Fast and Scalable PIC-Based QRNG for Advanced Solutions

Domenico Tulli, Miquel Rudé, José R.M. Saavedra
Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels (Barcelona), Spain
SPAIN

dtulli@quside.com

ABSTRACT

In the last years, the number of cyber-attacks has grown tremendously. The actual geopolitical situation has defined a new era for cyberwarfare and hacktivism and their impact on conflicts. Governmental bodies, public administrations, and intergovernmental organizations are the main targets of these criminal acts, putting at serious risk our digital economy and global security. Moreover, the continuous development of more powerful quantum computers poses a serious threat to current Public Key Cryptography protocols. The development of products and infrastructure offering long-term security guarantees and stronger computational capabilities becomes a global priority to ensure the socio-economic growth. Solutions to transition to quantum-safe infrastructure are coming – governments, academia and industries are most notably developing post-quantum cryptography (PQC) and quantum key distribution (QKD). Random number generators are at the foundation of nearly all cybersecurity. Quantum random number generators (QRNGs) leverage the inherent, provable randomness of quantum mechanics to efficiently create truly entropic keys. In this work, we describe a QRNG device based on an Indium Phosphide (InP) photonic integrated circuit (PIC), which offers high-speed operation (Gb/s) with unprecedented security guarantees and reduced form factor. The QRNG is also the core of the Randomness Processing Unit (RPU), an innovative hardware accelerator designed for world-class performance, optimization, and efficiency in Post-Quantum Cryptography (PQC) and stochastic High-Performance Computing (HPC). This solution makes it the perfect candidate to enhance the performance of military equipment, which demand un-hackable security systems.

1.0 INTRODUCTION

Data transmissions are protected by cryptographic algorithms based on keys generated by random number generators (RNGs). To be secure, the key must be unpredictable. The higher the randomness of the generated sequence, the harder to break it for an eavesdropper. Many methods have been presented to realize true (hardware based) random number generators (TRNG) to replace pseudo-RNGs (PRNGs) [1], which are based on a deterministic algorithm generated by a computer and thus having repetitive occurrences and patterns. A hardware based RNG, instead, is based on physical noise sources, such as thermal noise, atmospheric noise, shot noise, radioactive decay, and so on. However, TRNGs based on classical physics, e.g. free running oscillators, are black boxes where deterministic processes run in an uncontrolled and chaotic manner. Thus, it is not possible to guarantee that an attacker could not manipulate, force or predict the output from a classical TRNG. The only way to produce true and unbreakable randomness is to utilize fundamentally unpredictable processes and understand and validate such physical process by which the randomness is generated. Quantum random number generators (QRNGs) are a particular case of physical TRNG where the data is the result of a quantum event, thus unpredictable by nature. The goal in quantum random generators is to utilize set-ups where this fundamental randomness arises in ways that are easy to describe and quantify. Only quantum sources can provide the randomness necessary to realize truly secure encryption systems as well as improved randomized algorithms [2]. Several quantum entropy sources (QESs) have been proposed for quantum random number generation, including single photon splitting [3], homodyne detection of the vacuum field [4], and phase diffusion (PD) in semiconductor lasers [5]. To date, PD-QRNGs have achieved the highest bit rates [6], up to 68 Gb/s [7] and their integration using monolithic photonic integrated technologies such as InP are commercially available. Random numbers are a critical enabling technology as they are used in two-factor authentication and underpin all encryption keys used in classical, PQC and QKD protocols. Independent of the quantum threat, QRNGs address existing cybersecurity vulnerabilities arising from weak random numbers [8] and can be combined with PQC to further enhance security. Quside exploits phase diffusion technology and photonic integrated circuits (PIC) [9] to build reliable high-speed and scalable quantum random number generators. Moreover, the QRNG is also the core of the Randomness Processing Unit (RPU) [9], a hardware reprogrammable platform designed for crypto acceleration.

2.0 QRNG BASED ON ACCELERATED PHASE DIFFUSION

Quside's QRNG is based on phase diffusion in gain-switched (GS) semiconductor lasers [6]. When modulated in GS (i.e. far above and below the threshold), the optical phase of a laser rapidly randomises due to vacuum fluctuations during turn-off. This random phase is amplified into a macroscopic signal by stimulated emission during power-up. Since the optical phase is too fast to be measured by a photodetector, it must be converted to a random optical intensity. In our case, this is achieved using a heterodyne scheme (Figure 1) with two DFB lasers. By modulating both lasers and mixing their output in a 2x2 MMI the intensity at the photodetector is given by:

$$i_{pd}(t) = i_1(t) + i_2(t) + 2\sqrt{i_1(t)i_2(t)}\cos{(\Omega t + \Delta\theta)}$$

