Unclonable key Generator Based on Chip signature and SRAM-PUF of ATmega328P chip

Embedded devices are now taking over the world, their presence in everyone’s pocket and home arouses questions around privacy and security concerns. What amplifies these concerns are the rapid spread of internet of things (IOT) devices and smart meters across the world. These devices become a target for attackers to compromise a device, or embed parasites on an authorized network. These kinds of attacks require an innovative method of authentication to protect unwanted parties from presence in an authorized network and its consequences from violating user’s privacy and other effects. This paper proposes a novel approach for using the ATmega328p microcontroller to generate an unclonable key based on the chip signature and manufacturing stored data as well as the static random access memory to act as a physically unclonable function (SRAM-PUF) of the Atmega328P chip. The generated key has been subjected to different statistical tests. A proof of concept model has been successfully built to test a suggested authentication scheme between two devices. It takes four steps, at the most, to accomplish the authentication process with a time of 90 ms for a key length of 256 bit