QUANTUM CRYPTOGRAPHY AND SECURITY a.y. 2021/22

Laboratory session 3

Quantum Key Distribution (QKD)

Raw Keys

This archive contains three files of raw keys:

- `input-keys.alice`: Alice's choices of basis and state.
- `input-keys.decoy`: Alice's choices of decoy state.
- `input-keys.bob`: Bob's detected states.

The raw keys are obtained from a QKD run after synchronization and discard of the qubits that were not received by Bob.

File encoding

Each file contains key blocks of different lengths. A file begins with 8 bytes that code for a `uint64` big-endian, which is the length `N` of the block (in bytes). After these first 8 bytes, `N` bytes (=8N bits) of raw keys follow. After the `N` bytes, another block begins, with 8 bytes that code for the block length `M` and then `M` bytes. This pattern is repeated until the end of the file.

To check that the decoding of the length is correct, the first block is 17823 bytes long.

Each block represents 1s of acquisitions for the QKD protocol.

Key encoding and bit endianness

Each QKD state is represented by two bits.

The encoding in `input-keys.alice` is:

- `00`:`H`
- `01`:`V`
- `10`:`D`
- `11`:`A` (never used because Alice uses the three-state protocol)

The encoding in `input-keys.decoy` is:

- `00` : High/Strong intensity

- `01` : Low/Weak intensity
- `10` : Unused
- `11` : Unused

The encoding in `input-keys.bob` is:

- `00` : `H`
- `01` : `V`
- `10` : `D`
- `11` : `A`

This encoding assumes little endian reading. To check that the endianness used in reading is correct, read the `input-keys.decoy` file and divide a key block into bit pairs (i.e. states). If you find `10` pairs, the endianness is NOT correct. If this is the case, either re-read the file with the other endianness, or swap the meaning of `10` and `01`.

The first 12 values (3 bytes) for the three arrays are

- Alice: `['V', 'V', 'V', 'H', 'H', 'V', 'H', 'V', 'D', 'H', 'H', 'V']`
- Bob: `['V', 'D', 'A', 'H', 'D', 'V', 'H', 'D', 'H', 'H', 'D', 'D']`
- Decoy: `['S', 'L', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'S', 'L']`

where `'S'` stands for strong intensity and `'L'` stands for low intensity.

Protocol & Decoy parameters

The protocol used is the 3-state 1-decoy efficient BB84 protocol discussed during the lectures and described in [1].

The basis selection probabilities at the transmitter are: 90% for H/V, 10% for D

The basis selection probabilities at the receiver are: 50% for H/V, 50% for D/A

The decoy probabilities are: 70 % (strong), 30% (weak). The decoy intensities are 0.4699 and 0.1093 photons per pulse.

Assignment

Using the provided dataset you should estimate the relevant parameters for classical post-processing and obtain the QBER in the two bases and the secret key rate as a function of time. You are not required to actually perform all the steps of the classical post-processing (for example Error Correction or Privacy Amplification) on the keys, in order to obtain the pairs of secret keys, just the estimation of the SKR is necessary.

The dataset is quite big and represents a few hours of data acquisition. If the computation takes too long to process the entire dataset you can analyze a subset of it.

You have the freedom to decide the block size and the security parameters to use.

Bibliography

[1] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden , "Finite-key analysis for the 1-decoy state QKD protocol", Appl. Phys. Lett. 112, 171104 (2018) https://doi.org/10.1063/1.5023340