On the Sustainability of Lightweight Cryptography Based on PUFs Implemented on NAND Flash Memories Using Programming Disturbances

Nikolaos Athanasios Anagnostopoulos [1], Yufan Fan [1], Muhammad Umair Saleem [1], Nico Mexis [1], Florian Frank [1], Tolga Arul [1], and Stefan Katzenbeisser [1]

[1]Affiliation not available

October 30, 2023

Abstract

In this work, we examine the potential of Physical Unclonable Functions (PUFs) that have been implemented on NAND Flash memories using programming disturbances to act as sustainable primitives for the purposes of lightweight cryptography. In particular, we investigate the ability of such PUFs to tolerate temperature and voltage variations, and examine the current shortcomings of existing NAND-Flash-memory PUFs that are based on programming disturbances as well as how these could potentially be addressed in order to provide more robust and more sustainable security solutions.

On the Sustainability of Lightweight Cryptography Based on PUFs Implemented on NAND Flash Memories Using Programming Disturbances

Nikolaos Athanasios Anagnostopoulos*†, Yufan Fan‡, Muhammad Umair Saleem§,
Nico Mexis*, Florian Frank*, Tolga Arul*†, Stefan Katzenbeisser*
*University of Passau, Faculty of Computer Science and Mathematics, Innstraße 43, 94032 Passau, Germany
Emails: {Nikolaos.Anagnostopoulos, Florian.Frank, Tolga.Arul, Stefan.Katzenbeisser}@uni-passau.de
†Technical University of Darmstadt, Computer Science Department, Hochschulstraße 10, 64289 Darmstadt
Emails: {anagnostopoulos, arul}@seceng.informatik.tu-darmstadt.de
‡Technical University of Darmstadt, Department of Electrical Engineering and Information Technology,
Merckstraße 25, 64283 Darmstadt, Germany
Email: yufan.fan@nt.tu-darmstadt.de
§Technical University of Darmstadt, Computer Science Department, Hochschulstraße 10, 64289 Darmstadt
Email: umsach-contact@protonmail.com

***Abstract*—In this work, we examine the potential of Physical Unclonable Functions (PUFs) that have been implemented on NAND Flash memories using programming disturbances to act as sustainable primitives for the purposes of lightweight cryptography. In particular, we investigate the ability of such PUFs to tolerate temperature and voltage variations, and examine the current shortcomings of existing NAND-Flash-memory PUFs that are based on programming disturbances as well as how these could potentially be addressed in order to provide more robust and more sustainable security solutions.**

***Index Terms*—sustainability, physical unclonable function, Flash memory, lightweight cryptography, environmental conditions, temperature variations, voltage variations, robustness**

Brief Overview of this Work

Flash-memory-based Physical Unclonable Functions (PUFs) have recently been proposed in the relevant literature [1]–[5] as a lightweight and sustainable security primitive, because their implementation and operation are rather cost-efficient. More specifically, only lightweight software is required for their operation, and they either may not require any hardware addition, as Flash memories are often inherent parts of computing systems, e.g., Internet-of-Things (IoT) devices, or may be reusable in different systems, as they are also often found in removable modules.

In general, PUFs are physical objects, such as hardware, which utilise minor manufacturing variations, in order to provide a rather unique output for a specific input under partcular conditions. In the case of NAND-Flash-memory-based PUF that utilises programming disturbances, certain pages of the Flash memory are programmed rapidly and repeatedly causing a unique error pattern to appear in nearby pages.

In this work, we will examine the quality of the responses of such Flash-memory-based PUF that have been implemented on multiple instances of the Waveshare NandFlash Board (A), which is a removable external Flash memory module that incorporates a 1-Gbit Samsung K9F1G08U0E NAND Flash memory, as shown in Figure 1. Following the example of previous works regarding NAND-Flash-memory-based PUFs that utilise programming disturbances [1]–[3], we also assume that each individual page of the relevant NAND Flash memory that is affected by the rapidly repeated programming of its nearby pages constitutes a different instance of this PUF. Therefore, in order to examine the sustainability of this PUF type, we examine the quality characteristics of the responses of each such PUF, i.e., the values of the cells of each Flash memory page used as a PUF instance, after the operation of this PUF under adverse environmental conditions, such as temperature and voltage variations.

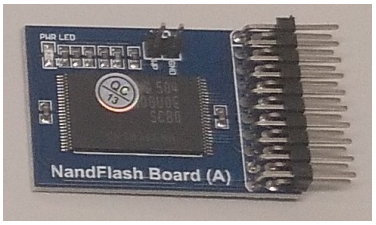

Fig. 1: A photo of the Waveshare NandFlash Board (A).

