ememory

Embedded Wisely, Embedded Widely

Secure IoT On-Chip Security Scheme Based on Silicon Fingerprint

WHITEPAPER

Introduction

A number of research reports have forecast that there will be tens of billions of IoT (Internet of Things) things in use worldwide by 2020. As the number of the IoT devices surges, security breaches are also on the rise. It is warned that most hackers today may use vulnerable IoT devices as starting points for attacks against other targets or even the entire system.

It came as no surprise that the latest survey by Economist Intelligence Unit (EIU) showed that global business leaders see “security” as a major obstacle to IoT implementation, only second to the cost concern [1]. A recent report by McKinsey also indicated that executives of the semiconductor industry view security as a major challenge to IoT growth [2]. However, the silver lining is that the semiconductor companies could actually help resolve the problem and add values to customers with well-designed security offerings.

This application note will first explore how PUF (Physical Unclonable Functions) – the digital biometrics of an IC – can be used to establish a hardware security scheme. This paper is also to show how eMemory’s NeoPUF technology can provide a highly reliable and secure PUF scheme to protect individual ICs and their embedded machines.

[1] The Internet of Things Business Index 2017: Transformation in motion, conducted by EIU, ARM and IBM. The survey showed 29% of 825 senior business leaders worldwide suggested that high cost of required investment as a main obstacle to IoT implementation, and 26% cited security and privacy as a major challenge.

[2] Internet of Things: Opportunities and Challenges for semiconductor companies 2016, by McKinsey&Co and Global Semiconductor Alliance(GSA).

In IoT applications, NeoPUF can be used as on-chip “fingerprint” to create an identifier for each device and prevent any cloning or counterfeiting. It can also be used for authentication and encryption to protect privacy and data security in communications between IoT endpoints, hubs, and clouds.

NeoPUF provides the kind of design-in flexibility for security solutions tailored to any points of IoT. Be it IoT machines that require the most stringent degree of security, or low-end devices that need simple protection, NeoPUF is able to enable security functions to meet varying needs.

PUF – Unique and Unclonable Silicon Fingerprint

Human fingerprint has long been used as a secure identifier for its “uniqueness”. In recent years, silicon PUF has also been well established as a hardware security primitive, providing ways to authentication, encryption, and secure key generation.

During IC manufacturing process, variability occurs and creates different physical microstructures. Those manufacturing variations cannot be fully controlled and re-fabricated intentionally, so the underlying physical properties are unique and become silicon fingerprints of individual ICs.

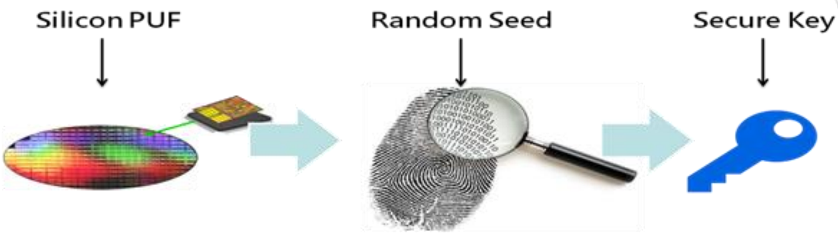

Figure 1: Extract Random Seed from Silicon PUF and use it to generate secure key.

Due to the physical disorder, when exposed to an external stimulus (challenge), the PUF will give a corresponding response that is unique in that context. That is, while the same challenge is applied, responses will vary among different ICs as a result of their physical differences.

The challenge-response mechanism can convert IC’s unique physical disorder into digital data, enrolled as random binary bits of “0” and “1”. The output can become a secure root of trust and be used to generate crypto keys in the field.

PUF is inherent from IC manufacturing process, and therefore can avoid tampering or cloning problems of externally-programmed security methods. It is not possible for hackers to reproduce the inherent properties of individual ICs, so the entropy source is immune to tampering or cloning. Most importantly, each IC has its own entropy source and there are no correlations among them. Any attacks will be isolated from one to another.

NeoPUF On-Chip Security Scheme – High Security, Low-Cost

eMemory’s NeoPUF is an embedded PUF technology which can provide multilayered protection. The technology is able to fix major problems of conventional PUF solutions such as high costs of complicated error correction codes (ECC).

In evaluating quality of PUF-based technologies, “reliability” and “security” are two major parameters. On reliability, a quality PUF scheme must be able to work consistently under all operating environments, unaffected by external factors such as temperature, voltage, and humidity.

