True Random Number Generation in an Optical I/Q Modulator

Nemanja Vokić, Dinka Milovančev, Christoph Pacher, Hannes Hübel, and Bernhard Schrenk
AIT Austrian Institute of Technology, Center for Digital Safety&Security / Security & Communication Technologies, 1210 Vienna, Austria.
Author e-mail address: bernhard.schrenk@ait.ac.at

We re-use a polarization-multiplexed I/Q modulator to acquire the quantum randomness of its seed laser light for the purpose of quantum random number generation. We obtain 9×10^4 256-bit AES keys/second after randomness extraction. Time-interleaved random number generation is demonstrated for PM-QPSK transmission.

1. Introduction

Data encryption, digital signatures and many other ICT applications require a high level of digital security. Random numbers, which are often used as seed for the primitives, should therefore be of highest quality. Quantum random number generation (QRNG) builds on the fundamental principles of quantum mechanics and offers such true randomness. Quantum states are inherently undetermined and display a very large entropy.

In particular, optical QRNGs exploit the quantum properties of light to generate unpredictable random numbers. However, dedicated opto-electronic circuitry is required, such as single-photon photodetectors that acquire the path choice of a single photon [1,2] or balanced detectors with low-noise transimpedance amplifiers (TIA) that measure the vacuum fluctuation of an optical field [3,4]. These customized detectors lack overlap with standard broadband telecom component technology so that practical implementation of QRNGs are often rendered as cost-inefficient.

In this work we exploit an optical I/Q modulator, as commonly used in coherent transmission systems, to yield truly random numbers time-interleaved with 40 Gb/s QPSK transmission. We experimentally prove the randomness extraction at a rate of 9×10^4 256-bit AES keys/second and validate these bit strings through a randomness test suite.

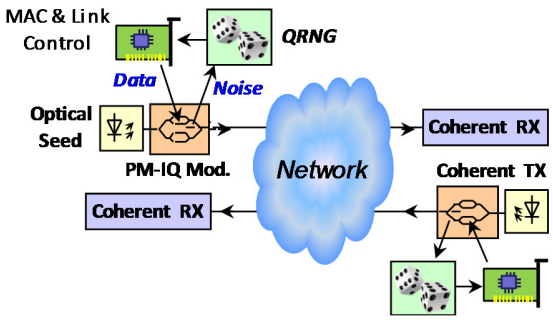

Fig. 1. Integrating true randomness in coherent links by leveraging existing transceiver components.

2. QRNG overlay in PolMux I/Q modulator

In order to establish a seed engine for various communication primitives, both parties of the optical communication link, need to integrate QRNG functionality (Fig. 1). Coherent receivers can be conveniently re-used for the purpose of QRNG,[3] provided that the corresponding TIA technology adheres to the noise requirements to correctly measure the vacuum fluctuations of the local oscillator.

On the contrary, transmitting sub-systems are principally missing the capability to perform reception at the quantum level. In order to address this shortcoming, we propose to exploit the integrated signal monitors in optical I/Q modulators to perform balanced homodyne detection of the seed laser feed.

In particular, the layout of polarization-multiplexed (PM) I/Q modulators adhering to the OIF implementation agreement [5] foresee to tap and monitor the output signal of its nested Mach-Zehnder modulators (MZM), over typical bandwidths in the range of 0.5 GHz. As we will experimentally demonstrate, the tap ratio and detector bandwidth suit the requirements to generate a net QRNG rate of ~80 Mb/s in time division multiplexing (TDM) to classical PM-QPSK transmission.

The QRNG overlay in such a PM-I/Q modulator is presented in Fig. 2a. While the parent configuration of the modulator is solely used for the purpose of power splitting its input (A), the interferometric child MZM in each polarization branch serves as tunable attenuator (B) that can be electrically controlled by its I,Q bias points. Both together, parent and child, form a high-precision 50/50 splitter, which together with the two monitor photodetectors (C) of the polarization branches compose a balanced homodyne detector (D). A large power difference between the optical shot noise of the seed laser and the electrical background noise of this homodyne detector is required for QRNG operation. This accomplishment of a high clearance between optical and electrical noise is challenged by the low monitor tap ratio (typ. -10 dB), the modulator losses and the TIA noise.

