mathematics

MDPI

Review

Advances in Physical Unclonable Functions Based on New Technologies: A Comprehensive Review

Yuan Cao [1], Jianxiang Xu [1], Jichun Wu [1], Simeng Wu [1], Zhao Huang [2,*] and Kaizhao Zhang [1]

[1] College of Information Science and Engineering, Hohai University, Changzhou 213200, China; caoyuan0908@mail.com (Y.C.); 2162910213@hhu.edu.cn (J.X.); 2162310203@hhu.edu.cn (J.W.); 2162910107@hhu.edu.cn (S.W.); zkz990101@163.com (K.Z.)

[2] Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China

* Correspondence: z_huang@xidian.edu.cn; Tel.: +86-1879-261-0378

Abstract: A physical unclonable function (PUF) is a technology designed to safeguard sensitive information and ensure data security. PUFs generate unique responses for each challenge by leveraging random deviations in the physical microstructures of integrated circuits (ICs), making it incredibly difficult to replicate them. However, traditional silicon PUFs are now susceptible to various attacks, such as modeling attacks using conventional machine learning techniques and reverse engineering strategies. As a result, PUFs based on new materials or methods are being developed to enhance their security. However, in the realm of survey papers, it has come to our attention that there is a notable scarcity of comprehensive summaries and introductions concerning these emerging PUFs. To fill this gap, this article surveys PUFs based on novel technologies in the literature. In particular, we first provide an insightful overview of four types of PUFs that are rooted in advanced technologies: bionic optical PUF, biological PUF, PUF based on printed electronics (PE), and PUF based on memristors. Based on the overview, we further discuss the evaluation results of their performance based on specific metrics and conduct a comparative analysis of their performance. Despite significant progress in areas such as limited entry and regional expertise, it is worth noting that these PUFs still have room for improvement. Therefore, we have identified their potential shortcomings and areas that require further development. Moreover, we outline various applications of PUFs and propose our own future prospects for this technology. To sum up, this article contributes to the understanding of PUFs based on novel technologies by providing an in-depth analysis of their characteristics, performance evaluation, and potential improvements. It also sheds light on the wide range of applications for PUFs and presents enticing prospects for future advancements in this field.

Keywords: physical unclonable function; advanced materials; hardware security; IoT; authentication

MSC: 68Q06; 94C11; 94C12

Citation: Cao, Y.; Xu, J.; Wu, J.; Wu, S.; Huang, Z.; Zhang, K. Advances in Physical Unclonable Functions Based on New Technologies: A Comprehensive Review. *Mathematics* **2024**, *12*, 77. https://doi.org/10.3390/math12010077

Academic Editor: Theodore E. Simos

Received: 13 November 2023
Revised: 8 December 2023
Accepted: 21 December 2023
Published: 25 December 2023

1. Introduction

In the era of the Internet of Things (IoT), the world has a vast number of interconnected entities. At this point, the number of interconnected physical entities is still increasing exponentially, accompanied by the generation of vast amounts of data daily, presenting severe challenges to information security [1]. Recent cyberattacks have resulted in significant data breaches at governmental and private organizations on a global scale [2].

Mainly, the contemporary cryptographic primitives that most authentication methods rely on are based on mathematical one-way functions like hash algorithms and the discrete logarithm problem [3]. Initially, research showed that they were susceptible to security vulnerabilities [4], but it was not until recent developments that this issue was truly exposed. Therefore, it became imperative to develop highly secure cryptographic primitives to enhance information security.

Then, physical unclonable functions (PUFs) appeared, which were highly anticipated to provide stable information security. Initially, Pappu et al. [5] came up with the concept of PUF when studying the physical microstructure in silicon integrated circuits (ICs) and discovering that process changes during manufacturing can be used to generate unique responses. PUFs can be thought of as the "fingerprint" of each IC because they are intrinsic, non-replicable, and unpredictable. In stark contrast to conventional mathematical one-way functions, PUFs provide fundamental security benefits by functioning autonomously, eliminating the need for number-theory-based methods, making it exceedingly challenging to replicate a PUF.

The fundamental concept behind PUFs is that, when provided with an input, referred to as a 'challenge', the PUF generates an output, known as a 'response'. PUFs' physical characteristics are subject to random variations in each IC, resulting in different behaviors for each PUF. Thus, for the same challenge, different PUFs will generate different responses, while, for an ideal PUF, the same challenge will generate the same response (within a certain margin of error). In this manner, each PUF possesses a distinct set of challenge–response pairs (CRPs), as illustrated in Figure 1, which can be utilized for identification or verification purposes. Moreover, we can see the PUFs' principles of defense from Figure 2. When a device containing a PUF is running, the PUF requires authentication, which matches the generated response with a set of data generated by the device in a trusted environment. Each incentive challenge is randomly selected and has never been used, so the attacker cannot predict and achieve the attack purpose.

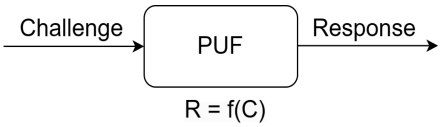


Figure 1. The challenge–response pairs (CRPS).

Figure 2. The PUFs' principles of defense.

There are several classification methods for PUFs based on the manufacturing process, including silicon PUFs and non-silicon PUFs. Based on the number of CRPs, they can be divided into strong PUFs and weak PUFs. The number of CRPs generated by the former is exponential, while the latter's is linear. Strong PUFs can be used for purposes such as authentication and generating secret keys, while weak PUFs can be used as identities or as mechanisms to participate in key protection. Strong PUFs have complex challenge–response behavior, where the response to new challenges cannot be predicted. The most important requirement for a PUF type to be a powerful PUF is to be able to generate a large amount of CRPs, and an attacker cannot build a model that can simulate them. A weak PUF has strong resistance to modeling attacks but is vulnerable to invasive attacks, side channel attacks, and virus attacks.

There are three major silicon PUFs defined by the physical features that generate them. They are analog electronic PUFs, memory-based PUFs, and delay-based PUFs as shown in Table 1 [6].

Table 1. Three major silicon PUFs.

Category	Type	Scheme
Analogue/Mixed		ICID-PUF, SNK-PUF, C-PUF, LC-PUF, PG-PUF, CN-PUF, ULPC-PUF, SHIC PUF, PUF-FSM, NEM-PUF, MV-L-PUF, ...
Digital	Delay-based	A-PUF, RO-PUF, G-PUF, IP-PUF, Clock PUF,SC-PUF,PE-PUF, MC-PUF, TERO-PUF, ...
	Memory-based	S-PUF, B-PUF, SR-L-PUF, FF-PUF, BR-PUF, M-PUF, ...

- **Analog/mixed signal PUF:** PUF units in this category include analog measurements of electrical or electronic quantities. Analog electronic PUFs mainly include ICID-PUF, Coating PUF, LC-PUF, and Power Grid PUF. Analog electronic PUFs are designed to provide fingerprints to circuits, which makes them more suitable for use as identities.
- **Memory-based PUF:** This PUF category focuses on memory element mismatches that result in random values in the boot state. These PUFs are based on storage units and are usually available in FPGAs. Memory chips in circuits can be used to generate signatures and identities for those circuits. Static RAM PUF (SRAM PUF) and butterfly PUF are two representative types of memory-based PUFs.
- **Delay-based PUF:** The main focus of delay-based PUFs is the propagation delay utilizing the circuit path and how quickly the microelectronics circuit can switch the output to 0 or 1. Delay-based PUFs mainly include arbiter PUF, ring oscillator (RO) PUF, glitch PUF, IP-PUF, etc.

Some researchers have reviewed these existing silicon PUFs. For example, Mall et al. summarized the relevant content of PUF-based authentication and key agreement protocols [7], while Dey et al. detailed how PUFs solve the security issues in modern development of IoT devices [8].

Nevertheless, silicon PUFs come with their own set of constraints and disadvantages. For example, silicon PUFs may be at risk of reverse engineering attacks; the proliferation of reverse engineering strategies has created new challenges and hazards [9]. In addition, endeavors involving reverse engineering have been put forth to test the resilience of established PUFs [10]. Moreover, PUFs often exhibit concerns including limited entropy, increased power consumption, and regional inefficiencies.

