Signature Analysis of SRAM-PUF for IoT Decentralized Identifier in Large-Scale Networks

Seungnam Han[1], Jeein Kim[2], Haewon Lee[1], and Euiseok Hwang[1,2]
[1]School of Electrical Engineering and Computer Science
[2]Artificial Intelligence Graduate School
Gwangju Institute of Science and Technology (GIST)
Gwangju, South Korea
{snhan0911, jeeinkim, haewonlii, euiseokh}@gist.ac.kr

***Abstract*—In this paper, we extract hardware signatures from numerous static random access memory (SRAM) and analyze the feasibility as a signature for Internet of Things (IoT) decentralized identifier (DID). Due to uncontrollable variations in the manufacturing process, SRAM contains inherent randomness that can serve as a physical unclonable function (PUF) to identify the device uniquely. In particular, with the massive deployment of IoT devices, research on SRAM-PUF based distributed device identification is being actively investigated. However, conventional SRAM-PUF research has mainly focused on application to a small-scale IoT environment, so a limited number of SRAM have been analyzed. To generalize the signature utilization, we investigate uniqueness of the PUF from a number of SRAMs. We employed commercial SRAMs and off-the-shelf development boards to extract SRAM-PUFs. Evaluation results demonstrate that SRAM-PUFs are suitable for DIDs even in large-scale IoT networks, considering both chip-by-chip and block-by-block uniqueness.**

***Index Terms*—Physical unclonable function, decentralized identifier, internet of things**

I. Introduction

Recently, decentralized networks have gained much interest due to their ability to support large-scale data streams in a distributed manner and mitigate single-point-failure attacks. Moreover, the employment of these networks in communication systems has been accelerated by the emerging Internet of Things (IoT). For example, in medical IoT [1], wearable devices and sensors sending data to a hospital server can be authenticated by using their decentralized identifiers (DIDs), and [2] suggests a privacy-preserving decentralized chain for IoT in smart home, office and factory. In other works, many researchers take advantage of decentralized IoT in various applications [3]–[6].

Meanwhile, extracting unique identifier from hardware has been utilized by using the physical unclonable function (PUF) [7]–[10]. PUF exploits hardware variation in the manufacturing process, not allowing attackers to mimic a certain PUF. Static random access memory (SRAM) based PUF is one of the popular PUF since it contains randomness information, and is easily implemented with no additional hardware utility. For this reason, SRAM-PUF is considered as a promising signature scheme for decentralized and resource-constrained IoT.

Despite of the prospect, however, existing SRAM-PUF based identification approaches are established on either assumption where the SRAM-PUFs have sufficient uniqueness and are distinguishable from each other, or demonstrations to a few SRAM. Even if the results can be applied to small-scale networks, it should be generalized in more practical implementation such as large-scale decentralized IoT.

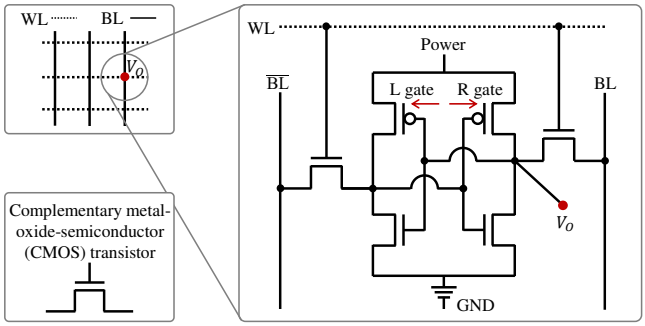

Fig. 1. Static random access memory (SRAM) architecture: word-line (WL) and bit-line (BL).

Thus, we evaluate the uniqueness of numerous SRAM for PUF utilization as a signature in large-scale networks. To this end, we customize the test-bed for SRAM-PUF extraction using the off-the-shelf development board and SRAMs. Experimental evaluations of PUFs are conducted on chip-by-chip uniqueness between SRAMs, block-by-block uniqueness within SRAMs, and their randomness.

II. Preliminaries and Related Works

In this section, we provide a brief introduction to the basic SRAM architecture, including the PUF generation mechanism. Fig. 1 illustrates an SRAM cell array consisting of word-line (WL) and bit-line (BL), as well as the output voltage (V_O). Each cell can store one bit of information using six complementary metal-oxide semiconductor (CMOS) transistors that manipulate WL and BL. To write a bit into a cell, we set the state of BL to either 'high' or 'low' while WL is 'high'. This information remains stored as long as the power remains on. However, if the power is switched off, the stored information in the cell is lost.

The generation of SRAM-PUF occurs when the power is switched from the off-state to the on-state. When the SRAM is in the off-state, the output voltage (V_O) is at a low level.

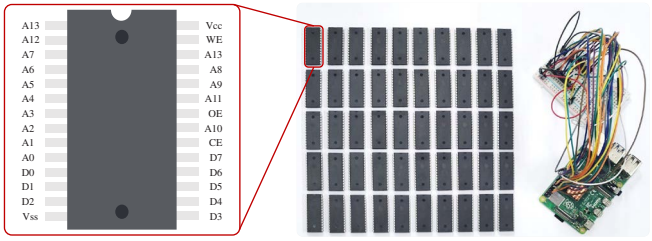

Fig. 2. Experiment setup for testing 50 SRAMs with the test-bed customized from the Raspberry Pi 4 Model B board.

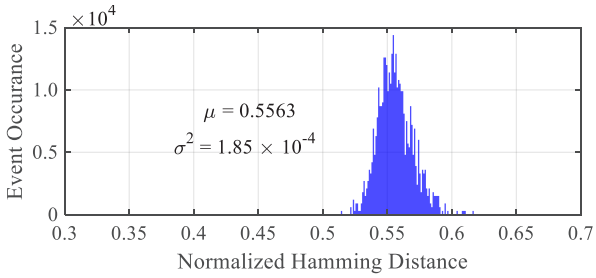

Fig. 3. Histogram of normalized Hamming distance among 50 SRAMs, average μ and variance σ^2.

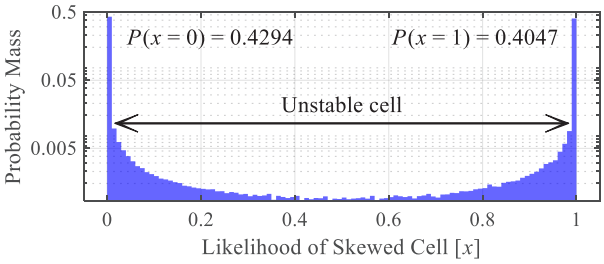

Fig. 4. Empirical probability mass function of x-skewed cell.

However, upon supplying power to a cell, the state of V_O is determined by the activation order of the CMOS gates. If the L gate is activated before the R gate, V_O assumes a low-level, indicating a '0' bit. Conversely, if the R gate is activated before the L gate, V_O becomes high-level, representing a '1' bit. Consequently, the initial value of a cell is categorized based on the probability of the cell being identified as a specific state, namely, 0-skewed, 1-skewed, and unstable cells, respectively. This random occurrence is a result of imperfections in the manufacturing process, which is the reason it is referred to as 'unclonable'.

Since its initial proposal by [11], the SRAM-PUF has been widely utilized for device authentication [7]–[10] and as a random number generator [12] in resource-constrained IoT systems. However, most existing approaches have been demonstrated using only a limited number of SRAMs. For instance, implementations described in [7]–[10] involve less than 15 SRAMs. Although [12] conducted tests on 16 SRAMs, it still falls short in representing large-scale decentralized IoT environments.

Thus, we customize a test-bed with multiple SRAMs and evaluated the performance of the signatures, taking into account large-scale decentralized IoT, in the following sections. To ensure reproducible results, we provided detailed descriptions of the specifications used in the test-bed.

