早稲田大学大学院情報生産システム研究科

博士論文概要

論文題目

Study on High Stability and Low Energy SRAM-Based Physically Unclonable Function for Hardware Security

申請者

Kunyang LIU

情報生産システム工学専攻
ディペンダブル情報システム研究

2021 年　01 月

The global market of Internet of Things (IoT) has been expanding rapidly in recent years. With increasing edge devices connected in the network, the security of IoT has become a great concern as many of these devices operate in the environments where human involvement is limited. This requires security to be considered not only at the software level, but also down from the integrated circuits (ICs) level. One critical issue is the secure generation of secret keys, which serve as the root of trust and a fundamental block of security applications like cryptography and authentication that is based on cryptography.

Physically unclonable functions (PUFs) are regarded as a promising solution for high-security and low-cost secret key generation. Leveraging the intrinsic random process variation of silicon devices, a PUF generates a chip-specific ID bitstream on-the-fly, and this bitstream can be used for secret key realization. Since process variation such as random dopant fluctuation is extremely difficult to observe, PUF is regarded as more resilient to reverse engineering than non-volatile memories (NVMs), and therefore, it is called physically unclonable.

However, there are many challenges in PUF circuit design. The most critical problem is that PUFs suffer from bit errors, because the process variation they leverage is usually in the millivolt (mV) range. Random noise, supply voltage/temperature (VT) variations, long-term aging, etc. cause errors in PUF data generation, which are not tolerable for cryptographic applications. In addition to stability problem, PUF should also be low-energy and small-area, because IoT edge devices are generally resource-constraint. Most importantly, robustness against physical attacks must be considered in PUF circuit design.

Static random access memory (SRAM)-based PUF or SRAM PUF is one of the most important categories of PUFs. It features small area, and it has a differential bitcell structure. The differential structure makes SRAM PUF naturally more resilient to power analysis attacks, which is a kind of popular physical attack, because the supply current waveforms of reading data “0” and data “1” have little difference. However, conventional SRAM PUFs suffer from higher bit error rate (BER) than low-native-BER mono-stable PUFs. In the conventional solution, heavy error-correcting code (ECC) circuits are implemented to meet the zero-error requirement for cryptography. This results in substantial overhead in latency, power, and area, which are not desired for IoT edge devices.

Therefore, to meet the demands, an SRAM-based PUF with natively high-stability bitcells and efficient post-processing techniques are required to reduce BER so as to reduce or even eliminate the use of ECC.

Based on these considerations, in this dissertation, two SRAM-based PUF solutions with novel bitcells and post-processing techniques are presented.

The first work achieved more than 10 times lower native BER than conventional SRAM PUFs by using EE SRAM bitcells, and the BER is comparable with the state-of-the-art mono-stable PUFs. It also achieves "zero" error by using only circuit techniques for post-processing. The proposed dark-bit detection technique achieves "100%" reduction on BER by masking 67.4% detected bitcells, while the previous work only achieved 60% BER reduction.

The second work presents a hybrid SRAM PUF that achieves 61 times lower energy than the EE SRAM PUF while having the same level of stability. In this work, device characteristics modification by HCI burn-in is applied, and the bitcell is designed to be compatible with HCI burn-in with little overhead. Through the bitcell stabilization by HCI burn-in, "zero" BER is achieved without masking loss.

The dissertation is organized with four chapters as follows.

In Chapter 1, the background of IoT security system is first introduced using an example of edge device authentication. Then, the drawbacks of conventional solution are discussed and the motivation for a PUF is derived. Afterwards, the basic concept of silicon PUFs and PUF-based authentication are introduced.

In Chapter 2, the evaluation metrics of a PUF are shown. After that, prior art on PUF is introduced, and the reason why high-stability SRAM PUF is preferred is discussed. Also, prior post-processing techniques on PUF stabilization are shown.

In Chapter 3, an EE SRAM PUF with two-dimensional (2-D) power gating and V_{SS} bias-based dark-bit detection techniques are introduced. The presented EE SRAM PUF utilizes an EE bitcell structure to improve the stability of SRAM PUF. This reduces BER by 14 times compared with conventional SRAM-based designs (3.04% BER), resulting in 0.21% native

BER. The EE SRAM bitcell also has a small footprint of 373 F^2, because only nMOS transistors are used, and the p-n boundary does not exist in its layout. By a novel 2-D power gating technique, the energy is reduced by approximately 64 times to 128 fJ/bit. The dark-bit detection using an integrated bias generator successfully detects “100%” dark bits (<5.99×10−7 BER) in the VT range across 0.8—1.4 V and −40—120 ℃. Another merit of this technique is that costly temperature sweep is not required for testing. The above-mentioned metrics have been verified with prototype chips fabricated in 130-nm standard CMOS.

In Chapter 4, a hybrid SRAM PUF using hot carrier injection (HCI) burn-in to reinforce stability is presented. The SRAM bitcell is a hybrid of EE SRAM and conventional CMOS SRAM to benefit from both designs. During evaluation, it works in the EE SRAM mode for high stability, and after that, it is switched to the CMOS SRAM mode to take advantage of the low-power feature. Moreover, this mode transition enables the PUF to work under low supply voltages (V_{DD}s) down to 0.5 V. As a result, its energy is greatly reduced to 2.07 fJ/bit. This is 61 times reduction compared with EE SRAM PUF. The hybrid SRAM bitcell is compatible with HCI burn-in stabilization. HCI effect is utilized to enlarge the Vth mismatch of PUF cells for stability reinforcement. By this technique, all bit errors are eliminated (<3.90×10−7 BER) for the 5120 measured bits across 0.5—0.7 V and −40—120 ℃ after 10-min burn-in. Compared with error-free prior art, the hybrid SRAM PUF achieves the lowest energy while HCI burn-in is the only technique that has no requirements on additional fabrication processes, helper data, or visible oxide damages. The above-mentioned metrics have been verified with prototype chips fabricated in 130-nm standard CMOS.

In Chapter 5, the conclusions of the dissertation are drawn.