Monolithic Integration of Source-Device-Independent QRNG with 35 Gbit/s Generation Rate

Peter Seigo Kincaid[1], Lorenzo De Marinis[1], Francesco Testa[1], Nicola Andriolli[2] and Giampiero Contestabile[1]

1. *Scuola Superiore Sant'Anna, Pisa, Italy – peterseigo.kincaid@santannapisa.it*
2. *Department of Information Engineering, University of Pisa, Via Caruso 16, 56122, Pisa, Italy*

Abstract: We report the first monolithic InP integration and black-box package of a Source-Device-Independent QRNG with electrical-only IO. The device offers generation rates of 35 Gbit/s, demonstrating suitability for QKD link applications.

Quantum mechanics provides an ideal entropy source for the generation of random numbers due to its inherent unpredictability. Quantum random number generators (QRNG) can be characterized based on the level of guaranteed security: device-independent systems are the most secure but offer low generation rates and require the verification of the Bell's inequalities, fully-trusted systems offer the contrary, with a full device characterization assumed and generation rates arriving at 100 Gbit/s [1]. Semi-device-independent QRNG offer a good compromise where assumptions are bound to a part of the system, and generation rates on the order of 10s of Gbit/s are achievable, sufficient for demanding applications in QKD links. The source-device-independent bulk heterodyne-based QRNG first realized using bulk components [2], and integrated in SiP [3], is realized here with a monolithic InP photonic integrated circuit (PIC), allowing a black-box device realization with only electrical I/O. The PIC is presented in Fig. 1a), with dimensions 4 mm x 8 mm, and integrates a DFB laser at 1550 nm which acts as a local oscillator and amplifies the quantum vacuum state, this feeds into a 4x4 MMI which acts as a 90° optical hybrid allowing a measurement of both quadratures of the quantum ground state at the balanced photodiodes, p and q.

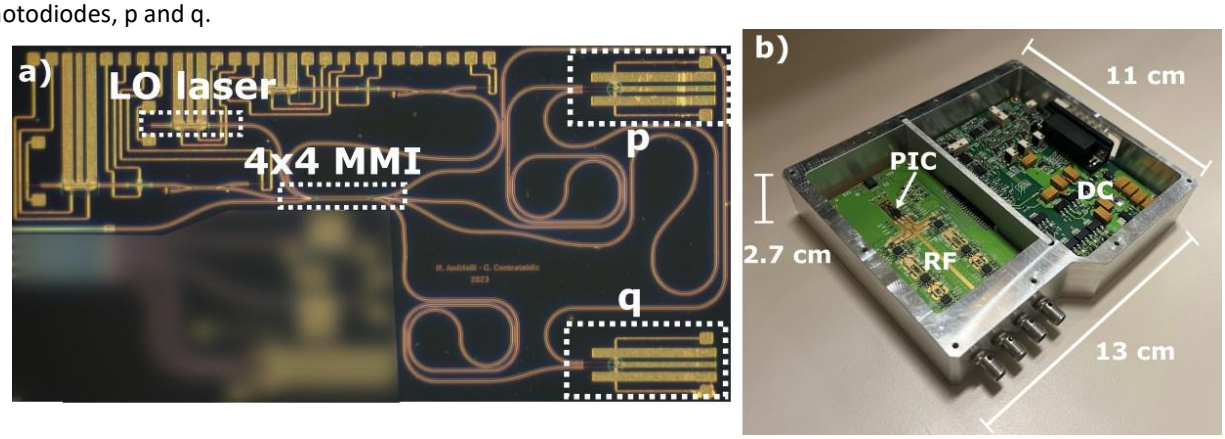

Fig. 1 a) InP photonic circuit, with the key components highlighted b) custom black-box package with only electrical IO.

The PIC was packaged with custom RF and DC PCBs (Fig. 1b) which provide all the necessary biases, output signals and amplify the quantum noise received at p and q. This system allows the definition of a lower bound on the number of secure random bits extractable, correcting for the presence of classical noise, which is established through a calibration procedure [1]; this was calculated to be 17.5 bits (out of the 24 bit resolution offered by our ADC) for a maximum LO laser power of 13 mW. Given the 2 GHz passband filtering and down sampling of the received signal, this achieves a generation rate of 35 Gbit/s. A randomness extraction was performed on the data according to the procedure in [4], the resulting bit streams pass the entire NIST battery of statistical tests.

Example References

[1] C. Bruynsteen, T. Gehring, C. Lupo, et al., "100-gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum 4, 010330 (2023).

[2] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nat. Commun. 9, 5365 (2018).

[3] T. Bertapelle, M. Avesani, A. Santamato, et al., "High-speed source-device-independent quantum random number generator on a chip," Opt. Quantum 3, 111–118 (2025).

[4] X. Ma, F. Xu, H. Xu, et al., "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A 87, 062327 (2013)