III. Experiment Environment

Fig. 2 illustrates the test-bed comprising 50 SRAMs and Raspberry Pi 4 Model B. The utilized SRAM is the LY62256PL-55LL, a low-power CMOS SRAM manufactured by Lyontek, with a capacity of 32768×8 cells. Each SRAM has BL pins (D0 to D7), WL pins (A0 to A14), control pins (OE, CE, WE), as well as Vss and Vcc connections (representing power and GND). Data is written to or read from the SRAM in word units. The WL is decoded to activate one of the 2^{15} WL lines. During write operations, the data is transmitted to the cells through the BL, while during read operations, the data is transferred from the cells to the BL. In this way, we perform data read and write operations on the SRAM cell array structure.

The experiments is conducted for three main metrics: chip-by-chip uniqueness between SRAMs, block-by-block uniqueness and randomness. The experiment involved repeatedly powering the SRAM on and off to collect the corresponding PUF readings. In the block-by-block testing, we assume a memory block in a SRAM with 64 bits.

IV. Experimental Evaluation

A. Chip-by-chip uniqueness test

This subsection aims to verify the extent of variation observed in different SRAMs. Let denote $\mathbf{x}_i = [x_{(1,i)}, x_{(2,i)}, \ldots, x_{(N,i)}]^T$ as the PUFs in i^{th} SRAM where N denotes the number of cells in an SRAM ($N = 32768 \times 8$). In this context, uniqueness is represented by the normalized Hamming distance, defined as follows:

$$\overline{HD}(\mathbf{x}_i, \mathbf{x}_j) = \frac{1}{N} \sum_{n=1}^{N} |x_{(n,i)} - x_{(n,j)}|. \quad (1)$$

Fig. 3 shows the histogram of $\overline{HD}(\mathbf{x}_i, \mathbf{x}_j)$ $(i \neq j)$ among 50 SRAMs, which is aggregated from 300 iterations. As demonstrated in Fig. 4, the probability mass function of a x-skewed cell tend to be biased as 0-bit or 1-bit, resulting in the average $\mu = 0.55$ rather $\mu = 0.5$ precisely in Fig. 3. Though, the PUF has still sufficient uniqueness for device signature, which is consistent with the conventional works [7]–[9].

B. Block-by-block uniqueness test in a chip

In decentralized networks, multiple sub-nodes are controlled by a semi-trusted node. Therefore, we examine the level of variation observed in different divided PUF blocks and the degree of randomness within each block. This verification is conducted to assess the capability of the semi-trusted node in managing multiple DIDs. Let denote $\mathbf{z}_{(w,i)|_W} = [x_{((w-1)N/W+1,i)}, x_{((w-1)N/W+2,i)}, \ldots, x_{(wN/W,i)}]^T$ as the w^{th} block in the i^{th} SRAM, where W denotes the total number

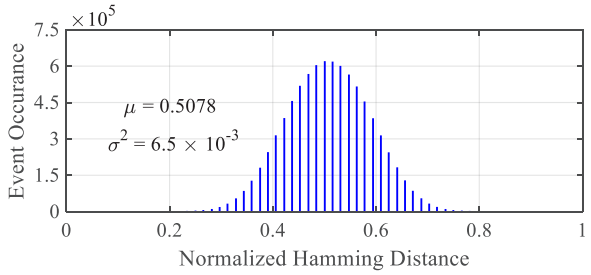

Fig. 5. Histogram of normalized Hamming distance among 4,096 blocks in an SRAM, average μ and variance σ^2.

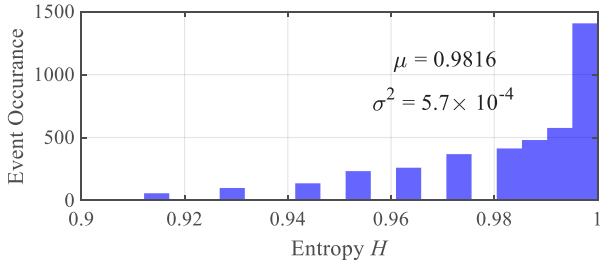

Fig. 6. Histogram of entropy of 4,096 blocks in an SRAM, average μ and variance σ^2.

