Hybrid Oscillator Arbiter PUF Using Manufacturing Variations for Robust Security in the Internet of Things

Venkata P. Yanambaka[1] Saraju P. Mohanty[2] Elias Kougianos[3]

Smart Electronic Systems Laboratory, Computer Science and Engineering, University of North Texas, Denton, TX 76207, USA.

Email: [1]vy0017@unt.edu [2]saraju.mohanty@unt.edu [3]elias.kougianos@unt.edu

The invention of transistors and integrated circuits are major milestones in the history of technology. Integrated circuits and transistor scaling allowed us to develop low-power, high-performance chips which are capable of performing complex operations with precision and efficiency. With such high-performance devices into existence, research in the area of the Internet of Things (IoT) has become simpler. Every IoT device is called a "thing" and is connected to the internet for communicating with other things or with a server and the cloud for data transmission and storage. This continuous connection to the network opened up various vulnerabilities using which an adversary can gain access to the system. Cryptographic applications demand more processing power which is limited in the area of IoT and things. Memory present on IoT devices is also limited which makes it difficult to store multiple cryptographic keys on the device itself. Pseudo random number generation using complex algorithms also requires high processing power to generate the random numbers.

Many off the shelf components are available for developing IoT applications. But IC fabrication presents its own challenges like nanoscale manufacturing variations. These are variations in various physical and electrical parameters like the geometry of the nanoscale devices. Even with the advancements of technology and cutting-edge research going on in the area of fabrication processes, when an IC is fabricated, no two devices will be the exactly the same in terms of geometry. This is used advantageously by Physical Unclonable Function (PUF) modules to generate various keys necessary for cryptographic purposes. The manufacturing variations that are introduced in the devices are naturally occurring, unpredictable and uncontrollable. So, when the keys are generated using them, they are going to be naturally random, unlike the pseudo random numbers that are generated using algorithms. As the PUF modules are hardware solutions to the generation of keys, extra processing power is not necessary to generate them. They can be generated when necessary and need not be stored in any memory. Hence no extra memory is required to store the keys and depending on the circuit design, the key size can be large. If reconfigurability is introduced in the design, the number of keys generated can be exponentially high which increases the robustness of the design. Fig. 1 shows the design of a Hybrid Oscillator Arbiter PUF which uses the manufacturing variations in Ring Oscillators to generate keys that can be used for cryptographic applications.

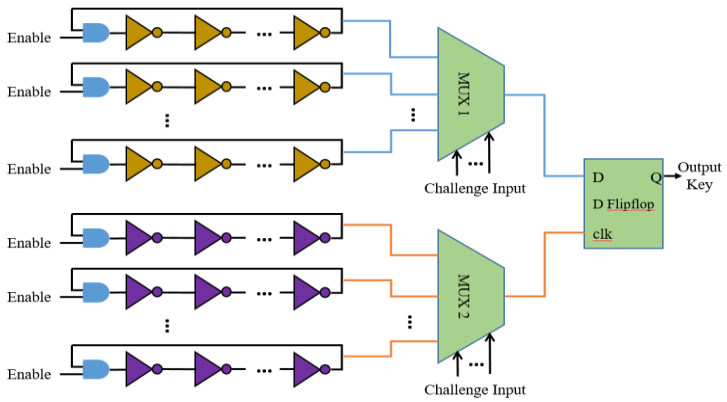

Figure 1 Hybrid Oscillator Arbiter PUF