protocol in which bits are encoded using two mutually unbiased bases (MUB) $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$ where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Bit 0 can be encoded by the states $\{|0\rangle, |+\rangle\}$, while bit 1 by the states $\{|1\rangle, |-\rangle\}$.

To implement the theory into a PC simulation I have written a python class called QKD, which automatically elaborates the operators needed if not provided in the initialization of the object. Once the simulation object is created, it is possible to apply quantum channel passing the operators which represent the channel action on the qubit sent from A to B; Then, the class allow computing primal and dual SDP.

The convex optimization is performed in python by the library cvxpy using the solver MOSEK which can be obtained under license here. Otherwise, cvxpy allow the use of license-free solver called CVXOPT or SCS.

The following subsections will bring some examples, in particular:

1. EB standard BB84 protocol;
2. EB standard BB84 protocol with efficiency mismatch at detector.

EB standard BB84 protocol

Suppose both Alice and Bob perform measurements in the Z basis with probability p_z and in the X basis with probability p_x. Alice and Bob POVM are then symmetric

$$\begin{aligned} P_0^A &= p_z |0\rangle\langle 0|_A, & P_0^B &= p_z |0\rangle\langle 0|_B, \\ P_1^A &= p_z |1\rangle\langle 1|_A, & P_1^B &= p_z |1\rangle\langle 1|_B, \\ P_+^A &= (1-p_z) |+\rangle\langle +|_A, & P_+^B &= (1-p_z) |+\rangle\langle +|_B, \\ P_-^A &= (1-p_z) |-\rangle\langle -|_A & P_-^B &= (1-p_z) |-\rangle\langle -|_B. \end{aligned}$$

Then the public announcement is composed by the Kraus operators

$$K_1^A = \sqrt{P_0^A}\,|0\rangle_{\tilde{A}}|0\rangle_{\bar{A}} + \sqrt{P_1^A}\,|0\rangle_{\tilde{A}}|1\rangle_{\bar{A}}, \quad K_2^A = \sqrt{P_+^A}\,|1\rangle_{\tilde{A}}|0\rangle_{\bar{A}} + \sqrt{P_-^A}\,|1\rangle_{\tilde{A}}|1\rangle_{\bar{A}},$$

$$K_1^B = \sqrt{P_0^B}\,|0\rangle_{\tilde{B}}|0\rangle_{\bar{B}} + \sqrt{P_1^B}\,|0\rangle_{\tilde{B}}|1\rangle_{\bar{B}}, \quad K_2^B = \sqrt{P_+^B}\,|1\rangle_{\tilde{B}}|0\rangle_{\bar{B}} + \sqrt{P_-^B}\,|1\rangle_{\tilde{B}}|1\rangle_{\bar{B}},$$

the sifting phase is defined by the projector

$$\Pi = |0\rangle\langle 0|_{\tilde{A}} \otimes |0\rangle\langle 0|_{\tilde{B}} + |1\rangle\langle 1|_{\tilde{A}} \otimes |1\rangle\langle 1|_{\tilde{B}}$$

and the key map is

$$V = |0\rangle_R |0\rangle\langle 0|_{\bar{A}} + |1\rangle_R |1\rangle\langle 1|_{\bar{A}}$$

with identity acting on the other subsystems. These operators define the G map and the problem is completely set.

If the choice of these Kraus operators, sifting and isometry is standard, as in this case, calling the python class QKD will create all the structure described above

```python
from src import qkd
import numpy as np
sim = qkd.QKD(dim_a=2, dim_b=2, n_of_signal_states=4, # of signal states
    list_states_a=[qkd.zero, qkd.one, qkd.plus, qkd.minus], list_of_prob_a=[.25,.25,.25,.25],
    list_states_b=[qkd.zero, qkd.one, qkd.plus, qkd.minus], list_states_b=[.25,.25,.25,.25])
```

Then, Eve presence in the communication is quantified by the quantum bit error rate Q (QBER) by means of the depolarization $p = 2 \cdot Q$ using (1)

```python
qber, key_primal, key_dual, key_th = np.linspace(0., .12, 15), [], [], []
for ii in qber:
    # for theorical curve and leak^{EC}
    hp = qkd.binary_entropy(ii)

    # apply quantum channel
    sim.apply_quantum_channel(qkd.depolarizing_channel(2*ii))

    gamma = []
    for jj in sim.povm: # get AB povm from QKD
        gamma.append(np.trace(jj @ sim.rho_ab)) # rho_AB is authomatically calculated by QKD

    # set contraints
    sim.set_constraints(gamma, sim.povm)

    # compute
    sim.compute_primal(epsilon=1e-11, maxit=50, finesse=100, "MOSEK") # finesse=finesse of the interval for \lambda\in[0,1]
    sim.compute_dual("MOSEK")

    # getting result
    key_th     = 1 - hp - hp # hp is the leak from error correction
    key_primal = sim.primal_sol - hp # hp is the leak from error correction
    key_dual   = sim.dual_sol - hp # hp is the leak from error correction
```

EB BB84 with efficiency mismatch on Bob's detectors

Consider the previous system with efficiency mismatch between the detection of bit 0 and 1 at Bob side. To treat the no-click event, the Hilbert space of system B must contain also the no-click event so $dim\mathcal{H}_B = 3$; For this reason, if η is the efficiency of the detector, Bob POVM become

$$\begin{aligned} P_1^B =& p_z |0\rangle\langle 0|_B \oplus 0, & P_4^B =& (1-p_z)\eta |-\rangle\langle -|_B \oplus 0, \\ P_2^B =& p_z \eta |1\rangle\langle 1|_B \oplus 0, & P_5^B =& \mathbb{I}_B - \sum_{i=1}^{4} P_i^B, \text{ where 0 indicates the no-click event,} \\ P_3^B =& (1-p_z)|+\rangle\langle +|_B \oplus 0, \end{aligned}$$

while Alice POVM remains unchanged with respect to the previous case.

In the public string announcement, Bob's announcement Kraus representation is

$$K_1^B = \sqrt{P_1^B}|0\rangle_{\tilde{B}}|0\rangle_{\bar{B}} + \sqrt{P_2^B}|0\rangle_{\tilde{B}}|1\rangle_{\bar{B}}, \quad K_2^B = \sqrt{P_3^B}|1\rangle_{\tilde{B}}|0\rangle_{\bar{B}} + \sqrt{P_4^B}|1\rangle_{\tilde{B}}|1\rangle_{\bar{B}}, \quad K_3^B = \sqrt{P_5^B}|2\rangle_{\tilde{B}}|0\rangle_{\bar{B}}.$$

With opportune adjustments, the sifting phase and the key map have the same structure as the standard BB84 simulation, so the G map can be defined inside QKD class. Depolarizing channel is also adapted to the 3-dimensional Hilbert space using the Kraus representation Ramzan und Khan (2011)

$$\begin{array}{ccc} E_1 = \sqrt{1-p} \cdot \mathbb{I}_B & E_2 = \sqrt{p/8} \cdot Y & E_3 = \sqrt{p/8} \cdot Z \\ E_4 = \sqrt{p/8} \cdot Y^2 & E_5 = \sqrt{p/8} \cdot YZ & E_6 = \sqrt{p/8} \cdot Y^2 Z \\ E_7 = \sqrt{p/8} \cdot YZ^2 & E_8 = \sqrt{p/8} \cdot Y^2 Z^2 & E_9 = \sqrt{p/8} \cdot Z^2 \end{array}$$

where

$$Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad \omega = e^{2\pi i/3}.$$

The code is then

```python
from src import qkd
# define states
states = [qkd.zero, qkd.one, qkd.plus, qkd.minus]

# with null clicks event
states_b = [np.append(i, [0]) for i in states]

# ... iteration over efficiencies
for depolarizing_prob in [0., .05, .1]:
    # iteration
    for efficiency in np.linspace(0.,1.,15):
        # ... definition of POVMB, KB, sifting and key_map
        # new simulation
        sim = qkd.QKD(dim_a=2, dim_b=3, n_of_singla_states=4,
            list_states_a=states, list_of_prob_a=[.25,.25,.25,.25],
            list_states_a=states_b, list_of_prob_a=[.25,.25,.25,.25],
            povm_b       =POVMB,
            kraus_b      =KB,
            sifting_phase =sifting,
            key_map      =V,
            announcement_register_b=[[1,0,0], [0,1,0], [0,0,1]])
        # apply quantum channel
        sim.apply_quantum_channel(qkd.depolarizing_channel(depolarizing_prob, 3))#dimension=3

        # compute primal and dual problem
        sim.compute_primal(1e-11, 1000, 20,solver_name="MOSEK")
        sim.compute_dual(solver_name="MOSEK")
```

3 Results

Standard BB84

In table 1 are reported the specific of time duration, primal problem result, dual problem result, precision (difference between primal and dual result) and tightness (difference between dual result and theoretical value). Looking at the table the precision and the tightness are well below the part per thousand.

In figure 1 are represent the result of each step and the theoretical value of the secret key rate for the standard BB84.

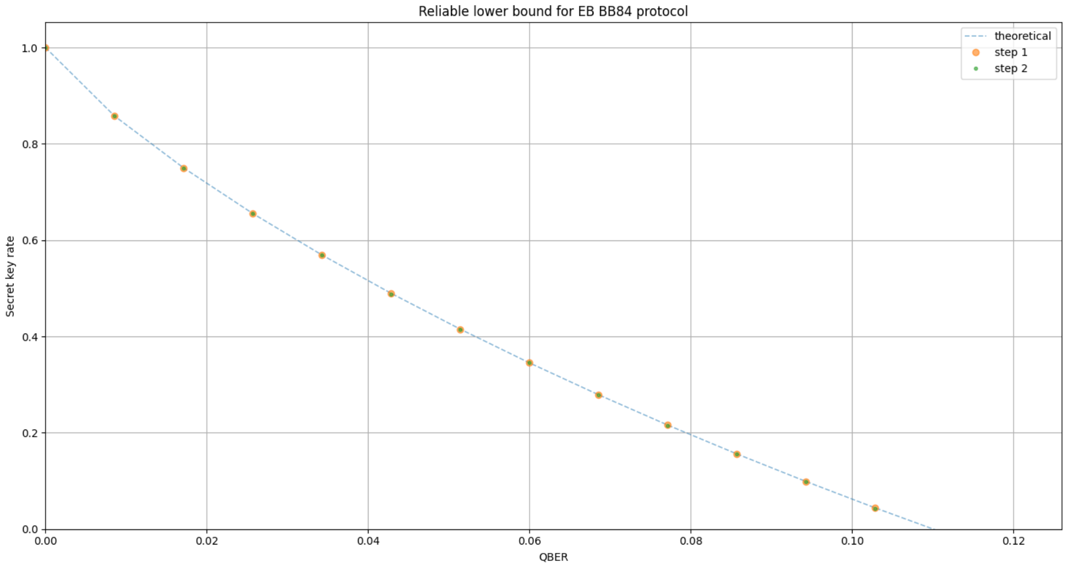

Figure 1: Standard BB84 secret key rate lower bound.

Efficiency mismatch

In the tables 2, 3 and 4 are reported the results for each value of the efficiency η for depolarization probability of the quantum channel $p = 0, 0.05, 0.1$.

The figure represents the values of the dual problem solution which is the reliable lower bound for the secret key rate. The calculations of precision (difference between primal and dual problem solution) for all depolarization probabilities $p = 0, 0.05, 0.1$ are below the part per billion.

QBER	CPU time[s]	theoretical	primal	dual	precision	tightness
0.000	43.469	1.000	1.000	1.000	3.04e-09	3.04e-09
0.008	28.991	0.928	0.928	0.928	3.09e-07	3.10e-07
0.017	28.492	0.874	0.874	0.874	7.61e-04	7.58e-04
0.025	43.003	0.827	0.827	0.827	1.69e-04	1.69e-04
0.034	28.564	0.784	0.784	0.784	1.28e-06	1.28e-06
0.042	28.795	0.744	0.744	0.743	9.33e-04	9.28e-04
0.051	42.643	0.707	0.707	0.707	3.47e-04	3.47e-04
0.060	41.923	0.672	0.672	0.672	2.30e-06	2.30e-06
0.068	28.265	0.639	0.639	0.639	2.66e-06	2.66e-06
0.077	29.915	0.607	0.607	0.607	5.36e-04	5.34e-04
0.085	42.638	0.577	0.577	0.577	5.24e-06	5.22e-06
0.094	28.698	0.549	0.549	0.549	1.03e-04	1.03e-04
0.102	29.094	0.522	0.522	0.521	7.35e-04	7.32e-04
0.111	44.381	0.495	0.495	0.495	1.26e-04	1.26e-04
0.120	44.381	0.470	0.470	0.470	4.92e-06	4.92e-06

Table 1: depolarizing channel effect on EB BB84 protocol.

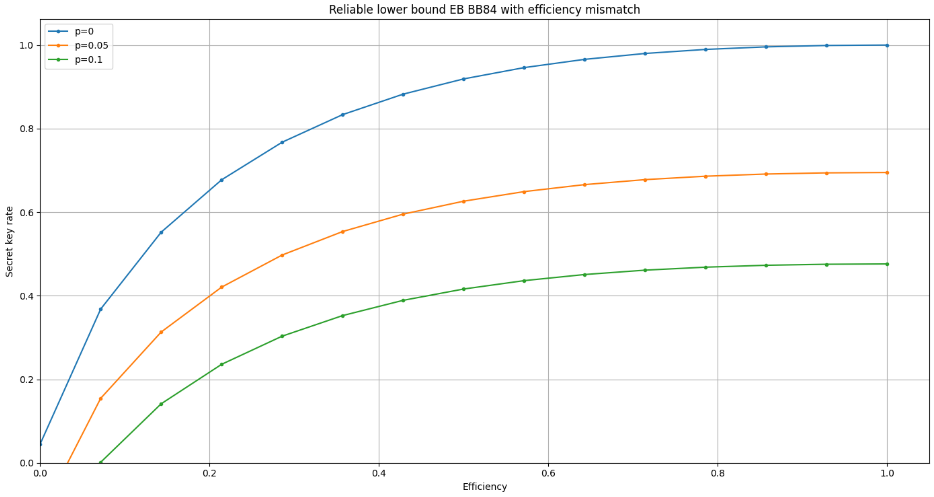

Figure 2: secret key rate changing the efficiency in $[0,1]$ for three possible depolarization probabilities $p = 0, 0.05, 0.1$.

