The International Society for Optical Engineering

SPIE Newsroom

10.1117/2.1200609.0415

A quantum random bit generator for secure communication

Marco Fiorentino and Raymond G. Beausoleil

An optics-based quantum measurement system generates random bits for cryptographic applications, with security guaranteed by the laws of quantum mechanics.

Random bit generators (RBGs) are used in computer-based numerical integration, simulations and, above all, cryptography. Software RGBs use an algorithm with an initial value, or seed, while hardware RBGs, intrinsically more secure, output random numbers by taking measurements of some unpredictable physical phenomenon.

With hardware RBGs, the actual physical system chosen is critical to maximum security. Most sample chaotic systems such as thermal noise or turbulence. The behavior of such phenomena, however, can be influenced or predicted (albeit for a short time) by a determined attacker. Quantum mechanics, by contrast, offers the ultimate randomness because certain of its measurements are intrinsically and fundamentally unpredictable. Photons, polarized at 45°, hitting a polarization beam splitter, are a good example. Half will be reflected and half transmitted, but the outcome in each instance is completely unpredictable.

While this kind of RBG has been used in the past,[1] we have improved it by quantifying randomness in a way that would effectively defeat any efforts to control the system.[2] Security can now be guaranteed not by assumptions about the computational resources of the attacker, but rather by the laws of quantum mechanics.

A secure random bit generator

A schematic of our quantum RBG is shown in Figure 1. We use a photon source coupled to a single mode fiber. To generate random bits, the light is linearly polarized at 45° and sent to a fiber polarization beam splitter that separates horizontally from vertically polarized photons. The two outputs of the beam splitter are sent to single photon counting detectors and, depending on which detector registers an event, we add 0 or 1 to the sequence of random bits.

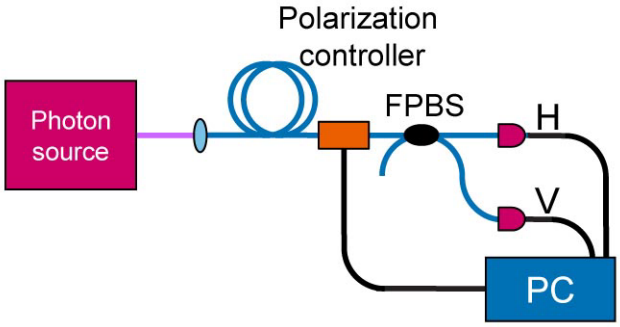

Figure 1. *In this schematic for quantum random bit generator, FPBS is a fiber polarization beam splitter, while the PC is used to store the bits, measure the min-entropy, and run the extraction algorithm.*

In a perfect world this would be sufficient to generate secure random bits. Imagine, however, that an attacker, Eve, takes control of the photon source. She transmits photons that are horizontally and vertically polarized in a fraudulent random sequence. A statistical analysis would not reveal the intrusion. How could the RBG user spot such an attack and take corrective measures?

Our solution is based on the observation that every time Eve (or a system failure) tampers with the photon source, she introduces classical pseudo-randomness.[2] We use a quantity called min-entropy[3] (H_∞) that can distinguish genuine quantum randomness from false pseudo-randomness. The min-entropy is a number between 0 and 1 that corresponds to the fraction of 'good' randomness in the bit sample: $H_\infty = 1$ being perfectly secure and $H_\infty = 0$ completely compromised. Interestingly, one can build an algorithm, called a *randomness extractor*, that deliv-

Continued on next page

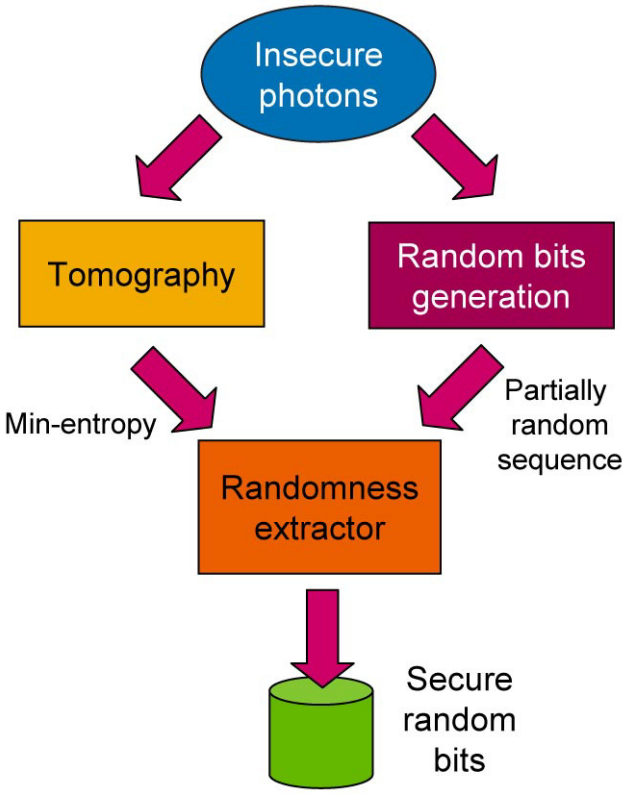

Figure 2. *In random bit generation, photons that are not secure are used to generate random bits and make measurements for tomography. The results of these measurements are used by the randomness extractor to generate secure random bits.*

ers a perfectly random sample (with $H_\infty = 1$) from a partially random one (with $0 < H_\infty \leq 1$).[3,4]

Measurement of the min-entropy of the bit stream is a key component of our RBG. We have recently demonstrated[2] that quantum tomography, a statistical process for reconstructing the state of the quantum systems, can be used to make this measurement.[5] Quantum tomography allows the quantum state of a system, in our case the polarization of the photons, to be completely characterized. It is equivalent in this case to constructing the Stokes parameters of incoming light[5] and can be implemented with a few measurements. We use the polarization controller and fiber polarization beam splitter to make the calculations necessary to reconstruct the quantum state, and then we measure the min-entropy. This value is then employed with the randomness extractor to provide a secure random bit sequence. The security of the RBG is guaranteed, thanks to the measurement of min-entropy, by the physics of the device, not by statistical tests that a sufficiently clever attacker could subvert.

Our current version generates 56k secure bits per second.We are currently working on an improved compact version with increased security and higher bit rates that can be used in quantum communication protocols such as quantum key distribution (QKD).

Author Information

Marco Fiorentino and Raymond G. Beausoleil
Hewlett-Packard Labs
Palo Alto, CA

References

1. A. Stefanov, O. Guinnard, L. Guinnard, H. Zbinden, and N. Gisin, *Optical quantum random number generator*, **J. Mod. Opt. 47**, p. 595, 2000.
2. M. Fiorentino, D. A. Fattal, C. M. Santori, S. M. Spillane, W. J. Munro, and R. G. Beausoleil, *Quantum information primitives using linear optics*, **Proc. SPIE 6305E**, 2006.
3. B. Barak, R. Shaltiel, and E. Tromer, *True random number generators secure in a changing enviroment*, **Workshop on Cryptographic Hardware and Embedded Systems**, 2003.
4. R. Shaltiel, *Recent developments in explicit constructions of extractors*, **Bulletin of the European Association for Theoretical Computer Science 77**, p. 67, 2002.
5. D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, *Measurement of qubits*, **Phys. Rev. A 64**, p. 052312, 2001.