Creating High-Speed Firmware for Random Number Generating Microcontrollers

Love Arreborn, Nadim Lakrouz

ABSTRACT

In computer security as well as cryptography, one key aspect revolves around generating truly random numbers. Traditionally, this has been done by utilizing non-predictable modules from the computer itself, such as the system time or similar. This is far from true randomness, and this thesis project is aimed at constructing one part of a random number generator which provides randomness by reading from an optical signal. The natural jitter in this signal will provide more randomness than any internal component can offer. This optical signal is then streamed through an Analog to Digital Converter (ADC), which then needs to be processed by a microcontroller. This thesis project aims to create firmware to then process this data into random numbers, with emphasis on creating high-speed implementations of said firmware in order to find the optimal solution for the end product.

1. INTRODUCTION

T