Indium Phosphide Monolithical Integration of a Photonic Source Device Independent Quantum Random Generator

Lorenzo De Marinis[1], **Peter Seigo Kincaid**[1], **Giampiero Cotestabile**[1]

1. *Scuola Superiore Sant'Anna, Pisa, Italy – lorenzo.demarinis@santannapisa.it*

Abstract: We report the fabrication of a monolithically integrated QRNG with an Indium Phosphide platform. The device offers a better level of security than fully-trusted systems, with a predicted secure generation rate > 13.3984 Gb/s.

As the demand for secure and reliable random numbers continues to grow, quantum random number generators (QRNGs) are becoming increasingly important in various scientific, technological, and industrial fields. In this context different schemes have been proposed and realized, which can be categorized by the level of trust of the hardware. Device-independent (DI) quantum crypto-graphic protocols aim to achieve a guaranteed security without relying on assumptions about the internal workings of the quantum devices used in the protocol. DI protocols offer the highest level of security, but their realization is still too demanding for any practical use [1]. In contrast, fully trusted systems provide a practical way to achieve QRNG, with a higher generation rate at the cost of a lower level of security, which must be ensured by rigorous characterization and verification of the constituent elements, bulk systems in this category have arrived at generation rates of 68 Gb/s [2]. In this paper we focus on a semi-device independent (semi-DI) scheme which offers a compromise between security and practicability, i.e., a solution where some weaker assumptions are made to bound the side information available to an attacker. We exploit the source-device independent scheme reported in [1], which assumes an untrusted quantum source, and present and assess a monolithically integrated realization on the InP platform offered by Fraunhofer HHI.

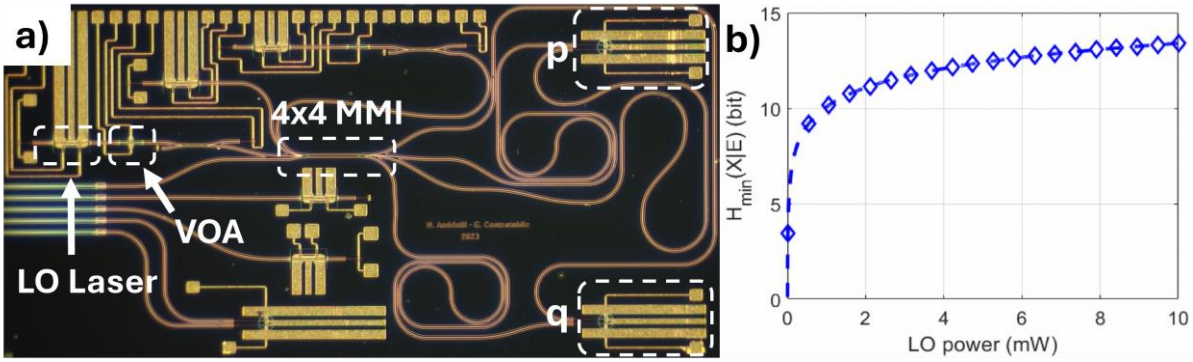

Fig. 1 - (a) Photograph of the chip with highlighted its constituent components (b) Quantum min entropy, as a function of LO power

Fig. 1a reports the nude fabricated InP chip. The semi-DI schematic is based on the heterodyne detection of two quadratures of the quantum ground state [1]. This is implemented by exploiting the interference between a local oscillator (LO), the integrated laser, and the quantum vacuum state (an empty input), fed to a 4-input 4-output multimode interferometer (MMI) used to implement a 90-degree optical hybrid. The outputs are then sent to 2 balanced photodetectors (PD), which retrieve the quadratures: amplitude *p* and phase *q*. The MMI outputs are connected through equal length paths to the PD inputs. We performed a numerical validation of the system, relating the quantum conditional min entropy $H_{min}(X|E)$ to the laser power [3], the number of extractable secure bits considering the side information available to an eavesdropper. Fig. 1b plots the resulting conditional min entropy. The highest value at max LO power is given by $H_{min}(X|E) = 13.3984$. Considering a bandpass bandwidth of 1 GHz, this yields a secure generation rate of 13.3984 Gb/s.

References

[1] M. Avesani, *et al.*, "Source- device-independent heterodyne-based quantum random number generator at 17 Gbps", Nature Communications, vol. 9, no. 1, pp. 5365, Dec 2018.

[2] Y.-Q. Nie, *et al.,* "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," Review of Scientific Instruments, vol. 86, no. 6, p. 063105, 06 2015.

[3] P. S. Kincaid, *et al.* "Source Device Independent Quantum Random Number Generator with Integrated InP Photonics," 2023 International Conference on Photonics in Switching and Computing (PSC), Mantova, Italy, pp. 1-3, 2023