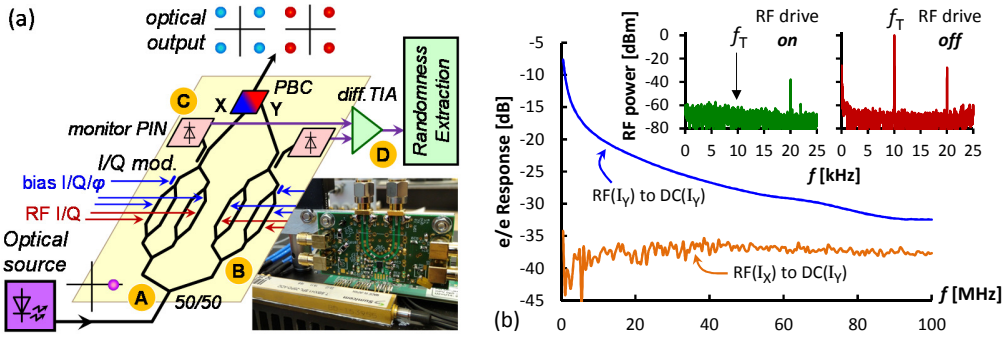

Fig. 2. (a) Random number generation in an I/Q modulator. (b) Electrical response between RF and DC electrodes of the modulator and bias tone spectra with/without RF drive.

3. Characterization of the QRNG engine

We first characterized the clearance of the balanced homodyne detector that shapes the QRNG. The 66-dBΩ TIA with differential feedback loop closed around an 8-GHz gain-bandwidth opamp uses a balanced configuration at its input and is fed by the two single-ended PIN photodiodes of the I/Q modulator. The bias points of the I/Q modulator were set to operate each of the child MZMs so that the photocurrent to the monitor photodiodes is maximized. At the same time, the relative adjustment of both child MZM outputs ensures balancing of the homodyne detector.

Figure 3a reports the electrical noise (ε) of the TIA circuit for a dark QRNG input, meaning that the seed laser has been switched off. When the I/Q modulator is lit, the shot noise (o) of the seed laser surpasses the electrical background, provided that a sufficiently high photocurrent is generated and that the child branches are balanced. The admissible range for the bias points of the child MZMs at this optimum bias setting was typically 0.05 Vπ, in order not to saturate the TIA output due to imbalance in its two input branches. The difference between dark and lit modulator is also visible in histogram of the detected voltage (Fig. 3a).

Figure 3b presents the clearance spectrum as function of the optical seed power to the modulator. We obtained a noticeable level above the intrinsic TIA noise for a seed level of 13 dBm over a bandwidth of ~150 MHz. A few crosstalk notes have been observed due to electro-magnetic interference. These, together with the presence of electrical background noise, require performing an additional randomness extraction step after opto-electronic detection and signal conditioning.

The dependence of the average clearance on the seed power is summarized in Fig. 3c. A clearance of 2.1 dB is obtained for a seed power level of 18 dBm at the I/Q modulator input. Moreover, the clearance shows a linear dependence on the seed level, which indicates that the generated noise derives from the vacuum fluctuations of the light.

