
Subject: Re: IDL random number generator
Posted by [condor](#) on Mon, 19 May 2003 23:51:10 GMT
[View Forum Message](#) <> [Reply to Message](#)

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).

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.