When reliability becomes an issue, the results produced by PUF will be seriously corrupt and unsecure. Many PUF schemes require costly error correction measures to fix the stability issue, but the results so far are not so convincing.

One of key challenges to produce reliable PUF results is to make it as less noisy as possible. Physical measurements are typically noisy. In PUF's challenge-response mechanisms, the responses inevitably would come with noise, due to differences in temperature, voltage and other operating conditions.

It is a common problem with PUF schemes such as SRAM-based PUF. Whenever the SRAM switches from a power-off to power-on mode, patterns of PUF responses will be influenced by external factors and become unstable.

On the other hand, NeoPUF is able to fix the noise problem with its proprietary techniques. First, it uses a relatively stable PUF challenge-response scheme to reduce the degree of noise. Second, its sophisticated amplification and self-feedback mechanism is able to remove noise in such a way that PUF responses are consistently stable in all operating conditions. NeoPUF results have been tested reliable and robust under temperature between -40°C and +125°C (or higher).

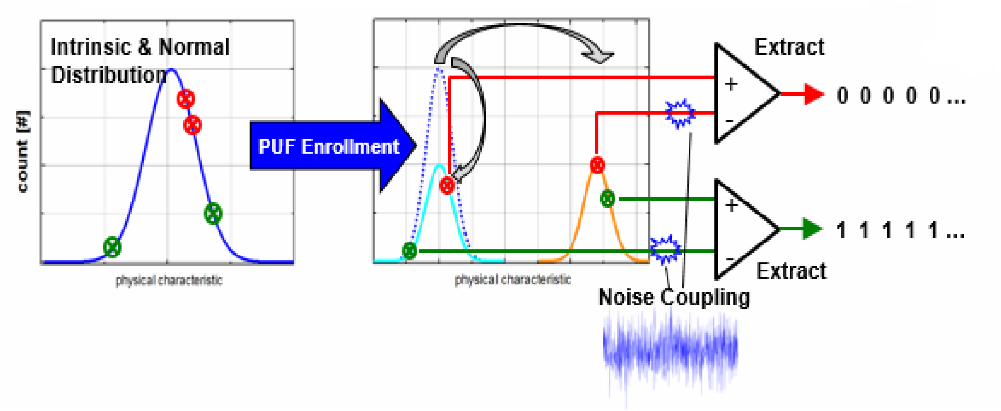

Figure 2: NeoPUF's innovative techniques are able to remove noise in converting physical disorder of an IC into digital values

The second parameter in evaluating a PUF technology is security, which is typically measured by randomness and disorder present in the PUF. The more random, the more secure. NeoPUF's challenge-response output is tested to be uniformly random, achieving a nearly 50-50 probability between "0" and "1".

In addition, NeoPUF is able to extract a highly scalable random seed of up to 1024 kbits. The extracted random bits are activated upon enrollment, and thanks to the large bits strings, users are provided the desired flexibility to choose their own key-generation approaches.

Available Foundries		TSMC/UMC		
Technology Node		55nm 0.9V/2.5V ULP		
Entropy Bits (Bit String)		256 Bits	512 Bits	1024 Bits
Bit Streams		256 IDs	128 IDs	64 IDs
Operating Temperature		-40°C~125°C		
Operating Voltage	VDD/VDD2	1.1V/2.5V		
Operation Modes		PUF Enrollment		
		Burst Response		
		Built-in Self Test		
Lifetime		>10 Years		

Table 1: NeoPUF Specs

Secure IoT with NeoPUF

Promising as it may be, the future of IoT has been faced with daunting challenges. Among them, security is frequently cited and hardware security is a particular focus of concern. This might have much to do with a series of attacks targeting IoT objects in recent years. The virtues of IoT - its ubiquity and omnipresence – may just well be the cause of its demise if the security issue is not addressed properly.

With numerous IoT objects exposed to threats, software alone is no longer adequate to protect the IoT system. Security coverage needs to extend down to hardware, and ultimately to the IC level. An embedded PUF-based scheme apparently can provide more fundamental and solid protection to the IoT objects than any security measures injected at later stages of supply chains.

When embedded with PUF-based security component, every chip bears its own unique “fingerprint” and can identify itself from others. Any IoT objects carrying the PUF identifier can be secured from the first point of hardware manufacturing process. The 2010 smart meter attack in Puerto Rico shows how vulnerable the IoT devices can be to tampering threats in the supply chain.