Each Waveshare NandFlash Board (A) used in our work was controlled using an ST Microelectronics STM32F429I Discovery (STM32F429I-DISC1) board, to which this Flash board had been connected using a Waveshare Open429Z-D Standard, an STM32F4 expansion/development board for the

This work has been funded by the German Research Foundation – Deutsche Forschungsgemeinschaft (DFG), as part of the Projects "PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories" (project number 440182124) and "NANOSEC: Tamper-Evident PUFs based on Nanostructures for Secure and Robust Hardware Security Primitives" (project number 439892735) of the Priority Program "Nano Security: From Nano-Electronics to Secure Systems" (SPP 2253).

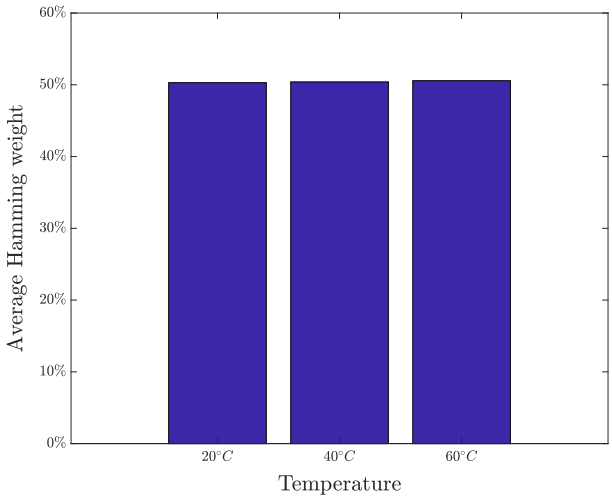

Fig. 2: Overall average fractional Hamming weight value of the examined NAND-Flash-memory-based PUF, for each value of the ambient temperature tested.

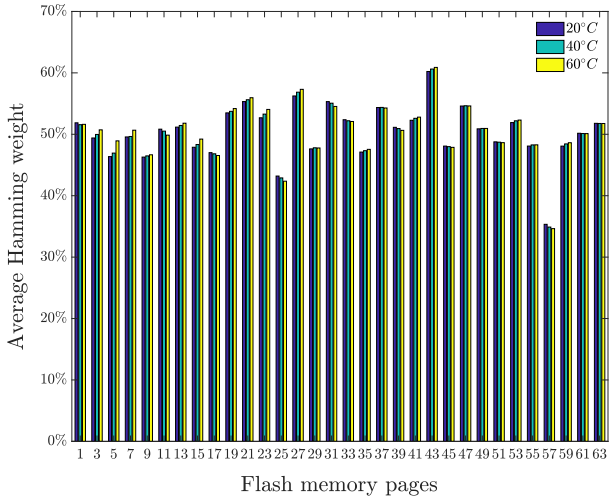

Fig. 3: Average fractional Hamming weight values per instance of the examined NAND-Flash-memory-based PUF, for the different values of the ambient temperature tested.

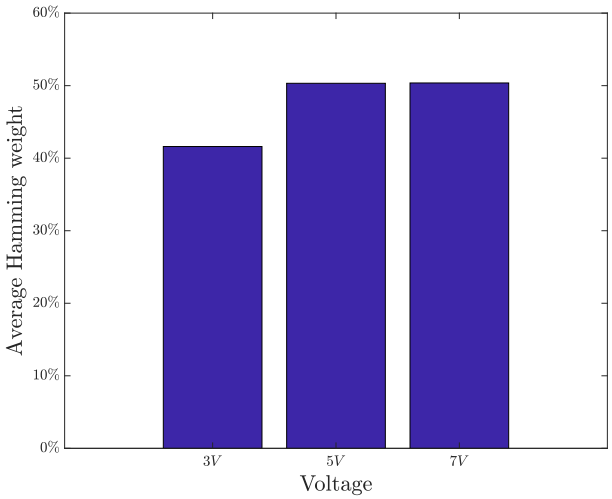

Fig. 4: Overall average fractional Hamming weight value of the examined NAND-Flash-memory-based PUF, for each value of supply voltage provided by the USB port of the STM32F429I-DISC1 board to the overall system.