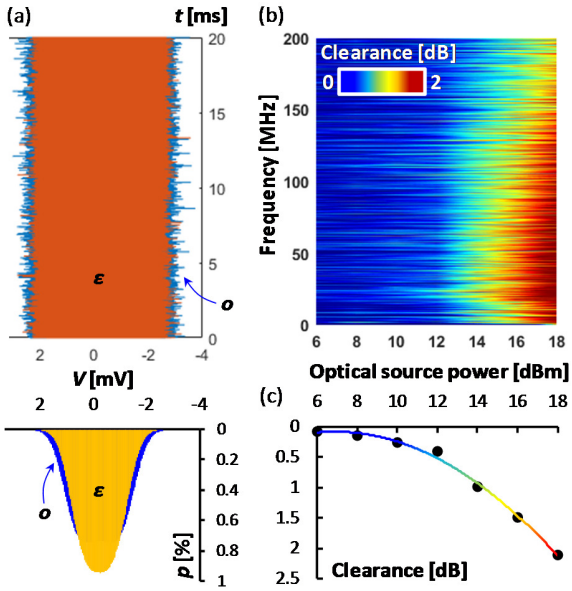

Fig. 3. (a) Noise and (b) corresponding spectra due to optical seed and electrical TIA background. (c) Clearance.

4. Time-interleaved QRNG in coherent link

The experimental setup presented in Fig. 4a has been used to evaluate random number generation time-interleaved with 10-Gbaud PM-QPSK transmission. Since there is a strong crosstalk of -7.6 dB between adjacent RF and DC modulator ports (Fig. 2b), two sets of time-multiplexed bias points are applied to the I/Q modulator. These are dedicated to PM-QPSK and QRNG operation, with and without RF drive; respectively. The shift introduced by the RF drive is also visible in the insets of Fig. 2b, which shows the spectrum of a DC bias tone at f_T = 10 kHz. While operation in the null point results in a minimized fundamental tone f_T and a noticeable second harmonic at $2f_T$, the activation of the RF drive shifts the bias point by ~1.56V or 0.42 Vπ in average, so that the fundamental tone is again pronounced. QRNG operation without RF drive, time-interleaved to PM-QPSK transmission, requires to compensate this shift.

An intradyne coherent receiver has been used to confirm correct bias operation for the transmitted 40 Gb/s PM-QPSK. The received constellations are presented in Fig. 4a.

Moreover, a TDM frame with a period of 5 ms has been applied. The duty cycle of 70% for data transmission leaves a 1.5-ms window that can be used for periodic random number generation. Figure 4b shows the traces acquired at an optical intensity monitor (M) at the I/Q modulator output and at the TIA output (T) of the I/Q modulator. Transients appear at the edges of the TDM slots due to lowpass filters (LPF) at the DC bias lines of the I/Q modulator, which are used to suppress electro-magnetic interference and thus prevent excess noise at the QRNG output. The 3-dB bandwidth of these LPFs was 22 kHz, which allows for bias tone probing and yet limits the native 700 kHz response of the DC electrodes when switching between bias points. With activated optical seed of the modulator, the QPSK modulation is visible in the TIA output. This prevents QRNG functionality. In the QRNG slot of the TDM frame, the QPSK data is thus blanked. The shot-noise (λ) of the optical seed is clearly visible. During the transient regions (σ) between the two TDM slots, the TIA becomes saturated due to a sub-optimal bias setting, which leads to imbalance of the balanced homodyne detector till the modulator bias point settles at the set point of operation. Figure 4b also shows the acquired traces when the optical seed is deactivated. During the QRNG TDM slot the TIA signal reduces in its magnitude to the electrical background noise (ε), according to the clearance reported earlier. RF-crosstalk is visible during the TDM-slot for QPSK transmission (ρ).

5.4M samples have been recorded at 8-bit resolution during QRNG operation. The sampled bits are, however, not perfect uniformly random due to several reasons: (i) the samples are Gaussian distributed, (ii) the non-ideal transmission function of the amplifier leads to correlations between samples, (iii) the amplifier could have some deterministic behavior that leads to a hidden pattern, (iv) any form of cross-talk. A seeded randomness extraction

algorithm [6] has been applied in order to improve the quality of the random numbers. This enhances the entropy per bit by shortening the random data using an independent random seed that can be re-used. The only requirement on the input for such an extractor is that it provides a lower bound on min-entropy. We estimated the lower bound to be 1/8 bit per acquired bit. Universal Toeplitz hashing has been employed as seeded randomness extractor. A block of 1 Mibit = 1,048,576 bits (4096 keys of 256 bit each, e.g. for AES) from 40 Mibit of sampled data has been extracted. The complete NIST SP800-22-rev1a randomness test suite [7] has been applied twice: before randomness extraction 69/188 tests of the NIST suite did not pass. After extraction all but one test passed successfully. Based on the aforementioned 1/8 ratio, we estimate that we can generate approximately 9×10^4 256-bit AES keys per second. An exemplary 256-bit true random number string is shown in Tab. 1.

