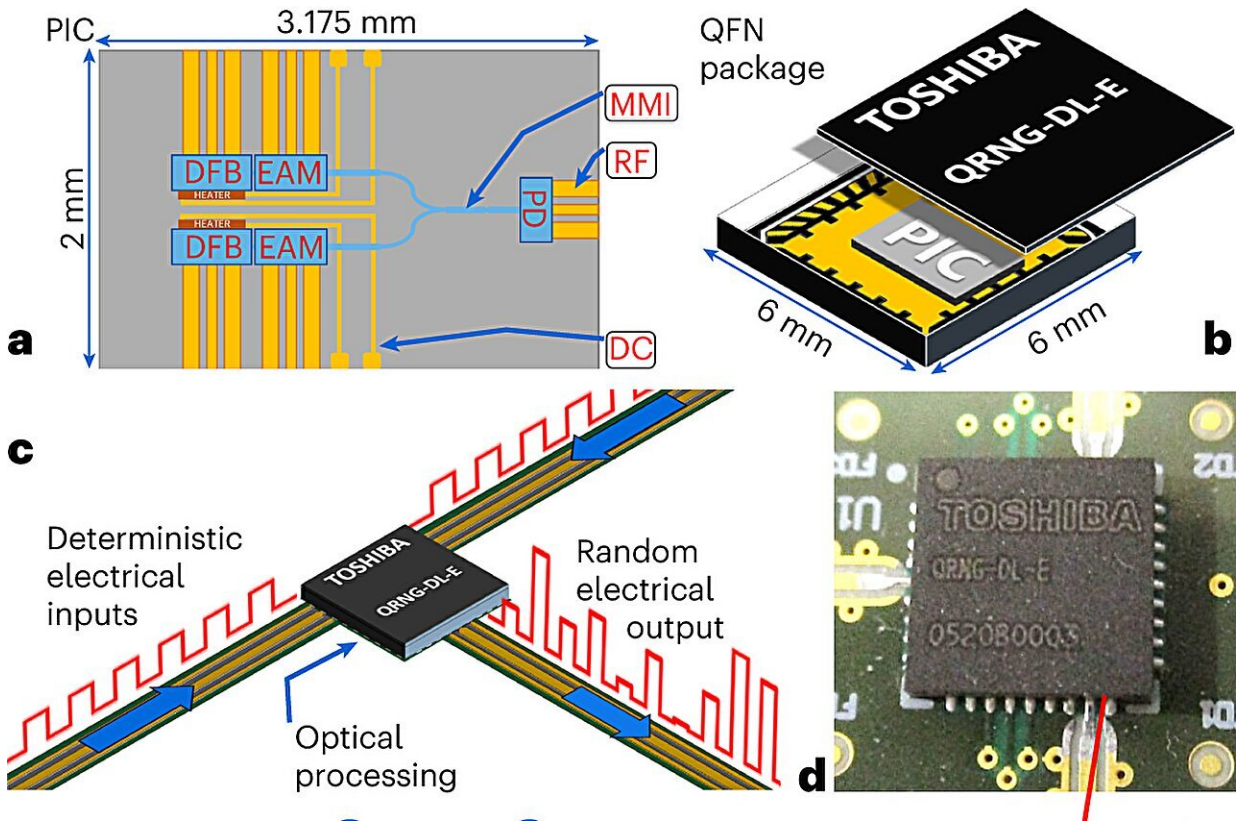
New quantum random number generator achieves 2 Gbit/s speed

June 11 2024, by Ingrid Fadelli



Implementation of a deployable OEC with integrated photonics. Credit: *Nature Electronics* (2024). DOI: 10.1038/s41928-024-01140-0

The reliable generation of random numbers has become a central component of information and communications technology. In fact,

random number generators, algorithms or devices that can produce random sequences of numbers, are now helping to secure communications between different devices, produce statistical samples, and for various other applications.

Researchers at Toshiba Europe Ltd. recently developed a new quantum random number generator (QRNG) based on a photonic integrated circuit that can be directly integrated in electronic devices. This QRNG, introduced in a paper published in *Nature Electronics*, can securely and robustly generate random numbers at a remarkable speed of 2 Gbit s^{-1}.

"Randomness is now a valuable commodity, as it drives nearly all digital protocols that enable private communication," Raymond Smith, Senior Research Scientist and co-author of the paper, told Tech Xplore.

"The common use of pseudo-random number generators (PRNGs) poses a potential security threat because PRNGs are merely deterministic algorithms and do not provide true randomness. This is particularly critical for secure communication systems."

Recent studies have highlighted the potential of generating truly unpredictable numbers using QRNGs, random number generators that leverage natural processes of a quantum origin. Smith and his colleagues at Toshiba have been experimenting with these techniques.

"Previous research efforts and ideas that inspired this work include the quest to simplify the hardware of QRNGs," Smith said.

"Typically, QRNGs employ photonic components such as lasers and detectors, which are bulky and require special handling when assembled with electronics. This complexity makes QRNGs more challenging to deploy on a large scale and more expensive. However, a technology called 'integrated photonics' is helping to overcome these challenges."

Integrated photonics circuits allow researchers to condense all central optical components into a single chip that is only a few millimeters in size. Smith and his colleagues tried to use integrated photonics technologies to create a photonic integrated circuit (PIC) that could simplify the complexity of their QRNG method, facilitating its future large-scale deployment.

"Over recent years, Toshiba has made a number of advances in PIC technology, including the development the world's first chip-based quantum key distribution (QKD) system," Smith said.

"This QKD system incorporated a QRNG PIC in a 14-pin butterfly package whose optical output needed to be fiber-coupled to a high-speed photodiode on the QRNG electronic board."

Credit: Marangon et al.

The primary objective of the recent study by the team at Toshiba was to develop a fully-fledged QRNG based on a PIC with only electronic inputs and outputs. In addition, the researchers planned to deploy the QRNG on real devices to validate its effectiveness.

"Typically, PICs are tested under controlled conditions using specialized laboratory equipment," Smith explained. "This approach makes it difficult to assess the performance of this technology once deployed in real systems, under real operating conditions."

Smith and his colleagues designed a compact printed circuit board that embeds the PIC they developed, called optical entropy core (OEC). OEC has standard packaging that resembles that of other electronic chips and measures 6 x 6 mm^2. The circuit board it is embedded in includes electronic modules that drive the PIC, as well as modules that read out its generated random signals.

"So, how is the random signal produced?" Smith said. "The PIC comprises two lasers that emit optical pulses with random phases due to quantum noise. These pulses interfere with each other, generating a pulse with random optical intensity, which is then converted into a random current signal by a fast detector. The detector signal is processed by the board and converted into random bits that can be distributed at a very fast rate (Gb/s)."

The primary advantage of the new integrated photonics-based QRNG is that its underlying PIC is cost-effective and can be assembled on electronic boards using conventional serial assembly methods. This could

facilitate its future large-scale deployment in various electronic devices, making it a competitive and better performing alternative to PRNGs.

"We built eight boards to study the variability of performance across different devices," Smith said. "Moreover, to ensure the security of its final output, the QRNG performs health tests on the OEC's output to verify that it continuously operates as expected, automatically adjusting the OEC driving parameters if required, as well as calculating the secure generation rate that it can achieve in real time. If this rate drops, the QRNG can automatically adjust the post-processing to ensure that the final output remains unpredictable."

While PICs are generally tested in isolation using specialized equipment, the PIC developed at Toshiba can be seamlessly integrated with electronics and tested in real-world settings. Initial tests were highly promising, demonstrating that OEC can operate as reliably as other standard electronic components.

"We embedded a QRNG board in a QKD system and operated it continuously for 38 days, producing a stable random signal despite significant temperature fluctuations," Smith said. "This test demonstrates the readiness of our QRNG for deployment in real systems, under real operating conditions. Another notable point is that we obtained very similar performances from all eight boards, which is critical for establishing a performance baseline."

The recent study by this team of researchers represents a key advancement in the development of integrated photonic-based QRNGs and could contribute to their future mass deployment. So far, Smith and his colleagues were able to attain a random bit generation rate of up to 8 Gbit/s, yet they soon hope to further increase this rate.

"This will make these QRNGs appealing for simulations and high-

performance computing," Smith added. "We also plan to continue to increase the robustness of our QRNGs to ensure that they can operate reliably in real-world use cases."

More information: Davide G. Marangon et al, A fast and robust quantum random number generator with a self-contained integrated photonic randomness core, *Nature Electronics* (2024). DOI: 10.1038/s41928-024-01140-0.