From: Chen, Lily (Fed)
To: Miller, Carl A. (Fed)
Subject: Re: Comments on "Quantum Entropy Chip" paper
Date: Tuesday, December 5, 2017 3:15:00 PM

Hi, Carl,

Thanks for the review. It is very helpful for us to understand their approach.

Lily

On 12/5/17, 2:50 PM, "Miller, Carl A. (Fed)" <carl.miller@nist.gov> wrote:

Hi Lily –

I read through the paper you gave me just before your trip:

"Quantum Entropy Chip (QEC) – Building Quantum Random Number Generator with Radioactive Isotope as Entropy Source"
Anonymous

Here are my comments:

The paper studies random number generation based on radioactive decay. This is out of my area of expertise, but roughly I understand it like this: when the radioactive decay is occurring, particles are emitted at random times, and the probability distribution that they follow is a Poisson distribution. Moreover, this distribution is supposed to represent a quantum (rather than classical stochastic) process, which means that the Poisson distribution represents true randomness (rather than merely a lack of knowledge on the part of the observer).

The paper proposes an approach to using this decay as the basis for random number generation. Besides the general "quantum" merit of the approach, they argue that it is especially well suited to small devices such as those used in the Internet of Things.

The authors have done an experiment in which they have counted the number of particles emitted in the decay over fixed time intervals, and found that the results closely approximate a Poisson distribution (as expected). They seem to have a method which takes the emission information and, by making use of the presumed probability distribution, converts it into almost uniformly random bits.

I like the paper, and I learned a few things from it. My only negative comment is that the authors make some favorable comparisons of their approach to the approach of using a beamsplitter to generate random numbers, and these comparisons don't seem entirely convincing. When discussing the beamsplitter approach, they point out that that there is necessarily some bias in the raw outputs of the beamsplitter, and that

"The artificial act of post processing is needed that can correct the bias such as XOR algorithm."

Meanwhile, of their own approach, they say,

"There is very little bias which enables statistically satisfactory random number generation."

This seems a little suspect to me. Although I haven't mastered all the details of their approach, there seems to be a significant postprocessing step for converting the radioactive decay information into uniformly random bits. This postprocessing seems at least comparable to the postprocessing in the case of a beamsplitter, so it's not clear to me what advantage is really being claimed here.

Let me know if there's anything else I can comment on. Hope you had a great trip!

-Carl

_____

Carl A. Miller

Mathematician, Computer Security Division

National Institute of Standards and Technology

Gaithersburg, MD