Towards a high-speed quantum random number generator

Damien Stucki[1a], Samuel Burri[b], Edoardo Charbon[b], Christopher Chunnilall[c], Alessio Meneghetti[d], Francesco Regazzoni[e]

[a]ID Quantique SA, Ch. de la Marbrerie 3, CH-1227 Carouge, Switzerland; [b]EPFL (SCI STI EC), INF 131 (Bâtiment INF), Station 14, CH-1015 Lausanne, Switzerland; [c]National Physical Laboratory (NPL), Hampton Road, Teddington, TW11 0LW, UK; [d]Department of Mathematics, University of Trento, Via Sommarive, 14, Trento, Italy; [e]Delft University of Technology, Faculty of Electrical Engineering, Mekelweg 4, 2628 CD Delft, The Netherlands

ABSTRACT

Randomness is of fundamental importance in various fields, such as cryptography, numerical simulations, or the gaming industry. Quantum physics, which is fundamentally probabilistic, is the best option for a physical random number generator. In this article, we will present the work carried out in various projects in the context of the development of a commercial and certified high speed random number generator.

Keywords: Quantum random number generator, QRNG, high-speed, randomness extractor, model, metrology, photon counting, photon counter, silicon avalanche photodiode

1. INTRODUCTION

Random numbers play an important role in a variety of applications such as cryptography, numerical simulations, or the gaming industry. There are two types of random number generator: algorithmic and physical. The first type is implemented on computers, which are deterministic, i.e. for a given input, the output will always be the same. The second type relies on classical or quantum physical processes. Random number generators based on classical physics are fundamentally deterministic – as is classical physics – even if the complexity of the system can hide the determinism. Random number generators based on quantum physics are true random number generators as quantum physical phenomena are intrinsically probabilistic.

In cryptographic applications, random numbers are vital whenever confidentiality and secure authentication are needed. To ensure the confidentiality of a message, a clear-text message is encrypted using a key. The quality of random numbers is vital to guarantee the strength of the key, and thus the security level of the cipher. As always in the field of cryptography, random numbers are also necessary to ensure the authenticity of communications by providing material for secret authentication keys. Random numbers are also used in numerical simulations. For instance, Monte Carlo simulations require high bit rates of high quality random numbers. The gaming and lottery industry also requires high quality random numbers to guarantee, by law, a uniform winning probability for all players. For all these applications, high-speed and high quality random number generators are required.

The presented quantum random number generator is based on a matrix of single-photon avalanche diodes (SPADs) (Swiss NCCR-QP FastQ project). The SPADs matrix is illuminated by a low intensity source of photons. During the propagation between source and detectors, the photon behaves as a wave and is described by a wave-function. Then, the photon will collapse randomly in the image plane, where the SPADs are located. Thus, the SPADs in the array will randomly click and generate a raw bit sequence. The generation of the random bit sequence can be obtained by pairing neighboring SPADs and by keeping only the case in which exactly one detector in the pair clicks. The bit value '1' ('0') is associated with a detection in the 'first' ('second') detector of the pair. Another possibility to extract a random bit sequence from the detection sequence is to evaluate the entropy of the sequence and then apply an extractor algorithm to generate the random sequence (Swiss NCCR-QSIT CREx project).

In order to better understand the behavior of the quantum random number generator, a model has been developed. In the model, various parameters were included: the detection efficiencies and dark count, after-pulsing, and cross-talk

[1] Damien.Stucki@idquantique.com

probabilities of the SPADs; the incident light distribution. Finally, the model assumes that the quantum random number generator is a Markov chain of order 1. The entropy and the collision entropy rate are computed from the model, which can be compared with the entropy computed from the raw sequence. To precisely estimate the values of the input parameters, measurements have been made in collaboration with European National Metrology Institutes through the European Metrology Research Programme (EMRP) project IND06-MIQC.

In section 2, the development of the SPADs matrix will be presented. In section 3, the procedure to extract the random sequence will be presented. In section 4, the metrological work and the model will be presented. Finally, in section 5 we will present how we expect to assemble all the components described in the paper to obtain a certified QRNG.

