Next-gen ICs will deliver a stronger level of protection

SECURITY

In a world where embedded electronic systems continue to come under attack, cryptography provides flexible and effective tools to address a myriad of potential security threats. Scott Jones, Maxim Integrated Micros, Security & Software Business Unit, explains:

Accordingly, a variety of options exist to implement crypto solutions with both hardware and software approaches. Given the dedicated and optimised implementations, it is understood that a hardware-based solution, i.e. a dedicated security IC, is the most effective formulation for the root of trust and the way to provide the countermeasures and protection that prevent numerous types of common attacks.

The reality is that there are valuable assets associated with embedded systems that face relentless threats. For example, such systems encounter intrusions such as theft of intellectual property, introduction of malware to disrupt or destroy equipment, unauthorised access to sensitive communication, tampering with data produced from IoT endpoints, etc. Security ICs and the cryptographic solutions available currently exist to address these threats. However, the security ICs themselves become the target of attack by an adversary attempting to circumvent or break the security.

ATTACKS ON SECURITY ICs

With an assumption of a security IC-based protection solution, there are two general categories of attack scenarios: non-invasive and invasive. Non-invasive attacks consist of operational measurements, sometimes combined with other externally applied stimuli, in an effort to obtain cryptographic keys or other sensitive data. Examples of such efforts include differential or simple power/electromagnetic analysis (DPA/SPA/DEMA/SEMA) or the inducing of fault states through voltage glitching.

Invasive attacks on a security IC consist of direct die-level circuit probing, modification, depackaging and reverse engineering, again with the objective of compromising the solution by obtaining keys, disabling functionality or completely reverse engineering the design to a netlist for reproduction. The skill set and required tools are more complex than in the non-invasive scenarios, but they do exist and are commonly used to attack the security ICs that protect high value assets.

For example, Figure 1 and Figure 2 are examples of the output from tools that may be used with an invasive attack to first image a portion of an IC and then extract the netlist and schematics from the imaging. An attacker would repeat this process for the entire IC with the ultimate goal of gaining some insight to launch a sub-circuit attack, or producing a database to replicate the IC.

Like in the non-invasive situation, there are circuit solutions available to combat invasive attacks. One example consists of top level die shields that are actively monitored for a tamper event and combined with detection circuitry that takes defensive counteraction. However, the skills and equipment of attackers employing invasive techniques evolve and have historically been a challenge to decisively defeat.

PUF – DECISIVE INVASIVE ATTACK COUNTERMEASURE

A decisive technology that has emerged to provide strong protection against the invasive threat is the physically unclonable function (PUF). PUF is a function that is derived from the complex and variable physical/electrical properties of ICs.

Because PUF is dependent on random physical factors (unpredictable and uncontrollable) that exist natively and/or are incidentally introduced during a manufacturing process, it is virtually impossible to duplicate or clone. PUF technology natively generates a digital fingerprint for its associated security IC, which can be utilized as a unique key/secret to support cryptographic algorithms and services including encryption/decryption, authentication and digital signature.

A PUF implementation from Maxim Integrated operates on the naturally occurring random variation and mismatch of the analogue characteristics of fundamental semiconductor MOSFET devices. This randomness originates from factors such as oxide variation, device-to-device mismatch in threshold voltage, and interconnect impedances. Similarly, the wafer manufacturing process introduces randomness through imperfect or non-uniform deposition and etching steps. Paradoxically, semiconductor device parameter variation is normally a challenge...
Next-gen ICs will deliver a stronger level of protection

In a world where embedded electronic systems continue to come under attack, cryptography provides flexible and effective tools to address a myriad of potential security threats. Scott Jones, Maxim Integrated Micros, Security & Software Business Unit, explains:

Accordingly, a variety of options exist to implement crypto solutions with both hardware and software approaches. Given the dedicated and optimised implementations, it is understood that a hardware-based solution, i.e., a dedicated security IC, is the most effective formulation for the root of trust and the way to provide the countermeasures and protection that prevent numerous types of common attacks.

The reality is that there are valuable assets associated with embedded systems that face relentless threats. For example, such systems encounter intrusions such as theft of intellectual property, introduction of malware to disrupt or destroy equipment, unauthorized access to sensitive communication, tampering with data produced from IoT endpoints, etc. Security ICs and the cryptographic solutions available currently exist to address these threats. However, the security ICs themselves can become the target of attack by an adversary attempting to circumvent or break the security.

