# QUANTUM CRYPTOGRAPHY AND SECURITY a.y. 2021/22

Laboratory session 1

### Quantum Random Number Generators (QRNGs)

In this laboratory session we have discussed the implementation of two types of QRNG, characterized by different degrees of trust on their elements. In particular, we have seen how an experimental setup based on a heralded single photon source and polarization measurements can be used to study trusted and Source-Device-Independent protocols.

In all the configurations one of the two photons generated by the spontaneous parametric downconversion source is directly detected by a single photon detector and the time of arrival is time-tagged as channel 2 by the time-to-digital converter. The instrument used in the lab records the timestamps in picoseconds.

Then, for each configuration we performed a projective measurement on the polarization of the second photon. The polarization measurement has been performed using a polarization beam splitter, which transmits horizontally polarized photons and reflects vertically polarized photons. This allows us to measure the polarization of the photon in the H/V basis. By inserting a half-wave or a quarter-wave waveplate before the polarization beam splitter, we could perform measurements in the D/A and L/R basis, respectively. Then, the photon was detected and time-tagged. The photons transmitted by the polarization beam splitter were tagged as channel 3 by the time-tagger and reflected photons were tagged as channel 4 by the time-tagger. In a few configurations, we inserted a polarizer before the measurement station to prepare a pure state instead of a mixed state.

For this experience we are only interested in the coincidence events, where we have a simultaneous detection between channel 2 and a detection either in channel 3 or channel 4.

## Setup 1

Using this setup we analyzed first the trusted QRNG under the following conditions:

- Preparing a mixed state and measuring it in the H/V basis (dataset: mixed_state_measured_on_hv_basis.mat)
- Preparing a pure D state and measuring it in the H/V basis (d_state_measured_on_hv_basis.mat)

In this case both the state preparation and the measurement stations are trusted and assumed to be working correctly.

The H/V basis is considered the basis for randomness generation.

The amount of randomness which can be certified can be quantified by the classical min-entropy, as discussed in the introduction of [1].

# Setup 2

Then, we analyzed the Source-Device-Independent QNRG, and we acquired additional data in the following conditions:

- Preparing a mixed state and measuring it in D/A basis (dataset: mixed_state_measured_on_da_basis.mat)
- Preparing a pure D state and measuring it in D/A basis (d_state_measured_on_da_basis.mat)

In this case the source is untrusted but the measurement station is trusted.

The previous datasets acquired in the H/V basis basis are still used for the generation, while the data in the D/A basis (which is the check basis) are used to bound the amount of randomness which can be certified.

The amount of randomness which can be certified can be quantified by the quantum conditional min-entropy.

Several approaches can be used to bound the quantum conditional min-entropy, but we will focus on the Entropy Uncertainty Principle [1] and the Tomographic method introduced in [2].

# Setup 3

Then, we acquired additional data to show the differences between the two Source-Device-Independent estimations when including measurements with pure states outside the equator of the Bloch sphere passing through H,V,D,A (full tomography).

We acquired additional data in the following conditions:

- Preparing a pure L state and measuring it in the D/A basis (l_state_measured_on_da_basis.mat)
- Preparing a pure L state and measuring it in the H/V basis (l_state_measured_on_hv_basis.mat)
- Preparing a pure L state and measuring it in the L/R basis (l_state_measured_on_da_basis.mat)

Also in this case we can use these data to bound the quantum conditional min-entropy, using the Entropy Uncertainty Principle [1] and the Tomographic method introduced in [2].

# Security level assessment

Finally, once we bound the min-entropy we can apply a seeded randomness extractor to the raw data generated in order to obtain the final string of private random numbers. For the extraction we can use a random Toeplitz matrix to perform the hashing. In this case, the

Leftover Hashing Lemma described in [3], tells us how to calculate the security parameter as a function of the min-entropy and the block size used for the matrix.

# Your tasks

The objectives of this assignment are the estimation of the min-entropy in the different configurations and the evaluation of the security parameter as a function of the block size.

In particular you will have to:

1. Read the dataset and keep only the events which have a coincidence between channel 2 with channel 3 or channel 4. You can decide the coincidence window, a suggested value is around 3 ns.
2. From the number of coincidence events estimate the probabilities for each projector of the measurement basis
3. For the trusted QRNG setup, use the first set of data to estimate the classical min-entropy for the mixed state and for the pure D state
4. For the Source-Device-Independent QRNG, use the first and the second set of data to calculate the quantum conditional min-entropy using the entropic uncertainty principle, for both the mixed state and the pure D state.
5. For the Source-Device-Independent QRNG, use the first and the second set of data to calculate the quantum conditional min-entropy using the tomographic method, for both the mixed state and the pure D state. ( since you don't have full tomographic measurements you can assume S2=0 )
6. For the Source-Device-Independent QRNG, use the third set of data to calculate the quantum conditional min-entropy using the entropic uncertainty principle, for the L state, using both the Entropic Uncertainty Principle and the tomographic method.
7. Using the min-entropies estimated in the previous steps, study how the security parameter from the leftover hashing lemma changes as a function of the block length.

# References


[1] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 90, no. 5, art. 052327, Nov. 2014.

[2] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 75, no. 3, art. 32334, Mar. 2007.

[3] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011.