Efficiency	CPU time [s]	primal	dual	precision
0.000	73.824	0.045	0.045	8.55e-09
0.071	272.240	0.368	0.368	4.37e-09
0.142	136.864	0.552	0.552	3.96e-09
0.214	71.155	0.677	0.677	1.91e-08
0.285	167.272	0.767	0.767	9.30e-09
0.357	223.856	0.833	0.833	1.12e-08
0.428	288.619	0.882	0.882	3.49e-08
0.500	238.178	0.918	0.918	7.22e-09
0.571	244.388	0.945	0.945	9.03e-09
0.642	170.951	0.965	0.965	1.28e-09
0.714	175.240	0.979	0.979	5.97e-08
0.785	596.072	0.989	0.989	7.65e-09
0.857	187.316	0.995	0.995	1.71e-08
0.928	192.420	0.998	0.998	4.32e-09
1.000	457.271	0.999	0.999	8.38e-08

Table 2: depolarization probability $p = 0$

Efficiency	CPU time [s]	primal	dual	precision
0.000	265.325	0.040	0.040	9.85e-07
0.071	245.214	0.323	0.323	2.17e-07
0.142	205.293	0.481	0.481	1.04e-07
0.214	203.671	0.589	0.589	2.77e-07
0.285	217.498	0.666	0.666	1.85e-07
0.357	234.874	0.722	0.722	3.35e-07
0.428	229.832	0.763	0.763	1.27e-06
0.500	244.347	0.794	0.794	5.20e-07
0.571	220.040	0.817	0.817	2.64e-07
0.642	206.758	0.834	0.834	2.76e-07
0.714	203.992	0.846	0.846	7.54e-07
0.785	214.197	0.854	0.854	6.43e-07
0.857	211.922	0.859	0.859	5.35e-07
0.928	211.338	0.862	0.862	1.80e-06
1.000	210.020	0.863	0.863	3.46e-07

Table 3: depolarization probability $p = 0.05$

Efficiency	CPU time [s]	primal	dual	precision
0.000	212.277	0.036	0.036	3.87e-08
0.071	212.460	0.287	0.287	1.19e-06
0.142	209.758	0.427	0.427	3.61e-06
0.214	211.222	0.522	0.522	1.04e-06
0.285	210.727	0.589	0.589	1.30e-06
0.357	210.353	0.638	0.638	1.50e-06
0.428	208.802	0.675	0.675	1.68e-06
0.500	209.674	0.702	0.702	2.68e-06
0.571	208.272	0.722	0.722	4.37e-06
0.642	208.197	0.737	0.737	5.96e-06
0.714	209.123	0.747	0.747	3.79e-06
0.785	212.709	0.754	0.754	3.07e-06
0.857	212.752	0.759	0.759	6.16e-06
0.928	217.413	0.761	0.761	5.01e-06
1.000	280.391	0.762	0.762	1.73e-05

Table 4: depolarization probability $p = 0.1$

4 Self-evaluation

The standard BB84 simulation is in complete accordance with the theoretical curve and guarantees a precision of over one part per thousand in the difference between the primal and dual solution.

Efficiency mismatch simulation confirms the precision of the algorithm far over one part per billion.

References

[Ferenczi und Lütkenhaus 2012] Ferenczi, Agnes ; Lütkenhaus, Norbert: Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. In: *Physical Review A* 85 (2012), May, Nr. 5. – URL http://dx.doi.org/10.1103/PhysRevA.85.052310. – ISSN 1094-1622

[George u. a. 2021] George, Ian ; Lin, Jie ; Lütkenhaus, Norbert: Numerical calculations of the finite key rate for general quantum key distribution protocols. In: *Physical Review Research* 3 (2021), Mar, Nr. 1. – URL http://dx.doi.org/10.1103/PhysRevResearch.3.013274. – ISSN 2643-1564

[Ramzan und Khan 2011] Ramzan, M. ; Khan, M. K.: Decoherence and entanglement degradation of a qubit-qutrit system in non-inertial frames. In: *Quantum Information Processing* 11 (2011), Jul, Nr. 2, S. 443–454. – URL http://dx.doi.org/10.1007/s11128-011-0257-7. – ISSN 1573-1332

[Winick u. a. 2018] Winick, Adam ; Lütkenhaus, Norbert ; Coles, Patrick J.: Reliable numerical key rates for quantum key distribution. In: *Quantum* 2 (2018), Juli, S. 77. – URL https://doi.org/10.22331/q-2018-07-26-77. – ISSN 2521-327X