ATTACKS ON SECURITY ICs

With an assumption of a security IC-based protection solution, there are two general categories of attack scenarios: non-invasive and invasive. Non-invasive attacks consist of operational measurements, sometimes combined with other externally applied stimuli, in an effort to obtain cryptographic keys or other sensitive data. Examples of such efforts include differential or simple power/electromagnetic analysis (DPA/SPA/DEM/SEMA) or the inducing of fault states through voltage glitching.

Invasive attacks on a security IC consist of direct die-level circuit probing, modification, deprocessing and reverse engineering, again with the objective of compromising the solution by obtaining keys, disabling functionality or completely reverse engineering the design to a netlist for reproduction. The skill set and required tools are more complex than in the non-invasive scenarios, but they do exist and are commonly used to attack the security ICs that protect high value assets.

For example, Figure 1 and Figure 2 are examples of the output from tools that may be used with an invasive attack to first image a portion of an IC and then extract the netlist and schematics from the imaging. An attacker would repeat this process for the entire IC with the ultimate goal of gaining some insight to launch a sub-circuit attack, or producing a database to replicate the IC.

Like in the non-invasive situation, there are circuit solutions available to combat invasive attacks. One example consists of top level die shields that are actively monitored for a tamper event and combined with detection circuitry that takes defensive counteraction. However, the skills and equipment of attackers employing invasive techniques quickly evolve and have historically been a challenge to decisively defeat.

PUF – DECISIVE INVASIVE ATTACK COUNTERMEASURE

A decisive technology that has emerged to provide strong protection against the invasive threat is the physically unclonable function (PUF). PUF is a function that is derived from the complex and variable physical/electrical properties of ICs.

Because PUF is dependent on random physical factors (unpredictable and uncontrollable) that exist natively and/or are incidentally introduced during a manufacturing process, it is virtually impossible to duplicate or clone. PUF technology natively generates a digital fingerprint for its associated security IC, which can be utilised as a unique key/secret to support cryptographic algorithms and services including encryption/decryption, authentication and digital signature.

A PUF implementation from Maxim Integrated operates on the naturally occurring random variation and mismatch of the analogue characteristics of fundamental semiconductor MOSFET devices. This randomness originates from factors such as oxide variation, device-to-device mismatch in threshold voltage, and interconnect impedances. Similarly, the wafer manufacturing process introduces randomness through imperfect or non-uniform deposition and etching steps. Paradoxically, semiconductor device parameter variation is normally a challenge
that IC designers face during development. In contrast, it is the fundamental basis and exploited for Maxim's PUF design.

Figure 3 provides a simplified block diagram of the Maxim PUF architecture showing an example key size of 128-bits. Shown within the PUF core block is a 16x16 array of 256 PUF elements each of which is an analogue structure. Through factory conditioning these 256 elements are combined into 128 pairs. Comparing structure to structure, random I/V characteristics due to the previously described parameters exist and are utilized to generate binary 1/0 values through precision circuit level comparison of each element within a pair. For example, elements {2, 1} and {14, 16} could constitute a pair, and their characteristics would be compared to derive a bit value. This is repeated with each of the 128 pairs to produce a 128-bit PUF key output (for this key size example).

From an invasive attack perspective, any probing or attempted analogue measurement of a PUF element causes the analogue electrical characteristic to change due to factors including capacitive/inductive/resistive loading. As a result, it is not possible to extract any key data through invasive measurements.

Also, due to the statistical nature of imperfect manufacturing techniques, there is a known method to discern any key information from inspection methods. Similarly, even knowledge of PUF element pairing does not reveal any information about the key value that would ultimately be derived from the analogue characteristics of the PUF element structures. Finally, the PUF key value only exists digitally when a cryptographic operation is performed - thereafter, it is instantaneously erased. Combined, these attributes of this PUF design result in a solution that is highly immune to invasive attacks.

PUF RELIABILITY AND CRYPTO QUALITY

From a cryptographic perspective, reliability and randomness are critical characteristics that a PUF solution must exhibit. For use as a cryptographic key, or root thereof.

The PUF output must have 100% reliability, meaning PUF-derived key bit values must be repeatable over time and all operating conditions. For semiconductor devices, this evaluation is performed using JEDEC defined industry standard methods of reliability study.

This includes selecting and subjecting a statistically significant sample set of devices to environmental and operational stress conditions that enable evaluation of lifetime reliability performance. These stresses include high temperature operating life (HOTL), temperature cycling, packaging and solder reflow influences, voltage and temperature drift, and highly accelerated temperature/humidity stress testing (HAST). Performing a reliability qualification study using these proven methods results in a statistical assessment of how a design will perform over the life of the use in a system. For example, consider a system end product could have a design life of ten years and operates within -40°C to +85°C environments with power sources that can fluctuate by ±10%.