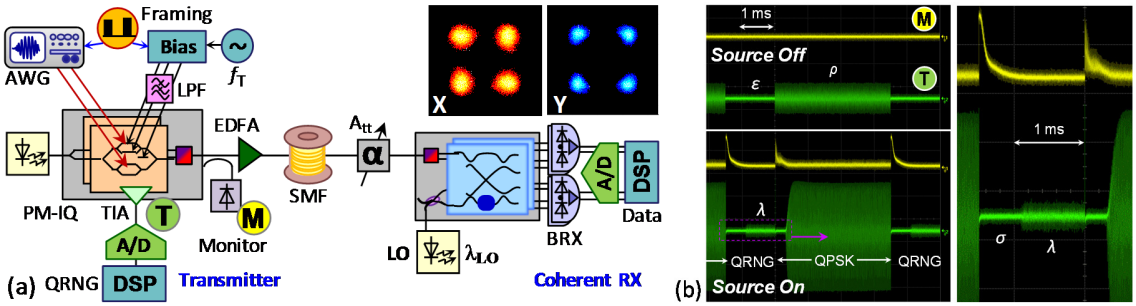

Fig. 4. (a) Setup for TDM-based QPSK transmission and true random number generation. (b) Acquired TDM frame.

11001001 10110010 00101011 01110100 01010100 11100110 11001101 01110111 10101001 11111110 01100001 10101101 01100001 10111011 00101001 01110001 10101100 10101001 00000011 11100000 11110001 01101000 11111001 11100000 11101000 00010010 10010000 01011110 11000010 11110110 00001011 00000111

Tab. 1. 256-bit truly random bit string extracted from the vacuum fluctuations of the laser sourcing the PM I/Q modulator.

5. Conclusions

We have experimentally demonstrated the re-use of an optical I/Q modulator for the purpose of quantum random number generation. By leveraging its integrated monitor photodiodes, the vacuum fluctuations of the seed laser have been acquired. Employing a Toeplitz randomness extractor, we have demonstrated how the quantum entropy source based on vacuum fluctuations can be converted into a true random number generator with a rate of 9×10^4 256-bit AES keys/second.

6. Acknowledgement

This work has received funding from the EU Horizon-2020 R&I programme under grant agreement No 820474 and the ERC under grant agreement No 804769.

7. References

[1] T. Jennewein et al., “A fast and compact quantum random number generator”, Review fo Scientific Instruments., vol. 71, no. 4, pp. 1675-1680, 2000.
[2] M. Fürst et al., “High speed optical quantum random number generation”, Opt. Exp., vol. 18, no. 12, pp. 13029-13037, 2010.
[3] C. Gabriel et al., “A generator for unique quantum random numbers based on vacuum states”, Nature Phot., vol. 4, no. 10, pp. 711-715, 2010.
[4] C. Abellan et al., “Quantum Entropy source on an InP photonic integrated circuit for random number generation”, Optica, vol. 3, no. 9, pp. 989-994, 2016.
[5] Optical Internetworking Forum, “Implementation agreement for integrated polarization multiplexed quadrature modulated transmitters”, OIF-PMQ-TX-01.2, 2015.
[6] Y. Mansour et al., “The computational complexity of universal hashing”, Theoretical Computer Science, vol. 107, no. 1, pp. 121-133, 1993.
[7] A. Ruhkin et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications”, NIST special publication 800-22, Revision 1a, National Institute of Standards and Technology, 2010.