Systematic Review of Physically Unclonable Functions on SRAMs for Secured Authentication

Khairul Syazwan Mamat [1], Pyi Phyo Aung [2], Chia Yee Ooi [3*]
[1, 2, 3] *Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
Email: [1] kshazwan3@graduate.utm.my, [2] pyiphyoaung.mdy@gmail.com, [3] ooichiayee@utm.my
*Corresponding Author

***Abstract*— Better security is essential for IOT devices since more and more devices today are connected and accessing the sensitive data stored in each other. Today's device authentications in IoT devices are using public and private key cryptography. In this paper, we review the study of Physically Unclonable Functions (PUFs) on embedded SRAMS for secured authentication. The review first categorizes PUFs into categories based on types of devices. Then, we discuss various performance metrics used to evaluate the performance of Static Random-Access Memory Physically Unclonable Functions (SRAM PUFs). This is followed by various methods of improving stability and reliability of the SRAM PUFs before the conclusion.**

Keywords*— *Physically unclonable function; authentication; memory cells; semiconductor memory; reliability;

I. INTRODUCTION

With the rapid advancement of technology, digital data storage and access have become crucial. The security and reliability of this data is especially vital in applications such as Cloud Computing, Internet of Things (IoT) Systems, and Artificial Intelligence (AI) Systems. The number of active IoT devices is projected to exceed 29 billion by 2030 [1], making secure data handling increasingly critical. IoT devices, which often manage sensitive information, are particularly vulnerable to risks such as identity theft, reputational damage, regulatory breaches, and financial loss [2]. The IoT enterprise market size is forecasted to grow at a compound annual growth rate (CAGR) of 19.4% to $483 billion from 2022 until 2027[1]. DBS Bank anticipates that IoT adoption will approach 100% within the next decade [3]. As the IoT market becomes one of the largest in consumer electronics, ensuring robust security measures for data access and storage will be essential to protect against these significant risks.

With the rapid growth of IoT applications, the risk of security breaches due to insecure data access, inauthentic and counterfeit devices is increasing. Although they are much more secure compared to conventional centralized IoT systems, there are still a lot of security risks in decentralized or distributed IoT systems which use blockchain or similar technologies. Fig. 1 illustrates the potential security risks in a typical centralized IoT System. Since most IoT devices detect and store their users' confidential data, the security of these devices is incredibly essential [4]. Moreover, the authenticity of each individual device is prone to several threats because most of the IoT devices are based on small and inexpensive processing chips without consideration of security challenges [5]. Not only that, but there have also been several cases of security breach due to the improper and unreliable security protocols of IoT Devices. Existing encryption and authentication systems for IoT devices rely on private and public-key cryptography. These systems require significant computational resources for key generation and must store security protocols in non-volatile memory [6]. Given that many IoT devices lack the necessary computing power for such tasks, implementing robust security and authentication protocols remains a challenge.

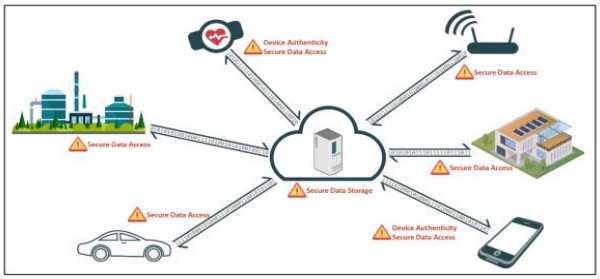

Fig. 1. Potential security risks in a typical centralized IoT System.

To address these issues, Physically Unclonable Functions (PUFs) offer a promising alternative. PUFs act as digital fingerprints for semiconductor devices, leveraging inherent physical variations in manufacturing to provide unique device identities. This approach eliminates the need for complex, power-intensive cryptographic algorithms while still offering strong security and authentication capabilities [7][8]. Research by Babaei and Schiele (2019) highlights that while PUFs present numerous advantages, challenges remain in their implementation [7]. Egowda and Thomas (2020) reviewed PUFs as key generators and emphasized their potential for cost-effective and reliable authentication. PUFs have been successfully integrated into microcontrollers and FPGAs, providing lightweight security solutions and supporting secure communication protocols [9][10]. Overall, PUFs represent a significant advancement in secure IoT systems, addressing the limitations of traditional

https://www.academicedgepub.co.uk/journals/journal-of-electrical-and-electronics-research-jeer
Received: 14-08-2024
Revised: 28-09-2024
Published: 26-10-2024

cryptographic methods and enhancing device security with minimal resource consumption.

II. SRAM Physical Unclonable Functions

The idea of using physical variations as a unique identity in electronic engineering was first proposed in 2002 by Gassend, B., et al [11,12]. But they did not use the term Physically Unclonable Functions; instead, they called them Silicon Random Functions. They showed that complex integrated circuits (ICs) can be represented as Silicon Random Functions which can be used to identify and authenticate those ICs. They also provided experimental results proving the reliability of identification and authentication using Field Programmable Gate Arrays (FPGAs). Their design performed well under various environmental conditions. Another research by Pappu, R., et al., describes random numerical functions based on physical variations in ICs which are easy to obtain but very difficult to reverse or clone using the term Physical One-Way functions [13]. They proposed the usage of mesoscopic physics of the physical medium in silicon chips instead of number theory for security and authentication protocols. Those functions can be applied in cryptography and authentication purposes. They also designed a simple and cost-effective authentication system as proof of concept. Their system managed to obtain a unique and stable identification key at incredibly low cost. The term Physical Unclonable Function (PUF) was coined by the same research group of Gassend, B., et al in their later publication in [14].

There are many different types of PUFs being researched. Most notable ones are Ring-Oscillator PUF, Arbiter PUF and SRAM PUF [15]. They can be classified into several categories using a categorization scheme based on their application, source of randomness (being implicit or explicit), family, and concept [16]. The application refers to the fact that the PUF system uses either all electronic design or hybrid design. For the second level of organization, the source of randomness refers to the randomness of PUF, which is either an implicit or explicit source. The implicit source has an intrinsic evaluation while the explicit source has an extrinsic evaluation. The classification of the PUFs can be time domain PUFs, memory based PUFs, Optical PUFs and so on. The categorization of different types of PUFs is shown in Fig. 2 [16]. The PUF types with the highest level of industry interest or the greatest number of research are denoted in bold type. Optical PUF is a transparent material that is doped with light scattering particles on which a laser beam shines to make a random and unique speckle pattern arise; time domain PUF such as ring oscillator PUF and arbiter PUF operates on variation in delay which are used mainly in complex systems such as FPGAs; memory based PUF derives responses based on the properties of the memory cell, which can be implemented by exploiting the existing SRAMs in simple microcontrollers [17, 18]; these include both the embedded SRAMs that reside on various microcontrollers as well as off-the-shelf SRAM chips. SRAM PUF is a popular memory-based PUF owing to SRAM being a standard component for most electronic devices.

A conventional SRAM cell is made of six or four transistors with an inverter loop. The schematic of a six-transistor SRAM cell is shown in Fig. 3 (a) and that of a four-transistor SRAM cell is shown in Fig. 3 (b). Although the manufacturing process of semiconductors is controlled very accurately, parameters such as threshold voltage, mobility, capacitance, and resistance of these transistors are distributed within some specified range [19]. These physical variations are too small to affect the correctness of a memory cell's function but large enough to cause different start-up behavior. The physical variations in size and shape of each SRAM cell can be seen clearly in the microscopic view of SRAM Cells from STM32F103 Microcontroller die in Fig. 4.