2. DEVELOPMENT OF A DETECTOR MATRIX

The goal of the NCCR-QP FastQ project is to develop a high speed and low cost QRNG. For this development, ID Quantique and EPFL developed SPAD arrays. ID Quantique provided specifications and EPFL designed the matrices in CMOS technology. Two matrices have been developed: the first comprises 300 SPADs (organized in 10 rows of 30 pixels, as shown in M1 below); the second comprises 1440 SPADs (30 rows of 48 pixels, M2 below). The layout of the two matrices is presented in Figure 1.

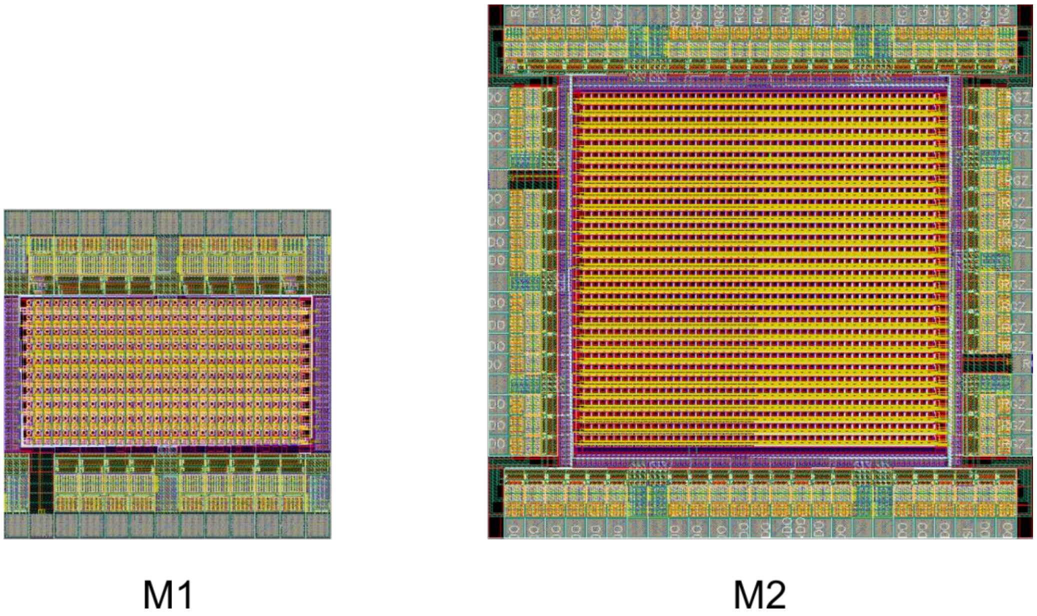


Figure 1: Layout of SPAD matrices. M1: 10 x 30 SPAD matrix. M2: 30 x 48 SPAD matrix.

Each pixel has a register bit associated with it. For M1, each row, or chain, of 30 register bits is clocked out on a clock cycle (30 clock cycles to clock out matrix). M2 works similarly. The last register of each chain is connected to an output pad to transfer the signal to an input of a field programmable gate array (FPGA). Some control signals are shared among the SPADs: a charge (CHG) signal to activate the SPADs; an off (OFF) signal to inhibit the SPADs; an enable (ENA) signal to capture the events in a latch; clock (CLK), load (LD) and reset (nRS) signals to control the registers. Additionally, a mask (MSK) signal can be used to disable noisy SPADs. It allows one to address each detector individually and inhibit noisy detectors by writing in a control register.

