Post-doc position in the intersection of hardware security, machine learning, information theory and statistics.

Funding: new National Science Foundation grant on ``Analytically predicting strong PUF responses from few known CRPs.''

Supervisors: Professor Natasha Devroye (information theory, statistics), Professor Wenjing Rao (digital systems, hardware security) in the Electrical and Computer Engineering department at the University of Illinois at Chicago (UIC), a public research university in downtown Chicago.

Requirements: a Ph.D. in electrical / computer engineering or computer science in which statistics was used extensively, or a Ph.D. in math or statistics.

To apply: Send Resume/CV, unofficial transcript of courses taken, and one paragraph description of why you are interested in working on this project with us. Send to devroye@uic.edu and wenjing@uic.edu.

Further description of the project: This project's goal is to develop a new framework for understanding, in a systematic, theoretically explained way, the fundamental limits and properties of Physically Unclonable Functions (PUFs). PUFs are computer hardware circuits, or hardware security primitives, that can easily be built into chips. They are expected to become essential in securing next generation communication / authentication protocols among Internet of Things (IoT) devices. However, much PUF research has been ad hoc and experimental in nature, with almost no fundamental understanding of their strengths and limits. For example, while ideally the behavior of a PUF should be unpredictable, thus unclonable, some "strong" PUFs have been shown to be "machine learnable". This means that by overhearing a large amount of the data exhibited by the PUF during communication phases, it is possible to predict the behavior of the PUF with high accuracy, thus enabling an attacker to mimic the PUF behavior, posing a severe challenge to the security foundation. Why this is possible is not fully understood, and the proposed work will lay statistical foundations for understanding how and why PUFs become predictable.

PUFs are fundamental security primitives that, when mass fabricated on chips, may provide devices with a low-cost, digital "fingerprint" by exploiting the random disorder in the manufacturing process. This PUF "fingerprint" provides richer content than a simple barcode by offering a unique output function that may be "challenged" with an input bit vector. These inputs interact with the random elements in the architectural configuration to produce a "response". Challenge-response pairs (CRPs) can be used to uniquely identify or authenticate a device. The investigators will determine – analytically in closed form expressions – how predictable the PUF output becomes given knowledge (by an attacker) of a (small) set of observed CRPs. This problem is approached through a new collaboration between two female researchers with expertise in computer engineering and information theory. PUFs will be modeled statistically, which will allow for the derivation of conditional probability mass function (and associated provably optimal predictors) of the PUF response to one (or more) challenge given knowledge of the response to one (or more) other challenge(s). This has the potential to transform how strong PUFs are designed and used for authentication in fundamental ways: ad-hoc approaches will be replaced by provably optimal designs built on sound theoretical underpinnings to maximize, or minimize the predictability. This project will tightly integrate two separate fields, bringing new tools and fresh directions for explaining the vulnerability of strong PUFs.