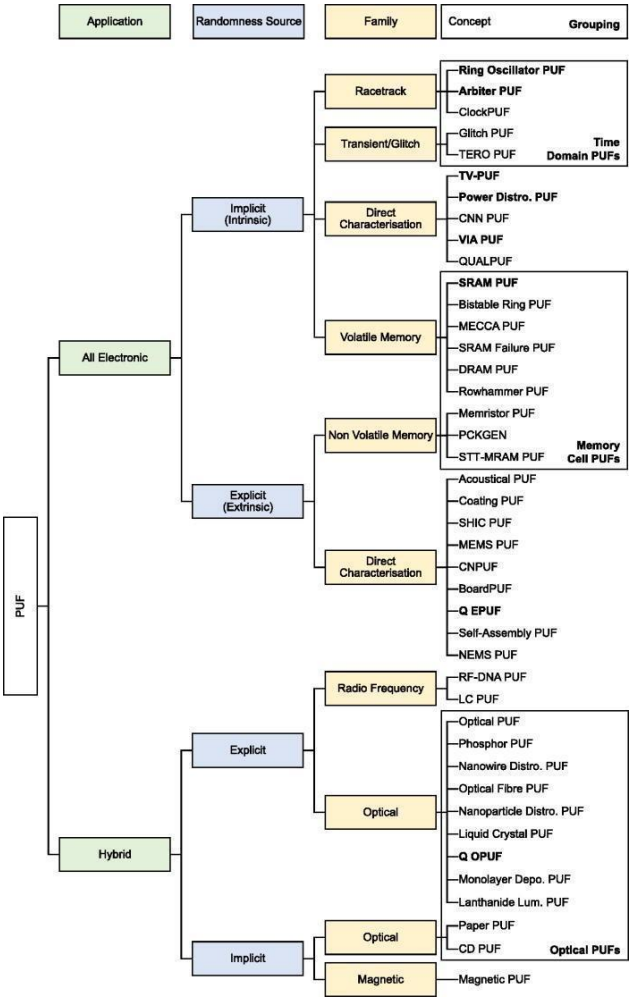

Fig. 2. Different Types of PUFs [16].

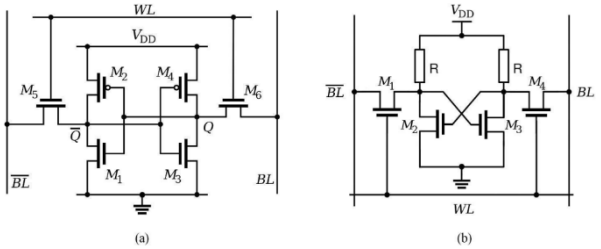

Fig. 3. (a) Schematic of a Six-Transistor SRAM Cell; (b) Schematic of a Four-Transistor SRAM Cell.

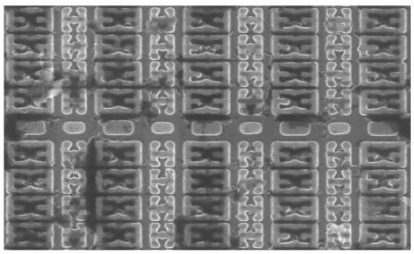

Fig. 4. Microscopic View of Actual SRAM Cells on STM32F103 Microcontroller.

SRAM PUFs utilize the initial state of each SRAM cell after start-up (power-up). When the SRAM receives power supply, the internal mismatch of transistors in each cell produces random and unpredictable data of '0' or '1' [20]. The random uninitialized data from all the SRAM cells together compose a unique identification key for the device. Once the initial data is acquired, the SRAM can be used again for the system. As the transistor sizes are becoming smaller and smaller in accordance with Moore's Law [21] for more complex and better operations, the variability in transistor performance increases significantly. In other words, the miniaturization of transistors in semiconductor chips leads to more variances in minimum threshold voltage Vth and other characteristics including mobility. Since the stability of the SRAM PUF is dependent on the variability of the transistors in each cell, the increase in the variability means an increase in the SRAM PUF performance [22]. This is because the wider variation means the operating margin of each SRAM memory cell is distributed more widely making them more consistent during the power up states [23]. SRAM PUF can be employed simply on a microcontroller for security and key generation without affecting its memory performance and behavior.

The concept of using SRAM start-up values as digital fingerprints for secure key generation was initially proposed by Holcomb et al. in 2007. They demonstrated that SRAM PUFs could generate 128-bit random numbers for cryptographic purposes from 256 bytes of SRAM using 160 different circuits. The SRAM PUFs were tested and found to meet various cryptographic standards [19]. In 2015, Van Aubel et al. explored the use of SRAM from AMD64 CPUs and Nvidia GPUs as PUF sources. They discovered that while AMD64 CPU registers exhibited non-random and non-fingerprint behavior, Nvidia GPUs showed promising potential for PUF applications, eliminating the need for external dedicated hardware [24]. A 2017 study by Wilde analyzed SRAM PUFs in 144 Infineon XMC4500 microcontrollers, each with 160 KB of SRAM. The study reported average results in Reliability, Bit-Alias, and Uniformity, and mid-range Uniqueness, consistent with findings from other microcontrollers [25]. Lipps et al. investigated SRAM PUFs using AtMega2560 Microcontrollers, assessing their entropy and the impact of environmental factors like temperature and supply voltage. Their results suggested that the AtMega2560 MCU is well-suited for security and authentication applications due to its reliable PUF characteristics [26].

However, the start-up values of SRAM do not always give the exact same PUF values, which are called unstable bits. The start-up conditions or the PUF's stability could be affected by temperature, supply voltage, and other environmental and external variations [27]. This is due to the nature of static memory and the voltage and current behavior of the CMOS SRAM chips. It also depends on the physical location of SRAM on the chip die [28]. In addition, since SRAM PUF makes use of small and variant mismatches that are inherent in circuit elements of individual chips, it is impossible to avoid errors and instabilities [29]. Some characteristics of SRAM PUF such as reducing Bit Error Rate (BER), stability, uniqueness and uniformity have been defined to evaluate the SRAM PUF responses, which can be used as a measure of the reliability and robustness of an SRAM PUF to be deployed in security systems. [30] proposed an SRAM PUF composed of 7T SRAM cells with noise immunity and performed BER benchmarking using 55nm CMOS chips. They verified the BER is 11 times lower than the 6T SRAM PUF. [31] suggested 8T cells using the 28 nm fully depleted silicon on insulator process and demonstrated the characteristics with respect to bit error rate (BER) as low as 0.72%.

III. Evaluation Metrics of SRAM PUFs

The Physically Unclonable Functions are usually described as Challenge Response Pairs (CRPs). The response (R) is the function (P) of the challenge (C). Hence, the PUF function can be represented as a Challenge-Response Pairs (CRPs) as shown in Equation 1.

$$R = P(C) \tag{1}$$

Different types of Physically Unclonable Functions (PUFs) use various methods to generate Challenge-Response Pairs (CRPs). For SRAM PUFs, the process is relatively straightforward. The challenge in SRAM PUFs is defined by the memory address and the bit position within the SRAM. For example, the challenge C could be a specific memory address and a particular bit location within that address. The response is the start-up binary value of the SRAM bit at the specified address. This value is obtained when the SRAM is powered on or initialized, revealing its inherent start-up state [32]. To collect CRPs, you first access the uninitialized SRAM to read the binary start-up values. This is typically done using a specialized program designed to retrieve a certain amount of data from specific memory addresses. For instance, the program might collect 64 bytes (512 bits) of data from a predefined range of addresses. The collected response values Rs are then stored along with their corresponding challenge addresses Cs in a database or file for subsequent analysis. This stored data can be used to assess the reliability, uniqueness, and other characteristics of the SRAM PUF. An example illustration of CRPs for SRAM PUFs is shown in Fig. 5.