2.1. The mode of operation

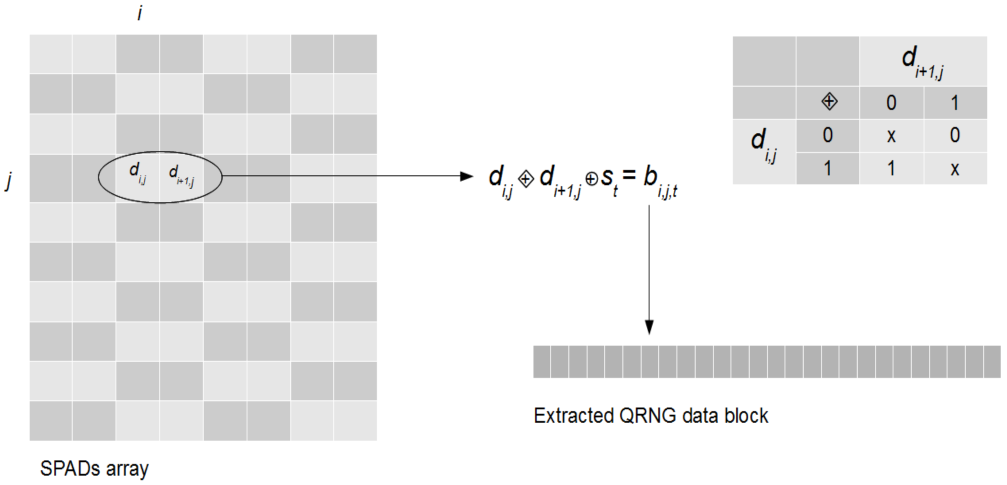
The two matrices are operated identically. During the startup phase, all noisy detectors are identified and deactivated. Then, during the normal operating time, there exist two phases. During the first phase ("capture"), the chip is activated with CHG set to low and OFF set to high. The output of each SPAD is captured by the latch when ENA is high. The output value of each detector can be captured at the same time. During the second phase ("readout"), the captured values in the latches are transferred to the shift registers that are read serially through the output pads (one per chain) to register the value of each SPAD in the FPGA. The sequence 'capture phase-read out phase' is repeated in a loop. At each clock cycle, the values in the registers are pushed by one step towards the registers' outputs. When they are in the last register they are transferred to the FPGA [1].

3. EXTRACTION OF RANDOM BIT SEQUENCE

Because of imperfections of the any physical device, it is difficult to generate perfect random sequences even if in theory a QRNG should. Thus, some post-processing is required to ensure high quality of the randomness of the generated bit sequence. This post-processing is done with a so-called randomness extractor. The principle of an extractor is to extract a sequence of k bits with very high entropy from a longer sequence of n bits with less entropy. Different algorithms can be applied to extract random bit sequences. Three categories of randomness extractors can be distinguished [2]: deterministic extractors, seeded extractors and multiple-source extractors. Two possibilities are presented below.

3.1. Pairing and switching or Von Neumann type extractor

This extractor is a deterministic extractor. The SPADs in the matrix are grouped by pair $(d_{i,j};d_{i+1,j})$. We discard the cases with no detections or two detections in the pair and we keep only those cases in which one detection occurs. The bit value is defined as in the table of Figure 2. The bit value is switched periodically by xor-ing it with s_t. This post-processing will remove the possible bias in detection efficiencies of the SPADs. However, it will not remove correlations. Although this extractor is not perfect, it has one main advantage: it requires very low processing resources, thus resulting in low production costs, a very important consideration in a commercial product.



i
j
$d_{i,j}$ $d_{i+1,j}$
$d_{i,j} \oplus d_{i+1,j} \oplus s_t = b_{i,j,t}$
Extracted QRNG data block
SPADs array

		$d_{i+1,j}$	
	⊕	0	1
$d_{i,j}$	0	x	0
	1	1	x

Figure 2: Pairing and switching extractor principle.

3.2. 2-universal hashing extractor

This extractor is a seeded extractor. An easy way to implement 2-universal hashing function is a bit-matrix-vector multiplication. The matrix is random and the seed of the extractor and it must be ε-close to a uniform distribution (the distribution expected for a random sequence). To generate the random matrix, we can XOR multiple matrices coming from independent sources. This principle is presented in Figure 3. This extractor has the advantage of generating random bit sequences, which are provably random according to information theory [3].

