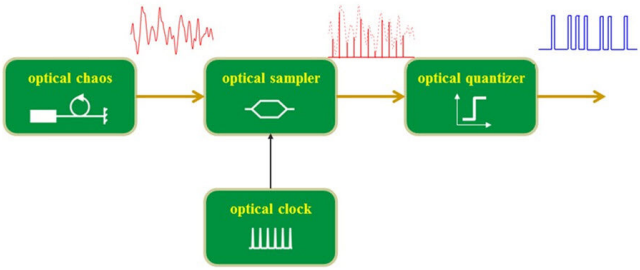
Photons can enable real-time physical random bit generation for information security app

2 May 2022



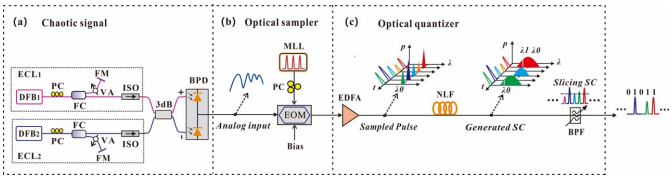
Ultrafast physical random bits can be generated in real time by combining broadband photonic entropy sources with all-optical signal processing techniques. Credit: Pu Li @TUT and GUT.

Cryptographic systems and information security rely on unpredictable, unmanipulable random bits that are physical in nature. Especially in the context of private key systems that enable unconditional security via "one-time-pad" cryptography, the real-time generation rate of physical random bits critically determines the secure communication rate.

Optical chaos presents a reliable way to generate fast and real-time random bits, due to its high bandwidth and large amplitude fluctuations. However, most random bit generators that are based on optical chaos perform their quantization in the electrical domain using electrical analog-to-digital converters, so an electronic bottleneck currently limits their real-time rates. The large gap between the physical random bit generation rates and modern communication rates is a fundamental weakness of these security systems.

As reported in *Advanced Photonics*, an international team of researchers from China and the UK recently proposed and experimentally demonstrated a novel, all-optical random bit generation (RBG) method. Chaotic pulses are quantized into a physical random bit stream in the optical domain by means of a length of highly nonlinear fiber. In the proof-of-concept experiment, they successfully generated a 10 Gb/s random bit stream in a single channel.

The team notes that the current rate-time of 10 Gb/s is only limited by the adopted chaos bandwidth. Their scheme can operate potentially at much higher rates than 100 Gb/s if the bandwidth of the chaotic entropy source is sufficient, considering that the Kerr nonlinearity of silica fiber with an ultrafast response of few femtoseconds is exploited for composing the key part of quantizing laser chaos.



Schematic of the proposed all-optical RBG: (a) optical chaos, (b) optical sampler, and (c) optical quantizer. DFB, distributed feedback semiconductor laser; PC, polarization controller; VA, variable optical attenuator; FM, fiber mirror; ISO, optical isolator; 3 dB, 3 dB fiber coupler; BPD, balanced photodiode; MLL, mode-locked laser; EOM, electro-optic modulator; EDFA, Erbium-doped fiber amplifier; HNLF, highly nonlinear fiber; BPF, optical bandpass filter. Credit: Guo et al, 2022

All-optical RBG can effectively circumvent the rate limitation of electronic signal processing. For future applications, electrical circuits may eventually be

completely replaced by solely optical devices due to the practical advantages of photons.

More information: Ya Guo et al, Ultrafast and real-time physical random bit extraction with all-optical quantization, *Advanced Photonics* (2022). DOI: 10.1117/1.AP.4.3.035001

Provided by SPIE--International Society for Optics and Photonics