IoT technology is an essential landmark for smart cities, manufacturing, and phone usage growth. This is very exciting as I look around at the IoT’s enormous capability. Without human or computer supervision, data exchanges occur between unique multiple IoT objects. IoT combines disparate technologies such as wireless communication, micro-electromechanical systems (MEMS), and sensor technologies to exchange critical system information. It also appears in manufacturing, energy management, medical and health systems, transportation, and building and home automation.

These are exciting times, but this overexuberance in the IoT market begs for a second look. Particularly, you will find that as you design or use these systems, you need a high degree of security. In other words, unknown or known sources can have access to your data or contribute to your data without your knowledge, and under the worst conditions, contaminate your systems. As an example, a spoofing attack is a source that masquerades as a trusted source and falsifies data. Unless you protect or lock your system from the outside, the best of the bad actors will successfully break into your system undetected and make it too late for you to recover.

Figure 1 Dedicated, hardware-based security ICs and the cryptographic solutions address security threats.
Dedicated, hardware-based security ICs and the cryptographic solutions currently exist to address these threats. However, the security ICs themselves can become the target of attack by the bad actors attempting to circumvent or break chip security to gain access of the protected system.

**Physically unclonable functions**

A decisive technology that protects security chips against invasive attacks is the physically unclonable function (PUF). PUF is a digital fingerprint that is unique to each IC with an output value that cannot be reverse-engineered. The PUF-generated value differs physically from chip to chip due to manufacturing variations. Inside an integrated PUF core, it is possible to generate a completely random code. The key length is scalable, being in line with the application’s requirements. The probing of a PUF circuit modifies the electrical properties. This probing then renders the PUF core useless. In this manner, the hardware-generated PUF output is tamper-proof. The PUF output is used as a unique key/secret to support cryptographic algorithms and services that include encryption/decryption, authentication, and digital signature.

An example PUF implementation operates on the naturally occurring random variation and mismatch of the analog characteristics of MOSFET device structures (Figure 2).

![Figure 2](image)

**Figure 2** The PUF core generates a repeatable cryptographic key from the random analog characteristics of the integrated circuit’s transistors.

**Authenticating with PUF**

**Figure 3** provides examples of how PUF could be used in a security IC. In one case, the PUF output becomes a secret that is used to encrypt. As shown with the advanced encryption standard (AES), all data is stored either internally or externally to the IC. Should a bad actor be successful in getting at this data, given the encrypted state it is useless. In another case, the PUF output becomes the private key component of a public-private key pair for signing data using the elliptic-curve digital signature algorithm (ECDSA). See the Maxim Integrated article entitled *The Fundamentals of an*
Secure authenticators are a class of security ICs which are used to protect the system from the attacks mentioned earlier. Integrating PUF into these devices makes sense given the value of the system assets to be protected. An example of a PUF-protected secure authenticator is the DS28E38 (Maxim Integrated).

**PUF - now you are protected**

I am finding that HW-based security ICs are a proven solution to protect your valuable application assets from theft, snooping, counterfeiting, etc. PUF technology protects the security chip itself against invasive types of attack threats. PUF technology, based on the random electrical properties of IC devices, produces a unique and repeatable root cryptographic key for each IC. As a result, no two PUF coding are the same. Additionally, the generation of a key happens when needed, and the chip never stores this valuable key. This removes any chance of future cyber-attacks. Reliability of your silicon is a tall order. It is critical that the PUF function be reliable over voltage, temperature, time, process, and age.

*Bonnie Baker* has been working with analog and digital designs and systems for more than 30 years and is writing this blog on behalf of Maxim Integrated.
- IoT security: hardware vs software
- IoT & cloud security overview
- The right and wrong way to implement cryptographic algorithms in embedded electronic systems
- Cryptography in software or hardware: It depends on the need
- Cryptography and network security—The basics