Re: How to develop a random number generation device

Source: http://sci.tech−archive.net/Archive/sci.electronics.design/2007−09/msg03270.html

- *From*: "Joel Kolstad" <JKolstad71HatesSpam@xxxxxxxxx>
- *Date*: Mon, 17 Sep 2007 13:56:36 −0700

"John Larkin" <jjlarkin@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:m5nte3ps9ff0papglqq4uiv86helfp2u23@xxxxxxxxxx

> But my PC doesn't
> have hardware problems, it has software problems.

Sure it does (have hardware problems), Intel was just smart enough to allow patching of the microcode so that buggy features are worked around or simply not used. When the buggy simply can't be fixed, it's the compiler writers who get burdened with having to keep up which bugs are still present and insuring that code isn't generated that would expose them (very few people program x86 CPUs in assembly anymore!). Intel is also smart enough to do a lot of testing any time a new CPU comes out −− I'm sure there are still plenty of people there who remember the nasty FDIV bug, as well as the lesser−known problem with the first 1GHz CPUs that would randomly fail to compile the Linux kernel

I've been surprised at just how buggy a lot of OC software is if you actually start pushing it to its limits −− it's clear that much software today only gets very rudimentary testing. (And as I've stated before, I personally know "programmers" who believe they can claim on a progress report that they "finished such and such software" as soon as it *compiles*. :−( )

.