The meter tampering incident attracted worldwide attention on that the breach occurred at the OEM level and that the hackers were able to take control of the meter, an object that is virtually connected to every electricity-powered machines at our homes. The incident first alerted the world of the importance of embedded hardware security, and in the age of IoT, there are even more imminent threats of such attacks.

As shown in Figure 3, smart meters and other IoT objects can enable various security functions of identification, authentication, data encryption, and secure key generation, when embedded with NeoPUF.

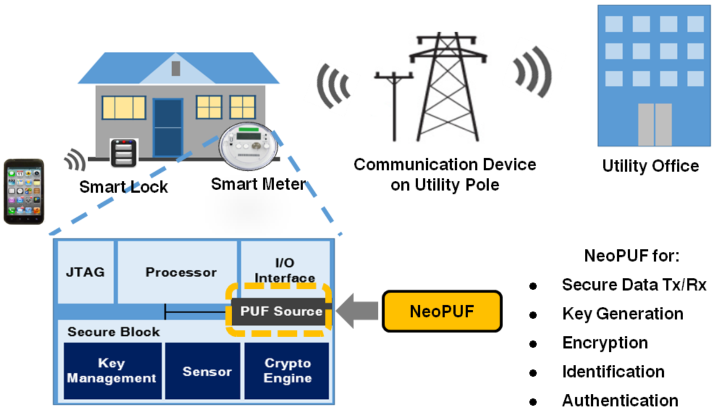

Figure 3: An embedded PUF scheme can enable various security functions, securing smart meters and other IoT objects.

The analogy to human fingerprint makes it easy to understand what silicon PUFs can do in authentication, encryption, etc. Wherever there is a need to verify a request is legitimate or not, the receiver can authenticate it via a NeoPUF-based scheme before issuing a corresponding response.

Imagine that you want to switch on your air conditioning before arriving home, and you use the device connected to your smart home system to send the request. The source of the request can be authenticated before the air conditioning being switched on.

Another use case of NeoPUF is: when a medical facility receives data transmitted from a patient's heart monitoring implants, it is able to find out if the monitoring device is tampered and to prevent against any fake data that could have endangered the patient's life. In the meantime, NeoPUF can also be used to encrypt the patient's medical data, so that only the authorized personnel can access it.

Simple as these concepts might be, the degree of protection the NeoPUF-based scheme can provide is anything but simple. Information centers of government and military facilities usually use PUF to provide most stringent security. The security level required by IoT applications should be no less, given the scale of connected things and how closely they are linked to one another.

Conclusion

The issue of IoT security has widely been discussed, and an embedded NeoPUF scheme derived from standard CMOS logic parts is so far the most comprehensive and cost-effective solution.

The nature of PUF makes it impossible for any hackers to tamper with the entropy source or produce fake identities, which is the most distinguishing feature of PUF-based schemes, comparing to external algorithm-based methods.

An embedded PUF can secure the chip and IoT objects from the first point of manufacturing process to their implementation and long-term operation. PUF's uniqueness also means one cannot possibly find any identical random seed among different chips and different IoT devices. Any incident of attack is absolutely isolated from another.

eMemory's NeoPUF IP is able to provide a reliable PUF scheme, bringing security to the chip level and significantly enhancing the effectiveness of an IoT security solution. As human biometrics is increasingly used in security areas, the digital biometrics of an IC is also to take off soon as a mainstream approach in the IoT security markets.

About eMemory

eMemory is a global leader in logic process embedded non-volatile memory (eNVM) silicon IP established in 2000. eMemory has devoted itself to research and development of innovative technologies, offering the industry’s most comprehensive platforms of patented eNVM IP solutions which are supplied to semiconductor foundries, integrated devices manufacturers (IDMs), and fabless design houses worldwide. eMemory’s eNVM silicon IPs support a wide range of applications, including trimming, function selection, code storage, parameter setting, encryption, and identification setting. The company has the world’s largest NVM engineering team and prides itself on providing partners with a full-service solution that sees the integration of eMemory eNVM IP from initial design stages through fabrication.

eMemory Technology Inc.
8F, No.5, Tai-Yuan 1st St., Jhubei City, Hsinchu County 30265 Taiwan
T +886-3-5601168 F +886-3-5601169
www.ememory.com.tw