Public deliverable for the ATTRACT Final Conference

In-silico quantum generation of random bit streams

M. Caccia[a,*], L. Malinverno[a], L. Paolucci[a], C. Corridori[a], E. Proserpio[a], A. Abba[b], A. Cusimano[b], W. Kucewicz[c], P. Dorosz[c], M. Baszczyk[c], M. Esposito[d], P. Svenda[e]

[a] *Universitá dell'Insubria, Dipartimento di Scienza ed Alta Tecnologia, Via Valleggio 11, 22100 Como, Italy*
[b] *Nuclear Instruments s.r.l., Via Lecco 16, 22045 Lambrugo (Como), Italy*
[c] *AGH-University of Science and Technology, Al. Mickiewicza 30, 30-59 Krakow, Poland*
[d] *Quantum Financial Analytics s.r.l., Via Broletto 39, 20121 Milano, Italy*
[e] *Masaryk University, Faculty of Informatics, Botanicka 68A, 60200 Brno, Czech Republic*

Abstract

The main goal of "Random Power" is the development of a platform for the generation of random bit streams by processing the time series of self-amplified endogenous stochastic pulses in a dedicated Silicon structure. The principle, based on the quantum properties of matter, has been validated applying the National Institute of Standard and Technology (NIST) protocols, complemented by other test suites. The advantages against competing techniques have been thoroughly analysed and the development of a dedicated small form-factor board has been completed.

The principle is protected by a patent application, currently in the international phase (PCT/IB2019/058340 deposited in October 2019).

Keywords: Random Number Generation, Silicon Photomultipliers, Cryptography

1. INTRODUCTION

Random number generation is critical in a number of significant applications:

- Computer security and cryptography, where the secrecy of a message (text, images or data) is strongly related to the production of encryption keys, namely random string of bits created explicitly for scrambling and unscrambling data. Randomness is also essential in the encoding process itself, notably in runner-up techniques like Homomorphic Encryption ([1]);
- Internet of Things (IoT) and high speed Wi-fi infrastructure (5G and beyond) where vulnerability to intrusion and data protection is a serious concern, raising a request for miniaturised, low cost, high performing security platforms;
- Numerical simulation of complex phenomena, crucial for Science, Industry, Economics and Sociology;
- Development of communication protocols for overcrowded networks, for instance in Network Random Coding [2];
- Gambling, where the role of randomness and unpredictability is obvious and poses significant challenges with the development of on-line platforms.

Random number generation can be based on algorithms or on observables related to unpredictable natural phenomena. The former is software or firmware implemented, the latter requires hardware systems for information gathering and methods to process it to extract series of stochastic numerical figures. Algorithms are deterministic therefore the randomness properties of the generated sequences is irreducibly limited (see for instance [3] and notably [4]). Hardware generation of random numbers based on chaotic systems or phase jitters in ring oscillators can provide practical unpredictability of the events, however the essence of the natural phenomenon is such

*Corresponding author
Email address: massimo.caccia@uninsubria.it (M. Caccia)

that the dynamics of the system can be externally driven or biased ([5, 6, 7]). On the other hand, phenomena at quantum level are intrinsically stochastic and, as such, unpredictable. For this reason, they are the ideal base for True Random Number Generators (TRNG), as opposed to Pseudo Random Number Generators (PRNG).

Random Power is focusing on the development of a Quantum-TRNG (QTRNG) platform, producing unpredictable bit streams analysing the time series of self-amplified endogenous pulses due to stochastically generated charge carriers in a dedicated Silicon device.

The principle at the base of the development represents a breakthrough with respect to the state of the art in terms of simplicity and robustness, efficiency of the bit extraction, intrinsic quality of the raw bit stream not requiring any post-processing and the mid-term perspective of engineering a system-on-chip. By the time of writing, Random Power designed, produced and qualified a small form factor board ($8 \times 3.5 cm^2$), embedding a single generator providing a bit stream up to 0.5 Mbit/s for a $1 mm^2$ generator. Randomness was qualified through the NIST standard [8] and, thanks to the extra-consortium collaboration with Masaryk University in the Czech Republic, using the complementary *Booltest* [9].

2. STATE OF THE ART

Historically, the very first quantum random number generator was based on unstable radioactive nuclei, decaying emitting alpha, beta or gamma particles [10]. Emissions occur in an unpredictable way and the number of decays in a pre-defined time window follows a Poisson distribution. Pulses are statistically independent and uncorrelated and random bit generation can be obtained in various methods, outlined for instance in [11]. Radioactive decays are yet today a very robust and reasonably simple way to obtain a random bit stream. However, they suffer from obvious questions of health protection, safety and security, preventing their large-scale adoption. Moreover, the particle detector features, notably its dead time and radiation damage, are limiting the obtainable throughput and undermine the stability.

As of today, the majority of quantum random number generators rely on low light sources and detectors with single photon sensitivity, in a variety of set-ups and arrangements; an excellent review can be found in [11] and references therein. This approach is certainly significant and it has been successfully commercially exploited (see for instance [12]). However, it suffers from intrinsic limitations:

- complexity in the set-up, due to the characteristics of the light source and the request of a dual source-detector system;
- lack of robustness associated to the request of extreme stability against temperature and voltage variations;
- a low rate of extracted random bits per event, due to the need of post-processing raw data for filtering left-over biases.

As a consequence, a few other approaches based on the endogenous generation of pulses have been pursued and developed up to get to the market (see for instance [13, 14]), including Random Power, which essentially mimicks the processes implemented using radioactive sources but in-silico, with no radioactivity.

3. BREAKTHROUGH CHARACTER OF THE PROJECT

Random Power is the result of a flash of serendipity while characterising spurious pulses in single photon sensitive devices made blind to light, turned into random bit generators by an act of ingenuity. State-of-the-art solid state sensors of light with single photon sensitivity and photon number resolving capability consist of a high density of ”cells”, actually p-n junctions operated beyond the breakdown voltage. The ultimate sensitivity is provided by the fact that a single photon absorbed in a cell has a high probability to release an electrical charge carrier pair, the ”seed” of an avalanche developing by impact ionisation, leading to a pulse of electrical current corresponding to millions of electrons over tens of nanosecond. The devices, known as Silicon Photo-Multipliers (SiPM) or Multi-Pixel Photon Counters (MPPC), underwent a tremendous development since their invention at the turn of the millenium and nowadays are replacing classical photomultiplier tubes in research and industrial applications (for a recent review see the special issue on Nuclear Instruments and Methods at [15]). However, SiPM are still limited by a high rate of pulses occurring independently from photon detection, a phenomenon well known since the early days of the Silicon technology development and described by a series of seminal papers, out of which it is worth mentioning at least the one by Shockley and Read [16]. Trap assisted thermally driven stochastic generation and recombination of free carriers is the mechanism responsible for the occurrence of random pulses in p-n junctions operated in the avalanche regime, as thoroughly studied by [17]. The key point is that the high density of carriers, the random occurrence of bringing them to the conduction band together with the stochastic probability of inducing an avalanche breakdown leads to a series of independent unpredictable pulses.

This is the principle at the base of the proposed device, consisting of a SiPM packaged in full darkness, identifying the randomly initiated pulses, time tagging them and turning the sequence in a series of bits. The endogenous generation mechanism makes the process and the device simple and robust, also against temperature variations expected to change the rate without impairing randomness. Self-amplification of the random ”seeds” makes the identification of the pulses robust and faultless. The avalanche time development, with a leading edge

of the signal at the sub-nanosecond level, makes time tagging extremely precise. Pulse rates can achieve $1 MHz/mm^2$ at room temperature with a very high bit extraction efficiency (currently at the level of 44%) since no post-processing is required. Last but not least, state of the art Silicon technology offers the possibility to embed the generator into a system-on-chip, essential for consumer applications. These features overcome the major limitations of single-photon based QTRNG's and make Random Power a breakthrough solution.

4. PROJECT RESULTS

The main goal during the ATTRACT project has been the design, production and qualification of a "Minimum Viable Product", namely a small form factor board based on a single generator, embedding the basic functionalities on a custom developed FPGA firmware. The essence is reported below and a detailed report can be found in [18].

