A Monolithic SPAD-based Quantum Random Number Generator with 0.875 bit/event Efficiency in 22-nm FD-SOI CMOS

Andrea Bonzi[1], Luca Parmesan[1], Nicola Massari[1], Fabio Acerbi[1], Aymane Bouzafour[2], Marc Renaudin[2], and Leonardo Gasparini[1]

[1]*Fondazione Bruno Kessler (FBK), 38123, Trento, Italy*

[2]*Tiempo Secure, 38330, Montbonnot-Saint-Martin, France*

Random Number Generators (RNGs) are critical for modern applications such as cryptography, simulations, and gaming [1]-[3]. While traditional Pseudo-RNGs (PRNGs) are deterministic, Quantum RNGs (QRNGs) leverage quantum physics to provide true randomness [4]. This work presents a high-performance, monolithic QRNG that marks a significant step toward the mass-market integration of quantum-grade entropy. Unlike traditional bulky or discrete solutions, the system is fabricated in an advanced 22-nm Fully Depleted Silicon-On-Insulator (FD-SOI) CMOS process. By integrating Single-Photon Avalanche Diodes (SPADs) directly into a deep-submicron node, this design proves the feasibility of embedding quantum entropy sources into modern processors, microcontrollers, and Graphics Processing Units (GPUs) for high-volume commercial applications. The architecture (Fig. 1, Left) implements a 3rd-order rank algorithm [5] by capturing the inter-arrival times of consecutive pulses via a Time-to-Digital Converter (TDC). These timestamps are processed through three cascaded stages: each level compares consecutive values to generate a random bit, while the greater value is propagated to the next stage. This multi-stage approach enhances entropy extraction, achieving a theoretical cumulative efficiency of 0.875 bits per event (comprising contributions of 0.5, 0.25, and 0.125 from the first, second, and third stages, respectively). The 1.63 mm x 1.28 mm chip (Fig. 1, Right) is fully controlled via a standard Serial-to-Parallel Interface (SPI), ensuring seamless compatibility with digital ecosystems. Statistical validation through the NIST SP 800-22 suite [6] confirms that the generated sequences pass all tests without the need for post-processing, highlighting the robustness of the proposed monolithic solution.

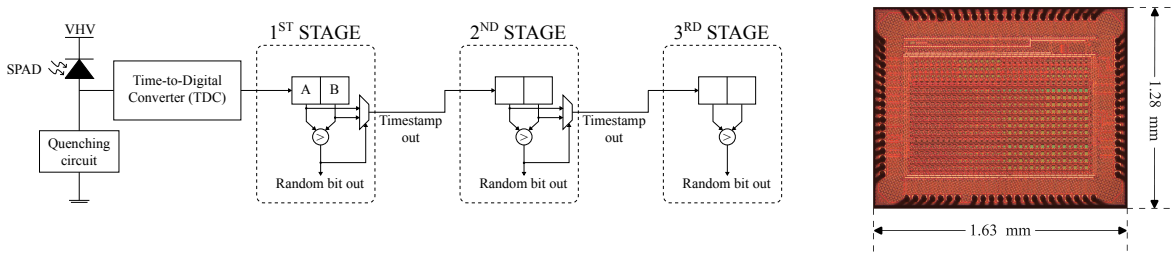

Fig. 1: *(Left) 3rd-order rank algorithm principle. (Right) 22-nm FD-SOI chip die micrograph.*

Funding acknowledgement

Supported by the European Defence Fund (EDF) SMiEQ project (Grant No. 101103001).

References

[1] N. Gisin *et al.*, Rev. Mod. Phys. 74, 145 (2002).
[2] N. Metropolis and S. Ulam, J. Am. Stat. Assoc. 44, 335 (1949).
[3] T. Fort, Thesis (2015).
[4] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. 89, 015004 (2017).
[5] A. Tontini *et al.*, IEEE Trans. Circuits Syst. II 66, 2067 (2019).
[6] A. Rukhin *et al.*, NIST Spec. Publ. 800-22 (2001).