Nuclear Inst. and Methods in Physics Research, A 980 (2020) 164480

Contents lists available at ScienceDirect

Nuclear Inst. and Methods in Physics Research, A

journal homepage: www.elsevier.com/locate/nima

In-silico 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

ARTICLE INFO

Keywords:
Random number generation
Silicon Photomultipliers
Cryptography

ABSTRACT

Silicon PhotoMultipliers (SiPM) are rapidly approaching a significant maturity stage, making them a well recognised platform for the development of evolutionary and novel solutions in a wide range of applications for research and industry. However, they are still affected by stochastic terms, notably a high Dark Count Rate (DCR), limiting their use when single photo-electron pulses convey the required information, for instance in chemiluminescence or fluorescence analysis of biological samples. In such applications, randomness of the spontaneous generation of carriers triggering the avalanche and the rate of occurrences is significantly decreasing the sensitivity of the system against solutions based, for instance, on traditional photo-multiplier tubes.

However, unpredictability of the "dark" pulses has a potential value in domains connected to encryption and, in general terms, cybersecurity. "Random Power" is a project approved within the ATTRACT call for proposals (https://attract-eu.com), having as a main goal the generation of random bit streams by properly analysing the time sequence of the Dark Pulses. The principle has been proven using laboratory equipment and its value assessed 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 board, integrating the system in a low cost, low power, scalable design is on-going.

The principle, protected by a patent application entered its international phase by the time of writing (application no.102018000009064, deposited at the Office of the Minister of Economic Development, as required by the Italian law; international PCT extension no.PCT/IB2019/058340 deposited in October 2019) will be described, together with the results obtained so far, the current development stage including an FPGA embedded Time-To-Digital Converter (TDC) and future perspectives.

1. Introduction

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

- in computer security and cryptography, the secrecy of a message (text, images or data) is guaranteed by three features: authentication, confidentiality and integrity [1]. Secrecy is strongly related to the production rate of encryption keys [2], namely random string of bits created explicitly for scrambling and unscrambling data. A software-based key generator can guarantee the required rate, but predictability is yet today considered a relevant issue [3]. In particular, the security of quantum-based communication protocols rely on the true randomness of the distributed key [4];
- the development of the Internet of Things (IoT) will lead to billions of interconnected devices and domestic appliances within a few years, making vulnerability to intrusion a serious concern [5–7] and raising a request for providing miniaturised, low cost, high performing security platforms;
- numerical simulation of complex phenomena is crucial for Science [8], Industry (aerodynamics, thermodynamics and manufacturing), Economics [9] and Sociology [10]. The quality of random numerical figures has been shown to be essential for the reliability of simulation outcomes [11,12];
- development of communication protocols overcrowded networks, for instance in Network Random Coding [13,14];
- gambling, where the role of randomness and unpredictability is obvious and poses significant challenges with the development of on-line platforms [15].

* Corresponding author.
E-mail address: massimo.caccia@uninsubria.it (M. Caccia).

https://doi.org/10.1016/j.nima.2020.164480
Received 14 December 2019; Received in revised form 12 June 2020; Accepted 28 July 2020
Available online 1 August 2020
0168-9002/

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. Algorithmic generation certainly benefits from computing power and optimal programming to achieve extremely high data rates, well in excess of 10 Gb/s. However, it suffers from fundamental and irreducible flaws:

- algorithms are deterministic. Therefore, the generated sequence is pseudo-random. It may have a period fitting most of the requirements but it will irreducibly be limited in its randomness properties (see for instance [11] and notably [16], the author of the famous quote *Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin*).
- the generated sequence relies on a numerical seed to initialise the procedure. An eavesdropper accessing it would have access to the full series of generated numerical figures.

Hardware generation of random numbers is based on natural phenomena, either described by classical physics or based on the quantum properties of Nature. A classical description is deterministic; even if the complexity of the system or its chaotic nature can be presumed to provide the base for practical unpredictability of the occurrences, the essence of the natural phenomenon is such that, once the initial conditions are known or reproduced in a controlled way, the dynamics of that system is well defined. 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).

Historically, the very first quantum random number generator was based on unstable radioactive nuclei, decaying emitting alpha, beta or gamma particles [17–19]. Emissions occur in an unpredictable way and the number of decays in a pre-defined time window follows a Poisson distribution. In other terms, the time lapse between two consecutive events follows an exponential probability density function, with a decay constant dependent on the isotope in use and on its radioactivity. Pulses are statistically independent and uncorrelated and random bit generation can be obtained in various methods, outlined for instance in [20]. 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. Finally, even in dedicated sites, handling and storage of the radioactive sources makes the system economically non-competitive.

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 [20] and references therein. This approach is certainly significant and it has been successfully commercially exploited (see for instance [21]). 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;
- in some of the embodiments, a low rate of extracted random bits per event.

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, as reported for instance in [22] and [23].

The device described here follows the same approach but with a different principle, described in Section 2. The actual implementation in a prototype board is described in 3 and the qualification according the test suite by the U.S. National Institute of Standard and Technology (NIST) and beyond are reported in 5. By the time of writing, a small form factor single generator board is being qualified; the essence of the board is an FPGA embedded Time-To-Digital converter introduced in 4. Conclusions and outlooks are reported in 6.

