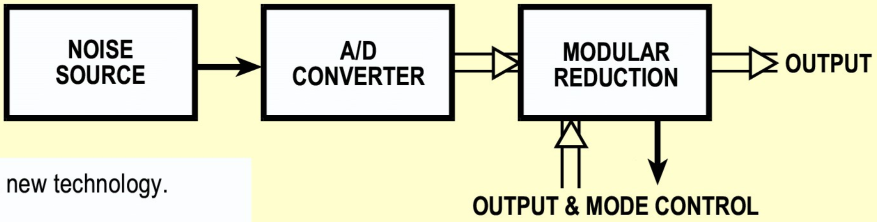
*x*RNG High Performance Random Number Generators

Add hardware true random number generation (RNG) to your application with our simple, inexpensive method.

If you can provide a noise source, an A/D converter, and a little bit of logic, then you can use our xRNG method.*



The purpose of this brief is to introduce a new technology.
Patent rights are available for license.

FEATURES

- NON-DETERMINISTIC (TRUE RANDOM OUTPUT)
- HIGH SPEED
- UNIFORMLY DISTRIBUTED OUTPUT
- SMALL BIAS
- SYNCHRONOUS
- REQUIRES NO CALIBRATION
- LOW COST

APPLICATIONS

- COMPUTER PLATFORM SECURITY
- SECURE INTERNET E-COMMERCE
- CRYPTOGRAPHY
- SECURITY KEY GENERATION
- ELECTRONIC GAMES
- COMPUTER MODELING
- ARTIFICIAL INTELLIGENCE

*x*RNG is a high-speed, hardware-based true random number generator (RNG) method which provides digital systems with unsurpassed performance, security, and value. The method is particularly well-suited to applications which already entail an analog-to-digital converter.

High-Performance computing applications will benefit from the extremely small bias, which can now be provided for true-random sequences generated synchronously at extremely high speed: high-quality numbers at up to PECL speeds.

Low-Cost security applications, such as personal computers, internet appliances, smart cards, cellular telephones, automotive remote key hubs, and other low-to-moderate speed applications, will benefit from the extremely small bias, which can now be provided for true-random sequences generated at moderate-to-high speed at low cost.

SOURCES

1. Intel Platform Security Division. (1999) *The Intel Random Number Generator.*
2. Rand Corporation. (1966) *A Million Random Digits with 100,000 Normal Deviates,* The Free Press. Glencoe Illinois.
3. Schmidt, H. (1970) Quantum-mechanical random-number generator. *Journal of Applied Physics, 41,* 462-468.
4. U.S. Patent No. 4,853,884 8/1989 Brown et al. (Motorola) Random Number Generator with Digital Feedback
5. U.S. Patent No. 5,224,165 6/1993 Reinhardt et al. (Hughes Aircraft) High Speed Word Generator
6. U.S. Patent No. 5,961,577 10/1999 Soenen et al. (Texas Instruments) Random Binary Number Generator
7. U.S. Patent No. 5,963,104 10/1999 Buer (VLSI) Standard Cell Ring Oscillator of a Non-deterministic Randomizer Circuit

*Patent rights are pending in this technology. No license to or transfer of any intellectual property rights are granted expressly or by implication, estoppel or otherwise by this document. All brands, names, and trademarks are the property of their respective owners. This document is furnished with no confidentiality requirement.

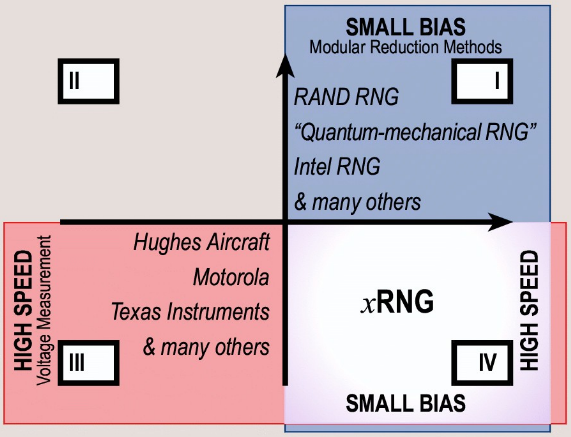
Get High Speed *and* Small Bias with *x*RNG

xRNG technology combines the high speed of voltage measurement with the small bias of modular reduction. Designers no longer have to choose between small-bias (quadrant I) and high-speed (quadrant III). With xRNG, designers can now have both in quadrant IV.

Quadrant I small-bias designs measure time with a modulo-counter. In 1947, RAND used a random pulse source to stop a 5-bit counter.[2] Today, the Intel RNG released in the 810 Chipset uses a random source and a 1-bit counter.[1] However, "it takes time to measure time."

Quadrant III high-speed designs measure voltage with a comparator. However, the median of a random voltage wanders, so that the 1-bit output has an unstable bias requiring correction. For example, Hughes Aircraft[5] and VLSI[7] exclusive-or the outputs from many 1-bit RNGs.

Quadrant IV xRNG designs measure voltage with an analog-to-digital converter for high speed and use modular reduction for small bias.



Contact: Andrew Vincze
avincze@rngresearch.com
Tel: 860-444-2996
Fax: 860-437-0662
40 Franklin Street, New London, CT 06320

rng
RESEARCH
www.rngresearch.com