Energy-Efficient Physical Unclonable Functions for Secure IoT Environment

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

Abstract: The Internet of things is currently the most promising solution for many day-to-day issues that we are facing today. Smart things are being deployed everywhere around the globe to breach various technological barriers. Many cities are being converted into Smart Cities. In such an environment, everyTHING is connected and where 'everything' is connected, security is one of the main concerns. If an environment is attacked and breached, an entire city or home can be in chaos. Hence, security becomes a main priority. At the same time, increasing security should not reduce the ease of use for the user. One of the most efficient solutions for this issue is hardware security. Physical Unclonable Functions (PUFs) have been known for a long time. But deployment of PUFs in the IoT is challenging due to various reasons, one of them being power consumption. In the current poster presentation, low power designs of PUF modules are presented, which can be deployed in the Smart Things for a secure Internet of Things Environment. The input to a PUF is Challenge Input (in the form of a binary string) and the output is a Response (also a binary string). The Response will be used for encryption.

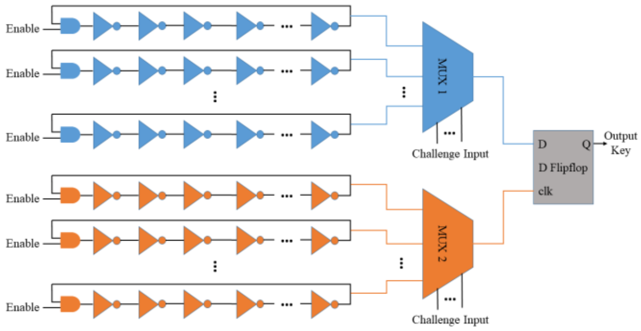

Fig 1. Inverter Based Hybrid Oscillator Arbiter PUF

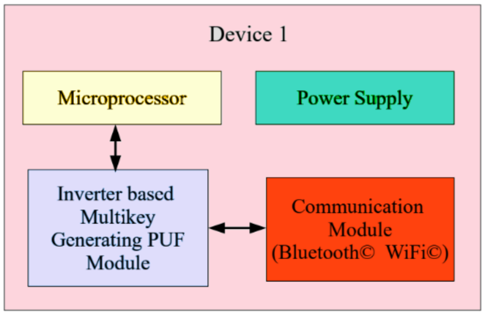
Device 1
Microprocessor
Power Supply
Inverter based Multikey Generating PUF Module
Communication Module (Bluetooth© WiFi©)

Fig 2. PUF Module Deployed in an IoT Device

When the PUF module is fabricated, variations will be introduced into the devices. Due to these manufacturing variations, no two devices in the module will give similar outputs. These variations will be extracted by the Physical Unclonable Function. The manufacturing variations are unique to a device, random and uncontrollable. So, the response generated by a PUF is also random and uncontrollable. This makes attacks much more difficult.

Figure 1 shows the design of a Physical Unclonable Function module. The multiplexer will select various ring oscillators based on the challenge input given and the oscillations generated will be sent to the D-Flipflop. Based on the signals at the D-input and the clock signal of the flipflop, the output response bit is generated. As the oscillations are different for different oscillators, the response bits will also be different. To generate an N-bit Response output, 2N oscillators are needed. Compared to other PUF designs, the power consumption of this design is significantly lower which is a great advantage when the PUF is being deployed in an IoT module. A key generated by a PUF module cannot be generated by another module. If the challenge input changes, the output response of the PUF will also change. Hence the the IoT environment can be made secure using Physical Unclonable Functions.