Fortunately, the decline of silicon PUFs affects and catalyzes the expansion of PUF technology centered around new materials and devices. PUFs based on novel materials, such as PUFs exploiting T cells, have been introduced, which make use of the inherent randomness in populations of colonized T cells [11]. Meanwhile, certain research focuses on resembling fingerprint-like features through the utilization of random surface patterns, such as micro–nano architectures molded from common plant tissues [12]. Also, innovative-technologies-based PUFs exist, such as PUFs based on printed electronics (PE), which exploit the inherent randomness and variability stemming from the material's surface roughness and morphology [13]. Additionally, a noteworthy accomplishment in the realm of PUFs involves the utilization of personal electrocardiogram (ECG) signals, as demonstrated in the study by Yin et al. [14]. This innovative approach capitalizes on individual ECG signals, extracting maximum ECG features for different individuals while minimizing time-variant ECG features for the same individual. Moreover, PUFs also encompass those based on memristors, which exploit the analog or digital characteristics inherent to these components.

Moreover, drawing inspiration from the achievements of silicon PUFs, Li and colleagues initiated groundbreaking research aimed at creating the inaugural series of genetic

PUFs residing within human cells [15]. Their pioneering research effectively incorporated PUFs into human cells, representing a significant application of PUFs across various domains, which also demonstrates that CRISPR-engineered PUFs (CRISPR-PUFs) can play a fundamental role in the development of reliable provenance attestation protocols.

1.1. Motivation

In the realm of survey papers, it has come to our attention that there is a notable scarcity of comprehensive summaries and introductions concerning these emerging PUFs. As mentioned earlier, the reviews conducted by these researchers did not involve the generalization of new materials or methods. To bridge this knowledge gap, our paper aims to provide an insightful overview of four distinct PUF types rooted in advanced technologies. Our objective is to stimulate fresh avenues of research, whether they stem directly from the methods expounded in this paper or draw inspiration from them to explore new research trajectories. We aim to seamlessly integrate these additional considerations with the existing content to offer a comprehensive and forward-thinking perspective.

1.2. Organization

In Section 2, we introduce the metrics for evaluating PUF performance and the formulas that can be used. In Section 3, we provide an insightful overview of four types of PUFs that are rooted in advanced technologies: bionic optical PUFs, biological PUFs, PUFs based on printed electronics, and PUFs based on memristors. In Section 4, we discuss the evaluation results of their performance based on specific metrics and conduct a comparative analysis of their performance. In Section 5, we discuss their potential shortcomings and areas that require further development. Moreover, we have outlined various applications of PUFs in Section 6. Finally, the conclusion and future prospects are presented in Section 7.

2. Metrics

There are several metrics for evaluating PUFs. While the names of these metrics may vary among different articles, they often represent similar concepts or meanings:

- **Randomness:** randomness denotes the inherent property of unpredictability and absence of patterns in the generated responses to challenges, ensuring that PUF outputs appear statistically random and cannot be easily replicated or predicted. The randomness evaluation of a PUF often involves the calculation of entropy, provided by the formula

$$H(X) = -\sum_{i=1}^{n} P(x_i) \cdot \log_2 P(x_i) \tag{1}$$

  where

  $H(X)$: Entropy, measuring the uncertainty or randomness of the system.
  n: Number of different events in the sample space.
  $P(x_i)$: Probability of event x_i occurring.

- **Reproducibility:** reproducibility characterizes a PUF by its consistent behavior, where each challenge generates a unique response that remains constant over time, ensuring that the same challenge consistently yields the same response. The formula for evaluating the reproducibility of a PUF involves calculating the variance, provided by

$$\mathrm{Var}(X) = \frac{1}{n}\sum_{i=1}^{n}(X_i - \bar{X})^2 \tag{2}$$

  where

  $\mathrm{Var}(X)$: Variance, a measure of the spread of the PUF responses.
  n: Number of measurements or trials.
  X_i: Individual PUF measurement or response.
  $\bar{X}$: Mean of the PUF measurements.

- **Unclonability:** unclonability represents a fundamental quality in a PUF, ensuring that, when a cloned system generates a response to a specific challenge, it is distinctly different from an authentic system's response, with differences not attributable to noise or environmental factors. The unclonability metric:

$$U = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{M}\sum_{j=1}^{M}\delta(f(a_i), f(b_j)) \tag{3}$$

where

U: Unclonability metric, indicating the resistance against cloning.
N: Number of pairs of distinct challenges.
M: Number of responses for each challenge.
a_i, b_j: Different challenge–response pairs.
$f(\cdot)$: PUF response function.
$\delta(\cdot,\cdot)$: Delta function, outputting 1 if the inputs are equal, 0 otherwise.

- **Reconfigurability:** reconfigurability refers to the inherent property of a PUF wherein it possesses the capability to undergo a transformation, rendering the CRPs of the altered PUF entirely unpredictable and uncorrelated with those of the original PUF. The reconfigurability of a PUF can be assessed using the coefficient of variation (CV) calculated as follows:

$$\text{CV} = \frac{\sigma}{\mu} \times 100 \tag{4}$$

where

CV: Coefficient of Variation, measures the relative variability of the PUF responses under different configurations.
σ: Standard deviation of the PUF responses.
μ: Mean (average) of the PUF responses.

- **Robustness:** robustness represents the ability of a PUF to maintain its functionality and produce reliable responses despite variations in operating conditions, environmental factors, or minor manufacturing discrepancies, ensuring its resilience and consistent performance. The robustness of a PUF is often assessed using the bit stability metric, defined as

$$\text{Bit Stability} = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{L}\sum_{j=1}^{L}\delta(b_{i,j}) \tag{5}$$

where

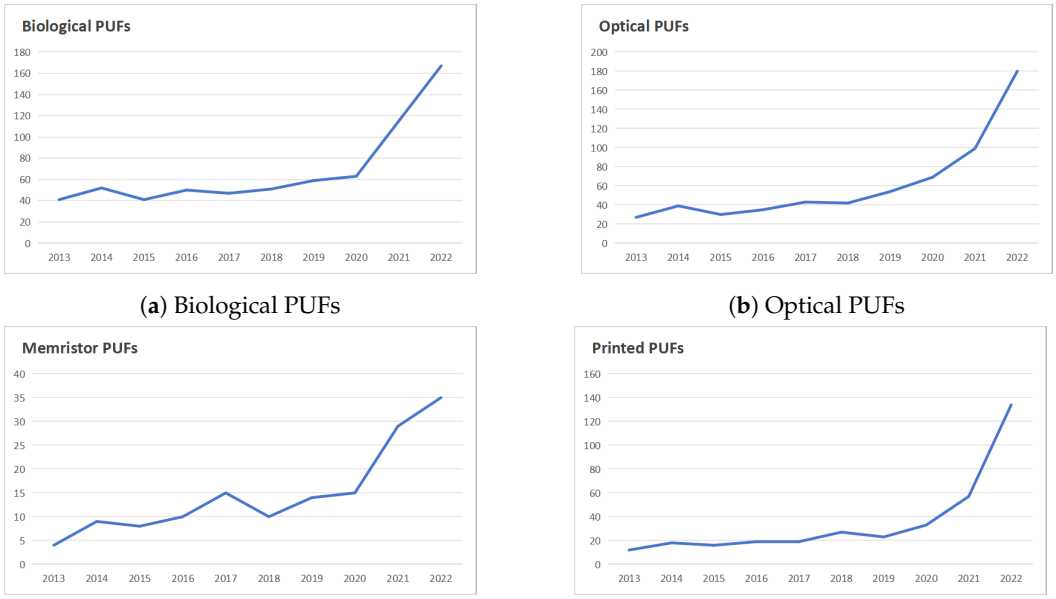
Bit Stability: A measure of the stability of individual bits across multiple measurements.
N: Number of measurements or trials.
L: Number of bits in a single PUF response.
$\delta(\text{b}_{i,j})$: Delta function indicating whether the j-th bit in the i-th measurement is stable
($\delta(\text{b}_{i,j} = 1)$) or not ($\delta(\text{b}_{i,j} = 0)$).

3. PUFs in Various Novel Materials and Methods

Significant progress within the field of PUFs has been achieved, with researchers and engineers delving into novel materials or methods. They are actively exploring novel materials in fields like nanofracture [16], PE, carbon nanotubes [17], nanowires [18], plasmonic surfaces [19], and nanoelectromechanical systems [20]. These pioneering approaches herald a promising era of diversified PUF development and applications.

