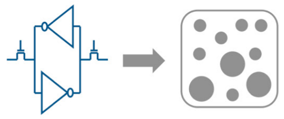
AUTHENTiCO
TECHNOLOGIES

SRAM PUF

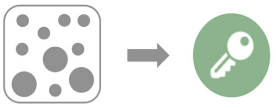
KEYS FROM SILICON CHARACTERISTICS

SRAM Physical Unclonable Functions or PUF use the behavior of standard SRAM memory, available in any digital chip, to differentiate chips from each other. They are virtually impossible to duplicate, clone or predict. This makes them very suitable for applications such as secure key generation and storage, device authentication, flexible key provisioning and secure user authentication. Due to deep sub-micron process variations in the production process, every transistor in SRAM cells has slightly random electric properties. This randomness is expressed in the startup values of 'uninitialized' SRAM memory. These values form a unique chip fingerprint, called the SRAM PUF response.

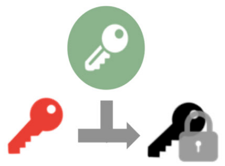
Uncontrollable nano-scale process variations make ICs unique



Start-up SRAM values establish a unique Silicon fingerprint



Fingerprint turned into a strong secret cryptographic key



User keys can be wrapped or encrypted with this PUF key (red/black system)

AUTHENTiCO
TECHNOLOGIES

The SRAM PUF response is a noisy fingerprint, and turning it into a high-quality and secure key vault requires further processing. The hardware reconstructs exactly the same cryptographic key every time and under all (environmental) circumstances. It generates an Activation Code which, in combination with the SRAM startup behavior, is used to reconstruct an intrinsic PUF key for use by the customer's client software. When the key is not needed anymore by the software, it can be removed from memory. When it is needed later it can be reconstructed again. The intrinsic PUF key can be used as a root key to wrap and manage user keys.

Secure: This has great security advantages compared to traditional key storage methods. Each chip has its unique unclonable key. SRAM bits settle in the one or zero state in a non-deterministic way that not even the manufacturer can duplicate. Furthermore, because the key is not permanently stored, it is not present when the device is inactive (no key at rest) and hence cannot be found by an attacker who is opening up the device.

Low Cost: Keys are extracted from the chip. No keys have to be programmed in NVM or OTP.

LOW COST AND STRONG SECRET KEY STORAGE TECHNOLOGY

IS CRITICAL TODAY TO ENABLE AFFORDABLE AND EFFECTIVE SECURITY SYSTEMS.

AUTHENTICO
TECHNOLOGIES

For many years, silicon Physical Unclonable Functions (PUFs) have been seen as a promising and innovative security technology that was making steady progress. Today, Static Random-Access Memory (SRAM)-based PUFs offer a mature and viable security component that is achieving widespread adoption in commercial products. They are found in devices ranging from tiny sensors and microcontrollers to high-performance Field-Programmable Gate Arrays (FPGAs) and secure elements where they protect financial transactions, user privacy, and military secrets.

THE SRAM BASED PUF

Due to deep sub-micron manufacturing process variations, every transistor in an Integrated Circuit (IC) has slightly different physical properties. These lead to small but measurable differences in terms of electronic properties like transistor threshold voltages and gain factor. Since these process variations are not fully controllable during manufacturing, these physical device properties cannot be copied or cloned.

Threshold voltages are susceptible to environmental conditions such as temperature, and voltage so their values cannot be used directly as unique secret keys or identifiers.

The behavior of an SRAM cell, on the other hand, depends on the difference of the threshold voltages of its transistors. Even the smallest differences will be amplified and push the SRAM cell into one of two stable states. Its PUF behavior is therefore much more stable than the underlying threshold voltages, making it the most straightforward and most stable way to use the threshold voltages to build an identifier.

SRAM PUF BEHAVIOR

An SRAM memory consists of a number of SRAM cells. Each SRAM cell consists of two cross-coupled inverters that each are built up by a p- and n-MOS transistor. When power is applied to an SRAM cell, its logical state is determined by the relation between the threshold voltages of the p-MOS transistors in the invertors. The transistor that starts conducting first determines the outcome, a logical '0' or '1'.

It turns out that every SRAM cell has its own preferred state every time the SRAM is powered resulting from the random differences in the threshold voltages. This preference is independent from the preference of the neighboring cells and independent of the location of the cell on the chip or on the wafer.

Hence an SRAM region yields a unique and random pattern of 0's and 1's. This pattern can be called an SRAM fingerprint since it is unique per SRAM and hence per chip. It can be used as a PUF.
Keys that are derived from the SRAM PUF are not stored 'on the chip' but they are extracted 'from the chip', only when they are needed. In that way they are only present in the chip during a very short time window. When the SRAM is not powered there is no key present on the chip making the solution very secure.

PUF RELIABILITY

The deep submicron process variations that determine PUF behavior are frozen during manufacturing and do not change afterwards. Hence the preference of the SRAM cells is persistent and stable over time.

However, there is still a degree of noise. A small number of the cells, close to equilibrium are unstable and display a seemingly random startup preference. So, each time the SRAM starts up, a slightly different pattern emerges. This noise component is dependent on temperature, voltage ramp, and operating conditions.

The noise of SRAM-based PUF responses has been exhaustively characterized and tested under a wide variety of circumstances and foundry processes:

- Temperatures ranging from -50ºC to +150ºC [-58ºF to 300ºF]
- Voltage variation +/-20%
- Humidity up to 80%

EMC tests at 3V/m (EN55020 0.15–150 MHz and IEC 61000-4-3 80-1000MHz)

In particular, the SRAM PUF has been qualified for automotive, industrial and military use in collaboration with customers and partners.

Millions of measurements have been performed. Under all these circumstances the average noise level of the SRAM-based PUF response was found to be lower than about 15%. Despite this amount of noise, it is possible to reconstruct a high-entropy device unique and reliable key every time the SRAM is powered. This can be done by applying error correction techniques like 'helper data algorithms'1 or `fuzzy extractors'2. These algorithms perform two main functions that will be explained below: error correction and privacy amplification.

ERROR CORRECTION

Error correction techniques for cryptographic key reconstruction require an enrollment phase and a reconstruction phase. In the enrollment phase (a one-time process) the PUF response is mapped onto a codeword of an error correcting code. Information about the mapping is stored in the Activation Code (AC) or helper data. The AC is constructed such that it does not leak any information about the key. It should be stored in memory that is accessible by the PUF algorithms but it can be stored off-chip as it is not sensitive. Any change to the AC, malicious or not, will prevent key reconstruction. The AC is only valid for the chip on which it was created.

Each time the device runs an authentication protocol and needs the secret PUF key, a new noisy PUF measurement is carried out and the PUF key (without noise) is extracted from the AC and this new PUF response. This is called the reconstruction phase.

The error correction algorithms have been designed to reconstruct the key with an error rate of less than 10-9 even under extreme circumstances of 25% average noise.

PRIVACY AMPLIFICATION

AND SECURITY

Secret keys provide security based on the fact that they are completely random and hence unpredictable. Physical measurements, like PUF responses, have a high degree of randomness, but are usually not completely uniformly random. Privacy amplification is used to generate uniformly random keys.
By combining error correction and privacy amplification, a 1kByte SRAM PUF response can be turned into a 256-bit uniformly random key and only 0.5 kByte is needed for a 128-bit key with full randomness. A typical SRAM PUF contains so much entropy that only a few dozen bytes are needed to provide a collision-free globally unique identifier that can be used as a unique (but noisy) electronic chip ID (ECID) or as a serial number.

REQUIREMENTS

The hardware components have to use un-initialized SRAM. This can be a separate SRAM block or a part of a bigger existing SRAM. Standard SRAM suffices. To store the Activation Code (AC), access to a storage medium is needed. This can be embedded Non-Volatile-Memory (NVM), a separate memory on the board, e.g. flash, or cloud storage. For the firmware version BROADKEY, a microcontroller is needed for which a C-compiler exists. The PUF algorithms can be stored in any NVM e.g., flash, ROM.
Note that SRAM is embedded in almost any microprocessor and SoC, in every technology node and is part of the standard manufacturing process. There is no need for time- consuming qualification and chip testing, since the actual PUF behavior has already been verified extensively on every technology node.