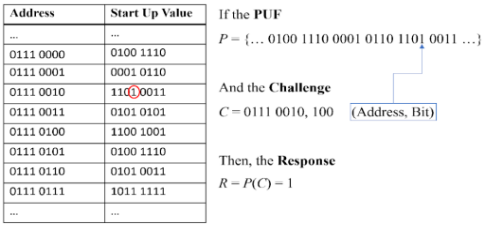

Fig. 5. An Example Illustration of CRPs for SRAM PUFs.

A. Error Rate

The error rate, *E* also known as Bit Error Rate (BER), quantifies the reliability of the PUF. It is calculated by determining the fraction of different bits between repeated measurements of the PUF response. The ideal error rate is 0%, meaning that every iteration of the PUF produces an identical binary stream. The difference in each bit of the R is called the Intra-distance D_{intra}. In other words, D_{intra} is the error bit of the response value R, and it can be used to get the error rate E of the SRAM PUF. The error rate E is sometimes abbreviated as Bit Error Rate (BER). The BER can determine whether the system is reliable enough to be used for security and authentication purposes. The ideal error rate is 0% where all the iterations of PUF produce the exact same binary stream. Equation 2 shows the error rate can be expressed as the fraction of the number of different bits over the total number of n bits in percentage.

$$E = \frac{D_{intra}}{n} \times 100\% \quad (2)$$

B. Uniqueness

Uniqueness in SRAM PUFs measures how distinct the response values are between different chips of the same type. This property is crucial for ensuring that each chip has a unique digital fingerprint, making it distinguishable from others. It can be represented using the value of Inter-distance D_{inter} which reflects how different the responses are between two chips of the same type. That can be evaluated by finding the difference between the response values obtained from different chips using the same challenge C. Uniqueness can be used to ascertain that a PUF stream is unique, and no other chip can produce the same value. In other words, it can be used to quantify how unique an SRAM PUF binary stream for a particular type of system is. The formula to calculate Dinter is presented in Equation 3.

$$D_{inter}(R_x, R_y) = \Delta(R_x, R_y) \quad (3)$$

Like error rate, the inter-distance of the PUF function can also be represented as the fraction of D_{inter} over the total number of bits *n* [33]. The fractional inter-distance *I* can be calculated using the formula given in Equation 4.

$$I(R_x, R_y) = \frac{\Delta(Rx,Ry)}{n} \quad (4)$$

Uniqueness can be used to ascertain that a PUF stream is unique. This ensures that no two chips produce the same response value for a given challenge, which is essential for applications requiring high security and distinct identification. In other words, it can be used to quantify how unique an SRAM PUF binary stream for a particular type of system is. It is a very important factor for the identification and authentication of chips. Since the SRAM PUF deals with binary values, the ideal uniqueness is 50% with zero standard deviation.

C. Uniformity

Uniformity is a key characteristic of PUFs that measures how balanced or biased a binary stream is towards '0's or '1's. This characteristic is crucial for assessing the randomness and quality of the PUF responses. It can be calculated as the ratio between the number of 0s and 1s in a stream of bits. It can determine how well-uniformed the PUF stream is. The uniformity or the bias of PUF is also known as Fractional Hamming Weight *W*. The ideal value of uniformity is 50% where the binary stream is well-uniformed and biased neither towards '1' nor towards '0'. Uniformity or the Fractional Hamming Weight *W can* be calculated using Equation 5.

$$W(R) = \frac{\#(i:R\neq 0)}{n} \quad (5)$$

D. Randomness

Randomness in a binary stream assesses how unpredictable or random the data is, which is crucial for evaluating the effectiveness of random number generators. The Binary Entropy Function, a form of Shannon Entropy, is used to quantify this randomness. The Binary Entropy Function is a type of Shannon Entropy, and it ranges from 0 (the least random value) to 1 (the most random value) [34]. It can be denoted as H(p) where p is the probability of the Fractional Hamming Weight W [35]. The formula for Randomness, H(p) is presented in Equation 6.

$$H(p) = p * log_2(p) - (1 - p) * log_2(1\text{-}p) \quad (6)$$

The graph for *H(p)* for all possible values of P is illustrated in Fig. 6. The randomness is the highest when the value of *p* is 0.5, which is when the uniformity is at its ideal value of 50%. When the PUF response is biased towards either 0 or 1, the randomness will be closer to zero.

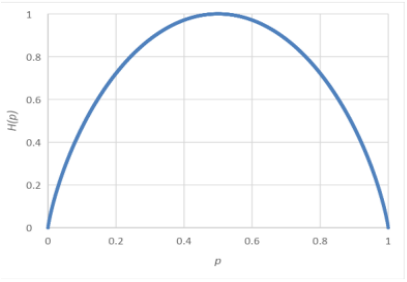

Fig. 6. Graph of *H(p)* for All Values of *p*.

E. Stability

Stability *S* of the SRAM PUF measures how consistent the PUF responses are over multiple iterations or different power cycles. It reflects the reliability of the PUF in maintaining the same response for the same challenge across various operations. Stability is also known as the steadiness of the PUF. In other words, it is the ratio between the number of the bits that never change their values throughout all iterations versus the total number of bits. It is also called the steadiness of the PUF. Stability can be represented as Equation (7).

$$S = \frac{\#(i:Ei=0)}{n} \quad (7)$$

Stability, together with the error rate, can determine the reliability and the repeatability of a PUF stream. The stability of as close to the ideal stability at 100% as possible is desired in reliable and robust systems.

IV. Categorization of SRAM PUFs Base on Robustness Improvement Techniques

Several research works have successfully demonstrated the potential of SRAM PUF and have shown that power-up values are useful as SRAM PUF response [36]. Wang et al. investigated the stability issues associated with SRAM PUFs and explored various power-on techniques to enhance their reliability for cryptographic applications. Their research focused on improving the consistency of SRAM PUF responses during power cycles by using different initialization methods [37]. Elshafiey et al. examined how the rising time of the power supply impacts the start-up values of SRAM PUFs. They implemented a 180nm Silicon Germanium Bipolar/CMOS (BiCMOS) SRAM and confirmed that variations in power supply characteristics can significantly affect the PUF's start-up behavior and stability [38]. Takeuchi et al. measured SRAM data following power-up for an addressable SRAM cell array. Their research revealed that factors such as address switching noise and memory effects can greatly influence SRAM PUF responses. They proposed methods to better characterize SRAM power-up behavior and improve the reliability and stability of the power-up state [39][40].

Several research works have successfully demonstrated the potential of SRAM PUF and have shown that power-up values are useful as SRAM PUF response but improvement needs to be done to optimize the stability and robustness of SRAM PUFs. This is important especially to produce the best security keys and true random number generations for security applications. The most common method to improve the stability and repeatability of SRAM PUF is using various Error Correction Codes (ECCs) or Fuzzy Extractors to minimize or eliminate the errors. SRAM PUFs could be categorized into six main categories based on the techniques of improving the SRAM power-on stability:

- PUF with error detection and correction;
- PUF with data extractors;
- Modified SRAM circuitry as PUF;
- SRAM PUF of various transistor technologies;
- SRAM PUF using stable bit selection.