of blocks. We investigate the normalized Hamming distance among the divided W blocks and the entropy $H_{(w,i)}$, defined as follows:

$$H_{(w,i)} = P_{(w,i)}\log_2(P_{(w,i)}) + (1 - P_{(w,i)})\log_2(1 - P_{(w,i)}). \tag{2}$$

Here, $P_{(w,i)}$ is the 1-bit probability in $\mathbf{z}_{(w,i)|_W}$ as follows:

$$P_{(w,i)} = \frac{N}{W}\sum_{k=1}^{N/W} x_{((w-1)N/W+k,i)}. \tag{3}$$

Fig. 5 shows the histogram of $\overline{HD}(\mathbf{z}_{(w_1,1)|_{4096}}, \mathbf{z}_{(w_2,1)|_{4096}})$ $(w_1 \neq w_2)$ assuming that the first SRAM represents a semi-trusted node and manages 4,096 DIDs of sub-nodes. The average is centered around 0.5, indicating that the blocks are generally different even if numerous sub-nodes are under the control of a single semi-trusted node. Additionally, Fig. 6 displays the histogram of entropy across entire blocks, indicating that the majority of blocks have a balanced occurrence of bits. As a result, SRAM-PUF is a desirable choice for a unique signature and can be utilized in large-scale networks.

V. Conclusion

In this paper, the feasibility of utilizing SRAM-PUF as a DID of IoT in large-scale networks was analyzed. To this end, we jointly evaluated 50 off-the-shelf SRAMs on the customized test-bed. Here, we considered two metrics: chip-by-chip uniqueness and block-by-block uniqueness. The experimental results demonstrate that SRAM-PUF has sufficient randomness even in numerous SRAMs, and blocks. This results indicate that SRAM-PUF has potential for authenticating a device identity in various applications, especially in large-scale IoT networks. Further research in this area could contribute to the advancement of secure and trust decentralized networks.

Acknowledgment

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-2021-0-01835) supervised by the IITP (Institute of Information Communications Technology Planning Evaluation), and supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2021R1A2C1009803)

References

[1] A. M. Alnour and K. H. Kim, "Decentralized identifiers (DIDs)-based authentication scheme for smart health care system," in *International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2022, pp. 443–438.

[2] H.-S. Choi, G. M. Lee, and W.-S. Rhee, "Hierarchical trust chain framework for IoT services," in *International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2019, pp. 710–712.

[3] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *Journal of Network and Computer Applications*, vol. 181, p. 103050, 2021.

[4] D. Wang, H. Wang, and Y. Fu, "Blockchain-based IoT device identification and management in 5G smart grid," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 5, pp. 1–19, 2021.

[5] I. Saviour Igboanusi, Allwinnaldo, R. Naufal Alief, M. Rasyid Redha Ansori, J.-M. Lee, and D.-S. Kim, "Ethereum based storage aware mining for permissioned blockchain network," in *International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2022, pp. 161–166.

[6] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205–8228, 2022.

[7] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of Everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[8] F. Farha, H. Ning, K. Ali, L. Chen, and C. Nugent, "SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5904–5913, 2021.

[9] S. K. Cherupally, S. Yin, D. Kadetotad, C. Bae, S. J. Kim, and J.-S. Seo, "A smart hardware security engine combining entropy sources of ECG, HRV and SRAM-PUF for authentication and secret key generation," in *Asian Solid-State Circuits Conference (A-SSCC)*, 2019, pp. 145–148.

[10] S. Yoon, S. Han, and E. Hwang, "Joint heterogeneous PUF-based security-enhanced IoT authentication," *IEEE Internet of Things Journal*, accepted for publication, 2023.

[11] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2007, pp. 63–80.

[12] R. Wang, G. Selimis, R. Maes, and S. Goossens, "Long-term continuous assessment of SRAM-PUF and source of random numbers," in *Design, Automation & Test in Europe Conference Exhibition (DATE)*, 2020, pp. 7–12.