Entropy Compensation for Random Pads

Horace Heffner April 2000

Bit wise random number generation is useful for one time pad cryptographic use, gaming, Monte Carlo simulations, or possibly for sensing the world psyche in projects like that at <noosphere.princeton.edu>. In looking at the claims for US Patent 5,830,064, the Mindsong Inc patent for devices related to the methods used in the projects described at <noosphere.princeton.edu>, it appears a systematic error arises.

To create a random string of bits, a pad, tandem amplifier stages can be used to amplify thermal noise, and a trigger used to sample the state of the output at a fixed rate much slower than the noise central frequency, or to count the state changes across a specific voltage threshold, say zero volts, over a fixed period. In any similar method, the output state does not have a 50-50 chance of being a 1, due to trigger or flip-flop hysteresis that can never be fully compensated, because it varies with ambient conditions. A complicated statistically self-correcting biasing mechanism can be used to adjust the hystereses so that the time average probability of a 1 vs 0 is maintained at 50 percent, or an arbitrarily close approximation thereof.

One method to correct for hysteresis is to invert the interpreted state of a flip-flop containing the output sample value, every other clock cycle. This can be done electronically, using an additional flip-flop and xor. It has the property of cutting the sampling rate in half, however. The state sequence of the xor value without correction is 10101010..., the state sequence after correction is 001100110011.... The state flip only occurs at half the clock rate, but the time interval is fully corrected, in reasonably steady-state operation, because each short interval of the state correcting flip-flop is paired with a long interval.

Mindsong uses similar techniques and also employs the technique of xoring masks with the random bit stream to attempt to further randomize it, notably the 010101... pattern. There clearly would be no use for such a pattern if the circuit used was not sensitive to hysteresis.

The interesting fact is that NO AMOUNT OF BIT XORING WITH A FIXED PATTERN WILL CORRECT THE NON-RANDOMNESS FROM HYSTERESIS.

Suppose for a moment that the timer flip-flop hysteresis is very bad, so that it is in a 1 state 3/4 of the time and a 0 state 1/4 of the time. This gives the following

Entropy Compensation for Random Pads

Horace Heffner April 2000

probability table for successive bit pairs:

bits	P1	P2	P1*P2
00	1/4	1/4	1/16
01	1/4	3/4	3/16
10	3/4	1/4	3/16
11	3/4	3/4	9/16

You can see that xoring the bit pairs with any chosen mask can never make the probabilities all exactly 1/4, which is necessary to achieve a truly random sequence. The probabilities remain the same, but get shifted around to other bit sequences. The uniform randomness can never be achieved. Any scientific study or application requiring uniformly random bit sequences is invalidated or corrupted to the degree exposed to circuit hysteresis problems, and that exposure is a function of temperature and possibly other ambient conditions.

So, how to correct the problem? One cheap solution is to sum (drive the clock with) randomly varying intervals instead of uniform intervals, which gives a random walk nature to the measured time of a random length event. In other words, both the clock timer and the measured interval must be random and independent. In the case where the time interval between radioactive disintegration events is used, the timer flip-flop state needs to be driven by a nonuniform clock, say by filtered noise from a high gain amplifier. The mean frequency used to drive the flip-flop clock needs to be at least 12 times higher than the random interval measured, and the switching speed of the timer flip-flop preferably a couple orders of magnitude faster at switching state than that. Two independent high gain amplifiers with high and low band pass filters can be used to achieve the two independent interval clocks. Two identical random interval clocks could be used, and the timed event duration clock would then consist of a 4 stage (or more) counter so as to lengthen the timed interval by a factor of at least 16.

Unfortunately, if you are statistically testing for the non-randomness of such a device to measure psychic output, your success rate over chance will likely be diminished by employing the suggested improved method.

UPDATE - FEBRUARY 16, 2006

Entropy Compensation for Random Pads

Horace Heffner April 2000

An arbitrarily close approximation to an hysteresis free circuit (a circuit producing bits with information entropy approaching 1) can be obtained by XORing the outputs from multiple independent circuits having hysteresis. The XORing can be achieved using simple clocked digital logic. Suppose a circuit is being used that is very fast, but exhibits a hysteresis of about 1 percent. That is to say the probability of a 1 is 0.495 percent, and the probability of a 0 is 0.505 percent. By XORing the output of the two independent circuits, the probability of a 0 drops to 0.495^2 + 0.505^2 = .5005. By XORing the output of four independent circuits, the probability of a 0 drops to 0.4995^2 + 0.5005^2 = .5000005. By XORing the output of eight independent circuits, the probability of a 0 drops to 0.4999995^2 + 0.5000005^2 = .5000000000005. The hysteresis is removed to less than 1 part in 10^12.

Using this method random pads can be generated at GHz rates. The initial bit production is by clocked sampling of a fast freewheeling oscillator modulated by output from an ultrahigh gain op amp with input from a thermally sensitive source, like an LED. The initial drivers consist of 8 bit producers feeding 4 XOR gates. Three additional XOR gates connected in cascade fashion to produce a single bit stream output with hysteresis reduced to less than one part in 10^12. This method can be extended to any desired degree of hysteresis removal at a logarithmic cost. It can readily be implemented on a small chip that also buffers the bit stream for delivery to a bus in parallel.

This method has the advantage over the Von Neumann whitening method (see: http://en.wikipedia.org/wiki/One_time_pad and http://www.cryptography.com/resources/whitepapers/VIA_rng.pdf) in that no data is rejected, thus the pad bit stream can be produced at a fixed and maximum speed with entropy performance that is also vastly superior to the Von Neumann whitening method. It also has the advantage that it compensates for differences in entropy between each of the input circuits, and changes in such differences with changing conditions, like temperature.

It is also noteworthy that a similarly improved entropy performance can be obtained, although with a reduction in bit rate, using *any* true random pad generator, by merely generating N pads and XORing them together. The exponential power of this method of entropy improvement is especially seen when N is 8 or greater.