# A Quantum Random Number Generator Based on a Polymer Photonic-Integration Platform

Martin Achleitner[1], Lena Hansen[2], Hauke Conradi[2], Moritz Kleinert[2], Christoph Pacher[1] and Hannes Hübel[1]

1 AIT Austrian Institute of Technology, Center for Digital Safety & Security, 1210 Vienna, Austria

2 Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany

✉martin.achleitner@ait.ac.at, ✉ lena.hansen@hhi.fraunhofer.de, ✉ hauke.conradi@hhi.fraunhofer.de, ✉ moritz.kleinert@hhi.fraunhofer.de, ✉ Christoph.pacher@ait.ac.at, ✉ Hannes.huebel@ait.ac.at,

## Abstract

Offering entropy derived from quantum mechanical principles, QRNGs are promising candidates to produce cryptographically secure random numbers. However, prices and form factors must come down, if this technology is to feed mobile or IoT devices in the future. We present a step in this direction by realizing a QRNG in the polymer-based photonic integration platform PolyBoard.

## Introduction

**Quantum Random Number Generators** (QRNG) are a well-studied quantum resource for information and communication technologies. The inherent randomness in quantum mechanical processes is used to generate true randomness, which is considered impossible in classical physics.

**Photonic integration** is a necessary step to minimize cost and form factors for better integration in consumer devices. In our project the QRNG is realized on a polymer platform (PolyBoard).

The QRNG uses the random output path of a photon impinging on a beamsplitter as an entropy source. A pulsed laser will create photon pulses with MHz repetition rate, which are attenuated to near single photon level using static and adjustable attenuators on the polymer board.

## Post-Processing

Practical implementations of Quantum Random Number Generators are subject to noise which is not fully controllable. This makes it necessary to process the output of the QRNG via a **randomness extractor**. We employed **Toeplitz hashing** as an extractor. To specify the Toeplitz matrix we need an upper bound on the min-entropy of our process[1]. With our currently estimated min-entropy and setup adjustments we extract 440kbit/s of random bits.

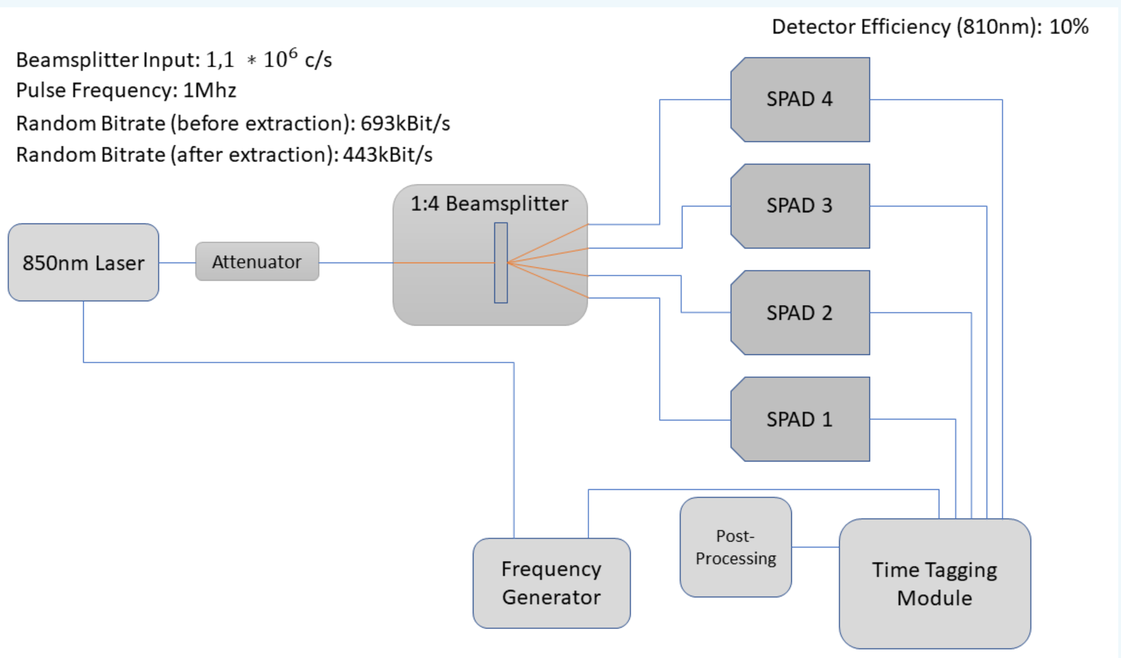
$$\begin{pmatrix} t_m & t_{m+1} & \cdots & t_{m+n-2} & t_{m+n-1} \\ t_{m-1} & t_m & t_{m+1} & \cdots & t_{m+n-2} \\ \vdots & t_{m-1} & \ddots & \ddots & \vdots \\ t_2 & \ddots & \ddots & t_n & t_{n+1} \\ t_1 & t_2 & \cdots & t_{n-1} & t_n \end{pmatrix} \cdot \begin{pmatrix} i_0 \\ i_1 \\ \vdots \\ i_{n-1} \\ i_n \end{pmatrix} = \begin{pmatrix} o_0 \\ o_1 \\ \vdots \\ o_{m-1} \\ o_m \end{pmatrix}$$

The input string times the Toeplitz matrix (constructed from a random, potentially public, seed) gives the extracted output.[2]