4.1. The single-generator board

The Random Power single-generator board is shown in Figure 1. It features a small form factor ($8 \times 3.5 \times 0.4 cm^3$) and electronic components fitted on a single tier. It is biased through a USB port and communication is controlled by an FTDI chip. The core of the board control is a Xilinx Spartan 7 Field Programmable Gate Array (FPGA), embedding a proprietary Time-to-Digital Converter (TDC), outlined in the following. The board can host both SiPM with $1.3 \times 1.3 mm^2$ and $3 \times 3 mm^2$ area, made light blind with a black resin cap. Sensor bias can be tuned in the 20-100V range; a digital temperature sensor in the SiPM proximity and a feedback loop guarantee gain stabilisation. GPIO pins allows to probe control signals for debugging purposes; FPGA and flash memory programming proceeds through the JTAG port. In terms of bit generation rate and data transmission speed, the board can sustain a throughput in excess of 1Mbit/s, making it suitable for the use in a real case scenario.

After the prototype qualification, a small production of 20 boards has been launched and completed.

Figure 1: The single generator board.

4.2. Development of an FPGA embedded Time-To-Digital Converter

The basic functionality of the custom TDC is shown in Fig. 2: a coarse counter records the number of cycles of the reference clock between the start (t_0) and stop (t_1) signals (C1); a multi-tap delay line built from carry chain blocks (Carry4), synchronised with the rising edge of the clock, measures the fine value T1. Time since the start signal is calculated as:

$$\Delta t = C1 \cdot T_{Clk} - T1 = C1 \cdot T_{Clk} - \frac{F_{max} - F1}{F_{max}} \cdot T_{Clk}, \quad (1)$$

where T_{Clk} is the period of the reference clock (4 ns), $F1$ is the number of delay units (taps) in the carry chain crossed by the signal before the stop and F_{max} is the number of taps that the input signal propagates through during one cycle of the reference clock ($F1 \leq F_{max}$).

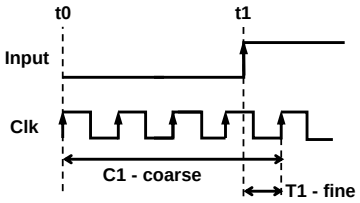

Figure 2: Coarse and fine counters with respect to internal clock

Particular care in the implementation of the TDC was taken to maximise the uniformity of the delays in the single taps and to reduce the so-called "bubble problem". In operation, delays are calibrated at start-up and during the data taking as long as a temperature variation exceeding $2°C$ is detected. The TDC was thoroughly characterised: the average granularity (delay corresponding to a single tap) was measured to be 73 ps for a resolution of about 50 ps.

4.3. Qualification of the generated bit stream

Raw bit streams generated by single-generator boards were qualified against the test suite by NIST [8], complemented by a study on the use of Boolean functions [9], in view of the implementation of a real-time sanity check.

The NIST protocol consists in 189 statistical tests to qualify the hypotheses that the bit sequence is unpredictable and corresponds to an equal probability to score a value of 0 or 1. **By the time of writing, about 40 Gb of raw data have been processed**, testing different sensor biasing conditions over a temperature range between 20 and 40 $°C$. Data have been analysed in subsets of 1-10 Gb and sequences of 1-10Mb. **It is remarkable that no data set was rejected, confirming the validity of the principle and notably its implementation, not requiring any post-processing to filter left-over biases, preserving the original bit generation efficiency and reducing the complexity of the proposed solution.**

The *booltest* suite is based on the dynamical construction of randomness distinguishers using an exhaustive search for boolean functions of a specified degree. If any boolean

function with significantly different distribution than expected for truly random data is found, the tested sequence is rejected as non-random. The two major advantages related to this method sits in the request for a limited data set with respect to the NIST and the diagnostics of detected violations. The *booltest* was applied so far over 100 sequences produced by the device with 10^7 bytes each and no anomaly was detected.

5. FUTURE PROJECT VISION

The project is currently beyond the proof-of-concept level (Technology Readiness Level (TRL) 3). The board developed during the ATTRACT phase-1 project may be considered a true "Minimum Viable Product". It has been validated in a laboratory environment (TRL 4) and provides a platform for certified and customised solutions for end-users (TRL 5 and above). However, it is clear that its potential goes very much beyond what currently exists and it shall be fully exploited to be able to compete with industrialised existing solutions. The roadmap of the project essentially addresses end-user driven technological developments, together with advances in selected applications where the Random Power QTRNG could represent a breakthrough.

