UNIVERSITY OF NOTRE DAME
NDnano
CENTER FOR NANO SCIENCE AND TECHNOLOGY

ND*nano* Undergraduate Research Fellowship (NURF)
2014 Project Summary

1. Student name: Quinn O’Rourke

2. Faculty mentor name: György Csaba

3. Project title: Creating A Physical Unclonable Function Using Nano-Oscillators

4. Briefly describe any new skills you acquired during your summer research:
I learned and gained a strong command of SPICE (Simulation Program with Integrated Circuit Emphasis). I used it for both design and testing purposes, learning to use both schematics and netlists. In addition, I became more comfortable with the Unix operating system, using it to access the CRC servers to run simulations in parallel.

5. Briefly share a practical application/end use of your research:

The practical application of the research is the production of unpredictable (but repeatable) encryption keys. The hope is that the synchronization (or lack thereof) of the oscillators will create a chaotic signal from which a key can be extracted. The reliance on physical components, instead of a mathematical algorithm, would provide a less vulnerable system.

Summary:

The need for advances in security runs parallel with advances in technology. There is a constant need for improvements in encryption methods. One possible approach is the Physical Unclonable Function (PUF). The idea is that a physical system could serve as a one-way function. This means there is an inherent, repeatable connection between the input and the output of the system, but its complexity inhibits imitation of the system. No amount of previous input and output data would allow an attacker to predict a future output based on input. The thought is that a system of weakly coupled nano-oscillators could serve this purpose. Their chaotic but relatively easily controlled nature seems a viable medium. This was the goal of the summer’s research: to design, test, and assess the utilization of weakly coupled oscillators as a Physical Unclonable Function.

The first part of the process was to design the oscillator. It was decided early on to utilize a Van der Pol oscillator to mimic the output of the nano-oscillators. The Van der Pol oscillator employs a capacitor, inductor, voltage source, and tunnel diode to produce a sinusoidal output. The oscillator was constructed in SPICE (Simulation Program with Integrated Circuit Emphasis) using a voltage controlled current source to replicate the negative resistance of the tunnel diode. The next step was to design a system for the oscillators. The system needed to have the capacity for many inputs and a readable output. Several iterations were created and tested; two showed promise. Both used capacitors for coupling, one connected the oscillators in parallel common node with the capacitor and the other placed the oscillators in series with a capacitor connecting them. Both would use switches to connect the oscillators to the system. The position of these switches would serve as the input. A fellow researcher had already moved forward with the parallel system, so further testing focused on this design with the hope that this would allow for eventual physical testing. The rest of the simulations focused on analyzing and perfecting this basic system. First, the strength of coupling was tested. Sweeping across many orders of capacitance with hundreds of simulations, it was determined that the coupling is most effective when the coupling capacitance is equal to, or slightly below, that of the capacitor inside the oscillator. To test the chaotic nature of the system, single oscillators were swept across a range of frequencies to analyze the effect on the system as a whole. While there was a trend to these results (the frequencies tended to increase as the sweeping oscillator increased its frequency), the data still had very high residuals, suggesting a chaotic nature. When testing for a correlation between average oscillator frequency and output frequency, a similar answer was found. As expected, the average does affect the output enough to cause a trend, but it is nowhere near an accurate predictor. Interestingly, the average frequency of the system does not have a significant effect on the response of individual oscillators. To our knowledge, this is the first study of nano-oscillators for physical unclonable functions. While further studies are needed, we have shown there is promise in this physical system.