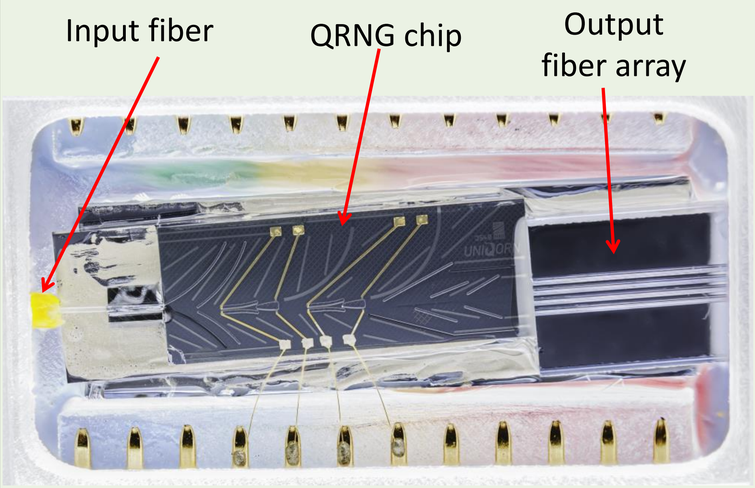
## QRNG Demonstration Setup

The **QRNG setup** consists of a pulsed 850 nm laser, which is attenuated to optimize the pulse for single photon splitting. A 1:4 beamsplitter generates 2 bits of randomness per incoming photon.

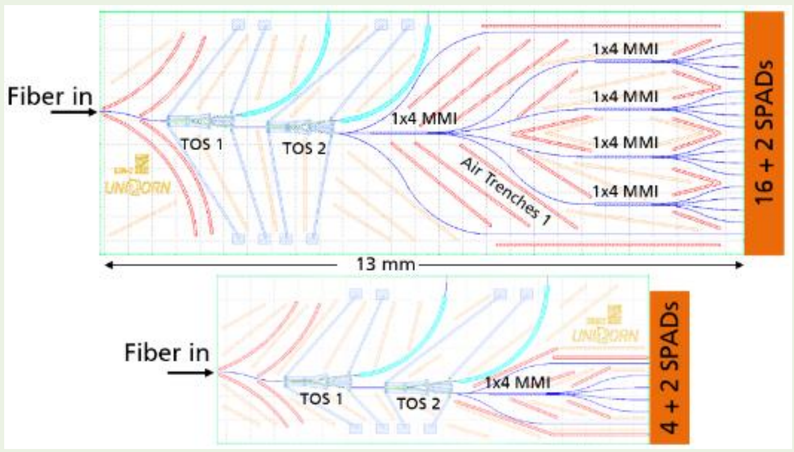
After detecting the single photons via 4 SPADs, the measurement data is sent to a TTM (time tagging module) which processes the data according to detected channel and detected time. The TTM data is filtered by a time window, to remove potential after-pulsing and noise. The random data at this point is possibly biased and partly known by an adversary and needs to be post processed with a **randomness extraction algorithm** to extract a uniformly distributed and unpredictable random number string.




## QRNG PolyBoard




The QRNG chip consists of an input waveguide designed for end-face coupling of a cleaved single mode fiber in a wavelength range around 800 nm. The light is guided through a stage of two thermo-optical switches (TOSs) that are used to attenuate the light in the main path to a single photon level. These photons propagate through a **multi-mode interference coupler (MMI)** with four outputs. In a 1x4 QRNG, these four waveguides are connected to a 4-channel SPAD array. In the 1x16 QRNG, each output serves as the input for another 1x4 MMI, yielding in total of 16 output waveguides connected to a **16-channel SPAD array**. By cascading further MMI stages, the number of SPADS can be increased further, allowing for higher bit rates. Here we report first work performed using the 1x4 QRNG module with bulk SPADS.



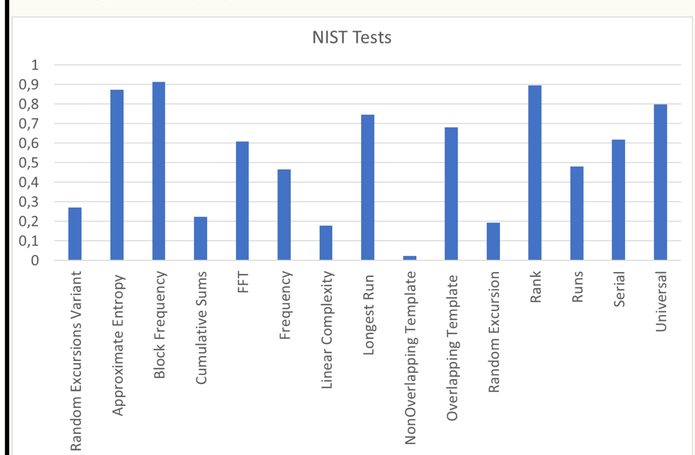

## References

1. D. Frauchiger, R. Renner and M. Troyer, *True randomness from realistic quantum devices*, arXiv:1311.4547v1 2013
2. Yishay Mansour, Noam Nisan, Prasoon Tiwari, *The Computational Complexity of Universal Hashing*. Theor. Comput. Sci. 107(1): 121-133 (1993).

## Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820474 (**UNIQORN**).

## NIST Tests




The NIST tests, a standardized statistical test suite for random and pseudorandom numbers, were used to confirm the sanity of our procedure. All 15 tests passed with a p-value over the significance level of 0.01.