A. PUF with Error Detection and Correction

There are several studies using various types of Error-correcting codes (ECCs) to reduce or eliminate the errors in different types of PUFs. ECCs are used to map the noisy PUF responses to codewords in a way that allows for error detection and correction. This process involves transforming the raw PUF response into a more stable PUF response. To correct errors in the PUF response, a helper data structure is used. This data is derived from the PUF golden responses and aids in correcting errors during the key reconstruction phase.

Kim et al. fabricated a chip with a power controller, circuits for error correction coding (ECC) module, a SRAM array and central processing unit in their work and pointed out that that using ECCs in SRAM PUF can reduce the error rate to less than 10^{-6}[42]. Chen, B., et al. researched on the uniqueness and intrinsic randomness of SRAM PUFs and discussed that they are the potential candidates for security and authentication of IoT devices. They stated that SRAM PUF suffered from noises and was affected by other environmental variations. They proposed to use the polar code ECC scheme for key generations. They managed to generate 128-bit keys using 1024 SRAM-PUF bits and 896 helper data bits and achieve a failure rate of lower than 10^{-9} with bit error probability of 15%. Moreover, they examined the adaptive list decoder for polar codes to increase the list size [43].

To simplify the ECC mechanism, [44] proposed to integrate error detection and hard masking methods where error detection detects the SRAM cells which produce erroneous outputs and hard masking excludes these cells from key generation. With the exclusion, this reduced the amount of data that needs to be protected by ECC and thus the helper data size.

Laban, M., and M. Drutarovsky., have done research on the improvement of SRAM PUF responses of a 32-bit microcontroller for cryptographic systems using Code Word Masking method. They proposed an improved Code Word Masking method for reconstruction of PUF response to maximize the PUF response size and to minimize requirements for the ECC. The modification resides in repeated encoding of one response. They managed to generate 140 bits using 512 PUF response bits without error, across various temperature and voltage levels [45].

ECC schemes are used not only for the improvement of error rates, but they are also used for aging related instabilities. Li, B., and S. Chen have used the Restrict Race Code (RRC) to prevent the aging effect on SRAM PUF. They used a dynamic PUF authentication method by combining software and hardware systems to improve the robustness of SRAM PUFs against aging. They implement the system on SRAMs of FPGAs and validate using Characteristic Value Challenge (CVC) randomness tests [46]. Neale, A. and M. Sachdev also proposed a hardware and software combination scheme for better SRAM PUF performance on 28nm CMOS SRAM. They combined majority voting and data integrity masking with custom circuit design to generate 100% reproducible PUF responses [47]. The combination of ECC and the specialized majority voting, namely two-stage temporary majority voting, as shown in [48] has further demonstrated the advantage of lower hardware overhead without compromising the performance of SRAM PUF.

In short, ECC is advantageous to improve the PUF's stability but apart from additional hardware, error corrections may require a lot of computation power and time, which is a challenge to deploy the ECC for PUF in IoT nodes. Additionally, they might contribute to leaking some of the information through the helper data of PUF which is supposed to be kept secret.

B. PUF with Data Extractors

There are three data extractors proposed so far to improve the robustness of SRAM PUF, namely Von Neumann extractor, Fuzzy extractor and Linear Shift Register extractor. The Von Neumann extractor is designed to extract uniform random bits from biased or correlated sources. It is particularly useful when the source bits are not perfectly random but have some level of bias or dependency. In short, this extractor improves the PUF's performance metrics of randomness and uniformity. On the other hand, a fuzzy extractor is designed to handle noisy or error-prone data

sources and produce stable and uniform outputs. This tool is used to improve PUF's performance metrics of stability and uniformity.

Liu, H., et al introduced an improved Von Neumann Extractor for error correction. The extractor processes pairs of bits of the raw SRAM PUF to produce uniformly distributed output bits, making it suitable for use with SRAM PUFs that have inherent biases or correlations. They achieved an error rate of less than 1% per bit and reduced the number of required responses by approximately 11/16, the amount of helper data by 2/3, and the number of masks by 3/8 compared to the original method [49].

Fuzzy extractors are designed to derive a stable, uniformly random key from noisy and variable PUF responses, using helper data to correct errors in future measurements. Ensuring that helper data does not leak sensitive information about the PUF challenge is crucial. Helper data should not allow unauthorized parties to infer the key or its structure. Therefore, A. Ali pour et al. introduced a PUF-based masking mechanism with variable positioning to enhance security; masking mechanism obfuscates the helper data from being exploited by attackers whereas variable positioning varies the position of masking bits based on other factors such as environment parameters to further strengthen the PUF's security [50].

The Code Word Masking construction for Physical Unclonable Functions (PUFs) in [51] introduces a novel way to enhance security and mitigate leakage risks by leveraging error correction codes (ECC) in the generation and handling of PUF responses. The masking method properly selects and masks PUF response bits based on the ECC code words to construct the helper data that does not leak information. Additionally, the helper data is obfuscated in a way that makes it difficult for an adversary to exploit. [52] practically demonstrated the integration of Physical Unclonable Functions (PUFs) and fuzzy extractors ensured secure communication between unmanned aerial vehicles (UAVs) and ground stations, as well as between UAVs themselves.

The SRAM PUF Linear Shift Register Extractor [53] is another data extractor which is an effective method for generating stable and secure cryptographic keys from SRAM PUFs. By using linear shift registers as an extractor, this technique extracts stable bits as PUF and improves the PUF's uniformity. The method eliminates the use of helper data which eliminates the risk of leaking information.

C. Modified SRAM Circuitry as PUF

An alternative method to produce more consistent or stable bits in PUF is by physically modifying to emphasize or amplify the variation. However, most of the modification techniques limit the modified SRAM cells for PUF usage only because the modification makes the memory read/write operation failures. Chang, C.-H., et al., proposed a method to solve the issues of amplifying the mismatch resulting in memory read/write failures. They designed a dual-mode SRAM cell optimization using word-line voltage modulation and dynamic voltage scaling to prevent SRAM PUFs from memory failures. They implemented their design on 45nm CMOS SRAM cells, and the analytic results showed improvements in SRAM PUF reliability while maintaining the ability to be used as normal SRAMs [22]. Other effective methods of SRAM cell modification for more stable SRAM PUF cells include (i) burning in the SRAM cells, (ii) manipulating the power supply voltage, (iii) altering the transistor level circuit design of the SRAM cells, and so on.

Liu, K., et al., obtained an error free SRAM PUF response by using Hot Carrier Injection (HCI) burn in process on the alternate direction NMOS. They achieved a 100% stable SRAM PUF with visible oxide damage without using additional fabrication processes or extra transistors in the SRAM cells. After going through a 21-year equivalent aging process, their design has an error rate of less than 1.0×10^{-7} [54]. They also have researched Enhancement-Enhancement (EE) SRAM PUF with a dark-bit detection technique. They used an integrated VSS-bias generator for improving the BER to less than 1.3×10^{-6} using supply voltage of 0.8 to 1.4 V under the temperature range from -40℃ to 120℃. They also implemented a 2D power-gating scheme for low operation energy, low standby power, and high attack tolerance [55].

