NAND Flash Memory Devices Security Enhancement Based on Physical Unclonable Functions

Zalivaka S. S.,[1]

Ivaniuk A. A.[2]

2022

[1]SK hynix memory solutions Eastern Europe, Minsk, Republic of Belarus

[2]Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Keywords: Physical unclonable function, NAND flash, True random number generator, Unique identification, Scrambler, Key-value pair, Error correction codes, ECC encoding, ECC decoding.

Abstract: According to the report (McIntyre, Annual flash controller update, 2009), solid-state drives (SSD) will take around 85% of enterprise storage capacities by 2026. However, due to frequent utilization of this kind of storage in different computing systems, security issues are arising (Tyson, Researchers find “pattern of critical issues” in SSD encryption, 2018). One of the many possible ways of decreasing the influence of vulnerabilities is the use of physical unclonable functions (PUFs) in NAND flash memory systems. Since PUFs are lightweight security primitives, it can be used in Internet of Things (IoT) devices which employ flash memory as nonvolatile storage (Pickering, NAND rises to the occasion in data-heavy IoT applications, 2021). There are also many implementations of true random number generators (TRNGs) based on PUFs (Rajendiran, Using PUFs for random number generation, 2021). Despite that TRNGs are widely used in different areas (e.g., stochastic process modeling, gambling, artificial intelligence, etc.), the main target application is security (e.g.,

Neustadter, True random number generators for heightened security in any SoC, 2021; Intrinsic ID, Zign RNG, 2021). In case when the application does not require true randomness, the proposed random number generator can be used without additional components (i.e., conditioner and deterministic random bit generator (DRBG)).

The purpose of this chapter is to show how PUFs can enhance security of NAND flash memory devices. It comprises five parts. The chapter summarizes the research efforts of SK hynix memory solutions Eastern Europe in this area. Sections 1 and 2 are devoted to true random number generators (TRNGs), which are the important part of any security protocol. Section 1 outlines general-purpose entropy source for TRNG, and Sect. 2 contains a description of a specific NAND-based entropy source. Section 3 shows the ID generation algorithms based on PUFs implemented using read values of NAND flash memory pages. Data scrambling scheme enhancements with PUFs are presented in Sect. 4. Section 5 includes PUF-based error detection algorithms which improve external mapping table storage in mobile NAND flash devices. Some of the described solutions are already patented; some of them are in the process of patenting.

Zalivaka, S. S. NAND Flash Memory Devices Security Enhancement Based on Physical Unclonable Functions / Zalivaka S. S., Ivaniuk A. A. // Frontiers of Quality Electronic Design (QED) / Ali Iranmanesh [editor]. – Los Altos Hills : Silicon Valley Polytechnic Institute, 2022. – С. 1-43. – DOI : https://doi.org/10.1007/978-3-031-16344-9.