Cloning the *UNCLONABLE*

By Marcus Janke and Dr. Peter Laackmann, Infineon Technologies AG

Uniqueness, in many forms, has been used for the purpose of security since thousands of years: From seals impressed on clay tablets, the unique distribution of fluorescent fibers in banknote paper, to the scattering of laser light on randomly manufactured surfaces on protected documents, uniqueness created authenticity. In the world of semiconductors, uniqueness also served as a task for engineers since decades, as it is a value which can be used for generating secrecy and authenticity.

One of its subgrups causes some upset, given the name 'Physical Unclonable Functions', or PUF. 'Unclonable', of course, is a teasing word for security experts who know that nothing is uncloneable by nature, like nothing is one hundred percent secure. Nevertheless, the term yields a good occasion to venture a glimpse into these technologies, in order to separate opportunities from tripwires.

Creating uniqueness

Uniqueness is usually created by processes containing randomness – which, in nature, is always available in abundance. The well-known unique fingerprint of each human often serves as a prominent example. But 'fingerprints' can also be taken from objects. Paper manufacturers know that the orientation of a single cotton or wood fibre in a piece of business paper cannot be predicted, but will be fixed after manufacture. Diving into the microscopic or nanoscale world, uniqueness is even more a factor, also including silicon chips. Single elements of a chip, like transistors, may differ from each other. As a consequence, each chip differs from each other. Usually, these small deviations are so minor that they are not significant for the proper function of a chip design. Nevertheless, through amplification, the differences can be measured, and even used in a chip to create unique data, keys or a unique algorithm.

'Strong' unique functions

The original ideas of using a chip's individual uniqueness as a source for secrets were born and implemented decades ago as so-called 'hardware watermark' procedures. Input data was pushed into an electronic circuit which, chip-individually, would produce different output values with low, or even no, predictability, like a secret algorithm unique for each chip. This concept would be called the 'strong' variant today, as no key or algorithm is directly stored on the chip, and also no key is directly processed in the chip. In older times, when keys were stored in the chip's memories, at first sight, such concepts seemed very promising.

Unfortunately, the characteristics of the chip-individual deviations, as they are very small, also came with severe disadvantages: The electrical differences are also heavily influenced by the environmental parameters (e.g. temperature, voltage, light, radiation and many others) and are subject to chip aging, resulting in strong reliability hazards – in other words, the designer could chose between security and reliability. To overcome these weaknesses, another variant of unique functions was created, the 'weak' but more robust version.

'Weak' unique functions

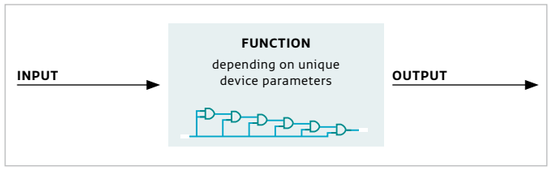

Figure 1: 'Strong' unique function

As the information, which is generated by one unique element, would be prone to environmental changes, solutions were needed. The simplest solution was to use redundancy: If, due to aging, information could get lost, simply more information was used as a 'backup'. Typical systems therefore collected the information from many unique elements and joined it together to form a more robust data set. Even if some of the unique elements would switch their behaviour, the result would stay constant. Being a nice solution at first sight, such 'robust' unique functions showed a totally different behaviour in terms of security. For the sake of robustness, security

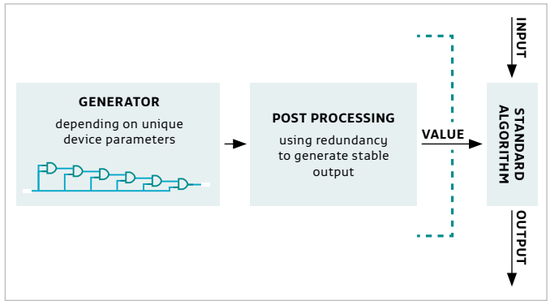

Figure 2: 'Weak' unique function

has to pay a heavy price: Now, the secrets are used and processed in the chip, and they are present. The original idea of unique functions suffers significantly, and therefore such variants are also called 'weak' unique functions today.

Physical 'Unclonable' Functions do not provide a security feature by themselves. Instead, they provide an extra functionality. This in turn means that extra doors for potential attackers may be added by the implementation.

If the secrets, which are used in digital form in the chip, would be extracted, subsequent cloning of the chip would be possible again by simple emulation. Extraction could be done, in turn, especially by probing attacks, but also observing and semi-invasive attacks must be taken into account. Therefore, as mentioned, the word 'unclonable' can be vastly misleading. Nevertheless, even 'weak' functions can be used for applications like the ones that are based on logic chips as a source of individual secret keys. For example, even a pure logic chip, like used in automotive or RFID, can be enabled to utilize chip individual encryption or other purposes now.

Attacks

Physical 'Unclonable' Functions do not provide a security feature by themselves. Instead, they provide an extra functionality. This in turn means that extra doors for potential attackers may be added by the implementation.

There are few functions that attracted such a vast dimension of potential attack vectors than the 'Physical Unclonable Functions'. In the last few years, dozens of new attack scenarios have been developed to overcome these functions. Today's existing attacks were derived from all three major attack groups (manipulating, observing and semi-invasive attacks). Also, logical/mathematical approaches were developed to break the underlying mechanisms. All these methodologies are called 'PUF-specific attacks'.

At first sight, a layman would think that Fault Attacks would rather turn the implementation unusable – which would be not more than a denial-of-service approach. But an intelligent attacker could do much more than this: By influencing the PUF related error-correction logic, data dependent leakage of secrets could be induced through a newly generated additional side channel. Also, fault attacks against so-called 'helper data', which is used by some PUF implementations, are known, and must be considered. First countermeasures have been developed since these attacks are known. If the PUF is directly used for cryptography on the chip, it should be also considered that an attacker would try to induce the use of a weak key that in a second step could be easy to break by conventional methods. Fault attack methods may include the use of radiation (alpha radiation, laser or electromagnetic localized impulses for temporary influence, X-rays, beta rays, UV irradiation, temperature exposure or gas diffusion to induce permanent changes).

The Side-Channel Attacks, which are well known in the form of SPA/DPA (Simple/Differential Power Analysis), take a full revival in the area of Physical 'Unclonable' Functions. Practically every electronic circuit's behaviour depends on the data processed therein. Through observation of the chip's power consumption, its electromagnetic emanation, local optical emission or laser voltage probing, an attacker can try to spy out confidential data. Techniques like Time-Resolved Emission analysis (TRE) and the use of infrared emission analysers with Solid state Immersion Lenses (SIL) allow the use also on modern, very small chip technologies. One would first suggest that side channel attacks, therefore, could be mainly applied to the error correction processes or extractor functions that are typically used in a PUF implementation. Nevertheless, meanwhile several experts demonstrated publicly that side channel attacks also could be used as an effective weapon against the PUF 'heart', the origin of the characteristic data, itself.

An intelligent attacker could do much more than this: By influencing the PUF related error-correction logic, data dependent leakage of secrets could be induced through a newly generated additional side channel.

Even the Physical Attacks, like probing or forcing signals with small needles placed on the chip, Atomic Force Microscopy (AFM) or Focused Ion Beam manipulations (FIB), may still be used effectively. One of the most interesting targets by using physical attacks is to induce the attacker's own data into the key generation, so that decryption of the complete chip content would be easy in a second step. Furthermore, many implementation options of PUF could make the error correction and extraction circuits a very interesting target for snooping data.

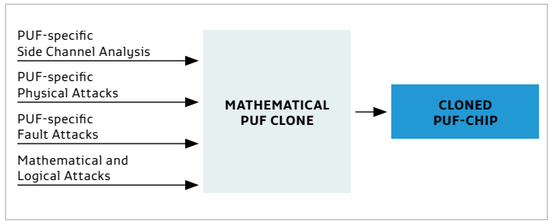

Figure 3: How to Clone the 'Unclonable'

Besides the typical three attack groups against hardware, the implementation of a PUF may allow the use of Mathematical Attacks as a backdoor to its secrets. To understand this threat, it is important to realize the difference between physical and mathematical clonability of a PUF. This means that even if it would be hard to clone the exact physical characteristics of a specific circuit, the chip itself could easily be cloned, as it usually does not matter at all to the outside world, how the PUF data is generated inside. If the reaction of a PUF circuit to an unknown input would be predictable, the attacker could implement his own solution to generate such data, and produce cloned chips. Unfortunately, typical PUF are NOT mathematically unclonable, so that a high risk may emerge:

Today, in the area of PUF, the so-called 'modelling attacks' were most prominent up until now. For a modelling attack, input and output data is first collected and then mathematically analysed. From that analysis, a computer model is generated that can give a prognosis for the PUF behaviour to an unknown input data. Today, every private person has access to large amounts of computing power, so that modelling attacks using machine learning, using for example 'logistic regression' techniques, could serve as a very dangerous tool. Countermeasures, like trying to prevent direct access to the PUF input and raw output, could succumb to a combination of the mathematical attacks with a physical attacks or side-channel analysis.

One of the most frightening aspects would be a potential misuse of PUF technologies for granting Hardware Trojan Backdoor Access to a security chip. In this case, the PUF function would be integrated into a chip to serve an additional purpose – an intended, dangerous security backdoor that could be very hard to detect. First publications covering this topic already appeared in the public, raising concerns in the light of globally distributed chip manufacture.

Conclusion and outlook

Unique functions for the generation of on-chip secret keys and individual algorithms have been researched for decades now. Especially in the last years, increased research has been applied to silicon-implemented logical circuits that would use the chip's individual characteristics to generate individual keys. Today, devices that by technological restrictions do not allow to use certified true random number generation, nor secure key derivation, could first benefit from PUF implementations. Pure logic circuits, for example, can be equipped with unique coding, or even combined in a system together with security microcontrollers.

Idea and implementation, on the other hand, are different parts. While allowing new functionalities for good reasons, carelessness, on the other hand, may open new doors for attackers. For a new PUF implementation, at least the relevant attacks known today should be carefully investigated for a proper security evaluation. Equipment for PUF-specific attacks should be at hand while developing appropriate attack countermeasures. Unique functions may serve as a source of security – if they, themselves, are properly protected against various attacks from amateurs to professionals. Although there seems to be a consensus that even today's technologies allow a reasonable use in selected applications, experts call for quantum-physics PUFs to achieve enough security, and strongly demand to invent new PUF construction principles. ☒

One of the most frightening aspects would be a potential misuse of PUF technologies for granting Hardware Trojan Backdoor Access to a security chip.

Literature

F. Armknecht, R. Maes, A-R. Sadeghi, F-X. Standaert, C. Wachsmann, "A Formal Foundation for the Security of Physical Functions", 32nd IEEE Symposium on Security and Privacy, 2011.

D. Schuster, "Side Channel Analysis of Physical Unclonable Functions (PUFs)", Diploma Thesis, Technische Universität München, 2010.

D. Merli, D. Schuster, F. Stumpf, G. Sigl, "Semi-Invasive EM Attack on FPGA RO PUFs and Countermeasures", Proceedings WESS2011 Workshop on Embedded System Security, ACM, New York 2011.

D. Merli, D. Schuster, F. Stumpf, G. Sigl, "Side Channel Analysis of PUFs and Fuzzy Extractors", Proceedings TRUST International Conference on Trust and Trustworthy Computing – Pittsburgh 2011, LNCS 6740, Springer 2011.

D. Karakoyunlu, "Differential Template Attacks on PUF Enabled Cryptographic Devices", Proceedings IEEE WIFS International Workshop on Information Forensics and Security 2010.

U. Rührmair, C. Jaeger, M. Algasinger, "An Attack on PUF-Based Session Key Exchange and a Hardware-Based Countermeasure", LNCS 7035, 2012, 190–204.

R. Plaga, F. Koob, "A Formal Definition and a New Security Mechanism of Physical Unclonable Functions", Federal Office for Information Security, Germany, 2012.

U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber "Modeling Attacks on Physical Unclonable Functions", Proceedings CCS2010, 17th ACM Conference on Computer and Communications Security, ACM New York 2010, 237-249.

J. Sölter, "Cryptanalysis of Electrical PUFs via Machine Learning Algorithms", MSc Thesis, Technische Universität München 2009.

Z. Gog, M. X. Makkes, "Hardware Trojan Side-Channels Based on Physical Unclonable Functions", in Proceedings WISTP 2011, LNCS 6633, 2011, 294-303.