We conduct an investigation on publications related to four types of PUFs based on novel technologies and obtain data from several journal databases, such as the Association

for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE) Xplore, and Springer Nature. The keywords used in the search are consistent with the new materials covered in this article, or similar concepts are used to expand the search scope, which may have some discrepancies. Figure 3 illustrates the trends in the number of articles published in the years 2013 to 2023 that are related to bionic optical PUFs, biological PUFs, PUFs based on PE, and memristor-based PUFs. We can see that there is an overall increasing trend in publishing in recent years. However, the number of publications on those PUFs has remained relatively low throughout the entire period, which demonstrates that the current state of the field is still in its early stages, holding great potential for future development.



(**a**) Biological PUFs (**b**) Optical PUFs

(**c**) Memristor PUFs (**d**) Printed PUFs

Figure 3. Publication trends in PUFs based on novel materials.

Among these four types, biological PUFs exploit the inherent randomness of T cells or extract ECG features for individuals, while bionical optical PUFs utilize optical inspections of natural plant tissues' micro–nano architectures for key generation, the third type of PUF is based on PE like inkjet-printed metal-oxide transistors, and the fourth type of PUF utilizing memristors leverage the analog and digital traits of memristors. The use of new materials and methods is an innovation in obtaining entropy sources, which is superior to traditional silicon PUFs.

3.1. Bionic Optical PUFs

Optical PUFs stand out due to their characteristics like high entropy, resource efficiency, and unparalleled tamper resistance thanks to their intrinsic complex optical randomness [21]. As a result, optical PUFs are regarded as an outstanding candidate for the future secure cryptographic primitives [22]. There are already many types of optical PUFs available, but most of the micropillar arrays and metasurfaces of these existing optical PUFs are traditionally manufactured through processes like lithography or ion beam etching. For example, the optical cryptographic surface found on the photonic architecture of a micropillar array proposed by Choi et al. is an optical cryptographic technology that combines photonic crystals and microcolumn arrays [23], and the fluorescent PUF utilizing perovskite quantum dot/chaotic metasurface hybrid nanostructures proposed by Chen et al. utilizes the characteristics of perovskite quantum dots and chaotic metasurface [24].

Inspired by unique biological architectures of natural plants, Wan et al. [12] proposed a new concept of bionic optical PUFs and used the surface micro–nano structure of natural

plant tissue to prepare four kinds of bionic PUFs; this method also has the advantages of environmental protection and economic sustainable development, and can promote environmental protection and economic sustainable development.

No two plant tissues in the world are identical, much like how no two leaves are alike. For a considerable period, nature has provided valuable materials and functional structures to humanity [25]. Moreover, actually, the bionic optical PUFs in this paper are studied from four different tissues of natural plants: the lotus leaf, the red rose petal, the rose leaf, and the ginkgo leaf.

Using natural plants as templates to create bionic films is a soft lithography technique. Due to its low-cost characteristics, this approach has found extensive applications within the flexible electronics domain [26,27].

The laser speckle pattern imaging technique can be employed in research experiments and practical applications to help better understand the three-dimensional (3D) micro–nano physical characteristics of objects [22,28].

Wan et al. also used laser speckle in their optical system stage and analyzed the performance of the bionic optical PUFs through laser speckle patterns. The whole implementation procedure of the bionical optical PUF they proposed is outlined in the subsequent stages. (i) The polymer materials used in their study include PVA (CAS number 9002-89-5, Aladdin headquartered in Shanghai, China) and PDMS (CAS number 63148-62-9, Sylgard 184, Dow Corning headquartered in Midland, Michigan, United States), which were coated onto the surface of the plant tissue used as a mold. After heat curing and peeling off, although the processing time varies slightly for different materials, they obtained a bionic membrane with a negative surface structure resembling that of a plant. Figure 4 illustrates an example of a bionic PUF key, wherein a bionic film featuring a negative surface structure similar to that of a plant is encapsulated in a card housing to provide mechanical protection and enable functionalization applications. (ii) This step involves the utilization of a collimated and expanded helium–neon laser beam. This laser beam is directed through a beam splitter, which subsequently illuminates a liquid crystal spatial light modulator. This modulator serves as a canvas for the display of random phase patterns, strategically chosen to generate specific challenges. These challenges are crafted by modulating the laser beam's wavefront through the independent adjustment of gray values for each pixel. (iii) Following this, the laser beam passes through a polarizer, a lens, and an iris. The generated input challenge is projected onto the front surface of the bionic PUF card, which is next placed in a slot locator to ensure its position is accurate and secured. (iv) Located behind the PUF card, a charge-coupled device (CCD) camera is employed to detect and capture the transmitted speckle pattern. This elaborate process represents a crucial component of the system's operation, contributing to the overall functionality and security of the setup. (v) Then, the speckle patterns are converted into a two-dimensional (2D) binary code with "1" assigned to the white pixels and "0" to the opposite after filtering with the algorithm of Gabor Hash [29], and eventually a one-dimensional (1D) key of 1280 Kbits is obtained. The second to fifth steps are shown in Figure 5.

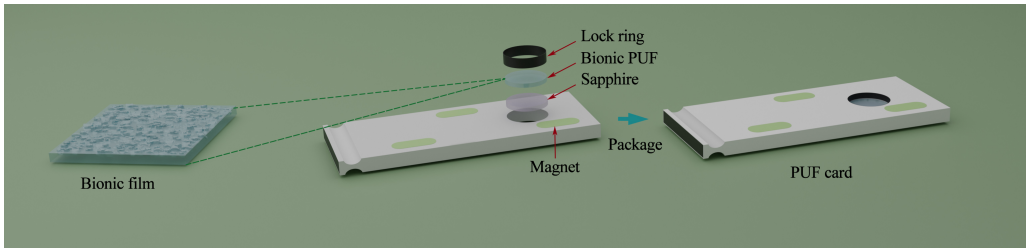


Figure 4. The production process of PUF card (the production process of previous bionic film has been omitted). Imitates the image in the original paper [12].

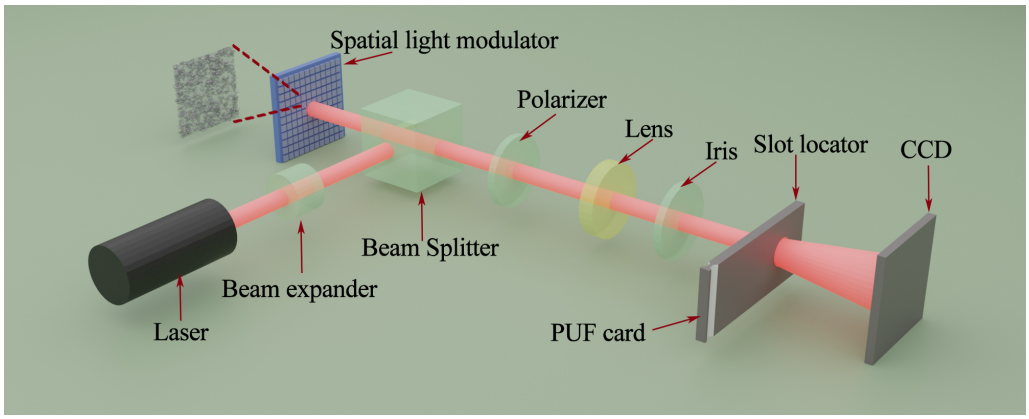


Figure 5. The second to fifth steps of the implementation procedure, also understood as the optical system stage. Imitates the image in the original paper [12].

3.2. Biological PUFs

Here, the term "biological" in biological PUF (in this paper) not only refers to the colonized populations of T cells but also refers to information on heart beat that can be observed through an ECG. Biological information exhibits strong randomness, unpredictability, and unclonable features. Biological PUFs exploit the spatiotemporal and collective behavioral dynamic changes inherent in various biological species [11]. These dynamic variations provide a unique and secure foundation for creating unclonable identifiers, making biological PUFs a promising avenue for enhancing security and authentication systems.

Some features can be observed at the macro level, but there are also some reflected at the micro level. In this section, two kinds of biological PUFs are introduced: one exploits the intrinsic randomness within colonized T cell populations, while the other extracts ECG features.

3.2.1. PUFs Utilizing T Cells

Before introducing this PUF, it must be noted that there is ambiguity in the classification of this PUF as it also utilizes optical inspections for key generation after certain processing of the material. So, in a certain sense, it can also be classified as optical PUFs.

