

Whitepaper

Gigabit Quantum Random Number Generator (QRNG) – Randomness in the Age of Quantum Technology

Author: Christoph Posenau

Random numbers form the foundation for cryptographic applications of all kinds. In computers, these are generated either using physical processes such as thermal noise or through algorithmic calculations. Both approaches reach their limits in the age of quantum technologies.

Randomness Becomes a Critical Resource

Almost every cryptographic procedure – key generation, initialization vectors, digital signatures – stands or falls with the quality of its random numbers. If these are predictable or correlated, security collapses regardless of the strength of the algorithm. At the same time, demand is rising rapidly: cloud services, hardware security modules, and quantum communication require entropy on the Gigabit scale. Randomness thus transforms from an implicitly assumed quantity to a scarce, security-critical resource.

QRNG Instead of PRNG & TRNG

Conventional Pseudo-Random Number Generators (PRNG) algorithmically expand a seed value. They are therefore deterministic and, in principle, vulnerable to attacks – in the future, also by quantum computers. Classical True Random Number Generators (TRNG) use physical effects but often deliver data rates that are too low for scaled applications.

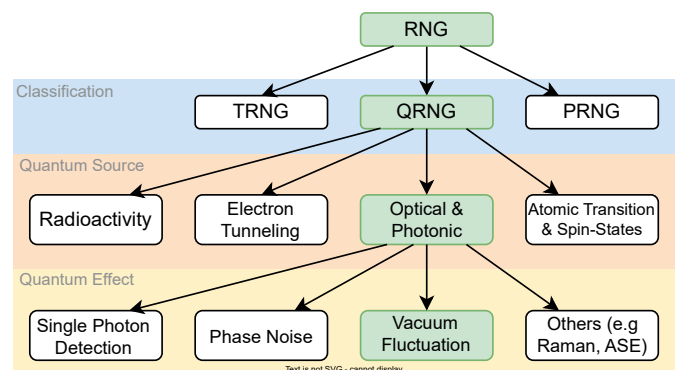


Fig. 2: IPMS approach (green) in world of (Q)RNGs

Quantum Random Number Generators (QRNG) utilize intrinsically non-deterministic quantum effects. The indeterminacy here is not a consequence of incomplete knowledge but a property of nature itself – making it a fundamentally reliable entropy source.

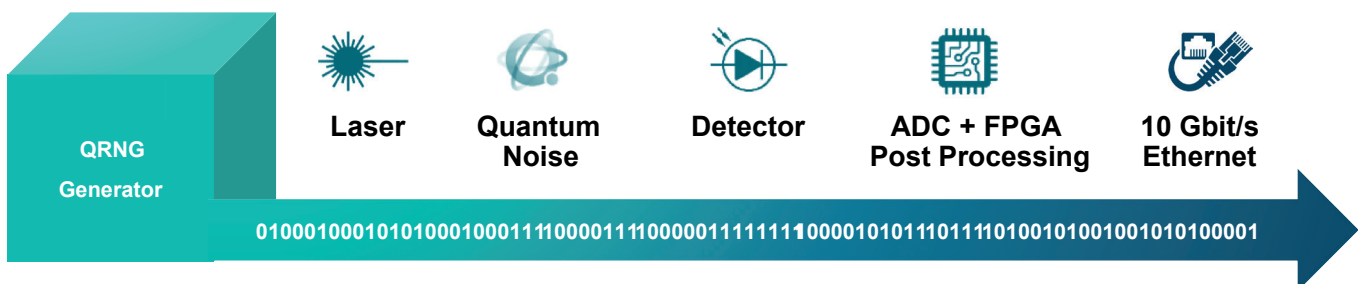


Fig. 1: IPMS Competencies Along the Entire Gigabit-QRNG Value Chain

The Vacuum Fluctuation Approach by Fraunhofer IPMS

Fraunhofer IPMS has compared various QRNG architectures and noise sources, such as photon counting or phase noise. The IPMS utilizes so-called vacuum fluctuations as the entropy source in its demonstrator. A classification of this approach within the world of (Q)RNGs is shown in Fig. 2. Vacuum fluctuations are the intrinsic, unavoidable, and non-manipulable fluctuations of the electromagnetic field in empty space, arising from Heisenberg's uncertainty principle, and are used as a true, unpredictable source of randomness for bit generation. This approach offers a balanced compromise between high data rates, moderate complexity, chip integrability, and – crucially – mathematically provable security.

Technically, the quadrature of the vacuum state is measured using balanced homodyne photodetection: a narrow-band 1550 nm Laser (Local Oscillator, protected against injection attacks by optical isolators) is superimposed with the vacuum state of the electromagnetic field via a 50:50 coupler and detected by a symmetric InGaAs PIN photodetector. Balanced detection prevents the unwanted measurement of the Laser's classical intensity noise (excess noise), as this could be manipulated by an attacker. The central challenge of the subsequent post-processing is to cleanly separate the quantum noise of the vacuum fluctuations from the classical noise of the measurement electronics used.

