**ABSTRACT:**

We are going to see about PUF (Physical Unclonable Function) in this Thesis document which gives an answer to the security for Internet of Things (IoT). This concept involves having an Integrated Circuit(IC) that generates unique digital signatures on their own without the need for storing it EEPROM’s or SRAM’s. Since they derive a secret from the physical characteristics of the IC they play a wide role in security recently. We exploit this characteristic to use it as a Pay per Device Licensing for IP’s and to introduce a modified model of the existing Anderson’s PUF with robust design and better properties. Its application not only stops with this but can also be extended for validating payment systems, ensuring safe connectivity, authenticates sensors and protecting sensitive military data and systems. This novel approach not only has less overhead but also saves more than 70% of the cost which is being spent for buying expensive encryption IP’s like AES (Advanced Encryption Standard) or 3DES (triple data encryption standard). The current security methods introduce security vulnerabilities (e.g. Physical attacks and side channel attacks).

We are going to a see an improved model of Anderson’s PUF that can be used for IP Protection which is embedded in the circuit. This circuit is called as the Hardware Trojan which can be used for the evaluation of Hardware IP protection. This work is being tested by SASEBO-G2 Board where the Xilinx Virtex-5 65 nm FPGA is being used to demonstrate the results.