The biological PUF proposed by Wali et al. [11] exploits the intrinsic randomness within colonized T cell populations. It is essential to underscore that T cells can only be used as entropy sources for PUFs in the form of colonized population as PUFs have the metric of reproducibility, which requires the same challenge input at different times to generate the same response. However, T cells may have temporary motion, which would not meet the requirements of reproducibility. However, after the formation of the local colony, T cells no longer have temporary motion, which can meet the conditions for preparing biological PUFs. Also, achieving ideal reproducibility is almost impossible due to various influencing factors. Therefore, they adopted a fuzzy authentication method [30], in which they set a threshold, and errors within this threshold can be ignored. Moreover, as the local colony of T cells forms, we can determine the threshold Hamming distance and the period required before utilizing the T cells.

They also provided a comprehensive description of the biological PUF generation process, as shown in Figure 6. (i) The process begins with the purification, stimulation, culture, suspension, and separation of T cells. (ii) Subsequently, the T cells are introduced into an imaging system equipped with an onstage incubator, allowing them to establish colonies over a period of approximately 20 h. (iii) Finally, computer-based processing can convert the imaging of the colonized T cell population into a 2D binary information source and generate biological PUF, following the same conversion process as the previous type of bionic optical PUF.

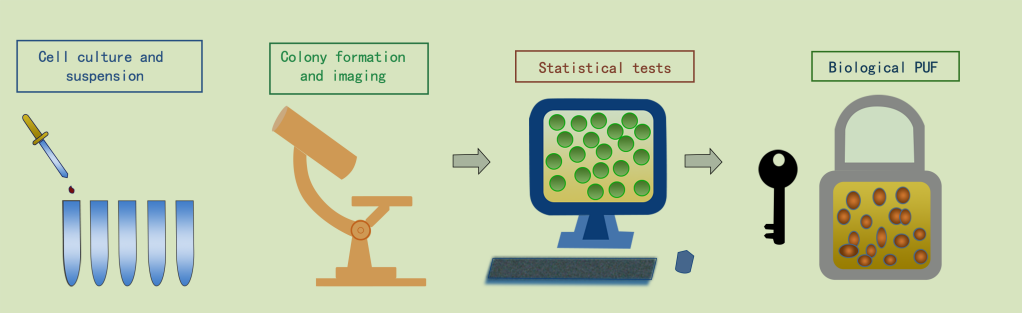


Figure 6. The generation process of the PUF utilizing T cells: (i) purification, stimulation, culture, suspension, and separation of T cells; (ii) establish colonies in an imaging system; (iii) convert the optical image into a 2D binary code. Imitates the image in the original paper [11].

Wali et al. [11] pointed out in their study that randomness inherent in other cellular or molecular biological processes can also be exploited to construct biological PUFs [11]. For instance, biological entities with smaller dimensions like mycoplasma gallicepticum can be used to increase the entropy sources of each biological PUF [31]. Furthermore, thermophiles can be employed to address the issue of increased susceptibility of T cells to cell death at elevated temperatures. Since they can survive not only high temperatures from 41 °C to 122 °C but also low temperatures from −20 °C to 10 °C, they have the ability to survive extreme temperatures, and this ability can be applied to building temperature-invariant biological PUFs [32].

3.2.2. PUFs Extract ECG Features

ECG is a medical examination that tracks the electrical activity of the heart over time. With the increasing use of wearable devices, personal ECG signals can now be captured easily. Then, some works [33,34] tried using personal ECG signals for authentication as this incorporates inherent liveness detection and is difficult to spoof. However, these studies do not measure or proactively reduce the overlap between the feature distributions within the same subject and across different subjects.

Yin et al. [14] designed ECG-based PUFs to enhance the security of personal wearable devices, which use the ECG signals as the entropy source of PUFs. In their proposed plan, the ECG-based PUF is verified over a large scale of a 741-subject database and can indeed reduce the overlap between the feature distributions within the same subject and across different subjects. In addition, this liveness factor can trigger a PUF response to provide a unique identification or validation that ensures it is only visible when worn by the device owner.

They proposed that, through signal processing steps, the features of the ECG signal can be extracted, and the features of the ECG signal can be generated by the neural network training algorithm to generate a unique 256-b random number, which plays an important role in PUFs. Figure 7 shows the top-level design. ECG signal processing involves key steps: FIR filtering, R-peak detection, outlier removal, and normalization. FIR filtering reduces noise and applies bandpass filters, improving signal quality. R-peak detection identifies ventricle depolarization peaks with dynamic thresholds, saving 160-sample segments. Outlier removal eliminates abnormal complexes using criteria like max/min values. Normalization has two phases: individual complex normalization, followed by global normalization for cross-individual consistency. These steps are vital for extracting meaningful ECG features, noise reduction, peak detection, outlier elimination, and data uniformity. Processed ECG data can serve in biometric authentication and encryption key generation.

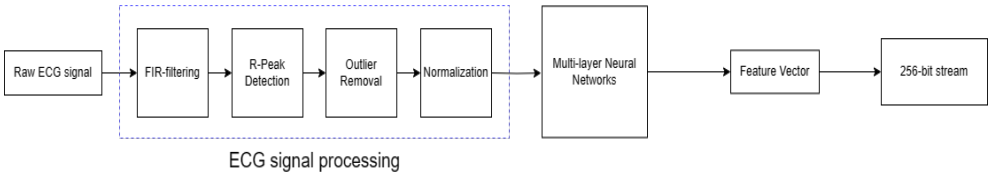


Figure 7. The top-level block diagram of ECG features extraction process for secret key generation.

"We need to extract certain features from ECG signals that makes the inter-subject Hamming distance of such features maximal and intra-subject Hamming distance minimal [14]". This sentence needs to be understood as follows: authentication is considered successful when the similarity between the new signal extracted from the wearable device's carrier and the registered signal exceeds a certain threshold using methods such as cosine similarity. However, it is important to note that this simplistic similarity-based approach may not provide sufficient security on its own, and additional layers of security and verification may be required in practical authentication systems. There is another challenge: for different individuals, some of their signals overlap, and we cannot allow these overlapping signals to influence the assessment of similarity. For the same person, their ECG signal is constantly changing over time, but a stable signal is needed for the same person, so researchers should find the most stable part of their ECG signal, which corresponds to the minimum Hamming distance. However, the neural network (NN) trained with one-hot labels [35] could not do that. Therefore, Yin et al. [14] proposed a new NN training method that can better optimize NN to solve the problems mentioned above by using application-specific cost functions in the last hidden layer [14]. This cost function is designed to directly govern the similarity or distance between individuals' ECG features, aiming to maximize the relative distance and minimize the equal error rate (EER). By training the NN with the cost function, the extracted features at the hidden layers are optimized for authentication based on cosine distance (CD) between features.

Then, they showed the experimental results wherein the ECG data used for testing are acquired using an ECG sensor at a rate of 250 Hz and with a resolution of 15 bits. The feature vectors are derived from the outputs of the trained neural network. To evaluate the performance of evaluation feature extraction, they proposed a new evaluation method by examining the CD distribution for inter-subject and intra-subject feature vectors. The overlap between the CDs derived from the neural network for intra-subject and inter-subject comparisons is indeed minimized significantly. To further refine the results of the data, they took the average value of multiple feature vectors generated by inputting various inter-subject ECG data, which mitigates the impact brought by time-variant ECG beats. Then, the average value is taken as a representative feature vector. Finally, the encryption secret key is derived from the most significant bits (MSBs) of the 256 features extracted from the representative feature vector.

3.3. PUFs Based on Printed Electronics

Printing technology holds great potential for the fabrication of cost-effective, flexible, and expansive electronic products, and there are currently some applications in various fields, such as printing digital and analog circuit components, manufacturing smart labels, printing microchips, and solving manufacturing challenges. As a crucial component of the 'Fourth Industrial Revolution', PE are gaining growing recognition for their role in facilitating the Internet of Things (IoT) [36].

PE, with their inherent randomness and variability stemming from the material's surface roughness, morphology, and resulting electrical properties, can generate unique device-specific identifiers that attackers cannot predict. Through the use of these subtle differences, PE can be used as a source of entropy; each instance of the generation and materials associates with a unique identifier.

Scholz et al. introduced a hybrid PUF by leveraging the features of printed electronics, as documented in their study [13]. Moreover, the design of this PUF integrates the inkjet-

printed core circuit with the silicon-based CMOS system environment seamlessly. In this design, they utilized the material composition, layer thickness, roughness, and interface properties of multiple printed layers to generate entropy, thereby reducing the likelihood of plagiarism detection. The manufacturing process of the printed PUF core not only involves the inkjet-print process but also involves the laser ablation process. Among the structures of the PUF core, the cursor, the gate insulator, and the top gate electrode material are all inkjet-printed out. In their experiment, the design of the PUF core included 8 inverters, where the number of inverters can be extended if needed. It is notable that PUFs relying on PE showcase innovative features, as Scholz et al. [13] noted that "To the best of our knowledge, designing, fabricating, and embedding a printed PUF core into a system level environment as well as the experimental analysis of PUF security metrics has not been presented before".

The challenge–response mechanism of this PUF is as follows. The full readout PUF challenge is 28 bit-width. One single output bit is produced by comparing the output voltages of two inverters, which are addressed at the same time. The complete PUF response as an identifier is generated by successively applying the subchallenges to the PUF. Furthermore, Scholz et al. [13] pointed out that the PUF they designed shows the largest response bit in width by comparing with other printed PUFs. Additionally, the system is divided into three separate functional units, including the development board, control logic board, and PUF core adapter board. This division allows for a more efficient and cost-effective characterization of printed PUF cores, reducing both production time and costs.

Scholz et al. [13] stated that the PE technology allows a root of trust to be established through decentralized manufacturing in the PUF supply chain, reducing the likelihood of plagiarism. This indicates a significant advancement in ensuring reliable security elements. As printing technology continues to advance, with improvements in material properties and printing techniques, we can expect even greater levels of randomness and variability in PUF responses. In the coming years, further research and development efforts can focus on optimizing printing processes, exploring new printing materials, and investigating novel PUF architectures to fully harness the potential of printing technology in enhancing security and privacy in various domains.

3.4. Memristor-Based PUFs

Memristor is a combination of "memory" and "resistor", possessing the outstanding ability to remember the resistance value even after the power is off. Different from resistors, capacitors, and inductors, memristors operate on the relationship between a change in flux and a change in charge. Consequently, it is called the fourth fundamental element of circuit design [37]. The classical definition of memristance is the differentiation in its magnetic flux from charge, with the same dimension as the resistance value, and it depends on the total amount of charge that has flowed through the device in the past. In other words, the current can change memristor's internal state and in turn affect its impedance and the current passing through it.

Leon Chua first proposed the concept of memristor in 1971 [38]; however, it took until 2008 before scientists at Hewlett-Packard managed to successfully fabricate a functional nanomemristor. Over the past few years, many researchers have achieved breakthroughs in improving the performance and stability of memristors. Many circuit structures based on memristors were invented. In addition, the application of memristor in the field of cellular neural networks (CNNs) attracts wide attention. Memristors have been proposed to work as synaptic weights in neural networks [39]. By using memristors as an alternative to synaptic connections, these networks are able to perform with higher computing parallelism and energy efficiency [40–42]. As the father of memristors, Leon Chua accrued many important achievements in his later work, such as Chua circuit, cellular neural networks, electronic computing, and so on. So far, the smallest memristor feature size is around two nanometers, allowing for high-density storage [43]. Memristors have garnered substantial interest

in the field of electronics due to their considerable potential for memory storage and computational applications, resulting in an increased level of attention.

The basic composition of memristor is a dielectric layer sandwiched by two electrodes, which is regarded as metal–insulator–metal (MIM) structure [44]. The metal oxide layer acts as the resistive element that exhibits different resistance states, representing the different memory states. The resistance of the metal oxide layer can be modified by applying electrical pulses, which induces the migration of oxygen vacancies or ions within the layer. This migration causes a change in the conductive path, resulting in a binary resistance state. The device can retain this resistance state even after power is turned off, allowing for non-volatile memory storage. By controlling the magnitude, duration, and timing of the applied electrical pulses, the resistance of the Resistive Random Access Memory (RRAM) device can be selectively switched between high and low resistance states, corresponding to the "1" and "0" states used for data storage.

Memristors are usually integrated in high density by means of crossbar array. A typical crossbar array consists of parallel metal lines. The metal lines in the array are divided into two groups; one group is called the word line and the other is called the bitline, forming the top and bottom electrodes. The memristor is positioned at their intersection. During the reading process, the selected unit reads its conductance through a sneak path. The sneak path carries unwanted current during the process, equivalent to a series resistance in parallel with the selected memristor. This results in additional energy consumption for unselected cells, which degrades read margin and limits the size of the array [44]. This memristor array can perform vector multiplication in parallel [45]. The factors of multiplication are stored directly in the memristor array and do not require a separate storage unit, thus bypassing the von Neumann bottleneck. This method can significantly reduce the data movement during calculation, having the advantages of low power consumption and high speed.

The potential of memristor-based PUF holds great promise because it offers advantages such as smaller device size, low power consumption, high sensitivity to manufacturing processes, and compatibility with modern CMOS manufacturing techniques [46]. Moreover, the study conducted by Zeitouni et al. points out that PUFs based on memristors have increased robustness and resistance against modeling attacks compared to PUFs that only use CMOS technology, primarily because of the random behavior exhibited by these nanodevices [47].

PUF structures usually produce only one bit for a given set of challenge bits, leading to the consumption of multiple CRPs to generate a single multibit key. This results in the inefficient use of valid CRPs [48]. In order to address these concerns, a new structure called pm-PUF is developed [49], combining nanocross point arrays and multiple subarrays for generating multibit responses, as shown in Figure 8. In their trial, a broader range of pulses resulted in an increased resistance drop in the analog memristor. Moreover, escalating the frequency of consecutive pulses with consistent widths further enhances this phenomenon. The data suggest that the duration of the electrical pulse affects the resistance of a memristor. Initially, the circuit employs control modules to establish connections between individual rows and columns and either the random pulse generator or decoder block, depending on the read/write command [50]. By consolidating a myriad of crosspoints within a limited space, this densely packed arrangement facilitates the storage and concurrent processing of a substantial quantity of CRPs in the PUF. Consequently, it leads to the production of responses with multiple bits. This architectural concept prioritizes the design of banks, leveraging the combination of numerous compact PUF units placed side by side and incorporating variations in manufacturing. Each subset of the given array possesses the capability to individually handle a specific portion of the given challenge and generate the corresponding binary response. Utilizing the parallel execution capabilities in response generation, the architecture of the bank design approach enhances the efficiency and safeguards the integrity of memristor-based PUFs [47].

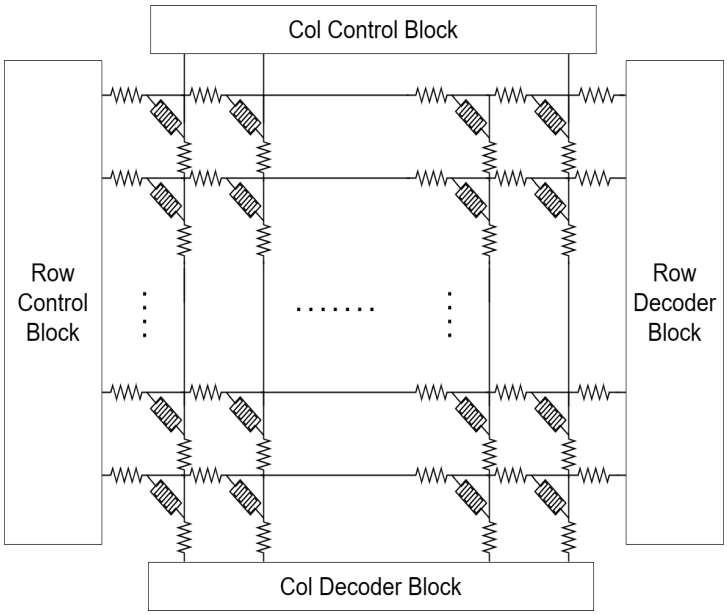
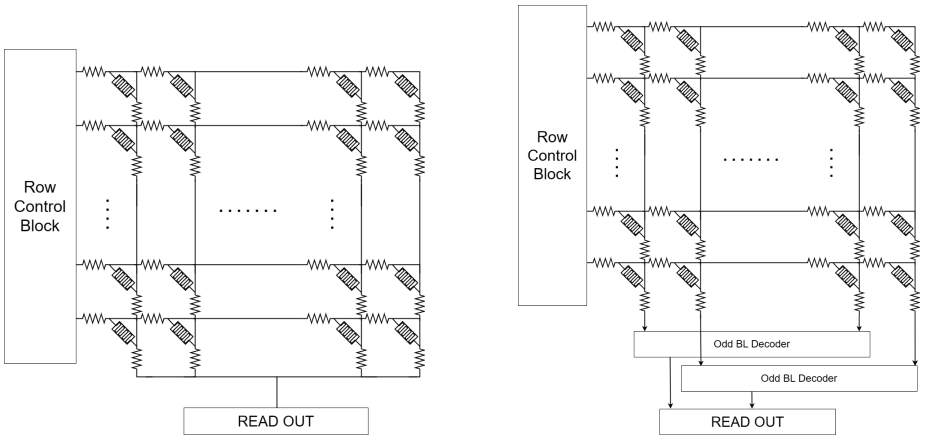


Figure 8. Simplified pm-PUF architecture.