Miller, A., et al. presented SRAM PUFs with an internal error reduction mechanism. They used a capacitive pre-selection test to detect unstable cells in one VDD / temperature corner. They implemented TSMC 65nm SRAM Chips with no impact on the randomness of the PUFs. They obtained a BER of 7.4×10^{-10} and an energy consumption of 16 fJ/bit [56].

Shifman, Y., et al., uses a modified SRAM PUF which is fabricated in TSMC 65-nm process. They proposed a new pre-selection test to remove all the unstable cells of SRAM PUF eliminating the need for ECCs [23]. They also fabricated an SRAM cell with two bits per cell response where only NMOS in the latch configuration responses. They then analyzed the Decision Voltage and measured the results [57]. Liu, C.Q., et al., also have introduced dual port (DP) SRAM to overcome the limited accessibility of conventional SRAMs and offer low power and high-speed memory transfer. Moreover, the DP-SRAM can generate two independent response bits per cell for better reliability, uniqueness, and randomness [58].

Mispan, M.S., et al., researched using instruction cache instead of on chip SRAM memory in 32-bit ARM Cortex M architecture. They also induced NBTI aging and claimed that their design can reduce the error rate from 14.18% to 5.58% in SRAM PUF resulting in reduced area overhead for ECC circuitry [59]. Lu, L., and T.T. Kim proposed a 2D sequence dependent SRAM PUF which uses the challenge response pairs by row and columns in SRAM arrays. They utilized horizontal word lines to connect four cells to generate 1-bit data. They achieved a BER of less than 3% with uniqueness of 49.7% and uniformity of 42.7% by using their design [60].

[61] improved the reliability and randomness of SRAM PUF by introducing a new timing control scheme that incorporates an additional NMOS transistor to address and eliminate the mismatches between the challenge and word-line inputs to both inverter arrays of the SRAM. [59] suggested to use a PMOS transistor as a power switch to ramp-up the SRAM cell voltage to supply voltage faster such that the cell is less susceptible to noise, leading to more stable PUF response. Shinohara, H., et al., proposed a method to reduce the BER of SRAM PUF by unbalancing the size ratio of PMOS and NMOS transistors for CMOS SRAMs. They increased the mismatch factor by unbalancing the transistor

size ratio hence reducing the BER by less than half of the original SRAM PUF [29].

Following some works analyzing memory aging factors such as the negative bias temperature instability (NBTI) of SRAMs to manipulate the SRAM PUF characteristics, [62] performed workload-aware aging analysis for On-Chip SRAMs to predict the performance degradation of the sense amplifiers in the memory. This analysis was then used in an aging-aware SRAM design exploration framework that optimized the SRAM PUF design in reliability. Similar work has been conducted in [63] which modelled the static noise margin of SRAM and performed the sensitivity analysis to optimize the SRAM cell design for better stability and reliability.

Zhang, H., et al. introduced a method to amplify the mismatch resulted from the pair of NMOS transistors of an SRAM cell through the cross-coupled invertor during the discharge process biased at the subthreshold region so that more stable SRAM PUF responses were obtained [64]. This is feasible by additional NMOS transistors as switch transistors to adjust the V_{gs} of the NMOS in the SRAM cell such that the voltage value is small enough to bias the cell in the subthreshold region.

Su Z. et al. proposed an 8T SRAM-based Physical Unclonable Function (PUF) to improve reliability and radiation tolerance. The enhancement involves adding two cascode PMOS transistors to a standard 6T SRAM cell. This design is particularly tested under various conditions using a 28 nm Fully Depleted Silicon on Insulator (FDSOI) process and obtained excellent uniqueness and BER as low as 0.72% [65]. The same researcher also proposed a 7T SRAM PUF with noise immunity; the structure can avoid the noise impact during the power-on transition period and amplify the mismatch voltage when entering a mono-stable sate before the bistable state, resulting a huge native BER reduction [66].

Garg, A., et al., presented a post fabrication SRAM PUF improvement method by exploiting the device aging to increase the mismatch between two cross coupled inverters. They increased the uniformity and reliability by using this method [67]. Vijayakumar, A., et al., proposed a design enhancement to improve the reliability and efficiency of SRAM PUF. They have generated a 128-bit SRAM PUF error rate of less than 10^{-6} using their proposed design [27].

Kim, M., et al. used the electromigration phenomenon on metal fuses for improved stability of SRAM PUFs. They programmed the start-up values of SRAM into the local metal fuses to improve the reliability and robustness of SRAM PUFs. They achieved 100% stable SRAM PUF cells by doing so [68]. Islam, M.N., proposed a new method to accelerate the device aging effectively. They used a low-cost proxy to measure the amount of mismatches for each chip during manufacturing and used previously proposed methods for device aging to accelerate the process. They managed to provide successful burn-in to obtain better reliability and more stable SRAM PUFs [69].

Clark, L.T., et al., proposed another method to modify the SRAM for better reliability. They used foundry cells by slightly modifying traditional SRAM cells for better PUF performance. They fabricated their design into large 1M-bit SRAM arrays on a 55-nm process using the foundry supplied SRAM cell layouts which amplify the transistor mismatch for lower error occurrence. They also discussed a way to eliminate the errors entirely by using helper data instead of other ECCs [70].

D. SRAM PUF of Various Transistor Technologies

Trujillo, J., et al. researched on implementing SRAM PUF on Silicon Germanium wafers and proved that their circuits are suitable for security purposes by evaluating randomness, hamming distance, uniqueness, and reliability [71].

Zhang, S., et al. proposed using Fin Field Effect Transistor (FinFET) SRAM PUFs as an alternative to conventional CMOS SRAM PUFs. They investigated the SNM of FinFET SRAM PUFs, finding it to be a critical factor in ensuring the reliability of these designs. They concluded that FinFET SRAM PUFs exhibit reasonable performance in terms of reliability compared to traditional CMOS SRAM PUFs [72]. Narasimham, B., et al. conducted research on 28nm and 16nm FinFET SRAM PUFs. They explored how well FinFET SRAM PUFs can withstand instabilities related to aging, a crucial factor for long-term reliability. Their findings indicated that FinFET SRAM PUFs can maintain stable performance despite the challenges associated with aging [73]. Further experiments in [74] concluded that using the evaluation technique of within class Hamming Distance for technology nodes 16nm, 14nm and 7nm, temperature variations have a marginal impact on the reliability, and both low-power and high-performance SRAMs can be used as a PUF without excessive need of error correcting codes (ECCs).

E. SRAM PUF using Stable Bit Selection

There are a few other methods being researched to obtain stable SRAM PUF cells by using other attributes of SRAM cells. Liao, Z. and Y. Guan conducted experiments to investigate spatial dependencies among SRAM cells, which can affect the stability and reliability of SRAM PUFs. They recommended strategies to mitigate unwanted dependency effects by carefully selecting SRAM cells to enhance the reliability of the power-up state [75]. Liao, Z., et al. explored the Discharge Inversion Effect (DIE) in SRAM chips and its impact on SRAM power-up behavior. Their study highlighted how this effect could influence data retention and stability. They provided procedural recommendations for more effective data collection to address these issues and improve SRAM PUF performance [76]. The same researcher shows the application of SRAM PUF in biometric authentication [77]. Alheyasat, A., et al. analyzed mismatch factors across different types of PUFs, including SRAM PUFs, and demonstrated the viability of robust methods for selecting stable PUF bits. Their research emphasized the importance of addressing mismatch issues to enhance the stability and robustness of PUF designs [78].