Equally critical with a PUF solution is the requirement for high performance cryptographic quality, with a key property being randomness. Low quality randomness can create a cryptographic attack vulnerability through predictability weaknesses. Statistical test suites, including NIST SP 800-22, provide an industry proven means to measure randomness of PUF output. Evaluation against the test suite provides several metrics which determine whether the PUF output is consistent with a random sequence. To be statistically significant, these tools require large data sets for the analysis, e.g., 20kbit sequences. Therefore, the output from a large set of PUF instances is required and used for the assessment.

RELIABILITY STUDIES ON PUF

The reliability of Maxim's PUF was proven from results obtained via a lifetime reliability analysis as described previously. Fundamentally, the reliability study produced data to understand the shift from aging, temperature/voltage drift, IC packaging, PCB assembly, etc. of the PUF elements.

Relative to the time-zero characteristics of two PUF paired elements, the post-reliability study paired elements have been shown to consume around seven percent of the total margin available to maintain the stability of the output binary value. The final output from the analysis is a PUF key error rate (KER) of ≤1ppm, where KER is defined as the probability that 1-bit within the total key size produced by the PUF, e.g., 256-bit, would flip over the life of the product.

A randomness assessment of the PUF relied on performance to NIST standard SP 800-22 monobit, poker, runs test and long run test. These are test suites that evaluate whether output data is consistent with a random sequence. Assessment results for each of the four tests validate excellent performance with respect to randomness. 

Above: Figure 4. Encrypting IC NVM with the PUF secret key

Below: Figure 5. ECDSA signing with PUF as the private key
that IC designers face during development. In contrast, it is the fundamental basis and exploited for Maxim’s PUF design.

Figure 3 provides a simplified block diagram of the Maxim PUF architecture showing an example key size of 128-bits. Shown within the PUF core block is a 16x16 array of 256 PUF elements each of which is an analogue structure. Through factory conditioning these 256 elements are combined into 128 pairs. Comparing structure to structure, random I/V characteristics due to the previously described parameters, exist and are utilised to generate binary I/O values through precision circuit level comparison of each element within a pair. For example, elements [2, 1] and [14, 16] could constitute a pair, and I/V characteristics of each would be compared to derive a bit value. This is repeated with each of the 128 pairs to produce a 128-bit PUF key output (for this key size example).

From an invasive attack perspective, any probing or attempted analogue measurement of a PUF element causes the analogue electrical characteristic to change due to factors including capacitive/inductive/resistive loading. As a result, it is not possible to extract any key data through invasive measurements.

Also, due to the statistical nature of imperfect manufacturing techniques, there is no known method to discern any key information from inspection methods. Similarly, even knowledge of PUF element pairs does not reveal any information about the key value that would ultimately be derived from the analogue characteristics of the PUF element structures. Finally, the PUF key value only exists digitally when a cryptographic operation is performed thereafter, it is instantaneously erased. Combined, these attributes of this PUF design result in a solution that is highly immune to invasive attacks.

**PUF RELIABILITY AND CRYPTO QUALITY**

From a cryptographic perspective, reliability and randomness are critical characteristics that a PUF solution must exhibit. For use as a cryptographic key, or root thereof, the PUF output must have 100% reliability, meaning PUF-derived key bit values must be repeatable over time and all operating conditions. For semiconductor devices, this evaluation is performed using JEDC defined industry proven methods of reliability study. This includes selecting and subjecting a statistically significant sample set of devices to environmental and operational stress conditions that enable evaluation of lifetime reliability performance. These stresses include high temperature operating life (HTOL), temperature cycling, packaging and solder reflow influences, voltage and temperature drift, and highly accelerated temperature/humidity stress testing (HAST). Performing a reliability qualification study using these proven methods results in a statistical assessment of how a design will perform over the life of its use in a system. For example, consider that a system end product could have a design life of 10 years and operates within -40°C to +85°C environments with power sources that can fluctuate by ±10%.

Equally critical with a PUF solution is the requirement for high performance cryptographic quality, with a key property being randomness. Low quality randomness can create a cryptographic attack vulnerability through predictability weakness. Statistical test suites, including NIST SP 800-22, provide an industry proven means to measure randomness of PUF output. Evaluation against the test suite provides several metrics which determine whether the PUF output is consistent with a random sequence. To be statistically significant, these tools require large data sets for the analysis, e.g., 200 bit sequences. Therefore, the output from a large set of PUF instances is required and used for the assessment.

**RELIABILITY STUDIES ON PUF**

The reliability of Maxim’s PUF was proven from results obtained via a lifetime reliability analysis as described previously. Fundamentally, the reliability study produced data to understand the shift from ageing, temperature/voltage drift, IC packaging, PCB assembly, etc. of the PUF elements. Relative to the time-zero characteristics of two PUF paired elements, the post-reliability study paired elements have been shown to consume around seven percent of the total margin available to maintain the stability of the output binary value. The final output from the analysis is a PUF key error rate (KER) of ≤5ppm, where KER is defined as the probability that 1-bit within the total key size produced by the PUF, e.g., 256-bit, would flip over the life of the product.

A randomness assessment of the PUF relied on performance to NIST standard SP 800-22 monobit, poker, runs test and long run test. These are test suites that evaluate whether output data is consistent with a random sequence. Assessment results for each of the four tests validate excellent performance with respect to randomness.
To evaluate immunity to invasive attack and reverse engineering, the Maxim PUF solution was evaluated by a leading US-based company that specialises in die level security assessments and IC reverse engineering expertise. With the given assessment time frame, there was no compromise of PUF operation, along with a qualitative conclusion that the solution is ‘highly effective and resistant against physical reverse engineering attacks’.

**PUF USE CASES**
Numerous use cases exist for a PUF solution. Three are shown in Figure 4, Figure 5 and Figure 6. In Figure 4, to secure all stored data on a security IC, the PUF derived key is used to encrypt/decrypt data as needed using an algorithm such as AES. Any NVM data extracted from an invasive attack is useless given its encrypted state and inability to obtain the PUF-based decryption key. Figure 6 shows the use of PUF as the unique private key for ECDSA signing operations. For this case the device would compute its own public key from the PUF private key, and a certificate would be installed in NVM by a certificate authority prior to end-use deployment. In Figure 6, the PUF private key is the root private key for the security IC and is used in conjunction with the end system to establish a ‘root of trust’ with the security IC for subsequent services.

**MAXIM’S COMMERCIAL PUF-BASED SECURITY IC**
Maxim introduced its first PUF-based security IC, the DS28E38, in November 2017. The DS28E38 is an ECDSA authenticator that utilises the company’s ChipDNA PUF output as key content to cryptographically secure all device stored data. Optionally, under user control, ChipDNA is used as the private key for ECDSA signing operations. The device provides a core set of cryptographic tools derived from integrated blocks including asymmetric (EC2-P256) and symmetric (SHA-256) hardware engines, a FIPS/NIST-compliant true random number generator (TRNG), 2Kb of secure EEPROM, a decrement-only counter, and a unique 64-bit ROM identification number (ROM ID). The ECC public/private key capabilities operate from the NIST-defined P-256 curve to provide a FIPS-186-compliant ECDSA signature generation function. A block diagram of the DS28E38 is shown in Figure 7.

**SUMMARY**
Embedded systems have electronic assets that can be protected by cryptography. Security ICs with cryptographic functions provide optimal protection, but, ultimately, become the attack point by those attempting to compromise the assets. Furthermore, attackers are becoming increasingly sophisticated in their techniques. A decisive countermeasure to the invasive attack is the PUF, which, due to its inherent qualities, can be highly immune to reverse engineering methods.
DESIGN

1-Wire INFC & CMD

64-BIT ROM ID

BUFFER

RNG

User Memory,
ECDSA Public Key,
Certificate

ECDSA
P256

ChipDNA - PUF

Private Key

Maxim’s Commercial PUF-based Security IC

Maxim introduced its first PUF-based security IC, the DS28E38, in November 2017. The DS28E38 is an ECDSA authenticator that utilizes the company’s ChipDNA PUF output as key content to cryptographically secure all device stored data. Optionally, under user control, ChipDNA is used as the private key for ECDSA signing operations. The device provides a core set of cryptographic tools derived from integrated blocks, including asymmetric (ECC-P256) and symmetric (SHA-256) hardware engines; a FIPS/NIST-compliant true random number generator (TRNG), 2Kb of secured EEPROM, a decrement-only counter, and a unique 64-bit ROM identification number (ROM ID). The ECC public/private key capabilities operate from the NIST-defined P-256 curve to provide a FIPS 186-compliant ECDSA signature generation function. A block diagram of the DS28E38 is shown in Figure 7.

SUMMARY

Embedded systems have electronic assets that can be protected by cryptography. Security ICs with cryptographic functions provide optimal protection, but, ultimately, become the attack point by those attempting to compromise the assets. Furthermore, attackers are becoming increasingly sophisticated in their techniques. A decisive countermeasure to the invasive attack is the PUF, which, due to its inherent qualities, can be highly immune to reverse engineering methods.