The use of physical modifiability as the characteristic for challenge and response is found in pm-PUFs, whereas total bitline current PUF (TBC-PUF) and selected bitline current PUF (SBC-PUF) utilize the memristor's set voltage distribution as an entropy source. The bitline current is measured to obtain their response following the application of voltage or current. TBC-PUFs and SBC-PUFs differ primarily in their utilization of bitline currents as features, as illustrated in Figure 9. All bitline currents are utilized as features in the TBC-PUF domain. The behavior of TBC-PUF is determined by analyzing the difference in currents flowing through the odd and even bitlines. This process enables TBC-PUFs to produce an exclusive and unforeseeable response. The benefit of employing this method is its ability to achieve increased device density and efficiency while remaining compatible with CMOS technologies and simple to implement [50]. SBC-PUF adopts a selective approach in picking certain bitline currents as its distinguishing characteristics. Rather than comparing the total current of TBC-PUF, SBC-PUF chooses a specific line from the group of even and odd bitlines and evaluates the read current to produce a 1-bit response. By strategically selecting certain currents on the bitlines, the SBC-PUF enhances resource utilization and boosts the efficiency of a PUF [51]. Both TBC-PUF and SBC-PUF meet the requirement of being considered a strong physical unclonable function in a crossbar array of size N $\times$ N.



(**a**) (**b**)

Figure 9. (**a**) The total bitline current PUF and (**b**) the selected bitline current PUF architecture.

Apart from this, the multiarray PUF (MA-PUF) incorporates various crossbar arrays as an entropy source [50]. Figure 10 exhibits the arrangement of numerous subcrossbar arrays, employing either a grouping of 2D crossbar arrays or the utilization of 3D stacked crossbar arrays [52]. This approach maximizes the efficiency of available space. Each of these subarrays adheres to the principles of TBC-PUF, yielding their own unique responses, which can be aggregated to generate a final multibit response signal. The MA-PUF design offers a crucial benefit by shortening the key generation time and reducing power usage, ultimately enhancing energy efficiency of the system. Furthermore, unlike conventional PUFs, where a considerable amount of CRPs is typically required to create a response signal with multiple bits because each pair is only capable of generating a single-bit response signal, MA-PUFs achieve a substantial reduction in the necessary CRPs, thereby enhancing the efficacy of response signal generation and the overall security performance.

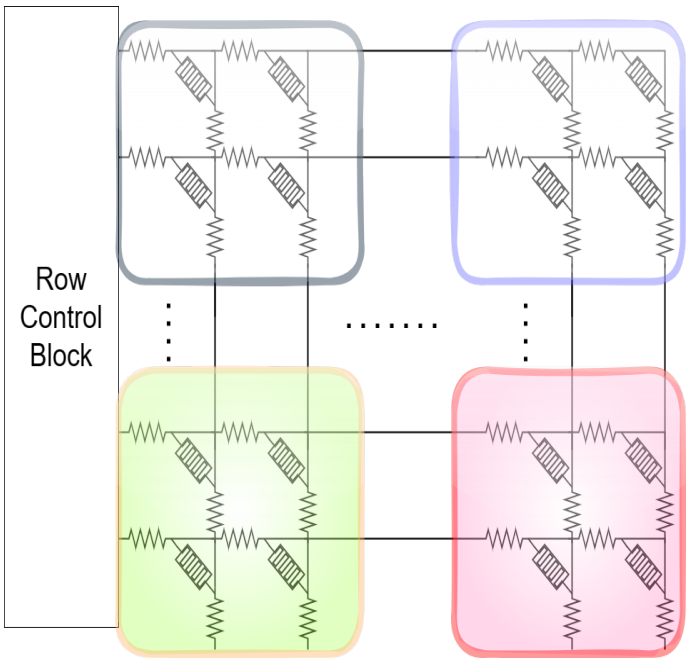


Figure 10. Simplified MA-PUF architecture.

Also, a unique type of PUF called memristive-device-based PUF (mrPUF), which is composed of two important elements: a nanocrossbar array with dimensions M × N and two current-mirror-controlled ring oscillators (CM-ROs), was developed [53]. This configuration is depicted in Figure 11. The individual memristor of a nanocrossbar array can be considered the source of security in a mrPUF. The design employs a pair of arbitrary memristors to regulate the current, inhibiting the current in each inverter of the loop of the ring oscillator. This leads to a configuration where the ring oscillator operates with limited current. The oscillation frequency is directly determined by the current, which in turn is influenced by the values of the memristor. The frequency of oscillation for each oscillator is determined by utilizing a counter, which then compares the count values from two counting circuits. Subsequently, a response bit is generated according to the outcome of this comparison. MrPUF is recognized for offering a significantly higher amount of potential CRPs compared to traditional PUFs [54].

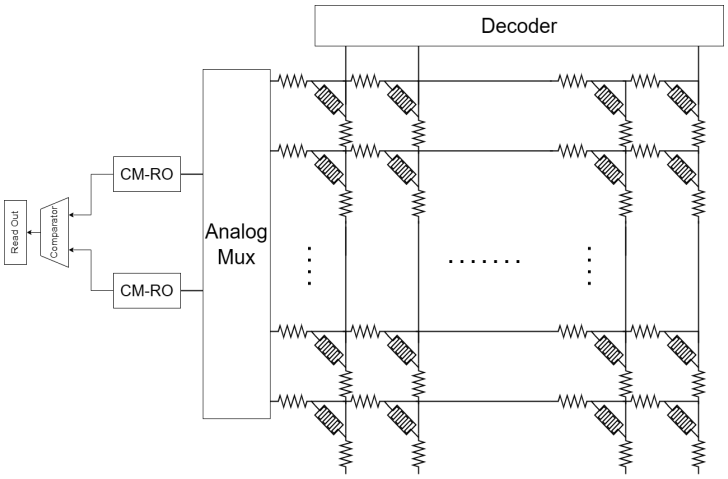


Figure 11. A nanocrossbar array of nanoionic memristive devices.

4. Performance Evaluation of PUF

Each of the aforementioned PUFs have been thoroughly assessed for their performance in the respective articles, and we have compiled them below.

For bionic optical PUFs, the experimental results in the paper demonstrate the randomness, uniqueness, and robustness. In the evaluation of randomness, the average entropy value is close to the ideal value "1", indicating perfect randomness, while, in the assessment of uniqueness and robustness of bionic optical PUFs, researchers [12] used two different mathematical analysis methods. One is to utilize the Hamming distance, inter-chip Hamming distance (inter-HD), and intra-chip Hamming distance (intra-HD), respectively. The other one is to utilize the correlation coefficient between response speckles. The results of the above two methods demonstrate that the bionic optical PUF has good uniqueness and robustness.

The four metrics of randomness, reproducibility, unclonability, and reconfigurability of biological PUFs using T cells are also demonstrated through experimental data. Randomness was quantitatively measured, and the total number of unique images in an area of 0.5 mm^2 was 10^{1233} [11], which sufficiently demonstrates the randomness. In terms of reproducibility, the relevant detection data consistently remain stable, providing evidence of reproducibility. In terms of unclonability, the experimental result from quantitative detection serves as compelling proof. In regard to reconfigurability, Wali. et al. [11] said that this biological PUF they proposed can seamlessly operate without necessitating physical system replacement or the addition of supplementary hardware components, achieving an unparalleled level of reconfigurability.

As for biological PUFs utilizing ECG signals, Yin et al. provided the results of verifying the randomness of PUFs. They performed a NIST randomness test [55] on the 256-bit random number, which consists of nine different tests. Moreover, the biological PUF utilizing ECG signals successfully passed all nine NIST tests.