Vatajelu, E.I., et al. focused on enhancing the stability of SRAM PUF cells by leveraging the dynamic behavior of SRAM cells during power-up. They analyzed the dynamic evolution of SRAM cells during power up to identify which cells are the most stable. This method assesses how SRAM cells transition from their power-down state to their operational state and aims to identify cells that consistently demonstrate stable behavior. They eliminate the unstable SRAM PUF cells by identifying the symmetrical cells based on dynamic SRAM stability tests. Their simulation results proved that their method could improve the SRAM PUF

reliability without using ECCs and without modifying the SRAM cells [79].

Saraza-Canflanca, P., et al. identified the strongest SRAM PUF cells by manipulating supply voltage after writing values to the SRAM cells. Their method is because strong SRAM PUF cells flip faster when storing their non-preferred values. They wrote all the cells with '1's and reduced the supply voltage so that the weakest '1' cells can be eliminated. Then, all cells have been written with '0's and encountered a similar power reduction. By this way, the strongest '1' cells and strongest '0' cells can be identified for a more stable and more robust protection against aging and circuit degradation SRAM PUFs [80]. Lee, J., et al., have also used the power supply ramp up method in combination with controlling the evaluation region of SRAM cells, to obtain more stable SRAM PUFs. Their experimental results on 180 nm SRAM cells provided a decrease in error rate of 55.05% and increased in reproducibility of 2.2x [81].

Liu, W., et al., proposed a method to generate stable responses from SRAM PUF using Fourier analysis. They examined the Fourier Spectrums of the SRAM PUF binary responses to determine the power-up behavior of RAM cells [82]. By doing so, obtaining the sign-bits of Fourier coefficients at some frequency values. They used the sign-bits as stable random keys together with an encoding algorithm.

The preselection test for SRAM Physical Unclonable Functions (PUFs) was proposed in [83] that induced a temporary intentional skew, or "tilt," within SRAM cells to assess their stability to determine whether the mismatch inherent in the SRAM cells is strong enough to overcome the induced tilt, allowing for the reliable selection of stable cells for use in PUFs. Cells that demonstrate stability under tilt are selected as stable cells for the PUF response.

In [84], Park S. et al. identified and utilized the access transistors with the highest read current mismatch in adjacent SRAM cells as SRAM PUF response. This technique improves the reliability of the PUF by leveraging the most significant mismatches to ensure stable and consistent responses. [85] introduced a newly designed compact response instability detector that enhances the reliability of SRAM Physical Unclonable Functions (PUFs) by detecting occurrences of bit-flipping under identical challenges as unstable responses to be filtered out.

Data Remanence is one of the important bit selection techniques. SRAMs can retain the data for a few hundred milliseconds after the supply voltage is removed due to charge leakage in internal capacitance of transistors in SRAM cells. However, how much of the data that is retained after a certain time varies for different chips. It becomes necessary to find the best power off duration suitable for each type of chip if data remanence based PUF is used.

Data remanence is used along with binary search to assess and select the SRAM cells as the SRAM PUF response, providing a more consistent and reliable key generation process [86]. [87] proposed a method based on the Data Retention Voltage metric to select the cells with the most stable power-up response. Using these cells to generate the PUF identifier will result in a more stable response, and thus a better PUF performance.

V. CONCLUSION

In conclusion, research consistently shows that SRAM PUFs have great potential for security keys and true random number generation. Efforts to enhance their stability and reliability often involve fuzzy extractors, ECCs, or modifications to SRAM cell designs. While these methods improve stability, they can be costly or affect SRAM memory performance. Data remanence for selecting PUF bits is promising but also presents challenges, including time, computation demands, and variability in power-off duration. Research on optimal power-off times and SRAM PUFs in IoT microcontrollers is still limited.

ACKNOWLEDGMENT

The research is partially funded by Malaysian Ministry of Higher Education's Fundamental Research Grant Scheme (FRGS) with vote number FRGS/1/2022/TK07/UTM/02/23.

REFERENCES

[1] A. Hassebo and M. Tealab, 'Global Models of Smart Cities and Potential IoT Applications: A Review', IoT, vol. 4, no. 3, pp. 366–411, 2023.

[2] B. Liao, Y. Ali, S. Nazir, L. He and H. U. Khan, "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review," in IEEE Access, vol. 8, pp. 120331-120350, 2020.

[3] S. Mittal, W.T. Tam, and C. Ko, "*Internet of Things: The Pillar of Artificial Intelligence*," Report produced by Asian Insights Office: DBS Group, 2018.

[4] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," Sensors, vol. 20, no. 13, p. 3625, Jun. 2020.

[5] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021.

[6] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, 'A survey on physical unclonable function (PUF)-based security solutions for Internet of Things', Computer Networks, vol. 183, p. 107593, 2020.

[7] Babaei, Armin ; Schiele, Gregor, A. Babaei, and G. Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges," Sensors, vol. 19, no. 14, p. 3208, 2019.

[8] K. P. Egowda and S. Thomas, "A Detailed Review on Physical Unclonable Function Circuits for Hardware Security," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018, pp. 609-612.

[9] A. Balan, T. Balan, M. Cirstea, and F. Sandu, "A PUF-based cryptographic security solution for IoT systems on chip," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, Nov. 2020.

[10] D. Vinko, K. Miličević, I. Lukić, and M. Köhler, "Microcontroller-Based PUF for Identity Authentication and Tamper Resistance of Blockchain-Compliant IoT Devices," Sensors, vol. 23, no. 15, p. 6769, Jan. 2023.

[11] B. Gassend, D. R. Clarke, M. Van Dijk, and Srinivas Devadas, "Controlled physical random functions," Annual Computer Security Applications Conference, Dec. 2002.

[12] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, 'Silicon physical random functions', in Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2002, pp. 148–160.

[13] R. Pappu, "Physical One-Way Functions," Science, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[14] D. Lim, Lee, Blaise Gassend, G. Edward Suh, M. Van Dijk, and Srinivas Devadas, "Extracting secret keys from integrated circuits," IEEE Transactions on Very Large-Scale Integration Systems, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[15] K. Lounis and M. Zulkernine, “Lessons Learned: Analysis of PUF-based Authentication Protocols for IoT,” Digital Threats: Research and Practice, Sep. 2021.

[16] T. McGrath, I. Bagci, Z. Wang, U. Roedig, and R. Young, ‘A PUF taxonomy’, Applied Physics Reviews, vol. 6, p. 011303, 03 2019.

[17] S. Vinagrero, H. Martin, Alice de Bignicourt, Elena-Ioana Vatajelu, and Giorgio Di Natale, “SRAM-Based PUF Readouts,” Scientific Data, vol. 10, no. 1, May 2023.

[18] M. Laban and M. Drutarovsky, “Leakage free helper data storage in microcontroller based PUF implementation,” Microprocessors and Microsystems, p. 103369, Nov. 2020.

[19] D. E. Holcomb, W. P. Burleson, and K. Fu, ‘Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags’, 2007.

[20] A. Alheyasat, G. Torrens, S. A. Bota, and B. Alorda, ‘Estimation during Design Phases of Suitable SRAM Cells for PUF Applications Using Separatrix and Mismatch Metrics’, Electronics, vol. 10, no. 12, 2021.

[21] S. E. Thompson and S. Parthasarathy, “Moore’s law: the future of Si microelectronics,” Materials Today, vol. 9, no. 6, pp. 20–25, Jun. 2006.