5.1. Technology Scaling

The evolution of the existing platform towards a class of industrial devices with a wide range of applications is envisaged to proceed along four main development lines:

- go "macro": scaling it up to multiple generators for infrastructural and server-based applications;
- go "micro": integrating the platform functionalities (generator, TDC, control) in a System-On-Chip;
- go "secure": embedding a real-time "sanity check" of the bit stream, possibly based on the *booltest*;
- go "fast": integrating in the FPGA advanced functionalities like prime number generation for cryptographic keys.

These steps, together with the required certifications in accordance with the end-users, are expected to bring the Random Power technology to TRL 7 (system prototype demonstration in operational environment) or beyond on a time scale of 3-4 years.

5.2. Project Synergies and Outreach

The current consortium is quite strong on the technology, engineering and analytics side. However, in order to fully exploit the potential of the idea, it shall certainly be enlarged to integrate:

- teams with expertise in designing micro-integrated systems, namely monolithic devices embedding sensors, front-end electronics and control, to complement the VLSI design skills at AGH;
- mathematicians and cryptographers;
- end-users, notably from industry, essential for steering the technological development, qualifying the design, identifying the certification procedures and the protocols required to achieve the desired TRL and to develop novel services/applications

A series of contacts with relevant partners in the public and private sectors have already been established and mutual interest verified. It is also worth mentioning the possibility to establish synergies with at least three projects already approved within the ATTRACT phase-1 intitiative: VISIR and XCOL, since the expertise by the team at IMASENIC (https://www.imasenic.com) perfectly matches the requests for going "micro"; LIROC, as the team at Weeroc (https://www.weeroc.com) develops front-end Application Specific Integrated Circuits (ASIC) for the class of sensors at the base of Random Power. Notably, LIROC specifications in terms of timing would allow a direct development of a board for the "macro" scale-up of the Random Power platform.

In terms of outreach, the experience during the phase-1 has been very positive but rather classical: the project has been presented during an international workshop, a booth was allocated during an innovation fair, a series of contacts established with investors, potential industrial partners and innovation managers. A hackathon was planned and it has been postponed because of the COVID-19 pandemia. For phase-2, these actions shall be complemented at least in two different directions: joining activities aimed for raising awareness about personal data security and privacy issues (see for instance the recent call identified as SU-DS03-2019-2020 within the HORIZON 2020 program, focused on the development of solutions for helping citizens to be more engaged and active in the fight against cyber, privacy and data protection risks); contributing to the EC supported actions for creating competence centres on cybersecurity issues on the way towards the creation of a EU-wide cybersecurity certification scheme.

5.3. Technology applications and demonstration cases

High quality true random numbers, as opposed to software generated pseudo-random numbers, are essential in several cybersecurity applications having a significant economic and social impact in terms of data protection and privacy preservation, notably:

- strengthening the security of crypto-key generation at infrastructural level, seeding the so-called Hardware Security Modules (HSM) and introducing an extra-security layer in the 5G infrastructure;
- developing high security protocols for the Internet of Things (IoT);
- developing practical Full Homomorphic Encryption (FHE), essentially a procedure that allows to process encrypted data to extract the information contained therein.

In particular, FHE is a visionary approach with the highest priority in the Random Power agenda since random numbers are required not only for crypto-key generation but for the encryption process itself. Moreover, FHE applications range from increased security on contact tracing apps to e-health secure, anonymous analytics and e-voting, today more relevant than ever.

In scientific terms, the evolution of Random Power will be nested in the development stream of SiPM with on-board intelligence. Standard sensors are widely used in the High Energy Physics and Biophotonics and moving towards system-on-chip would represent a significant step in terms of cost effectiveness and simplification of large systems.

5.4. Technology commercialisation

The exploitation plan for Random Power is considering both Intellectual Property (IP) licensing and company creation but the priority nowadays is on entrepreneurship. An initial step has been taken and Insubria University, the home institution of the Principal Investigator, already granted officially the possibility to proceed. Negotiations are ongoing with AGH-University of Science and Technology in Krakow, Poland, the other academic Random Power partner. In terms of access to venture capital, we sampled the reaction of major banks and investment funds addressing a few relevant players in Italy and Israel. Reactions were in general positive and the consortium intends to strive to enter *talent gardens* supported by investors to grow up entrepreneurial spirit and capitalize on the ingenuity of the team.

