Aaron Mills
M.S.
Computer Engineering
Major Professors: Doug Jacobson and Joe Zambreno

Design and evaluation of a delay-based FPGA physically unclonable function

Abstract:
The Physically Unclonable Function (PUF) is gaining increasing interest for its potential use as a hardware primitive in secure computing systems. In the most basic sense, a PUF is a device that harnesses the natural entropy in a physical system. A delay-based PUF in particular depends on the process variation that is inherent in the manufacturing of any integrated circuit. A particular instance of an ideal PUF will consistently output a particular bit pattern. Each instance of the exact same circuit, however, will produce a substantially different pattern. As a result, having full knowledge of its design will not help an attacker to predict its output, nor to successfully clone such a device. For this research, a new PUF variant was developed on an FPGA, and an evaluation of its quality is performed. It is conceptually similar to PUFs developed using standard SRAM cells, except it utilizes general FPGA recon gurable fabric, which offers several advantages. First, it allows greater control over the position and arrangement of each PUF cell. This ability increases our ability to study the various factors that impact a PUF's performance. Second, the PUFs can be reset without requiring the entire device to be reset, which is needed for the application of error correction. Third, it becomes possible to access the output of a large PUF array in parallel rather than word-by-word as in the case with standard SRAM. This can decrease the time it takes to retrieve the PUF output. A quantitative comparison between our approach and other recent PUF designs indicates that our design is competitive in terms of repeatability within a given instance, and uniqueness between instances. A single PUF cell consumes only a single FPGA Slice, and has very low dynamic power dissipation, making it suitable for authentication applications on resource-constrained embedded systems. However, the design can also be tuned to achieve desired response characteristics, which broadens the potential range of applications.