Docket #: S11-487

All Optical Random Bit Generator

Researchers at Stanford University have developed a high-speed, all-optical random number generator based on quantum randomness. This novel random number generator uses a twin degenerate optical parametric oscillator (OPO) that comprises two identical OPOs, each of which can stably oscillate in one of the two possible phase states. An unequal arm interferometer can then analyze the relative phase states of the two OPOs; the optical beam at the output randomly toggles between two intensity levels with a well-defined clock signal; with absolutely no post-processing, this device is capable of generating quantum random numbers. A sequence of 1-billion bits obtained by this method successfully passed standard statistical randomness tests, yielding a 0.5000 probability for either pulse state. Existing software-based random number generators are only pseudo-random (they depend on a breakable security key) and are thus susceptible to attacks; this quantum random number generator, which has the capability of running continuously for several days, is not vulnerable to the aforementioned attacks. This true random number generator can be easily integrated and miniaturized, making it desirable for applications ranging from cryptography to computer simulations.

Applications

- Cryptography
- Computer simulations
- Data storage
- Secure data transfer

Advantages

- *Fundamentally random*
    - **Not dependant** on a breakable “random seed”
    - Test results have proved **statistical randomness of the output**

    - Random numbers generated through quantum noise
        - Minimal influence from other noise sources (i.e. thermal, mechanical, etc)
    - None of the design parameters favors oscillation in one or another
- *Not vulnerable to attacks*
    - True quantum random number generation **guarantees immunity to attacks**
- *Absolutely no post-processing*
    - Unlike other physical random number generators, no need for electronic or computer post-processing
- *Robust and reliable*
    - Capable of running **continuously** for several days
- *Easy to integrate*
    - **Compatible** with commercially available fiber lasers
    - **Integration and Miniaturization** for increased applicability
        - Optical parametric oscillators can be reduced to Sub-millimeter size
        - Can be implemented on a chip
- *Fast*
    - Speed is not fundamentally limited
    - Allows for bit-rates as high as in the **Mbps range**, while smaller OPOs can allow bit-rates in the **Gbps range**
- *All-optical Quantum System*
    - Photons are more **easily handled** than atoms
        - Unlike quantum electronic / atomic system, implementation doesn't require sophisticated environment
    - Unlike many quantum optical experiments, very-sensitive detection system is not required
    - Photodetection is not part of the random process

Publications

- Alireza Marandi, Nick C. Leindecker, Konstantin L. Vodopyanov, and Robert L. Byer, All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators, Optics Express, Vol. 20, Issue 17, pp. 19322-19330 (2012), http://dx.doi.org/10.1364/OE.20.019322
- Marandi, Alireza, Nick C. Leindecker, Konstantin L. Vodopyanov, and Robert L. Byer. Twin Degenerate OPO for Quantum Random Bit Generation, Conference

paper presented at Nonlinear Optics: Materials, Fundamentals and Applications (NLO), Kauai, Hawaii, July 17, 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper NME4.

Patents

- Published Application: 20140016168
- Issued: 9,423,819 (USA)

Innovators

- Alireza Marandi
- Konstantin Vodopyanov
- Robert Byer

Licensing Contact

Chris Tagge

Technology Licensing Program Manager

Email