Where $i_j(t)$ is the intensity of each laser, Ω is the beat frequency (i.e. the difference between their optical frequencies), and Δθ is the random phase due to vacuum fluctuations. This means that by periodically sampling the modulated signal at $\tau_s = 1/f_{mod}$,one obtains a random amplitude proportional to the cosine of a random phase (arcsine distribution), allowing one to obtain random bits at a frequency limited only by the modulation speed of the DFB laser. The QRNG is implemented on a small size InP PIC. The device contains two DFB lasers and photodetectors, a 2x2 MMI and two integrated metallic heaters that allow to tune the beating frequency to a value smaller than the photodetector bandwidth. The fabrication is performed in a regrowth free epitaxy in 4" InP wafers and allows to obtain more than 1000 devices per wafer.

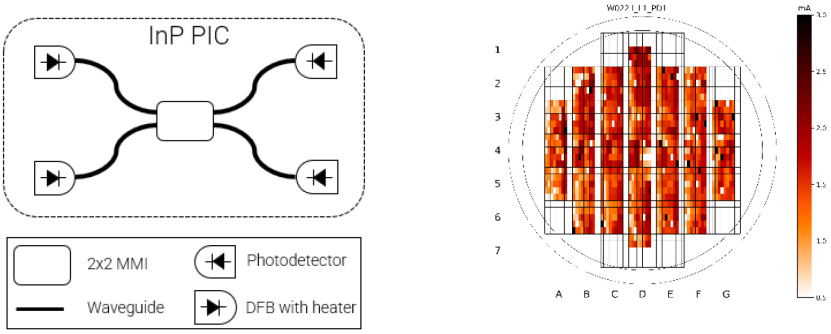


Figure 1. a) Schematic of the QRNG architecture. b) Results of automated wafer level testing in a wafer containing more than 1000 dies.

Moreover, wafer-level-testing (WLT, Figure 1) allows to analyse and select known-good-dies (KGD) that will be later integrated into final products. Finally, the chip only contains electrical connections to its different building blocks, allowing to easily integrate it into a standard QFN package (5x5 mm^2, 32 pins), which reduces the SWAP-C and ensures scalability. Figure 2 shows an example of generation of random numbers at 1 Gbps. Modulating both lasers in GS at 1 GHz and setting the detuning frequency Ω < 1 GHz, one obtains a train of pulses with random amplitudes (Figure 2 top-left and right). By fixing a sampling point in the middle of the pulse (dashed line) one obtains an arcsine distribution (Figure 2 bottom-left) that can be easily digitized into a stream of random bits at 1 Gbps. Finally, we have developed a fully automated calibration routing that sets all the chip parameters and finds the best sampling point in terms of randomness, which is then analyzed using different metrics (as shown in Figure 2 bottom-right, showing autocorrelations of 1 Gbit of raw random bits).

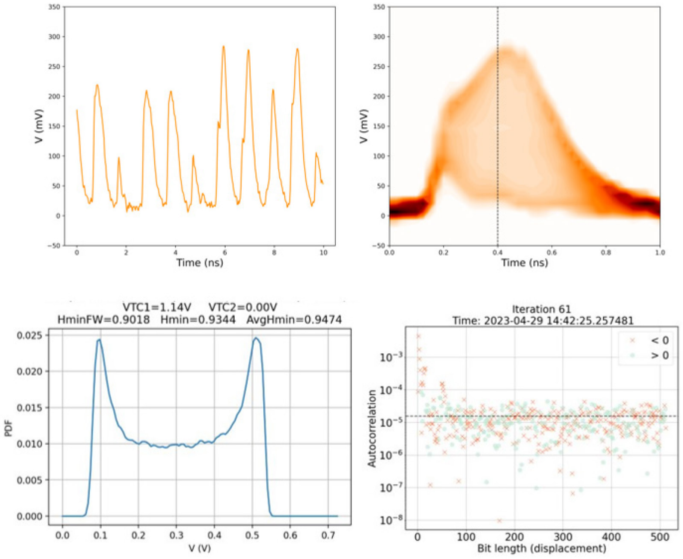


Figure 2. a) Random amplitude pulses read by the photodetector. b) Accumulated trace and sampling point (dashed black line) inside the pulse. c) Accumulated probability at the sampling point, showing an arcsine probability distribution. d) Autocorrelation results for 1 Gbit of raw random data with ~10^{-5} statistical noise.