5.5. Envisioned risks

As of today, two major risks can be envisioned: on the technical side, difficulties in the system-on-chip integration essentially due to the need of making the "generator" fully CMOS compliant; on the exploitation side, the request by potential customers in the security field to proceed through exclusive license-based integration, essentially constraining and blocking any other use or development of the Random Power principle. The technical mitigation action consists in moving from a monolithic to a hybrid approach, where optimal technologies are chosen for the "generator" and for the VLSI chip integrating all of the control functionalities and low-level processing. On the exploitation side, negotiation will focus on guaranteeing the research exemption, namely the possibility to use the project results for no-profit basic research activities, and for limiting exclusive license to specific fields of use.

5.6. Liaison with students teams and socio-economic studies

Involving M.Sc. student teams is certainly a significant part of dissemination and outreach activities. As far as Random Power, the focus will be on learning-by-doing, designing ad-hoc experiments and set-up to introduce students to the fundamentals of sensing (light & particles), signal processing to extract the raw information, post-processing to get to the observable of interest and optimisation. Designing a "curriculum" requires skills, experience and dedication and the partners intend to appoint a person with a solid background in high level education based on innovative methods to pursue this objective.

Random Power is sitting on a privileged stage across disciplines and compartments of society. The dynamics of the interaction among the different actors is a relevant case-study; partnering with expert teams with a strong background in economics, sociology and psychology would lead to a mutual benefit and it is expected to help the consortium to develop optimal strategies while providing investigators data of interest for their socio-economical analysis.

6. ACKNOWLEDGMENT

The activities reported in this paper have received funding by the ATTRACT project (https://attract-eu.com), funded by the EC under Grant Agreement 777222. Petr Svenda was supported under the GA20-03426S grant awarded by the Czech Science Foundation.

7. Bibliography

[1] C. Gentry, A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. http: //crypto.stanford.edu/craig.

[2] R. Stoian et al., Random network coding for wireless ad-hoc networks, 2009 International Symposium on Signals, Circuits and Systems, Iasi, Romania, proceedings published by the IEEE Xplore, DOI: 10.1109/ISSCS.2009.5206142

[3] H. Bauke and S. Mertens, Pseudo random coins show more heads than tails, J. Stat. Phys. 114 (2004), 1149-1169, DOI:10.1023/B:JOSS.0000012521.67853.9a

[4] J. Von Neumann, Various techniques used in connection with random digits, National Bureau of Standards Applied Mathematics Series. 12: 36-38, 1951

[5] S. Ergun, Vulnerability Analysis of a Chaos-Based Random Number Generator, 2018 IEEE International Conference on Systems, Man, and Cybernetics, DOI 10.1109/SMC.2018.00564

[6] S. Ghandali et al., Temperature-Based Hardware Trojan For Ring-Oscillator-Based TRNGs, arXiv preprint arXiv:1910.00735, 2019

[7] A.T. Markettos and S.W. Moore, The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators, CHES 2009 - Lecture Notes in Computer Science, vol 5747, DOI: 10.1007/978-3-642-04138-9_23

[8] A. Rukhin et al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standard Technology, SP 800-22 Rev. 1, 2008

[9] M. Sys, D. Klinec, P. Svenda, The Efficient Randomness Testing using Boolean Functions, Secrypt 2017, pp. 92–103, ISBN 978-989-758-259-2, 2017.

[10] H. Schmidt, Quantum Mechanical Random Number Generator, J. Appl. Phys. 41, 462-468,1970

[11] Miguel Herrero-Collantes, Quantum random number generators, Reviews of Modern Physics, Volume 89, January-March 2017, DOI: 10.1103/RevModPhys.89.015004

[12] ID Quantique, SA — Chemin de la Marbrerie 3, 1227 Carouge - Genéve — Switzerland

[13] B. Reulet, Method for generating random numbers and associated random number generator, patent no. WO2015 168798 A1

[14] R. Chan, Tunable tunnel-diode based digitised noise source, patent no. WO2018 045410 A1

[15] Nuclear Inst. and Methods in Physics Research, A 926 (2019)

[16] 28. W. Shockley and W.T. Read, Statistics of the recombination of Holes and Electrons, Physical Review 87 835-841 (1952)

[17] R. Heitz, Mechanism contributing to the noise pulse rate of avalanche diodes, Journal of Applied Physics, 36 3123-3131 (1965)

[18] M. Caccia et al., In-silico generation of random bit streams, Nuclear Inst. and Methods in Physics Research, A 980 (2020) 164480