Reconfigurable HOA-PUF Using Manufacturing Variations for Efficient 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

Applications are efficiently making use of high performance of the chips being manufactured. These devices are consuming less power while delivering high performance. With the low-power, high-performance devices coming to the market, Internet of Things (IoT) applications are growing in leaps and bounds. An IoT environment contains devices that are constantly connected to the network, collecting and exchanging data with each other or with the cloud or server. The number of devices connected to the network is increasing exponentially every year and the number is expected to reach the trillions soon. There are security issues with IoT devices deployed in remote areas: they are not constantly monitored by any authorized personnel. This leads to various issues with the security of the devices. When all of them are connected to the network, a set of new vulnerabilities are opening to an adversary to attack the system. Cryptography can protect the network to some extent but to perform complex cryptographic tasks, the IoT devices should have more memory and the processor should be powerful, which is not the case in most of the "things".

As a solution to this issue, Physical Unclonable Functions (PUF) are proposed. PUFs take advantage of manufacturing variations that occur during the fabrication process. Process variations are unintentional, unpredictable, and uncontrollable. These are naturally occurring variations on the IC. These are used advantageously to create cryptographic keys that are necessary for performing encryption and decryption processes. PUF modules can also be used in various other applications like IP protection and anti-counterfeiting. In various cryptographic applications, pseudo random numbers are generated as keys. However, with the implementation of PUF modules natural random numbers can be generated without implementation of complex algorithms that require high performance computing. Fig. 1 shows the design of a Reconfigurable Hybrid Oscillator Arbiter (HOA) PUF. This design uses the variations present in the ring oscillator and configuration module to generate the output keys used for various cryptographic applications. Fig. 2 shows the design of configuration module which provides reconfigurability and the necessary variability to the module.

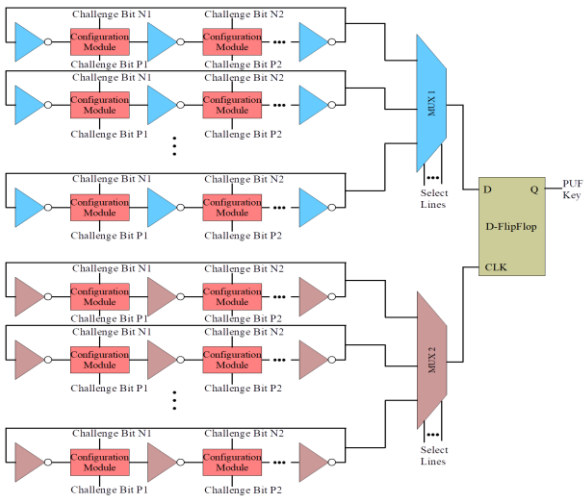

Figure 1 Reconfigurable Hybrid Oscillator Arbiter PUF

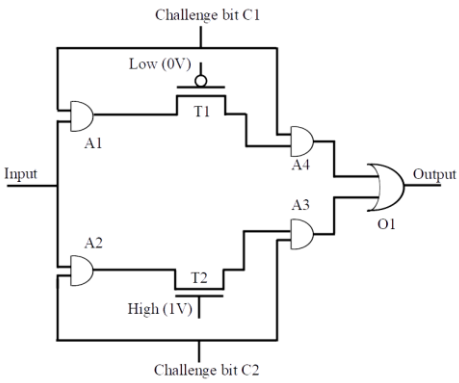

Figure 2 Configuration Module