# 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 pseudorandom, 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. In this project, we will be writing firmware for one such solution, which reads from an optical signal which has a variable amount of jitter. 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 [1] in order to process these bits into random numbers. 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. 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.

[1] 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.