Competitive PUF architecture-based OTP solution for embedded system

As Internet-of-Things (IoT) devices are growing, security in embedded systems has become a critical issue. The levels of security for the system depend on applications. Some applications need a relatively high-security level and it is unnecessary to have high computational power, such as smart luggage tags, smart locks, etc. In the current market, MCU equipped with a security engine and large memory may lead to higher cost and complexity of the system design. In fact, the security algorithms themselves like AES are not actually safe that are public knowledge and predictable. The secure system also requires a hardware root-of-trust to enhance the security. Therefore, we propose a cost-competitive PUF architecture for a compacted embedded system.

What is Physical Unclonable Function (PUF)?

Physical Unclonable Function is a noisy function that can generate a unique output (response/digital fingerprint) from a given input (challenge). Typically, the properties of PUFs are unclonable, unpredictable and unduplicated. It can be used to generate challenge/response pairs.

There are many different types of PUFs, such as delayed-based PUFs, memory-based PUFs and coating PUFs. The mainstream is SRAM PUF which uses the manufacturing process variations and the random start-up patterns. The memory address is used as a challenge and the content of the corresponding memory address is the response. For enrollment, it needs a fuzzy extractor to generate a secret key and its helper data. The helper data can restore the secret key. A-China PUF is one of the PUF technology that use one-time programmable (OTP) memory to generate a “digital fingerprint” by using the silicon manufacturing process. This technology does not require the fuzzy extractor and is user-friendly.

How A-China PUF works

An A-China PUF Bit-cell consists of two MOS capacitors connected to a high voltage.

During the enrollment process, a high voltage is applied on both sides. Only one of the MOS capacitors is ruptured to generate ‘0’ or ‘1’ as the PUF value, and this process is random and guarantees the ID to be unique and unclonable.

How MCU equipped with A-China PUF generates CR pairs

MCU like MCU007 embedded PUF module and security engine together make the developers can use it easily. For example, the security engine in MCU007 includes DES, TDES and the company’s PUF algorithm and gets the PUF key through the internal circuit. After that, it uses the PUF key and an input challenge to generate the response. During the process, the PUF key is not disclosed and it guarantees the confidentiality of the PUF key.

Typical Applications

It can be widely used in anti-counterfeiting and unique identification. For example, a validation server enrolled an object’s CR pairs. Other clients use the application to check whether the object is listed on the validation server. If it is true, the object is genuine.

Author: Wilson Ho (IC design engineer @ A-China semiconductor Hong Kong)

Email: [Wilson.ho@achinasemicon.com](mailto:Wilson.ho@achinasemicon.com)

Date: 16/06/2022

 