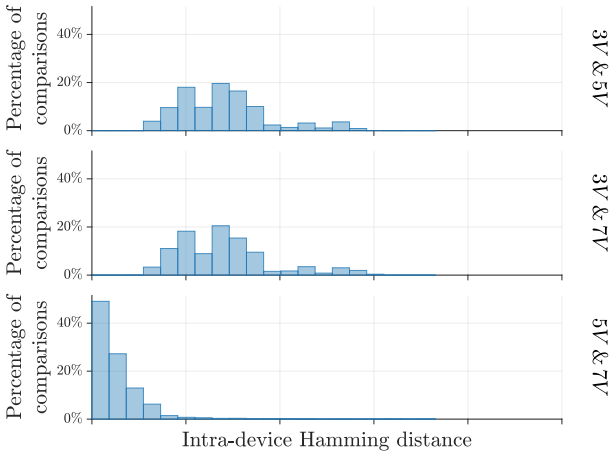

Fig. 5: Intra-device Hamming distance values for the examined NAND-Flash-memory-based PUF, for pairs of PUF responses taken at different supply voltage levels provided by the USB port of the STM32F429I-DISC1 board to the overall system.

ST Microelectronics STM32F429I Discovery (STM32F429I-DISC1) board. A single Flash memory block was fully erased and, thus, the initial bit pattern of cells utilised in the relevant PUF response was `0xFF` (all ones), while the other cells of the same block were rapidly and repeatedly programmed with the bit pattern `0x00` (all zeros), for 10,000 programming cycles or until at least 2040 addresses (corresponding to 1 B each) have had at least one bit flip each, whichever condition was fulfilled first. Thus, in case the latter condition holds true, in each of the 2040 bytes of the relevant PUF page, which consists of 2048 bytes in total, there will be at least one bit flip, ie, all but one of the page's bytes will contain at least one bit flip.

As each memory block of the Samsung K9F1G08U0E NAND Flash memory is made up of 64 pages, 32 of these pages will constitute individual PUF instances, with 31 of them (pages '1', '3', '5', . . . , '61') receiving disturbances from both of their adjacent pages (double-side program "hammering"), and one of them (page '63') receiving disturbances from its only adjacent page (single-sided program "hammering", from page '62'). For each page constituting a PUF instance, 20 responses have been received of a size of 2 KB each, for a total size of 64 KB per block measurement.

Our results for measurements taken at 20°C, 40°C, and 60°C indicate an overall fractional Hamming weight of 50% for the memory pages utilised as PUFs (Figure 2), but quite varying Hamming weights for each individual page serving as a PUF (Figure 3), clearly suggesting that it would be preferable to consider a whole memory block as a PUF, and not each individual page of such a block, as certain pages acting as PUFs appear to be biased towards one logical value or the other. Additionally, measurements taken at power supply voltages lower than the nominal lead to an overall Hamming

weight value that is significantly below 50%, indicating a bias towards the logical value of '0' and leading into intra-device Hamming distances significantly higher than 10%, which may affect the ability of this PUF to act as a sustainable security mechanism. In this case, the employment of an internal voltage regulator, of a rather simple design, may potentially mitigate the observed effects of power supply voltage variations.

Therefore, although a number of issues that may reduce the practical applicability and sustainability of the examined NAND-Flash-memory-based PUFs have been identified, it may be possible to address them through rather realistic design modifications and improvements, which, however, remain to be implemented and tested in practice as part of future works on this scientific field. At the same time, however, we can also conclude that the examined PUFs are able to provide flexible and scalable security applications in a practical, liightweight, and highly sustainable manner, under nominal environmental conditions.

REFERENCES

[1] S. Jia, L. Xia, Z. Wang, J. Lin, G. Zhang, and Y. Ji, "Extracting Robust Keys from NAND Flash Physical Unclonable Functions," in *Information Security – ISC 2015*, ser. Lecture Notes in Computer Science (LNCS), J. Lopez and C. J. Mitchell, Eds., vol. 9290. Springer, 2015, pp. 437–454.

[2] S. Sakib, A. Milenković, M. T. Rahman, and B. Ray, "An Aging-Resistant NAND Flash Memory Physical Unclonable Function," *IEEE Transactions on Electron Devices*, vol. 67, no. 3, pp. 937–943, 2020.

[3] P. Prabhu, A. Akel, L. M. Grupp, W.-K. S. Yu, G. E. Suh, E. Kan, and S. Swanson, "Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations," in *Trust and Trustworthy Computing – Trust 2011*, ser. Lecture Notes in Computer Science (LNCS), J. M. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, and Y. Beres, Eds., vol. 6740. Springer, 2011, pp. 188–201.

[4] Y. Wang, W. Yu, S. Wu, G. Malysa, G. E. Suh, and E. C. Kan, "Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 33–47.

[5] T. Saito, H. Nagase, M. Izuna, T. Shimoi, A. Kanda, T. Ito, and T. Kono, "High-Temperature Stable Physical Unclonable Functions with Error-Free Readout Scheme Based on 28nm SG-MONOS Flash Memory for Security Applications," in *2017 IEEE International Memory Workshop (IMW)*. IEEE, 2017, pp. 1–4.