# SimulaQron Project Report - Group 37

Technische Universiteit Delft

Broekhoven, Rik; Bryce, Elliot; Gómez Iñesta, Álvaro; Miles, Sebastian

January 20, 2019

We implemented a version of the original BB84 protocol devised by Bennett and Brassard in 1984. It consists in two communicating parties (Alice and Bob) and an adversary (Eve), who wants to break into their communication.
In this report, we review the different parts of the protocol and give some results of the simulations. You can find the original codes and a README file with instructions at `https://github.com/AlvaroGI/SimulaQron_2018`.

## 1 The protocol

Alice and Bob can communicate through a public quantum channel and an authenticated classical channel. The authentication could be attained by using a message authentication code (MAT), but we just assume that Eve cannot alter the communication on the public channel, although she is able to listen everything. In our protocol, the classical channel was implemented as classical communication that traverses Eve on its way between Alice and Bob. Moreover, we make use of tags in the classical messages as receipts of communication between Alice and Bob. The quantum channel was realized using the same setup, with all communication passing over Eve. Nevertheless, Eve can measure any of the qubits sent through this channel.

## 2 Qubit creation and measurements

The qubits on Alice's side are initialized as follows. First, two lists of random bits are created. One of these lists contains the states of the qubits (0 or 1) and the other one, the bases (0 for standard, 1 for Hadamard). SimulaQron always initializes qubits in $|0\rangle$, so we apply the corresponding bit flips and basis changes (rotations) in a for-loop to create all the qubits sequentially. In each iteration, the created qubit is sent to Eve and forwarded to Bob. Then, Bob receives the qubit and measures it in random basis while saving both values, the basis and the measurement outcome. After finishing the loop for all the qubits, Bob sends a confirmation of receipt containing the number of qubits he received. This message is checked by Alice. If the number is not correct, she aborts the protocol (and lets Bob and Eve know about that). If the check passes, Bob sends a list with all his basis choices to Alice. Alice selects only rounds in which they chose the same basis, and lets Bob know through the classical channel. They discard the rest of rounds.
Bob now selects a set of test rounds (pairs measurement-basis) and sends them to Alice via the classical channel for her to compare. Alice computes the error rate of their test measurements (counting the number of rounds in which their measurements do not match, as this is an indication that Eve tampered with the transmissions and projected the qubit into a different state). If the error rate is below a chosen threshold, both parties continue, otherwise they abort the protocol.

## 3 Extracting key

At this point Alice has acquired all information needed to extract key. The raw key is formed by all the measurements corresponding to the rounds in which the bases matched and were not used for test. First, she generates the seed $y$ for the extractor function ($\mathrm{Ext}(x, y) = \sum_{i=1} N x_i y_i$, where $x$ and $y$ are N-bits strings). Alice sends this seed to Bob over the authenticated public channel. As extractor, we employ the addition modulo 2. Hence, Alice and Bob individually XOR this seed with the raw key to obtain their shared private one-bit key. The key generated is stored conveniently in a log file such that a longer key can be formed using one-bit keys from several executions of the protocol.

# 4 Attacking

Our codes allow to select from 3 options: no attack, attack 1 or attack 2.

## 4.1 Attack 1

Eve measures each qubit in the standard or Hadamard basis at random. In the rounds in which Alice's and Bob's measurements match, Eve has a 50% chance of using the correct basis, which translates into a 50% error rate in the test bits and the raw key.

## 4.2 Attack 2

In the Julia lab from week 6, we computed the optimal measurement for Eve to distinguish between BB84 states. This operator is used by her to extract her own private key while tampering with the state as little as possible. The way she does so is by rotating the qubit in the plane perpendicular to $\hat{x}$ and $\hat{z}$ using the associated rotation around the $\hat{y}$ axis, then measuring in the standard basis, and finally rotating back the post-measurement state into the plane of the original input.

## 4.3 Test errors based on the attack

We performed an experiment on each of the two attacks we implemented. We computed the number of errors over 200 test rounds (rounds in which Alice and Bob used the same basis), obtaining 94 and 58 for attacks 1 and 2, respectively. This yields an experimental error rate of 47% and 29%, respectively.
First, note that the error rate is clearly lower in the second case, as expected. This optimal attack allows Eve to be more stealthy, yielding a lower error rate in the test stage.
Let us discuss now attack 1. The error in these measurements can be modeled as a random variable $X$ with a Bernoulli distribution with success probability $p = 0.5$: $X \sim \text{Bernoulli}(p)$. The average error in our $N = 200$ experiments corresponds to the maximum likelihood estimator: $\hat{p_e} = \frac{1}{N}\sum_{i=1}^{N} X_i$. It can be shown that, for this estimator and this type of distribution, the variance of the estimator is given by:

$$\text{Var}[\hat{p}] = \text{Var}\Big[\frac{1}{N}\sum_{i=1}^{N} X_i\Big] = \frac{p(1-p)}{N} = 1.25 \cdot 10^{-3} \tag{4.1}$$

Hence, the standard deviation is $\sigma = \sqrt{\text{Var}[\hat{p}]} = 3.5\%$. This value agrees with our result, which lies in the confidence interval $(p - \sigma, p + \sigma)$, i.e., $46.5\% < 47\% < 53.5\%$.