KEY RATE RELIABLE LOWER BOUND FOR BB84 PROTOCOL

Sebastiano Cocchi

October 11, 2021

Abstract

A key rate reliable lower bound for the standard four states BB84 protocol is calculated in condition of:

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

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. Classical channel is public and authenticated, so Alice and Bob recognize each other.

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.

Alice and Bob communicate via classical channel to perform error correction and privacy amplification in order to extract the key.

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

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 $\mathcal{E}_A B$ 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-procecessing

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 qubit in which they have used the same basis;
4. key map: Alice performs a key map function able to extract a key based on the public and private part of the keys of both Alice and Bob;
5. error correction: using classical methods, Alice and Bob agree on 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.

Protocol modelling

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 POVMs $\{P_i^A\}$ and $\{P_j^B\}$

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

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}, θ_i constraints defines a set

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

and for P&M schemes

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

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

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

where (a, b) are the public parts of Alice and Bob key and $\bar{a}, \bar{b}$ are the private one. The two POVMs acts on the system AB

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

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

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

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 $R \to Z^R$

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

where the identity acts over all the other dimensions.

If the post-selection process involves only a sifting phase and base announcement, then the formula reduces only to system A and B without other registers. Suppose $\{Z_i^A\}$ is the Alice key map POVM, then (9) reduces to

$$f(\rho_{AB}) = D\left(\rho_{AB} \middle\| \sum_i (Z_i^A \otimes \mathbb{I}_B) \rho_{AB} (Z_i^A \otimes \mathbb{I}_B)\right). \tag{8}$$

Reliable lower bound

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

$$f(\rho_{AB}) = D\left(\rho^3_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} \middle\| \rho^4_{Z^R A\tilde{A}\bar{A}B\tilde{B}\bar{B}}\right). \tag{9}$$

having defined the states as

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

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 key rate is

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

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, a strategy can be split the algorithm into two steps:

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 upper bound.

Let's see 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 the estimation of the lower bound does not depend on the state shared by AB. Indeed, the initial density operator ρ_0 can be written as

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

where $\{\tilde{\Gamma_l}\}_{l=1}^{j} \cup \{\tilde{\Omega}_k\}_{k=1}^{dim\mathcal{H}_{AB}^2 - j}$ 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 $l < m$ 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); $\{\Omega_k\}_{k=1}^{dim\mathcal{H}_{AB}^2 - j}$ 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

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

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

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

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 $\{|1\rangle, |-\rangle\}$.

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.

I develop a python class called QKD able to simulate:

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. Then the public announcement is composed by the Kraus operators

$$\begin{aligned}
K_Z^A &= \sqrt{p_z}|0\rangle\langle 0|_A |0\rangle_{\bar{A}} |0\rangle_{\bar{A}} + \sqrt{p_z}|1\rangle\langle 1|_A |0\rangle_{\bar{A}} |1\rangle_{\bar{A}} \\
K_X^A &= \sqrt{1-p_z}|+\rangle\langle +|_A |1\rangle_{\bar{A}} |0\rangle_{\bar{A}} + \sqrt{1-p_z}|-\rangle\langle -|_A |1\rangle_{\bar{A}} |1\rangle_{\bar{A}} \\
K_Z^B &= \sqrt{p_z}|0\rangle\langle 0|_B |0\rangle_{\bar{B}} |0\rangle_{\bar{B}} + \sqrt{p_z}|1\rangle\langle 1|_B |0\rangle_{\bar{B}} |1\rangle_{\bar{B}} \\
K_X^B &= \sqrt{1-p_z}|+\rangle\langle +|_B |1\rangle_{\bar{B}} |0\rangle_{\bar{B}} + \sqrt{1-p_z}|-\rangle\langle -|_B |1\rangle_{\bar{B}} |1\rangle_{\bar{B}},
\end{aligned}$$

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

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

and 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

```
        from src import qkd
        import numpy as np
        # ...
        sim = qkd.QKD(da=2, db=2, nst=4, # dim A, # dim b, # of signal states
            [qkd.zero, qkd.one, qkd.plus, qkd.minus], [0.25, 0.25, 0.25, 0.25], # A states and prob
            [qkd.zero, qkd.one, qkd.plus, qkd.minus], [0.25, 0.25, 0.25, 0.25]) # B states and prob
```

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)

```
        qber, key_primal, key_dual, key_th = [0., 0.02, 0.04, 0.06, 0.08, 0.1, 0.12], [], [], []
        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()
            sim.compute_dual()

            # 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 detectors

In this case

3 Results

Standard BB84

Efficiency mismatch

Trojan-horse attack

4 Self-evaluation

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

[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