For PUFs utilizing PE, three metrics of uniqueness, bit aliasing, and reliability [56] have also been evaluated and confirmed through experiments. The hybrid PUFs were subjected to rigorous testing that involved varying temperature, humidity, and supply voltage conditions. The results reveal that the average value of uniqueness is 51.1% and an average value of bit aliasing is 44.5%, and the bit error rate is found to be less than 2%, which indicates that the PUFs generated responses that are both distinguishable and stable. Additionally, under optimal operating conditions, the average reliability value is 78.5%, and it is anticipated to approach the ideal value.

The metrics of uniformity and uniqueness of PUFs using memristors are also demonstrated in the papers [47,50]. The performance of the five electronic memristor-based PUFs is close to ideal. The ideal values for uniformity and uniqueness are both 50%. The data

provided in the papers [47,50] indicate that the average values of these metrics are very close to 50%, and they may also fluctuate slightly with the size of the PUF.

Table 2 presents a comprehensive comparison between the aforementioned PUFs based on novel technologies, including bionic optical PUFs, biological PUFs, PUFs utilizing PE, and memristor-based PUFs. With the advancement in emerging technologies, the application potential of PUFs has extended. Bionic optical PUFs, which utilize random surface patterns resembling micro–nano structures found in common plant tissues, demonstrate notable characteristics such as high entropy, non-volatility, low power consumption, and, to some extent, reconfigurability [5]. Bionic optical PUFs can be categorized as strong PUFs, capable of withstanding reverse engineering attempts. Biological PUFs hold the potential to surpass all other PUFs mentioned here [11], emerging as strong PUFs. They offer substantial advantages, including high entropy, cost-effectiveness, low power requirements, seamless reconfigurability, an exponential number of CRPs, and formidable resistance to reverse engineering, even when equipped with exhaustive knowledge of the biological system. Notably, the biological PUFs utilizing T cells mentioned in this paper can seamlessly operate without necessitating physical system replacement or the addition of supplementary hardware components, achieving an unparalleled level of reconfigurability.

Table 2. Comparison of PUFs involved in this article.

	Bionic Optical PUF	**Biological PUF**	**PUF Utilizing PE**	**Memristor-Based PUF**
Entropy	High	High	Medium	High
Uniqueness	Yes	Yes	Yes	Yes
Randomness	Yes	Yes	Yes	Yes
Reproducibility	Limited	Yes	Yes	Yes
CRPS	Exponential	Exponential	Exponential	Linear
Volatile	Non-volatile	Non-volatile	Non-volatile	Non-volatile
Weak/Strong PUF	Strong	Strong	Strong	Strong

The PUFs based on PE, as discussed in this article, exhibit pioneering characteristics, as Scholz et al. [13] noted that "To the best of our knowledge, designing, fabricating, and embedding a printed PUF core into a system level environment as well as the experimental analysis of PUF security metrics has not been presented before". They also fall under the category of strong PUFs due to their mostly non-volatile nature, low power consumption, high entropy, and formidable resistance to reverse engineering.

Similarly, PUFs employing memristors, acknowledged for their basis in nanotechnology, also belong to the category of strong PUFs. They exhibit non-volatility, high entropy, and remarkable resilience against reverse engineering attempts. However, it must be mentioned that PUFs using memristors are susceptible to modeling attachments using state of the art machine learning (ML) algorithms.

In summary, these PUFs based on novel materials and methods all hold promise as potential candidates to enhance the security and privacy of vast amounts of information in the future.

5. Potential Shortcomings or Areas for Improvement

Although PUFs based on new materials have outstanding performance in areas where traditional silicon PUFs have problems, some of them still have potential shortcomings or areas for improvement. These can serve as the direction and focus of future research.

The lack of reproducibility seems to be one of the major weaknesses of bionic optical PUFs. Even if the same plant tissue is used, there may still be errors in the reproduction results during the mold-making process of PUF cards due to factors such as bubbles and transcoding errors in laser speckle optical processes. As the above errors may only cause minor deviations, researchers can use revised approaches such as fuzzy authentication [30] when using this type of PUF, which is also used in other types of PUFs.

For the two categories of biological PUFs, the former one utilizes the colonized populations of T cells; when it comes to survival rates and lifespan issues at temperatures

such as extreme low and high temperatures, it is possible to consider using microbial populations with other characteristics, as Wali et al. also noted in their paper [11]. The latter one extracts ECG features due to the time-varying characteristics of ECG signals; the inter-subject features cannot be accurately or stably obtained. Therefore, there is still room for improvement here, where algorithms can be improved or new error correction techniques can be utilized to generate more stable keys.

As for PUFs utilizing PE, to enhance the reliability and achieve bit-stable PUF responses [13], the temperature stability needs to be improved through structural design. Furthermore, once inkjet printing circuit technology further develops, the whole PUF design can be completely printed, including silicon-based logic peripheral circuits.

While memristor-based PUFs are claimed to be resistant to modeling attacks, recent research suggests that the majority of them fail to pass comprehensive tests against modern ML techniques [47]. Zeitouni et al. conducted an assessment of the security of PUFs based on hybrid memristor technology. Various machine learning algorithms are applied to model different types of attacks, such as voting ensembles [57], stochastic gradient boosting [58], and bagged decision trees [57]. The researchers examine a method that involved gathering a limited number of real CRPs from the PUF and using them as a training dataset to create an ML model capable of predicting the responses. The results of the assessment indicate that memristor-based PUFs actually can be attacked by sophisticated machine learning algorithms that specialize in modeling attacks.

6. Application

PUFs take advantage of the physical changes inherent in semiconductor manufacturing to create a basic security mechanism to verify integrated circuits, and this security strategy, popularized by the electronics industry, can be applied in a variety of fields to help improve security and ensure data confidentiality. In the previous sections, we mentioned that PUFs have a wide range of applications in areas such as identity authentication and secure cryptographic primitives.

In our daily life and industry production, identity authentication is critical [59], which is one of the key factors in ensuring the security of data and systems. In terms of identity authentication, PUFs provide a very effective means to verify identity and protect data security. As each hardware component has its own unique physical characteristics, PUFs provide a high level of security and reliable authentication, effectively preventing unauthorized access and attacks.

As for secure cryptographic primitives, they are highly desirable for safeguarding information communication in modern digital society [21]. PUFs play an important role in the field of secure cryptographic primitives and are regarded as a fundamental building block. Compared with traditional encryption algorithms, keys generated by PUFs make it impossible for attackers to predict or copy the correct key, providing security for the encryption and decryption process. Moreover, PUF-based primitives can resist various attack vectors and provide important technical support for ensuring the security of data and systems.

Furthermore, Li et al. [15] completed an important groundbreaking study, building upon the success of silicon PUFs, in which they achieved the development of the first generation of genetic PUFs within human cells, successfully integrating PUFs into human cells. This study provides a theoretical and practical basis for the application of PUF technology in the biomedical field, and shows that CRISPR-PUFs can be used as a foundational cornerstone to establish robust provenance protocol to ensure data authenticity and traceability.The application of genetic PUF technology can not only be embedded in cell lines to prove their origin but also serve as a quality control tool for cell lines.

As shown in Figure 12, Li et al. [15] utilized CRISPR technology to engineer CRISPR for genome editing. They inserted a five-nucleotide barcode library into human embryonic kidney (HEK) 293 cells and used polymerase chain reaction (PCR) and next-generation

sequencing (NGS) to detect and monitor these barcodes. The study aimed to assess gene editing by employing single-guide RNAs (sgRNAs) to target a fluorescent reporter gene. After CRISPR treatment, they analyzed genomic DNA, identifying 569 indel variations associated with barcodes. This information formed a unique CRISPR-PUF identifier, which offers a novel approach for genomics research. Li et al. [15] pointed out that CRISPR-PUFs can be used in various fields and can be used as an effective tool to verify the source and ensure quality.

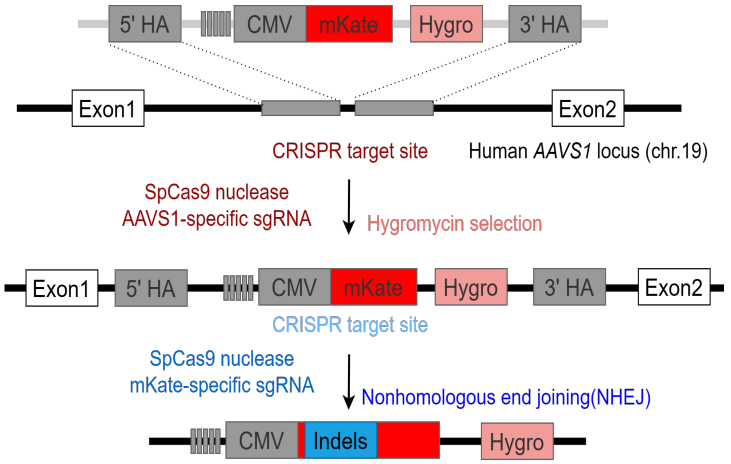


Figure 12. Schematic illustration of implementation of CRISPR-PUFs. Imitates the image in the original paper [15].

