Entropy Engine: Utilizing Non-Deterministic Electron Cascade Dynamics for Cryptographically Secure Password Generation

Monahan, Bode (School: Liberty High School)

The purpose of this project was to design and test a true random number generator using physical noise from an analog input. Most random number generators in common use rely on software algorithms, which can produce predictable results. This project focused on creating a simpler and more reliable hardware based method for generating random data. The first step involved collecting electrical noise from a zener diode and inputting it into a microcontroller. This data included some bias, so additional processing was required to improve randomness. A Von Neumann unbiasing method and bit whitening techniques were used to ensure that the output contained an equal distribution of ones and zeros. The random number generator produces a continuous stream of binary data that can be captured and analyzed. Large data sets containing up to one million bits were generated and evaluated using statistical tests. These tests included bit frequency analysis, entropy measurement, run length testing, autocorrelation analysis, and frequency based analysis. An important outcome of this project was the consistency of the results across different conditions. The generated data showed entropy per bit extremely close to one and no visible patterns over time. This shows that a low cost hardware system can effectively produce high quality randomness suitable for security and scientific applications.

Awards Won: