Long term test of a fast and compact Quantum Random Number Generator

D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A.W. Sharpe, Z. L. Yuan, and A. J. Shields

Toshiba Research Europe Limited, Cambridge Research Laboratory, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom

Introduction

The role of cryptography is fundamental to guarantee the privacy and the security of exchanged and stored digital information. Recent studies [1] have demonstrated that a common weakness of cryptographic protocols is the key generation algorithm, which is based on pseudo random number generators. This weakness has been exploited indeed in recent attacks [2].

As a consequence of the ever-increasing capacity of the communication channels and the ever-increasing amount of data produced and accessed daily, it is necessary to equip the cryptographic systems with a reliable and fast source of true random numbers.

In this work we will present the results of a long test run of the Toshiba compact and ultra-fast Quantum Random Number Generator (QRNG).

True randomness

The physical mechanism exploited by the Toshiba QRNG to generate random numbers is the spontaneous emission from a pulsed laser. The physical core of the generator comprises a 1550 nm laser that emits pulses with a repetition rate of 1 GHz. The delay of 1 ns between two consecutive pulses is sufficient to empty the laser cavity between two successive emissions. Therefore, each newly stimulated emission is triggered by a spontaneously emitted photon that carries the phase of the vacuum field, which is completely random in the interval $[0, 2\pi]$. This phase is then measured by interfering pairs of optical pulses in a one-bit-delayed fibre-based interferometer whose optical output is sent to a fast photodiode. The outputted numbers are therefore unpredictable to any external adversary by virtue of the physical uncertainty associated to the vacuum state.

Fast generation rate

The photodiode converts the random intensity optical input into a randomly varying current that is read by an analog-to-digital converter (ADC) with a resolution of ten bits. The ADC sampling rate is set as twice as the laser repetition rate so as to monitor the system noise background as well as the random outcomes of the interference.

The probability distribution of the random outcomes is not uniform due to the nonlinear response of the interferometer (cf. [3]). Before using the numbers for cryptographic applications, it is therefore necessary to pass them through a post-processing stage. This consists of a finite-impulse response filter (FIR) that makes the numbers uniformly distributed and removes possible artefacts introduced by the physical implementation of the generator. After the post-processing, the net rate of the QRNG is 8 Gbit/s.

Figure 1: The Toshiba QRNG. The device has dimensions of 10 x 23 x 5 cm.

Compactness

In the literature, generation rates of similar magnitude are typically obtained from bulky systems, acquiring data with oscilloscopes and post-processing them off-line. On the contrary, the Toshiba QRNG performs signal generation, acquisition and post-processing in real time, in the same compact unit. Laser source, interferometer, photodiode and ADC are all embedded on an FPGA board which constitutes the electronic and digital backbone of the generator. In Figure 1, a picture of the generator is reported. As it can be noticed, the generator features output ports for different communication protocols and for the fast transfer of random numbers to computer or encryption system.

Long term testing

A common objection against the use of physical random number generators for cryptographic applications is related to the possibility of a hardware failure.

To support the widespread use of a QRNG, it is of paramount importance to extensively test it and assess its resiliency to a continuous and prolonged operation.

In this work we report the results of a continuous test of the generator for 71 days. During this testing period no drifts in the generated entropy were registered, as can be appreciated from Figure 2.

In addition to the live monitoring of the entropy, large sets of numbers were tested with the most stringent statistical test suites. We used the NIST STS SP-800-22 [4] and the “Big Crush” TestU01 [5]. A total of 2850× 1 Gbits samples were tested against the NIST

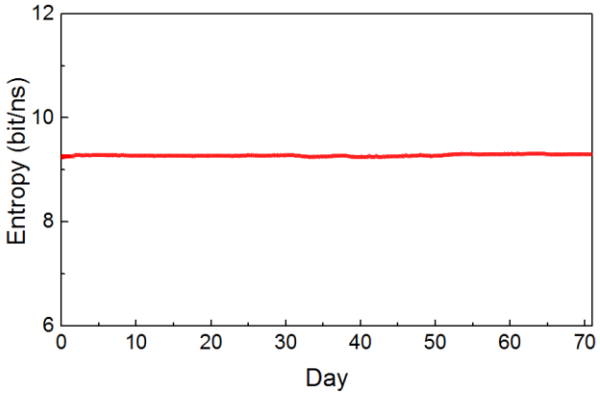

Figure 2: The live monitoring of the generator entropy didn't present any drift in continuous testing of 71 days.

suite during the 71-day period. Care was taken to ensure that each sample consists of only a continuous data stream from the RNG. For the TestU01 test, 285 samples, each of them containing 11.43 Tb of random bits, were analysed in the period of the 71 days.
From this extensive testing session, the number of test failed was in agreement with the expected number derived from the tests' confidence intervals. The statistical suite did not detect any systematic failure or deviation from the hypothesis of identically and independently distributed random numbers, thus suggesting the suitability of this QRNG for cryptographic applications.

Conclusions

The results obtained from the long term test of the Toshiba QRNG suggest that it might represent a suitable solution to the ever-increasing demand for secure random numbers. Its ultra-fast generation rate, the tested resilience and the unpredictability related to the laser spontaneous emission favourably meet the needs of our modern society.

References

[1] A. Lenstra, J.P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, C. Wachter, "*Ron was wrong, Whit is right*", (2012). Santa Barbara: IACR: 17.

[2] R. Chirgwin, "*Android bug batters Bitcoin wallets*", (12 August 2013). The Register.

[3] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, A.J. Shields, "*Robust random number generation using steady-state emission of gain-switched laser diodes*", Appl. Phys. Lett. 104 (26), (2014), p. 261112.

[4] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert et al., "*A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"* (NIST, 2010).

[5] P. L'Ecuyer and R. Simard. "*TestU01: a software library in ANSI C for empirical testing of random number generators*", (2007).