4. METROLOGY OF RANDOM NUMBER GENERATOR COMPONENTS

As mentioned before, even though, in theory, a good QRNG will generate perfect random bit sequences, in practice some imperfections will appear. To estimate theses deviations from theory, a precise characterization of the components is necessary, so as to estimate the entropy through a model of the QRNG. With the estimation of the entropy, the extractor can be optimized. The metrology and model of the QRNG are a component of the European Metrology for Industrial Quantum Communications (MIQC) project [4]. Note that another model has also been developed in the scope of the NCCR-QSIT CREx project. For the MIQC project, two QRNGs are studied:

- A QRNG based on a photon source, a beam splitter and two single photon detectors;

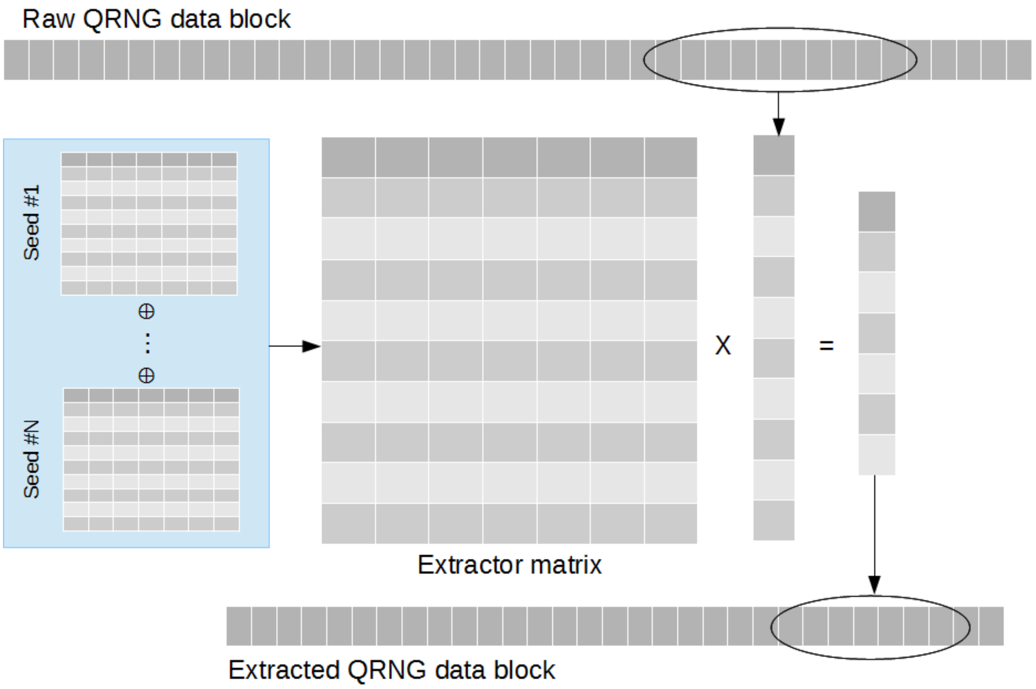
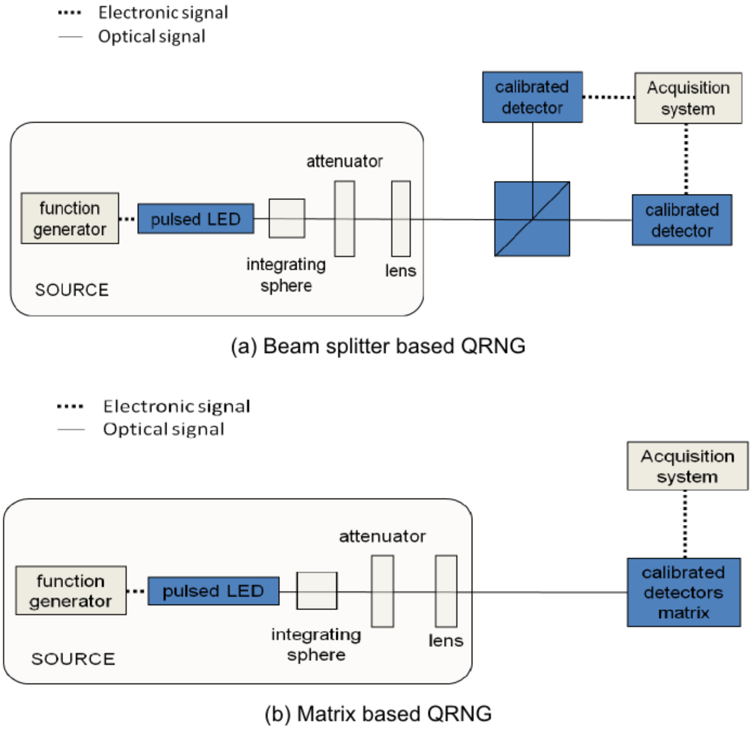


Figure 3: 2-universal hashing function extractor principle.