2. Fundamentals and basic principles

The TRNG proposed and qualified here is generating an unpredictable bit stream analysing the time series of self-amplified endogenous pulses due to stochastically generated charge carriers in an array of p–n junctions operated beyond the breakdown voltage, namely devices known as Silicon Photomultipliers or Multi-Pixel Photon Counters (for a recent review see for instance [24–27], complemented by articles in the same special issue of the journal devoted to applications). The quantum nature of the energy bands in semiconductor devices, the distribution of electrons on the energy levels according to the Fermi–Dirac statistics and the effects of local high electric fields provide the mechanism for pulse seeding. This is well known since the early days of the Silicon technology age and it has been described in a series of seminal papers, out of which it is worth mentioning at least the one by Shockley and Read [28]. Trap assisted thermally driven stochastic generation and recombination of free carriers is dominant in Silicon and other indirect semiconductor materials and it is the physical phenomenon at the base of the generation electrical current in the depletion region of p–n junctions [29]. Moreover, if the junction is operated in the avalanche regime [30,31], this mechanism is responsible for the occurrence of random pulses, as outlined in [32], where thorough modelling supported by experiments leads to the identification of four primary mechanisms, namely thermal generation, re-emission of carriers from metastable states, field assisted emission and band-to-band tunnelling. Irrespective from the mechanism, the key point here is that the high density of potential carriers, the random occurrence of bringing them to the conduction band together with the stochastics probability of inducing an avalanche breakdown leads to a series of independent pulses that are expected to follow a Poissonian distribution.

This is the principle at the base of the proposed device, consisting in a SiPM packaged in full darkness, identifying the randomly initiated pulses, time tagging them and turning the sequence of pulses in a series of bits. The amplitude of the pulses, millions of electrons over a few tens of nanoseconds, makes their identification robust and faultless; the avalanche time development, with a leading edge of the signal at the sub-nanosecond level, makes time tagging extremely precise; the endogenous generation mechanism makes the process robust, also against temperature variations expected to change the rate without impairing randomness. Pulse rates can achieve 1 MHz/mm^2 at room temperature at a few volts over breakdown, offering the possibility to engineer very compact devices with a very high bit extraction efficiency, currently at the level of 40%, namely two bits are generated every five tagged pulses.

The fundamental assumption behind any use of the spontaneously generated pulses for extracting random bits is that occurrences are independent. However, it is well known that SiPM suffer from "after-pulsing", namely signals induced by the release of charge carriers in the primary avalanche trapped by impurities or linked to the absorption of photons generated therein in the un-depleted region of every cell [25]. After-pulsing clearly introduces a correlation between neighbouring events, over a time scale determined by the specific sensor in use, its technology and temperature [33]. Even if after-pulsing has been reduced today to the percent level by most of the sensor producers, it is still an issue for streams of gigabit length. In the device proposed here, the problem has been fixed by a proper setting of the hold-off in the time stamping procedure. The net result, as reported in Section 5, is actually one of the major achievements, namely proven randomness of the raw bit stream, not requiring any post-processing.

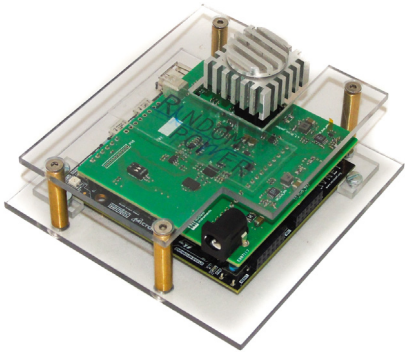

Fig. 1. The demonstrator board.

The principle described here is the core of a patent application, filed to the Italian Patent Office in October 2018 and extended internationally after a favourable report in October 2019 (patent application no. PCT/IB2019/058340).

3. The demonstrator and prototype boards

After the qualification of the principle with advanced laboratory equipment, a first demonstrator based on commercially available components was produced. The board, shown in Fig. 1, has dimensions of $7.5 \times 7.5 \times 5$ cm^3. It has a two tier structure where:

- the first tier comprises the circuits for SiPM biasing, via a Nuclear Instrument NIPM12 module [34], and time stamping through a TI TDC7200 Time-To-Digital converter [35]
- the second tier board is a single core commercial platform for FPGA development [36].

The SiPM in use is a S13360-1350 sensor by Hamamatsu, encapsulated in a TO8 package with a Peltier cell to control temperature. The SiPM was embedded in a heat sink in order to achieve a more efficient thermal exchange. The TO8 package also includes a thermistor for temperature reading.

The HV module can provide a bias in the 20–100 V range, with a feedback system to stabilise the gain against temperature variations, if required. The SiPM output is connected to a comparator, with a threshold controlled by a dedicated DAC. The leading edge of the comparator is the stop signal for the TDC and it is used to stamp the time of arrival of the Dark Pulses.

The TI-TDC features a granularity of 12 ps and it is commercially available at a price of less than one dollar per piece. However, since it was engineered for LIDAR applications, it is characterised by a low throughput, not exceeding a few tens of KHz, de facto limiting the system performance.

Time stamps measured by the TDC are processed by the FPGA. The bit extraction algorithm is applied within the FPGA and the resulting bits are sent to the System on Chip (SOC). The SOC is a custom unix server that is accessible through a web-socket protocol. It receives the command that allows to control the DAC for the Peltier Cooler, the sensor bias, and the comparator settings, delivered to the FPGA on board. The SOC receives from the FPGA the bits and makes them available as text on a webpage.

A Python/Matlab based GUI was designed in order to send the command sequence and read the bits, providing as well simple on-line bit quality tests. Although the board allows to test all the principles and functionalities, it is hardly useable in a real use case since its bit rate, taking in account the TDC throughput and the data transmission, does not exceed 20 kb/s, and the communication protocol cannot be presumed to work, for example, in a server farm.

Fig. 2. The prototype board.

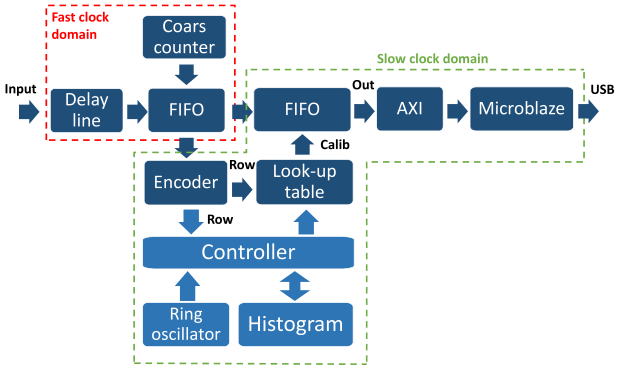

Fig. 3. Block diagram of the FPGA embedded Time-To-Digital converter.

3.1. The prototype board

Following the feasibility studies performed with the demonstrator, a new custom board was designed by Nuclear Instruments, assisted by the team at AGH. The board, shown in Fig. 2, is significantly smaller ($8 \times 3.5 \times 0.4$ cm^3) than the demonstrator and all the electronic components are fitted on a single tier. It has significant differences with respect to the previous one in terms of communication, now based on USB and FTDI dx22 driver and the FPGA, a Spartan 7 embedding the TDC and the Micro Blaze processor. The latter provides the communication layer between the USB and the FPGA peripherals. Further details on the TDC programmed on the FPGA will be reported in the next section. Moreover, GPIO pins are present for debugging purposes, together with a JTAG port for the FPGA and flash memory programming. On the board it is possible to mount a 1.3×1.3 mm^2 SiPM or a 3×3 mm^2 SiPM. The board has a TMP100 digital temperature sensor but no active feedback was required.

In terms of bit generation rate and data transmission speed, the new board can guarantee a throughput in excess of 1 Mb/s, making it suitable for the use in a real case scenario.

4. Development of an FPGA embedded Time-To-Digital converter

4.1. Description of the TDC

A custom TDC was implemented in the Xilinx Spartan-7 FPGA. The block diagram of the TDC is presented in Fig. 3. A delay line and a coarse counter are the main parts of the TDC. They are implemented in the fast clock domain. The delay line is built from carry chain blocks (Carry4) where input signal propagates through multiplexers. Fig. 4

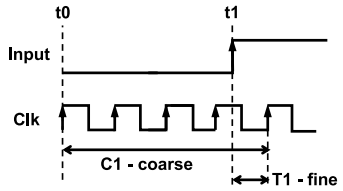

Fig. 4. Coarse and fine counters with respect to internal clock.

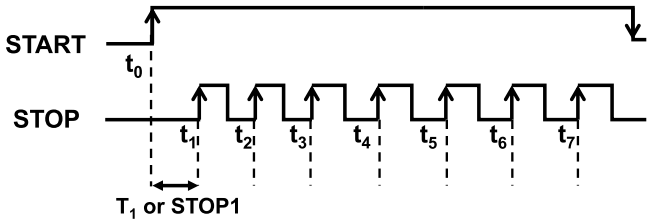

Fig. 5. Generation of time stamps by the TDC in response to input signals.

presents the principle of the TDC operation. The coarse counter records a number of cycles of the reference clock (coarse value C1). The delay line is used to measure the fine value (fine value T1). The fine value is defined by a multi-tap delay chain. It is covering more than one clock cycle and is measured with respect to the reference clock rising edge.

Time since a start signal is calculated as:

$$t1 = C1 \cdot T_{Clk} - T1 = C1 \cdot T_{Clk} - \frac{F1}{F_{max}} \cdot T_{Clk} \quad (1)$$

where T_{Clk} is the period of the reference clock. $F1$ is the number of delay units (taps) in the carry chain that the input signal managed to propagate through before a rising edge of the reference clock arrived. F_{max} is the number of taps that the input signal propagates through during one cycle of the reference clock ($F1 \leq F_{max}$). The TDC works in three modes: measurement mode, startup calibration and on-line calibration. The TDC enters the startup calibration mode after each power cycle. During this phase the delay of each unit in the carry chain is calculated and stored in the look-up table. In measurement mode, the data from the delay line and the coarse counter are stored in the first FIFO which crosses the clocks domains. The encoder converts the thermometric code from the delay line. Afterwards, data propagates through the look-up table to be converted into calibrated delays. The Microblaze reads the data through the second FIFO. Since delays in the carry chain change with the variation of the temperature and supply voltage, an on-line calibration mode was implemented, recalculating the delays without stopping the measurement. The structure of the encoder and the delay line was optimised to maximise the uniformity of the delays in the single units (taps) in the carry chain and to reduce the so-called "bubble problems".

4.2. Qualification tests of the TDC

The FPGA Time-To-Digital converter operates with two input signals: "Start" and "Stop". In response to a rising edge (event) of both signals the TDC produces a time stamp. The measurement is initialised by the first "Start" event. Afterwards, TDC detects a user defined number of consecutive "Stop" events and awaits for the next "Start". Fig. 5 presents the naming convention of both inputs, for the exemplary illustration of having required seven stops in a row.

The embedded FPGA Time-To-Digital converter was qualified in three key tests. The aim of the first two tests was a qualification of the delay chain in the TDC. For this part of the qualification tests the "Stop" signal was strictly deterministic and issued by a function generator not synchronous to the FPGA clock. As a consequence, each time an event is detected by the TDC the fine counter can propagate to a different tap number with a uniform distribution. However, when the event rate is fixed and multiple of the coarse clock period, the fine counter corresponding to two sequential Stops are expected to be the same, modulo left-over statistical fluctuations or systematic effects. For qualification purposes, fine counters for two consecutive stops are subtracted. Their distribution against the tap number of the first event is recorded and their distribution shown in Fig. 6 (left), for a period of 200 ns (multiple of the coarse counter period). The differences nicely align along an average zero value, with a width of the distribution providing an indication of the time resolution.

During the second qualification test the "Stop" period was not multiple of the coarse counter period (Fig. 6 - right). In the reported test, it was set to 201.2 ns. In such situation, the period is "shifted" from the nearest multiple of 4 ns by −1.2 ns (200 ns – 201.2 ns) and 2.8 ns (204 ns – 201.2 ns). Taking into account that the average duration of a tap is 73 ps, it can be calculated that the shift in the tap number difference for two sequential Stops correspond to −16.4 taps and 38.4 taps respectively. Once more, no systematic error was observed.

The third qualification test of the embedded FPGA Time-To-Digital converter was performed in comparison with the Texas Instruments TI-TDC 7201. The TI-TDC has excellent LSB resolution on a single shot (55 ps) and standard deviation (35 ps over a time lapse up to 1 μs). The FPGA embedded TDC and the TI-TDC were fed with the same Start and Stop signals, where the "Start" was provided with 200 ms period by a function generator and the "Stop" signals were generated by the stochastic Dark Pulses of a SiPM. Fig. 7 illustrates the results of the test. Time stamps generated by FPGA TDC are plotted against corresponding

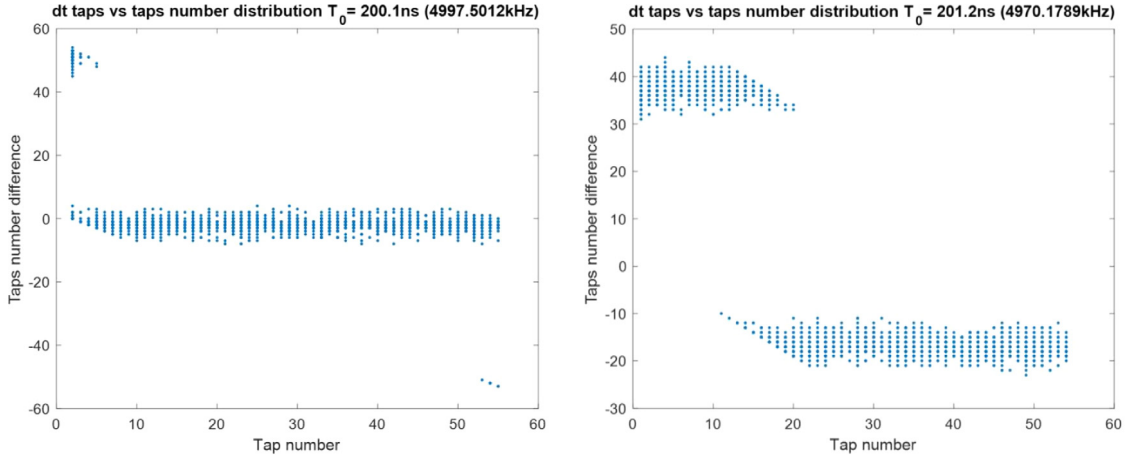

Fig. 6. Qualification tests of delay line with various "Stop" signal period: 200 ns (left) and 201.2 ns (right).

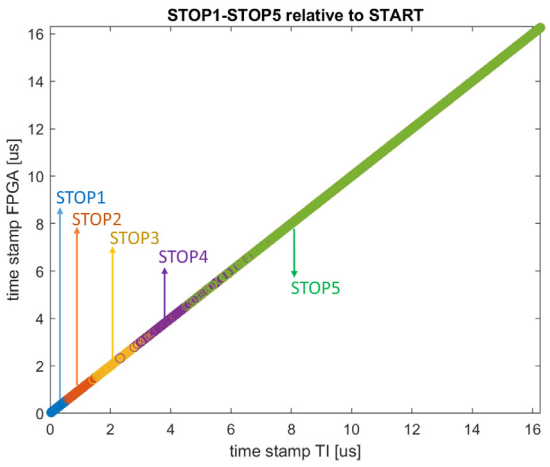

Fig. 7. Comparison of time stamps generated by TI TDC and FPGA TDC for the same stochastic events.

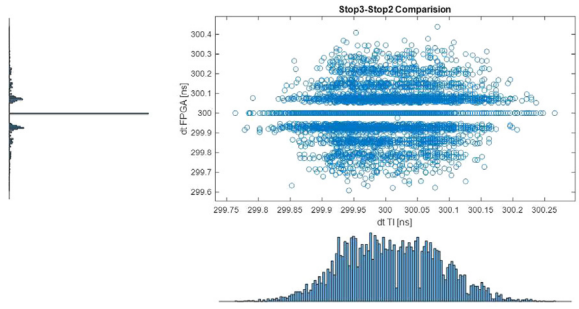

Fig. 8. TI TDC and FPGA TDC detecting deterministic events of Stop signal. Event generation period is 300 ns.

time stamps of TI TDC. It was confirmed that no systematics was affecting the FPGA TDC.

As a final test, the distribution of the measured duration of a nominal 300 ns long time window set by a pulse generator was considered. Fig. 8 shows the scatter plot of the measured durations by the FPGA and TI TDC's, together with the marginal histograms. The mean value of the period measured by the FPGA is 299.999 ns against 300.009 ns for the TI TDC. The latter, featuring a 12 ps granularity, actually measures the intrinsic width of the pulse duration by the waveform generator, corresponding to 76 ps. In the FPGA TDC, the granularity of the delay line actually corresponds to an average value of 73 ps and the effect is clearly visible in the marginal histogram, with no evident systematics.

5. Qualification of the generated bit stream

Raw bit streams generated by the demonstrator and the prototype boards were qualified against the test suite by the National Institute of Standard and Technology [37,38]. However, since these tests are hardly applicable in real-time, a new approach was also implemented, following a study on the use of Boolean functions [39]. The main results are reported in the two following subsections.

5.1. The NIST test suite

The battery consists in statistical methods to qualify the hypotheses that the bit sequence is unpredictable and corresponds to an equal probability to score a value of 0 or 1. Simpler tests, like the Monobit or the Frequency tests, measure the asymmetry, or bias, between the 0s and 1s. Other tests, more complex, evaluate for instance the Shannon entropy, the distribution of the cumulative sum of sub-sequences, the

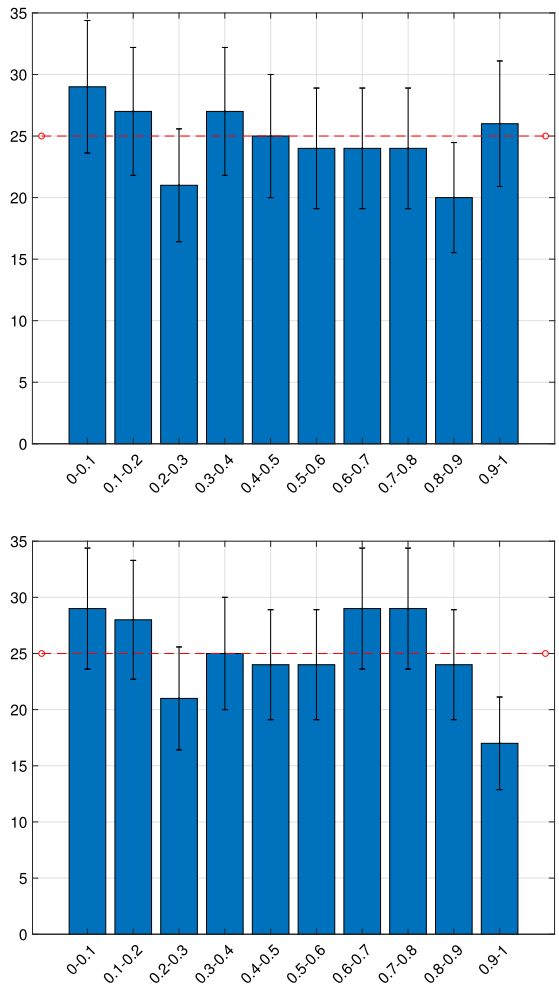

Fig. 9. P-Value distribution for two tests: the Monobit(upper panel) and the Cumulative Sum Test(lower panel). The dashed red line corresponds to the expected number of entries/bin presuming a uniform distribution.

rate of particular patterns (Matching Template) and the distribution of the occurrences of possible combination of 2^n bits. Altogether, more than 170 test are performed on each sequence.

Each test is performed on N sub-sequences of M elements each, that is $M \cdot N \leq$ Sequence Length. The minimum request are that $N \geq 10^5$ for all the tests except the Universal test that requires at least 10^6 bits. The results of the test is a p-value with respect to the binomial hypotheses. The p-value distribution is expected to be uniform, so far a fraction of sequences equal to the p-value limit chosen to assess the randomness of a sequence is expected to fail the tests [38].

From the demonstrator board a sequence of 10^8 bit was generated and tested. The sequence was sliced in 100 sequences of 10^6 bits. Exemplary *pval* uniform distributions for two tests, the Monobit and the Cumulative Sum Test are reported as exemplary illustration in Fig. 9.

In Fig. 10 the percentage of the sequences that passes the test are reported for each test. It can be seen that the result is comparable with the expectation where more than 95% of sequence are random, since the a $pval = 0.05$ is chosen as limit.

The same test were performed on a set of bits obtained with the prototype board and the results are reported in Fig. 11.

In both cases the original raw sequence can be declared random, since the percentage of sub-sequences that passes the single test are in accordance with the uniform distribution hypothesis.

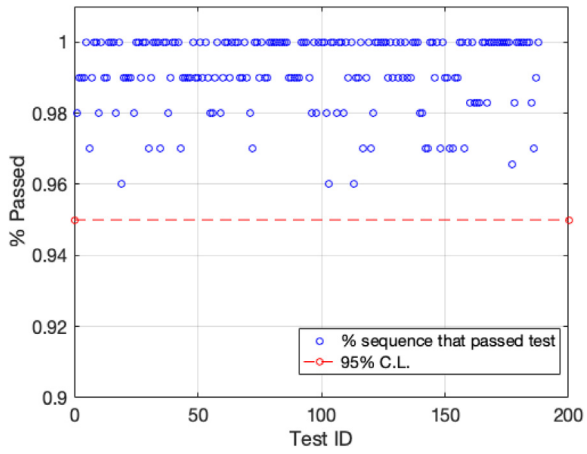

Fig. 10. Percentage of sequences, generated with the prototype board, that passes the test for each of the 170 test. The x-axis reports the test index, and the y-axes the percentage of sequences that passed the test.

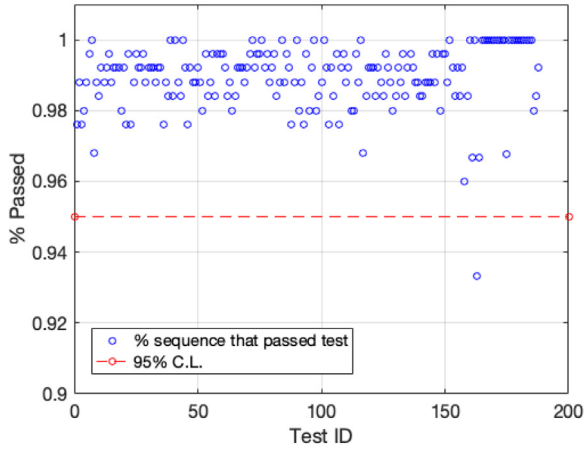

Fig. 11. Percentage of sequences, generated with the new board, that passes the test for each of the 170 test. The x-axis reports the test index, and the y-axes the percentage of sequences that passed the test.

5.2. A test suite based on boolean functions

While commonly used randomness testing batteries like STS NIST contain predefined suite of fixed tests, the *booltest* suite [39] constructs randomness distinguishers dynamically, 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 *booltest* suite was applied to the evaluation of pseudorandom generators like block ciphers or hash functions, but without a specific focus on truly random number generators.

The *booltest* approach is inspired by the well-known Monobit test, which examines the proportion of ones and zeros within the provided sequence. The frequencies of ones and zeros computed in the Monobit test represent results of a boolean function $f(x_1) = x_1$ when applied to all bits of the tested sequence. The generalisation to an arbitrary boolean function $f(x_1, x_2, \ldots, x_m)$ of m variables is applied to non-overlapping blocks of m subsequent bits. The resulting distinguisher (boolean function) is first constructed for all possible monomials of the specified degree (typically 1, 2 and 3), followed by the second combination phase exhaustively combining only selected best-performing monomials from the first phase. For more details, the reader is referred to [39] (see Fig. 12).

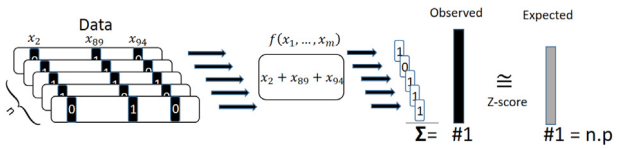

Fig. 12. The example evaluation of the analysed data and computation of *Z-score*, using boolean function $f(x_1, \ldots, x_m) = x_2 + x_{89} + x_{94}$. *Z-score* is computed as the statistical distance of observed #1 for tested data and #1 = *n.p* expected for truly random data [39].

Table 1
A summary of results obtained for three specific configurations of *booltest* (block length = [128, 256, 512], monomial degree 2, number of monomials 2) with observed and expected reference range of *z-scores*. One hundred non-overlapping sequences, each 10 MiB long were analysed, totalling 1 GiB of analysed data.

Booltest configuration	Observed range (from 100 runs)	Reference range (from 10^5 runs)
b = 128, deg = 2, k = 2	4.794 – 6.320	4.410 – 7.196
b = 256, deg = 2, k = 2	5.245 – 6.516	4.831 – 7.292
b = 512, deg = 2, k = 2	5.658 – 6.990	5.185 – 7.494

The *booltest*'s exhaustive search is parameterised by the degree of monomials constructed (typically 1, 2, and 3) as well as the number of combined monomials (typically 1 and 2). Higher the degree or number of monomials, more complex distinguishers can be constructed — but the parameters are limited by quickly increasing search space, which has to be exhaustively analysed.

Another important parameter is the length of the elementary block over which are the polynomials evaluated. For PRNGs, multiplies of 128 are typically used as the analysed functions internally operate with structures of such sizes. As the *booltest* analyses correlations between the groups of bits at the same positions of the block, the proper partitioning of the analysed data into series of blocks is significantly impacting the bias detection ability of the tests based on the boolean functions. The "correct" partitioning is easier to perform for PRNGs, where the lengths of internal structures are fixed and known while being more difficult for TRNGs based on the sampling of some physical phenomena. In the preliminary tests performed here, four output random bits are extracted from the series of seven subsequent time stamped Dark Pulses. Once extracted, the next seven events are sampled and processed to create another four subsequent random bits. To test for potential correlation between the groups of four extracted bits and seven events, *booltest* parameterised with the block length of 28 and 56 bits are analysed. The commonly used longer blocks of 128, 256, and 512 subsequent bits are also tested to detect correlation among larger groups of bits.

The *booltest* was applied over 100 sequences produced by the device with 10^7 bytes each (1 GiB total). The obtained results with the measured *Z-score* for each analysis compared with the expected reference *Z-score* range for truly random data are shown in Table 1. The reference *Z-scores* were obtained from 10^5 reference runs with reference sequences believed to be truly random (PRNG constructed from the AES block cipher with full number of 10 rounds was used[1]). The range of reference *Z-scores* corresponds to the confidence level of 10^{-5} typically used for the evaluation of standard randomness testing batteries like STS NIST or Dieharder. As no *Z-score* more extreme than from reference runs, the null hypothesis of analysed data being random cannot be rejected on the confidence level and *booltest* parameterisation used.

Another analysis of *booltest* results is the frequency of occurrence of pairs of specific bits in the several best-performing (highest *z-score*) monomials. Intuitively, if any pair is significantly more common than the expected average, the indicated bits are likely biased. No prominent pair of bits was found for block lengths of 28 and 56 bits as seen on Fig. 13.

[1] No distinguisher for AES-based PRNG better than for AES limited to 5 rounds is currently known.

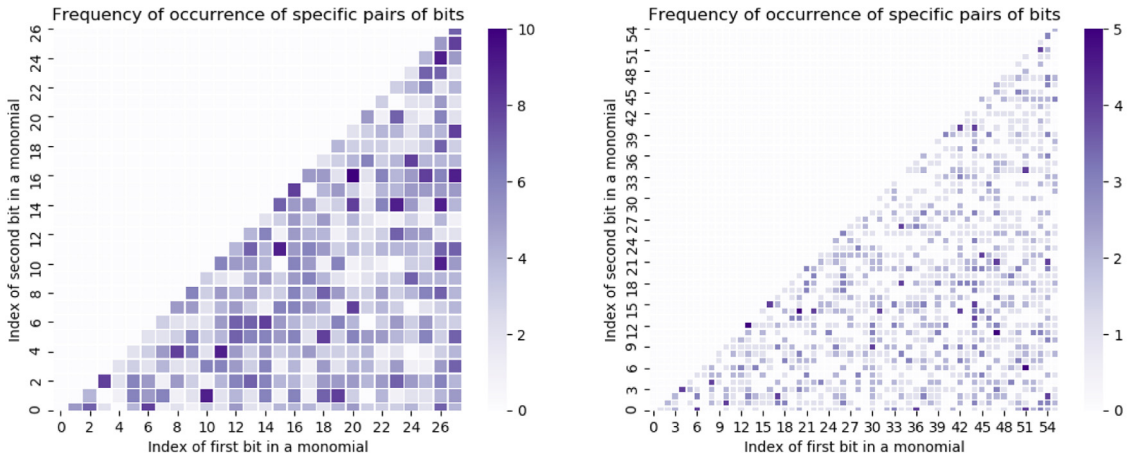

Fig. 13. A heatmap showing the occurrence of specific pairs of bits in the best performing monomials found by *booltest* for block length of 28 and 56. The 15 best-performing monomials are considered over 100 analysed files. No unexpectedly frequent pair of bis is visible.

6. Conclusions and outlook

The principle and the actual implementation of a True Random Number Generator based on the analysis of the time series of Dark Pulses in a SiPM was presented. The qualification of the bit streams shows that the raw data appear to be truly unpredictable and satisfy the most stringent tests. The robustness of the proposed method and the ultimate possibility to embed all the functionalities in a single ASIC pave the way for its exploitation, in Research applications and beyond.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

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.

References

[1] Scott Durrant, Random Numbers in Data Security Systems - Intel Random Number Generator, Intel Platform Security Division. doi:10.1/1.113.3231.
[2] Claude E. Shannon, Communication Theory of Secrecy Systems, Bell Syst. Tech. J. 28–4 (1949) 656–715.
[3] Omar Salhab, et al., Survey paper: Pseudo random number generator and security tests, J. Theor. Appl. Inf. Technol. 96 (7) (2018) 1951–1970.
[4] G. Benenti, G. Casati, G. Strini, Principle of Quantum Computation and Information, Volume I, World Scientific, 2004.
[5] M.A. Razzaq, et al., Security issues in the Internet of Things (IoT): A comprehensive study, Int. J. Adv. Comput. Sci. Appl. 8 (6) (2017) 383–388.
[6] M. Hossain, et al., Towards an analysis of security issues, challenges and open problems in the Internet of Things, in: 2015 IEEE World Congress on Services, New York, U.S.A. proceedings published by the IEEE Xplore, http://dx.doi.org/10.1109/SERVICES.2015.12.
[7] K. Zhao, L. Ge, A survey on the Internet of Things security, in: 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China, proceedings published by the IEEE Xplore, http://dx.doi.org/10.1109/CIS.2013.145.
[8] G. Cowan, The Monte Carlo Techniques, Particle Data Group, 2017, available at http://pdg.lbl.gov/2019/reviews/rpp2018-rev-monte-carlo-techniques.pdf.
[9] D. Crnjac Milic, Ljiljanka Kvesic, Role of Random Numbers in simulation of economic processes, in: Interdisciplinary Management Research, Vol. 4, 2007.
[10] H. Rahmandad, John D. Sterman, Reporting Guidelines for simulation-based research in social sciences, Syst. Dyn. Rev. 28 (2012) http://dx.doi.org/10.1002/sdr.1481.
[11] H. Bauke, S. Mertens, Pseudo random coins show more heads than tails, J. Stat. Phys. 114 (2004) 1149–1169, http://dx.doi.org/10.1023/B:JOSS.0000012521.67853.9a.
[12] P- Ball, Random numbers hit and miss - Math pinpoints cause for faulty computer simulations, Nature (2003) http://dx.doi.org/10.1038/news030728-1.
[13] A. Ahlswede, et al., Network information flow, IEEE Trans. Inform. Theory 46 (4) (2000).
[14] R. Stoian, et al., Random network coding for wireless ad-hoc networks, in: 2009 International Symposium on Signals, Circuits and Systems, Iasi, Romania, proceedings published by the IEEE Xplore, http://dx.doi.org/10.1109/ISSCS.2009.5206142.
[15] Berget, et al., Central Random Number Generator for Gaming System, Patent Number: 5, 779545, Date of Patent: Jul.14, 1998.
[16] J. Von Neumann, Various techniques used in connection with random digits, Natl. Bur. Stand. Appl. Math. Ser. 12 (1951) 36–38.
[17] B. Manelis, Generating random noise, Electronics 8 (1961) 66–69.
[18] H. Schmidt, Quantum Mechanical Random Number generator, J. Appl. Phys. 41 (1970) 462–468.
[19] A. Figotin, et al., Random number generator based on the spontaneous alpha-decay, 2004, US patent no. 6, 745, 217B2.
[20] Miguel Herrero-Collantes, Quantum random number generators, Rev. Modern Phys. 89 (2017) http://dx.doi.org/10.1103/RevModPhys.89.015004.
[21] ID Quantique, SA | Chemin de la Marbrerie 3, 1227 Carouge - Genéve | Switzerland.
[22] B. Reulet, Method for generating random numbers and associated random number generator, patent no. WO2015 168798 A1.
[23] R. Chan, Tunable tunnel-diode based digitised noise source, patent no. WO2018 045410 A1.
[24] F. Acerbi, S. Gundacker, Undesrtanding and simulating SiPM, Nucl. Instrum. Methods Phys. Res. A 926 (2019) 16–35.
[25] C. Piemonte, A. Gola, Overview on the main parameters and technology of modern Silicon Photomultipliers, Nucl. Instrum. Methods Phys. Res. A 926 (2019) 2–15.
[26] R. Klanner, Characterisation of SiPMs, Nucl. Instrum. Methods Phys. Res. A 926 (2019) 36–56.
[27] P.P. Caló, et al., SiPM readout electronics, Nucl. Instrum. Methods Phys. Res. A 926 (2019) 57–68.
[28] W. Shockley, W.T. Read, Statistics of the recombination of Holes and Electrons, Phys. Rev. 87 (1952) 835–841.
[29] S.M. Sze, Semiconductor Devices, Physics and Technology, John Wiley & Sons, 1985.
[30] K.G. McKay, Avalanche breakdown in Silicon, Phys. Rev. 84 (1954) 877–884.
[31] B. Senitzki, J.L. Moll, Breakdown in Silicon, Phys. Rev. 110 (1958) 612–620.
[32] R. Heitz, Mechanism contributing to the noise pulse rate of avalanche diodes, J. Appl. Phys. 36 (1965) 3123–3131.
[33] S. Cova, et al., IEEE Electron Device Lett. 12 (12) (1991) 685?687.
[34] http://www.nuclearinstruments.eu/nipm12.html.
[35] http://www.ti.com/product/TDC7200.
[36] http://zedboard.org/product/minized.
[37] https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.
[38] SP 800-22 Rev. 1 (08/10/2008), L. Bassham, others, National Institute of Standard Technology.
[39] M. Sys, D. Klinec, P. Svenda, The efficient Randomness Testing using Boolean Functions, in: Secrypt 2017, ISBN: 978-989-758-259-2, 2017, pp. 92–103.