Subject: Re: IDL random number generator
Posted by James Kuyper on Tue, 20 May 2003 14:30:43 GMT
View Forum Message <> Reply to Message

Big Bird wrote:
>
> David Fanning <david@dfanning.com> wrote in message
news:<MPG.192c7f24abbae652989b96@news.frii.com>...
>> Folks,
>>
>> You guys might want to check out this Quantum Random
>> Number Generator. This one takes a LONG time to repeat! :-)
>>
>>   http://www.idquantique.com/qrng.html
>>
>> Cheers,
>>
>> David
>
> I would mistrust this for the following reasons.
>
> The website states:
>
>> Being deterministic devices, computers are not capable of producing random
>> number generators.
>
> That statement is false: any odd soundcard has a noise-generator
> (essentially a glorified resistor with a big amplifier attached to it)
> that is capable of producing perfectly fine thermal random noise. I've
> used that for creating random numbers since back in the days of the
> Atari-800 (OK, so I'm dating myself here).

It's an exagerration, rather than being false. Their real point was that
the standard random number generators are not truly random, and can't be
truly random as long as they are entirely based in software.

> Even if a piece of external hardware was desirable for this process it
> could be cobbled together for $5 from a couple resistors, an opAmp for
> amplification and an RC high-pass filter (to get rid of slow drifting
> in the opAmp). Potentially another opAmp driven open-loop as a
> Schmitt-trigger. Gives you clock-free(!) bit-noise.
>
> Anybody who tries to sell a quantum-ANYTHING to make noise(!!) is
> direputable from the word 'go' in my eyes.

Thermal noise is not as fundamentally random as the quantum fluctuations
that determine radioactive decay. Among other things, your circuit will
pick up and therefore be influenced by EM radiation, which is not

random, and since it's thermal noise you're looking at, it will be influenced by the temperature. I'll admit, it's a subtle difference, but if you were doing serious scientific work using those random numbers, it's one you should worry about when designing the program.