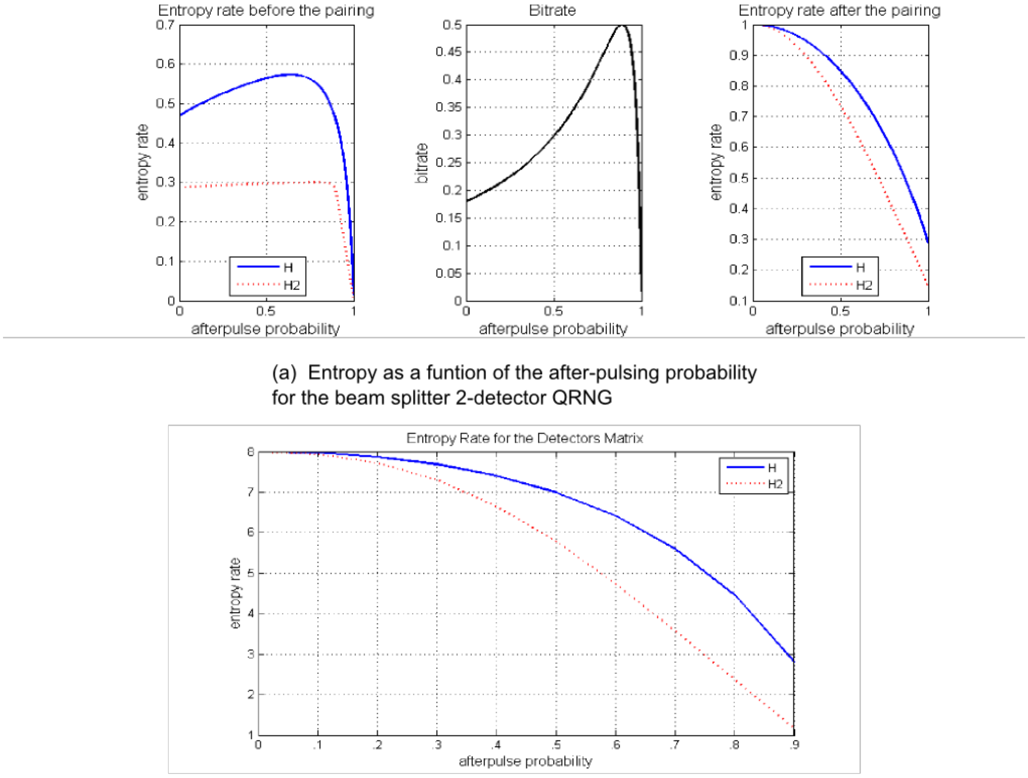
(a) Beam splitter based QRNG

(b) Matrix based QRNG

Figure 4: QRNGs principle for metrology.

- A QRNG based on a photon source and a SPAD array.

The setups are presented in Figure 4. The photon source is an LED emitting at 830 nm (Hamamatsu, L3989). The beam splitter is a 1 inch (25.4 mm) non-polarizing cube beam splitter (Thorlabs, BS014, anti-reflection coated for 700-1100 nm wavelengths). The bucket detectors for the first QRNG are silicon SPADs (ID Quantique, id100-20, 350-900nm). The matrix detector is a 1 x 8 SPADs array (ID Quantique, id150, 350-900nm). In addition to these components, an integrating sphere/ lens combination is added to improve the flatness of the light beam profile. It is very important to ensure that the light intensity is almost identical on the full SPAD array, so as to avoid bias in the photon flux per SPAD. An attenuator can be added to reduce the photon flux.



(a) Entropy as a funtion of the after-pulsing probability for the beam splitter 2-detector QRNG

(b) Entropy as a function of the after-pulsing probability for 2 x 4 detector matrix.

Figure 5: Simulations of the entropy for beamsplitter and matrix QRNGs.

The model yields an estimation of the entropy. It assumes an order 1 Markov chain and takes account of important parameters: the spatial light distribution, the dark count, the detection efficiencies bias, the after-pulsing probability, and the crosstalk of SPADs. The entropy and the collision entropy are computed from the model with parameters values obtained from the components characterization. Estimation of the entropy is then compared to the measured entropy. Two simulations are presented in Figure 5.

5. HIGH SPEED RANDOM NUMBER GENERATOR

The final objective of these three projects is to develop certified high-speed random number generators. With the M2 (M1) SPADs matrix and the pairing and switching extractor, the bit rate should reach about 600 Mbits/s (70 Mbits/s). With the 2-universal hashing function, the bit rate should be of about 400 Mbits/s (45 Mbits/s). The best option to obtain a certification for a QRNG is to follow the procedure proposed by the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany [5]. The document presents the requirement for various classes of deterministic random number generators (DRNGs) and physical true random number generators (PTRNGs). Following these recommendations, it is possible to obtain Common Criteria certifications. Figure 6 presents the requirements for a PTRNG of class PTG.3. This is the strongest class proposed by the BSI and so random bit sequences generated by PTG.3 class PTRNG can be used for the more demanding applications. It requires internal tests of the entropy source, i.e. tests of the physical components, to detect failure of the entropy source. It also requires statistical tests of the raw random numbers to detect non-tolerable statistical defects. The raw photons are processed through a DRNG of class DRG3. Thus security relies on two bases: information-theory security for the QRNG and computational security for the DRNG. For a physicist the first basis can be sufficient, but for authorities a second security is required for the most demanding applications.

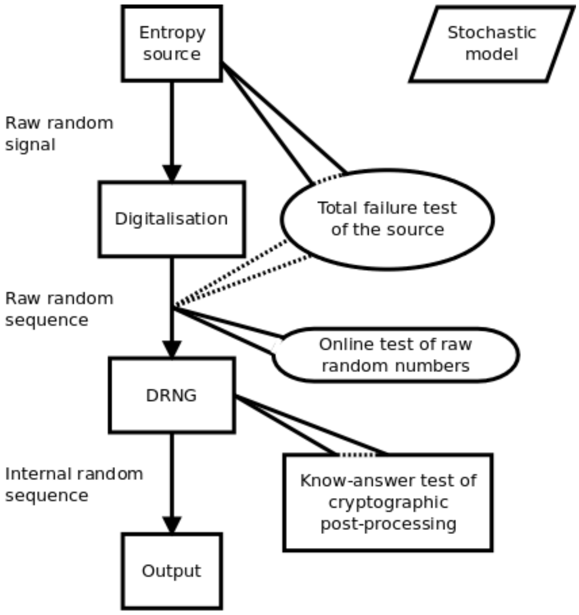

Entropy source
Stochastic model
Raw random signal
Digitalisation
Total failure test of the source
Raw random sequence
Online test of raw random numbers
DRNG
Internal random sequence
Know-answer test of cryptographic post-processing
Output

Figure 6: PTRNG of class PTG.3 according to BSI.

6. ACKNOWLEDGMENTS

For the development of the matrix, D.S., S.B., E.C. and F.R thank the Swiss NCCR-QP FastQ project. For the development of 2-universal hashing extractors, D.S. thanks the Swiss NCCR-QSIT CREx project. For the metrology of QRNG components, D.S. and C.C. thank EMRP (project IND06-MIQC). The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union.

REFERENCES

[1] Samuel Burri, Damien Stucki, Yuki Maruyama, Claudio Bruschini, Edoardo Charbon, Francesco Regazzoni, Jailbreak Imagers: Transforming a Single-Photon Image Sensor into a True Random Number Generator. In proceedings of 2013 INTERNATIONAL IMAGE SENSOR WORKSHOP, Snowbird Resort, Utah, USA June 12-16, 2013

[2] R. Shaltiel, An introduction to randomness extractors, Invited paper for ICALP 2011.

[3] A practical approach to true quantum randomness generation, Daniela Frauchiger and Renato Renner, SPIE Security+Defence, 23-26 September 2013, Dresden, Germany.

[4] http://projects.npl.co.uk/MIQC/.

[5] A proposal for: Functionality classes for random number generators, Wolfgang Killmann and Werner Schindler, 18 September 2011. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile.