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

*x*RNG High Performance Random Number Generators

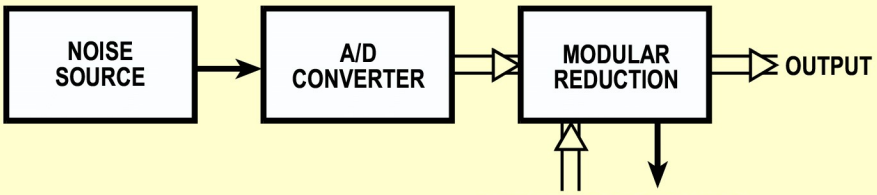

Figure 1

INTRODUCTION

*x*RNG random number generators (RNG) provide an extremely fast, low-cost method of producing random numbers which are consistent, virtually unbiased, and secure. The *x*RNG method accomplishes this by measuring the output of an analog noise source with an analog-to-digital converter and applying a modular reduction method to these measurements. This results in truly unpredictable (non-deterministic) random numbers of any desired bit length with uniform distribution and ultra-low bias.

FUNCTIONAL DESCRIPTION

As shown in Figure 1, output from an electronic noise source is converted by an analog-to-digital (a/d) converter to provide a normally-distributed digital random variable. The output of the a/d converter is subjected to a modular reduction, as shown by the "modular reduction" functional block, which is also the output stage of the random number generator.

NOISE SOURCE

This may be any source which provides an analog random variable. For example, a reverse-biased P-N junction (noise diode) may be ac-coupled to a pre-amplifier to provide random Gaussian noise. The input level to the a/d converter should be the maximum level for which no clipping occurs over the entire range of operating conditions. For high-end applications, AGC is recommended.

A/D CONVERTER

This may be any a/d converter. (Note that correlated non-linearity errors may affect the quality of the RNG output, so care should be taken when selecting a converter. Treatment of this issue is beyond the scope of this document, however some guidance should be presented: Exceptional results have been obtained with Analog Devices part No. AD776 and one is advised to use an a/d of similar architecture. In general, one should use a converter for which the DNL and INL plots show no discernable patterns.)

MODULAR REDUCTION

The modular reduction stage of the *x*RNG takes digital input from the a/d converter, and outputs modular residues. These residues are uniformly distributed and are the output of the RNG.

As a practical matter, the reduction is most efficiently performed by discarding most significant bits, and outputting the remainder.

For example, a 16-bit a/d converter may be used. Given that the a/d converter output is normally distributed with a mean near center scale and a standard deviation of at least 256 codes (with no clipping), data bits D8 – D15 may be discarded and bits D0 – D7 provided as an 8-bit uniformly distributed output.

The distribution of the noise need not be normal (or even consistent). As shown in Figure 2a, the probability in an arbitrary distribution is divided into 64 slices by a 6-bit a/d converter. Probabilities for odd codes are shaded. Data bits D1 – D5 are discarded and bit D0 is outputted (reduction *modulo*-2). In Figure 2b, the modular reduction is illustrated by regrouping the slices according to residue. This yields a set of mimic distributions – one for each output (two in this case). The distribution is thus 'dealt' to the respective outputs like consecutive cards in a deck. As long as the converter resolution is high enough, the mimic distributions will be very similar and the probabilities of the outputs will be nearly equal to a very good degree.

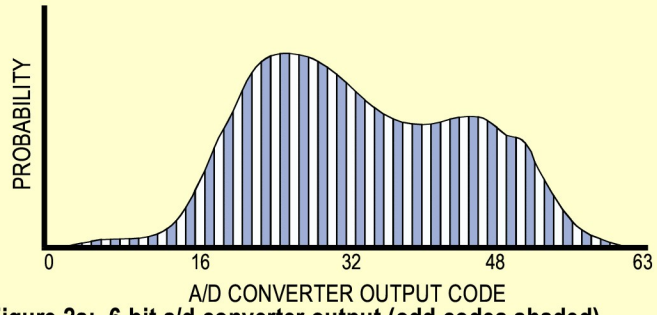

Figure 2a: 6-bit a/d converter output (odd codes shaded).

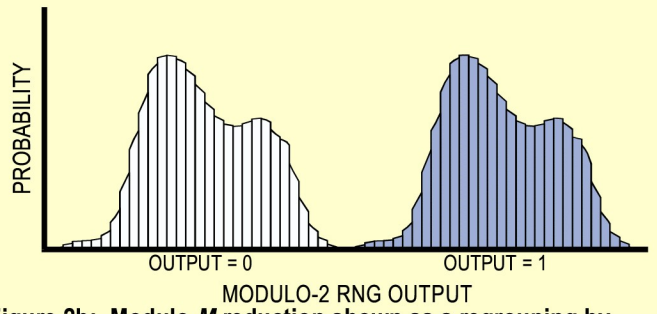

Figure 2b: Modulo-*M* reduction shown as a regrouping by output into a set of *M* mimic distributions.

Test data, random numbers, and more information: www.rngresearch.com/xrng