Certainly, there will be ongoing and future research on the application of PUFs in various fields. Inspiration can be drawn from nature, including microorganisms, animals, and plant structures. Future research may concentrate on interdisciplinary intersections, conducting extensive investigations on PUFs from multiple perspectives and levels. This involves physics, chemistry, biology, as well as information science, contributing to a comprehensive understanding and application of PUFs. Simultaneously, efforts should be directed towards improving the interpretability and transparency of PUFs, enhancing people's comprehension and trust in this technology, and facilitating human–computer interaction. These considerations can serve as new focal points for research.

7. Conclusions

In conclusion, this comprehensive review introduces four types of PUFs based on novel technologies. All four types of PUFs exhibit excellent performance, but there are also areas that need improvement. Lack of reproducibility is one of the major weaknesses of bionic optical PUFs; biological PUFs utilizing colonized populations of T cells need to expand their operational temperature range, while biological PUFs extracting ECG features require improvements in their time-variant stability; PUFs utilizing PE need to enhance their temperature stability; for memristor-based PUFs, further improvements are required to withstand attacks from modern machine learning techniques. The use of new material is an innovation in obtaining entropy sources, which is superior to traditional Si-PUFs. Based on the review, we further discuss the potential issues with some of these PUFs. These PUFs based on novel materials all hold promise as potential candidates to enhance the security and privacy of vast amounts of information in the future. Furthermore, the paper also highlights PUFs' applications, such as CRISPR-PUFs in human cells and applications in identity authentication and secure cryptographic primitives.

In the future, research on PUFs needs to be further deepened and expanded to explore the greater application potential of new materials in PUFs and broaden the scope of their applications. From our perspective, researchers can explore various ways to obtain entropy sources. As mentioned in this article, inspiration can be derived from nature, such as microorganisms, animal and plant structures, and so on. It is also worth investigating

whether emerging manufacturing processes possess specific characteristics between different entities. Continuous innovative research in technology is also necessary to reduce costs and improve efficiency. Considering the continuous progress of technology and the expanding application scenarios, novel materials-based PUFs hold promise as potential candidates to enhance the security and privacy of vast amounts of information in the future.

Author Contributions: Methodology, Z.H.; project administration, Y.C.; supervision, Z.H.; writing—original draft, J.X., J.W. and S.W.; writing—review and editing, Y.C., Z.H., J.X., J.W. and K.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Natural Science Foundation of China (62274056), the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (SKLACSS-202209), Key Research and Development Program of Jiangsu Province (BE2022098), Postdoctoral Science Foundation of Jiangsu Province (2021K605C), Guangzhou Municipal Science and Technology Project (SL2022A04J00404), Fundamental Research Funds for the Central Universities under Grant (XJS220306), Natural Science Basic Research Program of Shaanxi (2022JQ-680), and Changzhou City Key R&D Plan (Industrial Foresight and Key Core Technologies).

Data Availability Statement: Data are available on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang, Z.K.; Cho, M.C.Y.; Wang, C.W.; Hsu, C.W.; Chen, C.K.; Shieh, S. IoT security: Ongoing challenges and research opportunities. In Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 17–19 November 2014; IEEE: New York, NY, USA, 2014; pp. 230–234.
2. Bada, M.; Nurse, J.R. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 73–92.
3. Goldwasser, S.; Micali, S.; Rivest, R.L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **1988**, *17*, 281–308. [CrossRef]
4. Schramm, K.; Wollinger, T.; Paar, C. A new class of collision attacks and its application to DES. In Proceedings of the Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, 24–26 February 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 206–222.
5. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [CrossRef] [PubMed]
6. Ning, H.; Farha, F.; Ullah, A.; Mao, L. Physical unclonable function: Architectures, applications and challenges for dependable security. *IET Circuits, Devices Syst.* **2020**, *14*, 407–424. [CrossRef]
7. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R. PUF-based authentication and key agreement protocols for IoT, WSNs, and Smart Grids: A comprehensive survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228. [CrossRef]
8. Dey, K.; Kule, M.; Rahaman, H. PUF based hardware security: A review. In Proceedings of the 2021 International Symposium on Devices, Circuits and Systems (ISDCS), Higashihiroshima, Japan, 3–5 March 2021; IEEE: New York, NY, USA, 2021; pp. 1–6.
9. Khalafalla, M.; Gebotys, C. PUFs deep attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs. In Proceedings of the 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 25–29 March 2019; IEEE: New York, NY, USA, 2019; pp. 204–209.
10. Wei, S.; Wendt, J.B.; Nahapetian, A.; Potkonjak, M. Reverse engineering and prevention techniques for physical unclonable functions using side channels. In Proceedings of the 51st Annual Design Automation Conference, San Francisco, CA, USA, 1–5 June 2014; pp. 1–6.
11. Wali, A.; Dodda, A.; Wu, Y.; Pannone, A.; Reddy Usthili, L.K.; Ozdemir, S.K.; Ozbolat, I.T.; Das, S. Biological physically unclonable function. *Commun. Phys.* **2019**, *2*, 39. [CrossRef]
12. Wan, Y.; Wang, P.; Huang, F.; Yuan, J.; Li, D.; Chen, K.; Kang, J.; Li, Q.; Zhang, T.; Sun, S.; et al. Bionic optical physical unclonable functions for authentication and encryption. *J. Mater. Chem. C* **2021**, *9*, 13200–13208. [CrossRef]
13. Scholz, A.; Zimmermann, L.; Gengenbach, U.; Koker, L.; Chen, Z.; Hahn, H.; Sikora, A.; Tahoori, M.B.; Aghassi-Hagmann, J. Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors. *Nat. Commun.* **2020**, *11*, 5543. [CrossRef] [PubMed]
14. Yin, S.; Bae, C.; Kim, S.J.; Seo, J.s. Designing ECG-based physical unclonable function for security of wearable devices. In Proceedings of the 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Jeju, Republic of Korea, 11–15 July 2017; IEEE: New York, NY, USA, 2017; pp. 3509–3512.
15. Li, Y.; Bidmeshki, M.M.; Kang, T.; Nowak, C.M.; Makris, Y.; Bleris, L. Genetic physical unclonable functions in human cells. *Sci. Adv.* **2022**, *8*, eabm4106. [CrossRef]
16. Zhang, T.; Shu, Z.; Zhang, L.; Chen, Y.; Feng, Z.; Hu, Y.; Huang, F.; Wang, P.; Li, D.; Yao, Y.; et al. Random Nanofracture-Enabled Physical Unclonable Function. *Adv. Mater. Technol.* **2021**, *6*, 2001073. [CrossRef]

17. Hu, Z.; Comeras, J.M.M.L.; Park, H.; Tang, J.; Afzali, A.; Tulevski, G.S.; Hannon, J.B.; Liehr, M.; Han, S.J. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol.* **2016**, *11*, 559–565. [CrossRef]
18. Park, K.; Jung, K.; Kwon, S.J.; Jang, H.S.; Byun, D.; Han, I.K.; Ko, H. Plasmonic Nanowire-Enhanced Upconversion Luminescence for Anticounterfeit Devices. *Adv. Funct. Mater.* **2016**, *26*, 7836–7846. [CrossRef]
19. Smith, J.D.; Reza, M.A.; Smith, N.L.; Gu, J.; Ibrar, M.; Crandall, D.J.; Skrabalak, S.E. Plasmonic anticounterfeit tags with high encoding capacity rapidly authenticated with deep machine learning. *ACS Nano* **2021**, *15*, 2901–2910. [CrossRef] [PubMed]
20. Hwang, K.M.; Kim, W.K.; Jin, I.K.; Lee, S.W.; Choi, Y.K. Multilevel States of Nano-Electromechanical Switch for a PUF-Based Security Device. *Small* **2019**, *15*, 1803825. [CrossRef] [PubMed]
21. Arppe, R.; Sørensen, T.J. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nat. Rev. Chem.* **2017**, *1*, 0031. [CrossRef]
22. