INTRINSIC ID

WHITE PAPER

SRAM PUF: The Secure Silicon Fingerprint

SRAM PUF Benefits

- Uses standard SRAM
- Device-unique, unclonable key
- No secrets reside on the IC
- No key material programmed
- Flexible and scalable
- Highly reliable across large range of operating environments and on every technology node
- Lifetime >25 years

Certifications

- EMVCo, Visa
- CC EAL6+
- NIST CAVP
- PSA, ioXt
- U.S. and EU Governments

Markets

- IoT
- Data Center / HPC
- Secure Transactions
- Aerospace & Defense

Enable Affordable and Effective Security Systems with Secret Key-Storage Technology.

Silicon-based physical unclonable functions (PUFs) represent a promising and innovative security technology. Today, static random-access memory (SRAM)-based PUFs offer a viable security component that's being widely adopted in commercial products and applications. They are found in devices ranging from tiny sensors and microcontrollers to high-performance performance field-programmable gate arrays (FPGAs) and secure elements where they protect financial transactions, user privacy, and even military secrets.

Figure 1: Extracting a strong secret key from SRAM behavior.

The SRAM-Based PUF

Many different types of PUFs are known, but by far the most-widely deployed one is the SRAM-based PUF, which has demonstrated great reliability, scalability, and ease of use. The SRAM PUF is easy and flexible to implement in a way that scales over the many different technology nodes. It offers a mature and viable security component that has achieved widespread adoption in commercial products and can be found in devices ranging from tiny sensors and microcontrollers to high-performance FPGAs and secure elements where they protect financial transactions, user privacy, and military secrets.

Due to deep submicron 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 such as 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 0s and 1s. 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 this 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, which makes the solution very secure.

PUF Reliability

Using error correction, SRAM PUF's can be developed that are extremely reliable

The deep submicron process variations that determine PUF behavior are created during manufacturing and do not change afterwards. Hence the startup state 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, whose startup state is 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. The SRAM PUF has been qualified for automotive, industrial, and military use in collaboration with customers and partners. During these qualification processes, millions of measurements have been performed at varying conditions:

- Temperatures ranging from -55°C to +150°C [-67°F to 300°F]
- Voltage variation +/-20%
- Humidity up to 80%
- EMC tests at 3V/m (EN55020 0.15–150 MHz and IEC 61000-4-3 80-1000MHz)

Under all these circumstances the average noise level of the SRAM-based PUF response was found to be <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, by applying error-correction techniques such as '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 enable reliable key reconstruction even under worst case conditions

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 an activation code (AC), sometimes called "helper data." The AC is constructed such that it does not reveal 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. Because the AC is created from a device-unique PUF response, the AC is only valid for the chip on which it was created.

---

[1] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in International Conference on Audio and Video-based Biometric Person Authentication (AVBPA'03), ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. 2688. Heidelberg: Springer-Verlag, 2003, pp. 393–402.

[2] X. Boyen, "Reusable cryptographic fuzzy extractors," in ACM Conference on Computer and Communications Security (CCS'04). New York, NY, USA: ACM, 2004, pp. 82–91. AND Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in EUROCRYPT'04, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Heidelberg: Springer-Verlag, 2004, pp. 523–540.

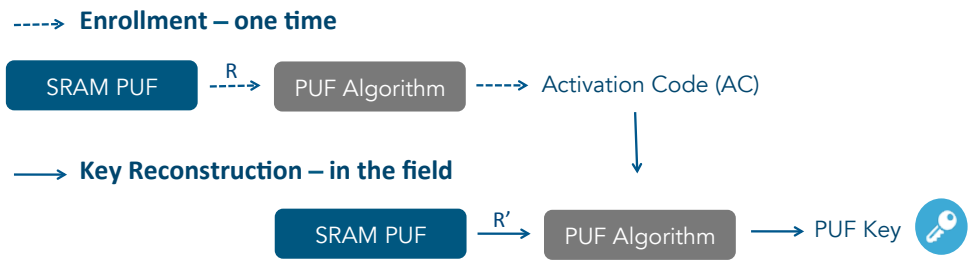

Figure 2: Enrollment and reconstruction phase for the generation of PUF keys. Note that R is the initial PUF response during enrollment while R' is a PUF response in the field with a noise component.

Each time the device runs an authentication protocol and needs the secret PUF key, a new noisy PUF measurement is carried out. Then 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 a typical error rate of less than 10^{-12}. [3] Both enrollment and reconstruction phases are illustrated in Figure 2.

Privacy Amplification and Security

The SRAM PUF is inherently secure and contains sufficient entropy

Secret keys provide security based on the fact that they are completely random and hence unpredictable. Physical measurements, such as 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, only approximately 0.5 kByte of SRAM PUF response data 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.

Dedicated security labs and security teams at customers have analyzed the security of the Intrinsic ID SRAM PUF against various invasive and non-invasive physical attacks without revealing any weaknesses. Attacks with scanning electron microscopes (SEMs), lasers, focused ion beams (FIBs), and probes have not been successful. Side-channel attacks have not lead to any leakage of sensitive information.

Aging

Aging can be counteracted ensuring 25 year lifetime

Accelerated aging tests have been performed on SRAM-PUFs to investigate the noise level as a function of time. By using a patented anti-aging technique[4], a 25-year lifetime can be guaranteed for Intrinsic ID SRAM PUF technology.

[3] Even under extreme circumstances e.g. due to extreme temperatures, if noise levels were to rise up to 25%, the reconstruction failure rate is still lower than 10^{-9}.

[4] R. Maes and V. van der Leest, "Countering the effects of silicon aging on SRAM PUFs", Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST), pp. 148-153 available at http://www.Intrinsic.id.com/wp-content/uploads/2014/09/PUF_aging.pdf

SRAM PUF Implementation – BK Software & QuiddiKey

QuiddiKey and BK are the industry leading SRAM PUF implementations from Intrinsic ID

Intrinsic ID has bundled the above error correction, randomness extraction, security countermeasures and anti-aging techniques into its products. They extract cryptographic keys from the SRAM PUF in a very secure manner and are available as hardware IP (netlist) called QuiddiKey®, firmware (ANSI C Code) called BK™, or a combination of these. Hybrid solutions, combining hardware and software, offer great efficiency when already integrated hardware accelerators, such as for (a-)symmetric cryptography, are used in combination with SRAM PUF technology.

The hardware IP is small and fast – around 25K gates / 50K cycles – and connects to common interconnects, such as AMBA® AHB, APB as well as proprietary interfaces. A Built-in self-test (BIST), diagnostics, and health checks are included in the logic. A driver is provided to ease integration with software. Since it is purely digital, single-clock logic, the hardware IP synthesizes readily to any technology.

Software reference implementations start from 4KB of code and are available for major platforms, such as ARM®, ARC®, Intel®, MIPS and RISC-V. Software implementations can be used to add PUF technology to existing products by a firmware upgrade. Intrinsic ID also provides versions of BK that are pre-integrated with ARM® TrustZone®.

QuiddiKey and BK are flexible products that can easily be integrated in any design.

Both QuiddiKey hardware and BK software solutions can be optimized for low footprint, low latency, or low memory use, depending on the application. Re-using or integrating with existing crypto cores and random number generators can further enhance performance and reduce footprint. Intrinsic ID solutions come with comprehensive product specifications and integration guidelines including reference code that illustrates usage of the API offered to the application programmer. The cryptographic algorithms are NIST-recommended or FIPS approved, and implementations have been CAVP certified. The Intrinsic ID solutions have been deployed and proven in hundreds of millions of devices certified by EMVCo, Visa, CC EAL6+, PSA, ioXt, and governments across the globe.

Requirements

QuiddiKey and BK 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 non-sensitive 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, BK, a microcontroller is needed for which a C-compiler exists. The PUF algorithms can be stored in any NVM, e.g. Flash, or 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, as extensive testing by Intrinsic ID and its partners has shown that technology reliably scales down to the smallest technology nodes currently available. More information on the reliability of SRAM PUF technology can be

found in the Intrinsic ID White Paper "The Reliability of SRAM PUF[5]."

Use in the Field

SRAM-based PUFs are commercially available from semiconductor companies. They are already deployed in a wide range of microcontrollers, FPGAs and smart card controllers. In other markets, software implementations[6] have enabled rapid deployment of this technology even as a retrofit solution. Intrinsic ID has partnered with leading semiconductor companies and developed solutions for protecting embedded systems, sensors, and controllers. More information about our SRAM PUF deployments can be found on our website: https://www.intrinsic-id.com.

Conclusion

SRAM PUF is a mature technology for embedded authentication even in the most demanding environments

SRAM PUFs have been successfully implemented in commercial products. They combine high security and reliability with low cost, low footprint designs, and easy implementation. They have been deployed in many devices, from tiny microcontrollers and sensors to high performance FPGAs and secure elements.

Numerous implementations have consistently demonstrated the reliability and security of the technology. SRAM PUFs are a mature and robust technology, designed for security and based on solid theoretical foundations. SRAM PUFs have established their credibility in high-security markets and are now gaining traction in markets ranging from low-cost IoT applications to high-end security solutions for government, defense, and the payment industry.

---

[5] The Intrinsic ID White Paper "The Reliability of SRAM PUF" is available at http://www.intrinsic-id.com/landing-page-white-paper-reliability-sram-puf

[6] H.Hodson – New Scientist, "Silicon fingerprint on chips could make any gadget unhackable" June 6, 2016 https://www.newscientist.com/article/mg23030771-400-physical-quirks-in-silicon-chips-are-key-to-unhackable-devices/ or "Chip design quirks make our lives more secure" in the June 11 printed issue page 24

info@intrinsic-id.com www.intrinsic-id.com INTRINSIC ID

Intrinsic ID Inc., 710 Lakeway Drive, Suite 100, Sunnyvale, CA 94085.
Intrinsic ID B.V., High Tech Campus 83, 5656 AG Eindhoven, The Netherlands.

© Copyright 2021 Intrinsic ID B.V. Intrinsic ID, QuiddiKey®, BK™ and other designated brands included herein are trademarks of Intrinsic ID. All other trademarks are the property of their respective owners.