Following digitization using a 14-bit ADC on an FPGA board, post-processing occurs: calculation of the min-entropy, subsequent algorithmic randomness extraction via Toeplitz hashing, and cryptographic post-processing via SHA-256. Via the integrated 10G Ethernet MAC, up to 8.2 Gb/s of cryptographically processed random numbers based on proven quantum entropy are provided. The architecture of the overall system is summarized in Fig. 3.

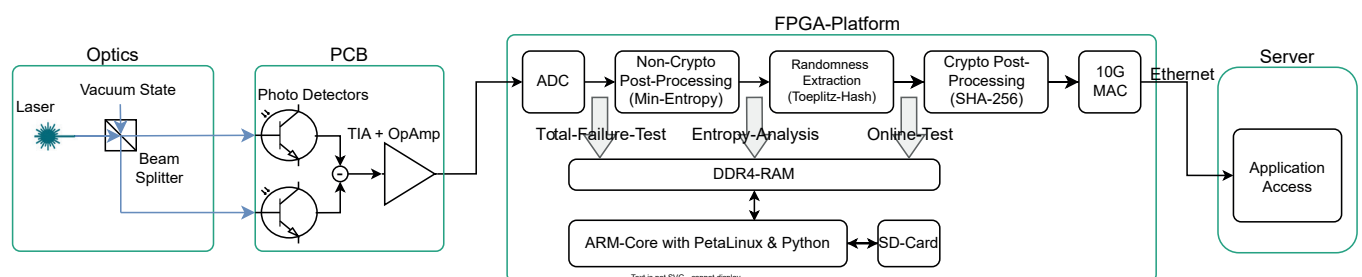


Fig. 3: Opto-Electronics and Post-Processing Architecture of the Q-Dice QRNG

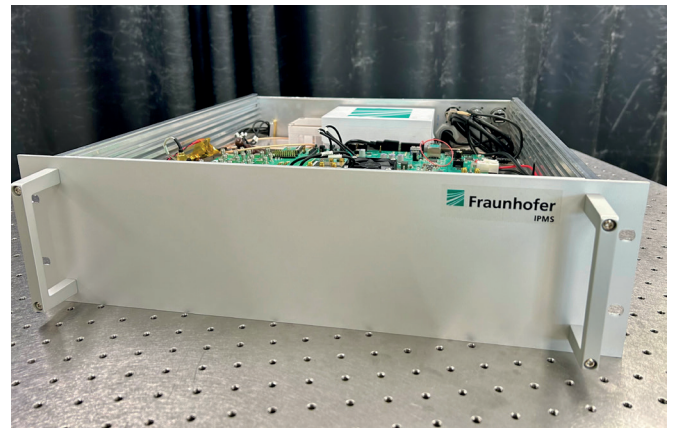


Fig. 4: Q-Dice QRNG as a 19" rack mount

Trust Models in Quantum Cryptography

In quantum cryptography and QRNG development, architectures are categorized according to so-called Trust Models. They define how much trust must be placed in the flawless and unmanipulated function of the hardware components (source, detectors, etc.). The quantum effects used are intrinsically non-manipulable. However, a so-called side-channel attack on the measurement electronics used must certainly be considered. For QRNG integrators, three trust model categories are relevant:

- **Device-Independent (DI):** Reflects the theoretical ideal state, as neither the source nor the detectors are trusted. Randomness is proven purely through parallel statistical measurements, independent of the device construction. In practice, however, DI systems are currently too slow (a few bits per second) and too complex for QRNG applications.
- **Semi-Device-Independent (SDI):** A compromise, as neither the source nor the detectors are fully trusted. But the system relies on a single, minimal assumption (e.g., that the energy of the incoming light is bounded from above). The approach offers high security but requires complex additional hardware for monitoring.

- **Device-Dependent (DD):** The standard model for today's high-speed QRNGs. It is trusted that the hardware works exactly according to specification and is protected against physical side-channel attacks by chassis security.

The IPMS approach is designed as Device-Dependent, as this allows the very high data rates to be achieved. A major advantage of the vacuum fluctuation approach is that source manipulation of empty space is ruled out – in contrast to Laser-based sources. Trust in the Device-Dependent model must therefore »only« focus on the shielding of the measurement electronics (e.g. protecting the Local Oscillator via optical isolators) and the chassis.

Key System Features

- 8.2 Gb/s quantum random numbers via Raw Ethernet
- FPGA-based post-processing incl. 10G Ethernet MAC interface
- Integrated Linux OS with Python and SD card access for online testing & test data extraction
- Certifiable according to BSI AIS 20/31 (PTG.3), NIST SP 800-22, NIST SP 800-90B, FIPS 140-3 / ISO 19790 & ISO 15408 (EAL3)
- 19« server rack chassis (see Fig. 4)
- Available as an online QRNG via HTTPS GET interface incl. TLS 1.3 with AES-256

This remaining basis of trust is formally audited and verified through the strict certifications according to BSI AIS 20/31 (PTG.3) and Common Criteria (EAL3).

PTG.3 according to AIS 20/31 – The Stricter Path

The internationally recognized standard NIST SP 800-90B »Recommendation for the Entropy Sources Used for Random Bit Generation« requires one-time stochastic analyses for quality assurance of a (Q)RNG. The BSI's AIS 20/31 goes significantly further: it requires a security proof based on a stochastic model of the entire setup as well as continuous online tests during operation. The IPMS QRNG is designed as PTG.3 – the highest security class defined in AIS 20/31, which, in addition to the physical entropy source and the stochastic model, also requires the algorithmic and cryptographic post-processing described above.

During operation, three quality tests for the output random numbers run continuously:

- **Total-Failure Test:** stops generation upon eight identical consecutive ADC samples;
- **Start-up Test:** performed prior to first use after every power-on;
- **Online Test:** continuous calculation of the min-entropy based on the QRNG's stochastic model incl. the 14-bit ADC used; the achieved mean value of the min-entropy is 9.48 bits with a variance of $3.21 \cdot 10^{-5}$ bits over 12 hours;
- **Black-Box Tests:** validates the extracted quantum random numbers again using various stochastic tests.

The crucial advantage is illustrated by a simple example: even a completely deterministic sequence like the digits of π can pass pure NIST statistical tests, although it is perfectly predictable. PTG.3, on the other hand, proves randomness continuously and model-based – thus closing exactly this gap.

Common Criteria & EAL according to ISO 15408

Beyond the quality of entropy, the Common Criteria (ISO/IEC 15408) address the trustworthiness of the product development itself. The Evaluation Assurance Level (EAL) – EAL3 is targeted – evaluates the methodology, documentation, and testing depth of the development process. Also relevant in this context are NIST FIPS 140-3 or ISO/IEC 19790 for the security of cryptographic modules, as well as ISO/IEC 20543 for the testing of random bit generators.

Taken together, this results in a two-tier foundation of trust: AIS 20/31 (PTG.3) verifies the quality of the random source, while Common Criteria (EAL3) verifies the trustworthiness of its development.

What a Certification Does Not Cover

For honest and sustainable customer communication, it is equally important to clearly state the limits of a certification:

- A certification verifies the entropy source and the module – not the correct integration on the customer's side (key derivation, interfaces, operating environment).
- It does not replace system-side entropy management: extraction rates, buffering, and error handling must be designed by the customer.
- They do not guarantee end-to-end security – subsequent protocol and application layers remain the responsibility of the customer.

In short: The certification provides a robust foundation of trust, but it does not shift the integration responsibility.

Use Cases

The concrete benefit arises, for example, in the following situations:

- **Entropy Starvation:** In scaled cloud, server, and container environments, many instances share the same entropy source. A high-speed QRNG decouples security from availability.
- **Post-Quantum Cryptography (PQC):** PQC methods require high-quality random numbers that are secure against quantum computer attacks; using PRNGs undermines even quantum-secure algorithms.
- **Quantum Key Distribution (QKD):** QKD requires physical randomness with high data rates at multiple points; and as with PQC, the QRNG integrates as a building block in the quantum value chain.
- **Simulations and AI Algorithms:** Monte Carlo simulations, financial models, or initialization vectors of machine learning models require large amounts of reliable random numbers.
- **Regulation:** Regulatory bodies and standards in areas such as finance and critical infrastructure (CRITIS) are increasingly formulating requirements for entropy sources, for which a PTG.3 proof provides the auditable evidence.

Conclusion and Availability

The Gb-QRNG from Fraunhofer IPMS combines high data rates of up to 8.2 Gb/s with a PTG.3 security proof according to AIS 20/31 and a development process designed for EAL3. It is available as a 19« rack mount for on-premise integration (10G Ethernet) as well as Entropy-as-a-Service (EaaS) via an HTTPS GET interface (TLS 1.3, AES-256).



About Fraunhofer IPMS

The Fraunhofer-Gesellschaft, based in Germany, is the world's leading organization for application-oriented research. With its focus on future-relevant key technologies and the utilization of the results in business and industry, it plays a central role in the innovation process. As one of 76 institutes, Fraunhofer IPMS deals with electronic, mechanical and optical components and their integration into miniaturized devices and systems. Our services range from conception and product development to pilot production in our own laboratories and clean rooms.

Contact

Stephan Kube
B2B Sales Marketing Manager
+49 351 88 23 - 1112
stephan.kube@ipms.fraunhofer.de

Fraunhofer IPMS
Maria-Reiche-Straße 2
01109 Dresden, Germany
www.ipms.fraunhofer.de/en