[22] C.-H. Chang, Chao Qun Liu, L. Zhang, and Zhi Hui Kong, “Sizing of SRAM Cell with Voltage Biasing Techniques for Reliability Enhancement of Memory and PUF Functions,” Journal of Low Power Electronics and Applications, vol. 6, no. 3, pp. 16–16, Aug. 2016.

[23] Y. Shifman, A. Miller, O. Keren, Yoav Weizmann, and J. Shor, “A Method to Improve Reliability in a 65-nm SRAM PUF Array,” IEEE Solid-State Circuits Letters, vol. 1, no. 6, pp. 138–141, Jun. 2018.

[24] P. Van Aubel, D. J. Bernstein, and R. Niederhagen, ‘Investigating SRAM PUFs in large CPUs and GPUs’, in Security, Privacy, and Applied Cryptography Engineering, 2015, pp. 228–247.

[25] F. Wilde, “Large scale characterization of SRAM on infineon XMC microcontrollers as PUF,” Jan. 2017.

[26] C. Lipps, A. Weinand, D. Krummacker, C. Fischer, and H. D. Schotten, “Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU,” Apr. 2018.

[27] W. Wang, A. D. Singh, and U. Guin, “A Systematic Bit Selection Method for Robust SRAM PUFs,” Journal of Electronic Testing, vol. 38, no. 3, pp. 235–246, Jun. 2022.

[28] S. Elgendy and E. Y. Tawfik, "Impact of Physical Design on PUF Behavior: A Statistical Study," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 2021, pp. 1-5.

[29] Shinohara, H., et al. Analysis and reduction of SRAM PUF Bit Error Rate. In 2017 International Symposium on VLSI Design, Automation and Test (VLSI-DAT). 2017.

[30] Z. Su et al., "SRAM-Based PUF with Noise Immunity Achieving 0.58% Native BER in 55-nm CMOS," 2024 IEEE International Symposium on Circuits and Systems (ISCAS), Singapore, Singapore, 2024, pp. 1-5.

[31] Z. Su et al., "Reliability Improvement on SRAM Physical Unclonable Function (PUF) Using an 8T Cell in 28 nm FDSOI," in IEEE Transactions on Nuclear Science, vol. 69, no. 3, pp. 333-339, March 2022.

[32] Aung, P.P., et al., Evaluation of SRAM PUF Characteristics and Generation of Stable Bits for IoT Security, in Emerging Trends in Intelligent Computing and Informatics. 2020. p. 441-450.

[33] M. Deutschmann, Lejla Iriskic, Sandra-Lisa Lattacher, M. Münzer, F. Stornig, and Oleksandr Tomashchuk, “Research on the Applications of Physically Unclonable Functions within the Internet of Things,” Aug. 2018.

[34] S. Larimian, M. R. Mahmoodi, and D. B. Strukov, ‘Lightweight integrated design of PUF and TRNG security primitives based on eFlash memory in 55-nm CMOS’, IEEE Transactions on Electron Devices, vol. 67, no. 4, pp. 1586–1592, 2020.

[35] Schaub, A., O. Rioul, and J.J. Boutros. Entropy Estimation of Physically Unclonable Functions via Chow Parameters. in 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton). 2019.

[36] P. Saraza-Canflanca, H. Carrasco-Lopez, P. Brox, R. Castro-Lopez, E. Roca and F. V. Fernandez, "Improving the reliability of SRAM-based PUFs in the presence of aging," 2020 15th Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Marrakech, Morocco, 2020, pp. 1-6.

[37] W. Wang, A. Singh, U. Guin, and A. Chatterjee, “Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs,” Mar. 2018.

[38] A. T. Elshafiey, Payman Zarkesh-Ha, and J. Trujillo, “The effect of power supply ramp time on SRAM PUFs,” UNM’s Digital Repository (University of New Mexico), Aug. 2017.

[39] K. Takeuchi, T. Mizutani, Takuya Saraya, M. Kobayashi, T. Hiramoto, and H. Shinohara, “Measurement of SRAM power-up state for PUF applications using an addressable SRAM cell array test structure,” International Conference on Microelectronic Test Structures, Mar. 2016.

[40] K. Takeuchi, T. Mizutani, H. Shinohara, Takuya Saraya, M. Kobayashi, and T. Hiramoto, “Measurement of Static Random-Access Memory Power-Up State Using an Addressable Cell Array Test Structure,” IEEE Transactions on Semiconductor Manufacturing, vol. 30, no. 3, pp. 209–215, Aug. 2017.

[41] Handschuh, H. Hardware intrinsic security based on SRAM PUFs: Tales from the industry. in 2011 IEEE International Symposium on Hardware-Oriented Security and Trust. 2011.

[42] M.-S. Kim et al., “Error reduction of SRAM-based physically unclonable function for chip authentication,” International Journal of Information Security, vol. 22, no. 5, pp. 1087–1098, Feb. 2023.

[43] Chen, B., et al. A Robust SRAM-PUF Key Generation Scheme Based on Polar Codes. in GLOBECOM 2017 - 2017 IEEE Global Communications Conference. 2017.

[44] S. S. Kudva et al., "16.4 High-Density and Low-Power PUF Designs in 5nm Achieving 23× and 39× BER Reduction After Unstable Bit Detection and Masking," 2024 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 2024, pp. 302-304.

[45] M. Laban and Milos Drutarovsky, “Improved Efficiency of PUF Response Reconstruction Method,” Apr. 2020.

[46] Li, B. and S. Chen, *A dynamic PUF anti-aging authentication system based on restrict race code*. Science China Information Sciences, 2015. 59(1): p. 1-12.

[47] Neale, A. and M. Sachdev. A low energy SRAM-based physically unclonable function primitive in 28 nm CMOS. in 2015 IEEE Custom Integrated Circuits Conference (CICC). 2015.

[48] Yue, M. (2024). A Two-Stage TMV SRAM PUF Preselection Method with Fewer ECC Resources. 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 7, 528–533.

[49] Liu, H., et al., *Methods for Estimating the Convergence of Inter-Chip Min-Entropy of SRAM PUFs.* IEEE Transactions on Circuits and Systems I: Regular Papers, 2018. 65(2): p. 593-605.

[50] A. Ali Pour et al., "Helper Data Masking for Physically Unclonable Function-Based Key Generation Algorithms," in IEEE Access, vol. 10, pp. 40150-40164, 2022.

[51] M. Laban and M. Drutarovsky, “Leakage free helper data storage in microcontroller based PUF implementation,” Microprocessors and Microsystems, p. 103369, Nov. 2020.

[52] R. Karmakar, G. Kaddoum and O. Akhrif, "A PUF and Fuzzy Extractor-Based UAV-Ground Station and UAV-UAV Authentication Mechanism With Intelligent Adaptation of Secure Sessions," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 3858-3875, May 2024.

[53] M. Gong, H. Zhang, C. Wang, Q. Tong, and Z. Liu, “Design and implementation of robust and low-cost SRAM PUF using PMOS and linear shift register extractor,” Microelectronics Journal, vol. 103, pp. 104844–104844, Sep. 2020.

[54] K. Liu, X. Chen, H. Pu and H. Shinohara, "A 0.5-V Hybrid SRAM Physically Unclonable Function Using Hot Carrier Injection Burn-In for Stability Reinforcement," in IEEE Journal of Solid-State Circuits, vol. 56, no. 7, pp. 2193-2204, July 2021.