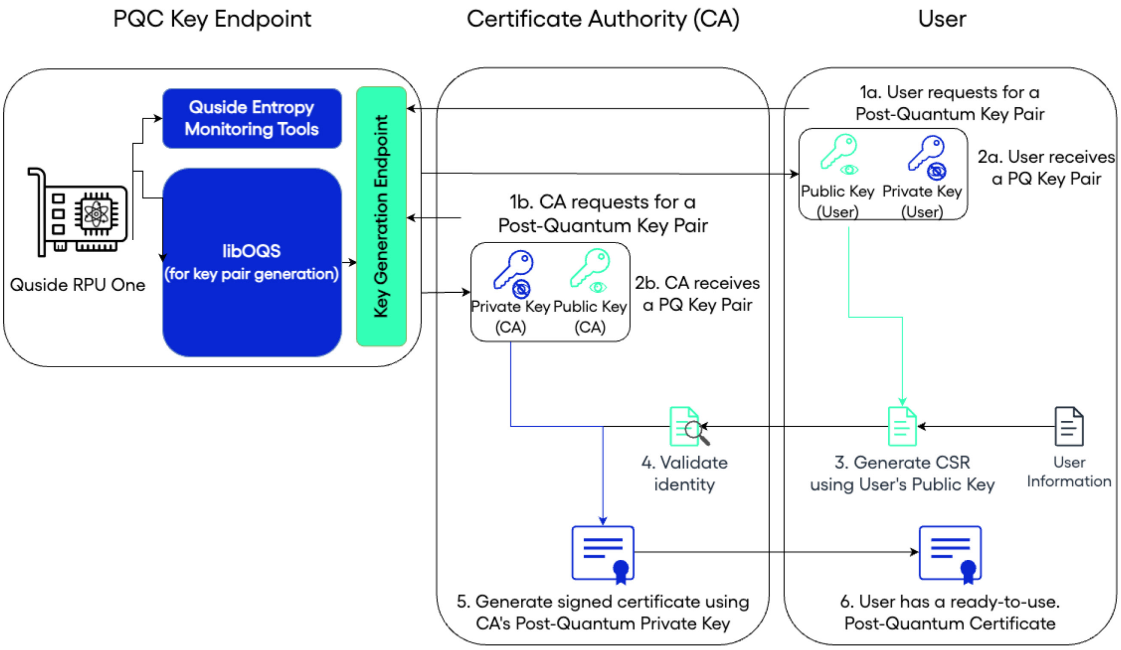
3.0 QUSIDE’S RANDOMNESS PROCESSING UNIT: A QUANTUM-ENABLED ACCELERATOR FOR POST-QUANTUM CRYPTOGRAPHY

The imminent arrival of post-quantum cryptography (PQC) marks a pivotal moment in security. By mandating compliance with standardised post-quantum cryptographic protocols, industry, governments, and the military will ensure that sensitive information remains protected from both conventional and quantum threats. However, from a technical perspective, implementing these algorithms is far from straightforward. Many of them are severely limited in their operational efficiency because they require a large amount of entropy, processing power or memory, or have a complex hardware implementation [10], [11]. All of this slows down the integration of these algorithms into current systems, making compliance more difficult and prolonging a risky situation. Traditionally, the way to compensate for these problems has been by implementing specialized circuitry (e.g., in the form of ASICs) that includes internally an optimized version of the algorithm to be implemented. This approach has been successful in the acceleration of classical cryptography workloads [13]. However, the remaining uncertainty about which of the existing algorithms are optimal (or at least those required by the standard) complicates the design of such ASICs: as it is an expensive technology to manufacture, the current risk associated with the “unfinished” state of the standards makes this activity a business of dubious profitability. In addition, the advent of quantum computers has taught us that we should not rely on a single encryption algorithm: there is always the possibility of finding mathematical methods that make these algorithms easily solvable [11]. Thus, tying our computational security to a single algorithm can lead to disaster if that algorithm is compromised. To avoid this, cryptographic agility is a fundamental skill, as the best cryptographic devices should be able to adapt the algorithms they use to the latest recommendations. This is the only way to ensure the highest level of security for our communications networks. With this vision in mind, we at Quside have developed our

Randomness Processing Unit (RPU), a reprogrammable hardware accelerator that integrates Quside's quantum entropy sources and reprogrammable logic. As a result, the RPU is intended for the efficient and secure execution of randomized workloads, such as cryptography or stochastic models. Although it has use cases in finance, machine learning, and scientific and engineering simulation, it is probably in cryptography (where the quality of randomness directly affects security, and the speed at which that randomness is generated directly affects performance) that the RPU is a truly differentiating product. This is largely due to the combination of three elements in one:

- First, by integrating the Quside quantum entropy sources within the RPU, which gives the RPU the quality and speed required for workload execution.
- Second, by providing an environment and architecture specifically designed to accelerate randomness-dependent code, such as PQC algorithms.
- And finally, the reconfigurability of the RPU makes it a future-proof device, with the ability to adapt to the demands and new PQC algorithms existing in standards and regulations.

The combination of these three elements makes Quside's RPU the go-to platform for these kinds of post-quantum cryptographic workloads.


PQC Key Endpoint
Certificate Authority (CA)
User
Quside Entropy Monitoring Tools
libOQS (for key pair generation)
Key Generation Endpoint
Quside RPU One
1a. User requests for a Post-Quantum Key Pair
Public Key (User)
Private Key (User)
2a. User receives a PQ Key Pair
1b. CA requests for a Post-Quantum Key Pair
Private Key (CA)
Public Key (CA)
2b. CA receives a PQ Key Pair
4. Validate identity
3. Generate CSR using User's Public Key
User Information
5. Generate signed certificate using CA's Post-Quantum Private Key
6. User has a ready-to-use. Post-Quantum Certificate

As a demonstration of these capabilities, we at Quside have integrated our RPU together with the Open Quantum-Safe libraries (libOQS), an open-source C library for cryptographic algorithms resistant to quantum attacks [14]. The library offers a collection of open-source implementations encompassing quantum-safe key encapsulation mechanisms (KEM) and digital signature algorithms. It provides a unified API for these algorithms. To facilitate real-world deployment and testing, libOQS integrates into prominent cryptographic frameworks like TLS and SSH via OpenSSL and OpenSSH. Regarding PQC algorithms, libOQS offers quantum-safe key encapsulation mechanisms such as BIKE, Classic McEliece, FrodoKEM, HQC, and Kyber. These mechanisms cater to varying security requirements and use cases. For instance, Kyber provides options like Kyber512, Kyber768, and Kyber1024, enabling cryptographic configurations that align with specific needs. Furthermore, libOQS extends its prowess to signature schemes, encompassing CRYSTALS-Dilithium, Falcon, and SPHINCS+ variants. By integrating the RPU with the libOQS libraries, we empower organizations to stride confidently into post-quantum cryptographic resilience. We do this by providing a double advantage: on the one hand, libOQS becomes a safe starting point from which they can begin their migration processes toward post-quantum security. On the other hand, the RPU provides them, from the very first minute, with a high-quality, high-speed entropy source, which can accompany them throughout the migration process and beyond. That way, users always have the entropy sources and cryptographic workload execution environment that will adapt to their needs, both during the migration and in the future.

4.0 CONCLUSION

We have presented a high-speed QRNG module based on a photonic integrated circuit. The resulting device shows high performance, including bit rate, degree of randomness (low correlation values), and stability, in a miniaturized packaged to reduce SWAP-C and ensure scalability. This QRNG is the core of the innovative reprogrammable hardware (RPU), developed by Quside to accelerate randomized workloads as PQC protocols, which require a high quantity of high-quality random numbers as well as a different statistical distribution of these random numbers.

5.0 REFERENCES

[1] P. Lacharme, A. Rock, V. Strubel, and M. Videau, “The Linux Pseu- ¨ dorandom Number Generator Revisited,” International Association for Cryptologic Research, pp. 1–23, 2012.

[2] M.H. Collantes, J.C.G.-Escartin, “Quantum Random Number Generators, “ Instituto Nacional de Ciberseguridad, Avenida Jose Aguado, 41, Edificio INCIBE 24005, Leon, Spain, Oct. 2016.

[3] J. G. Rarity, P. Owens, and P. R. Tapster, “Quantum random-number generation and key sharing,” J. Mod. Opt. 41, 2435–2444 (1994).

[4] C. Gabriel et al., “A generator for unique quantum random numbers based on vacuum states,” Nat. Photonics 4, 711–715 (2010).

[5] M. Jofre et al., “True random numbers from amplified quantum vacuum,” Opt. Express 19, 20665–20672 (2011).

[6] C. Abellán et al., “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” Opt. Express 22, 1645–1654 (2014).

[7] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, and J. Zhang, “The generation of 68 Gbps quantum random number by measuring laser phase fluctuations,” Rev. Sci. Instrum. 86, 063105 (2015).

[8] J. Kilgalin, “The Irony (and Dangers) of Predictable Randomness,” 19 December 2019. [Online].

[9] https://quside.com/products/

[10] https://doi.org/10.6028/NIST.IR.8413-upd1

[11] https://csrc.nist.gov/pubs/ir/8105/final

[12] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

[13] Gaj, K., Chodowiec, P. (2009). FPGA and ASIC Implementations of AES. In: Koç, Ç.K. (eds) Cryptographic Engineering. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-71817-0_10

[14] https://openquantumsafe.org/