

Generating True Random Numbers From Vacuum Fluctuations in a Quantum System

Love Arreborn, Nadim Lakrouz

ABSTRACT

TODO

1 INTRODUCTION

In cryptography, there are many applications for randomly generated numbers. However, the process of producing these random numbers tends to be pseudo-random, e.g. utilizing the current states of various modules. These numbers do not generate true randomness, and in order to heighten security other methods of generating these are required. Current random number generators (RNG) are usually implemented in code, using certain states of the host machine as a starting point before running a predetermined algorithm. This pseudo-random number generation (PRNG) comes with the drawback that the result is always deterministic, provided that the initial state is known.

True random numbers, then, cannot be produced solely through code. These systems require some input that is neither replicatable nor reproducible. One proposed solution for this is quantum random number generation (QRNG) [1]. By reading quantum fluctuations from any given source, for instance an optical signal, the inherent unpredictability of said source can be harnessed in order to produce a random number from a state that is nigh impossible to reproduce accurately.

In this project, we will be writing firmware for one such solution, which reads quantum variations from from an optical signal. Further details about how this signal is produced will be introduced in section 2 and builds on the work of M. Clason [2]. This optical signal will be converted to a stream of random, raw bits via an Analog to Digital Converter (ADC). In turn, these random bits will be processed via Toeplitz-hashing [3] in order to process these bits into random numbers. Some processing has to be done on the microcontrollers themselves in order to ensure that the data is workable, and Toeplitz-hashing is a tried and tested method to accomplish this. These random numbers will then be output from the microcontroller to the host computer via USB. This thesis will aim to answer one key research question: How can a vacuum fluctuations in quantum system be sampled in order to generate true random numbers?

In producing this firmware, several key considerations have to be made in order for this system to be usable in a production environment. The vision for the end product is a simple USB-stick that can be connected to a host, and produce true random numbers from ambient quantum fluctuations. While this system could very well be implemented on physically larger hardware, thus avoiding the constraints that limited hardware introduces, **add something more clever here**. However, due to this portability constraint, our implementation needs to work quickly and efficiently on resource constrained hardware. As such, our main question is broken down into two concrete research areas:

Research area 1 (RA1): How can Toeplitz-hashing be implemented as effectively as possible on resource constrained hardware, such as a microcontroller?

Toeplitz-hashing been optimized quite well, and previous research can be utilized for this. However, there are still considerations when implementing the firmware for the microcontroller in order to optimize the code. Our goal is to attempt several implementations in order to find the most optimal implementation with the least amount of CPU-cycles.

Research area 2 (RA2): How can data effectively be streamed with a high bitrate to output a host computer?

This will entail several bottlenecks out of our control, which will be discussed in the section regarding the limitations. However, the key consideration is how effectively these quantum random numbers can be streamed to a host computer via USB. We will focus our efforts on the implementation of the code on the microcontrollers in order to ensure that the firmware does not become the primary bottleneck.

2 BACKGROUND

This work is a practical continuation of the work of Clason [2]. In this work, the author aimed to study quantum shot noise originating from photodiodes, and in so doing built a device which read from an optical source, outputting analog voltage from the data “seen” by the diodes. A prototype was constructed, in which a LED is read by a photodiode soldered millimetres apart.

- [1] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb. 2017, doi: 10.1103/RevModPhys.89.015004.
- [2] M. Clason, “Development of a QRNG front-end for shot noise measurement: Analysis of quantum shot noise originating from photodiodes,” Independent thesis Advanced level (degree of Master (Two Years)), Linköping University, Department of Electrical Engineering, Information Coding, Linköping, Sweden, 2023.
- [3] X. Zhang, Y.-Q. Nie, H. Liang, and J. Zhang, “FPGA implementation of toeplitz hashing extractor for real time post-processing of raw random numbers,” in *2016 IEEE-NPSS real time conference (RT)*, 2016, pp. 1–5. doi: 10.1109/RTC.2016.7543094.