[55] Liu, K., et al. A 373 F2 2D Power-Gated EE SRAM Physically Unclonable Function With Dark-Bit Detection Technique. in 2018 IEEE Asian Solid-State Circuits Conference (A-SSCC). 2018.

[56] Miller, A., et al. A Highly Reliable SRAM PUF with a Capacitive Preselection Mechanism and pre-ECC BER of 7.4E-10. in 2019 IEEE Custom Integrated Circuits Conference (CICC). 2019.

[57] Shifman, Y., et al. An SRAM PUF with 2 Independent Bits/Cell in 65nm. In 2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019.

[58] Liu, C.Q., Y. Zheng, and C. Chang. A new write-contention based dual-port SRAM PUF with multiple response bits per cell. in 2017 IEEE International Symposium on Circuits and Systems (ISCAS). 2017.

[59] Mispan, M.S., et al., *A reliable PUF in a dual function SRAM*. Integration, 2019. 68: p. 12-21.

[60] L. Lu, T. Yoo and T. T. -H. Kim, "A 6T SRAM Based Two-Dimensional Configurable Challenge-Response PUF for Portable Devices," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 6, pp. 2542-2552, June 2022.

[61] Van Khanh Pham, Chi Trung Ngo, J.-W. Nam, and J.-P. Hong, "A Reconfigurable SRAM CRP PUF with High Reliability and Randomness," Electronics, vol. 13, no. 2, pp. 309–309, Jan. 2024.

[62] A. Listl, D. Mueller-Gritschneder, U. Schlichtmann and S. R. Nassif, "SRAM Design Exploration with Integrated Application-Aware Aging Analysis," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 2019, pp. 1249-1252.

[63] Shayesteh Masoumian, Georgios Selimis, R. Maes, Geert-Jan Schrijen, Said Hamdioui, and Mottaqiallah Taouil, "Modeling Static Noise Margin for FinFET based SRAM PUFs," Data Archiving and Networked Services (DANS), May 2020.

[64] H. Zhang et al., "A Dynamic Highly Reliable SRAM-Based PUF Retaining Memory Function," Research Portal (Queen's University Belfast), May 2021.

[65] Z. Su et al., "Reliability Improvement on SRAM Physical Unclonable Function (PUF) Using an 8T Cell in 28 nm FDSOI," in IEEE Transactions on Nuclear Science, vol. 69, no. 3, pp. 333-339, March 2022.

[66] Su Z, Li B, Liu C, et al. SRAM-Based PUF with Noise Immunity Achieving 0.58% Native BER in 55-nm CMOS. In: 2024 IEEE International Symposium on Circuits and Systems (ISCAS), 2024:1-5.

[67] Garg, A., et al., Improving uniformity and reliability of SRAM PUFs utilizing device aging phenomenon for unique identifier generation. Microelectronics Journal, 2019. 90: p. 29-38.

[68] Kim, M., et al. Leveraging Circuit Reliability Effects for Designing Robust and Secure Physical Unclonable Functions. in 2019 IEEE International Electron Devices Meeting (IEDM). 2019.

[69] Islam, M.N., V.C. Patil, and S. Kundu, *On Enhancing Reliability of Weak PUFs via Intelligent Post-Silicon Accelerated Aging.* IEEE Transactions on Circuits and Systems I: Regular Papers, 2018. 65(3): p. 960-969.

[70] Clark, L.T., et al., *Physically Unclonable Functions Using Foundry SRAM Cells.* IEEE Transactions on Circuits and Systems I: Regular Papers, 2019. 66(3): p. 955-966.

[71] Trujillo, J., C. Merino, and P. Zarkesh-Ha. SRAM Physically Unclonable Functions Implemented on Silicon Germanium. in 2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019.

[72] Zhang, S., et al. Evaluation and optimization of physical unclonable function (PUF) based on the variability of FinFET SRAM. in 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC). 2017.

[73] Narasimham, B., et al. SRAM PUF quality and reliability comparison for 28 nm planar vs. 16 nm FinFET CMOS processes. in 2017 IEEE International Reliability Physics Symposium (IRPS). 2017.

[74] Masoumian, S., Selimis, G., Wang, R., Schrijen, G.-J., Hamdioui, S., & Taouil, M. *Reliability Analysis of FinFET-Based SRAM PUFs for 16nm, 14nm, and 7nm Technology Nodes*. 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2022. 1189–1192.

[75] Liao, Z. and Y. Guan. The Cell Dependency Analysis on Learning SRAM Power-Up States. in 2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). 2018.

[76] Liao, Z., et al. The impact of discharge inversion affects learning SRAM power-up statistics. in 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). 2017.

[77] Z. Liao and Y. Guan, 'Rudba: Reusable user-device biometric authentication scheme for multi-service systems', in 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2021, pp. 214–225.

[78] Alheyasat, A., et al. Weak and Strong SRAM cells analysis in embedded memories for PUF applications. in 2019 XXXIV Conference on Design of Circuits and Integrated Systems (DCIS). 2019.

[79] Elena Ioana Vatajelu, Giorgio Di Natale, and P. Prinetto, "Towards a Highly Reliable SRAM-based PUFs," HAL (Le Centre pour la Communication Scientifique Directe), Jan. 2016.

[80] Saraza-Canflanca, P., et al. Improving the reliability of SRAM-based PUFs in the presence of aging. in 2020 15th Design & Technology of Integrated Systems in Nanoscale Era (DTIS). 2020.

[81] J. Lee, D.-W. Jee, and D. Jeon, 'Power-up control techniques for reliable SRAM PUF', IEICE Electron. Express, vol. 16, p. 20190296, 2019.

[82] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng and Z. Liu, "A Novel Security Key Generation Method for SRAM PUF Based on Fourier Analysis," in IEEE Access, vol. 6, pp. 49576-49587, 2018.

[83] Y. Shifman, A. Miller, O. Keren, Y. Weizman and J. Shor, "A Method to Utilize Mismatch Size to Produce an Additional Stable Bit in a Tilting SRAM-Based PUF," in IEEE Access, vol. 8, pp. 219137-219150, 2020.

[84] S. Park, M. Jeong, J. Kim, D. Kim and Y. Lee, "A 6T-SRAM-Based Physically-Unclonable-Function with Low BER Through Automated Maximum Mismatch Detection," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 71, no. 7, pp. 3493-3497, July 2024

[85] S. Baek, G. -H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian and J. -P. Hong, "A Reconfigurable SRAM Based CMOS PUF With Challenge to Response Pairs," in IEEE Access, vol. 9, pp. 79947-79960, 2021

[86] Pyi Phyo Aung, Nordinah Ismail, Chia Yee Ooi, Koichiro Mashiko, Hau Sim Choo, and Takanori Matsuzaki, "Data Remanence Based Approach towards Stable Key Generation from Physically Unclonable Function Response of Embedded SRAMs using Binary Search", *J. Adv. Res. Appl. Sci. Eng. Tech.*, vol. 35, no. 2, pp. 114–131, Dec. 2023.

[87] A. Santana-Andreo, P. Saraza-Canflanca, R. Castro-Lopez, E. Roca, and F. V. Fernandez, "Reliability improvement of SRAM PUFs based on a detailed experimental study into the stochastic effects of aging," AEU - International Journal of Electronics and Communications, vol. 176, pp. 155147–155147, Mar. 2024.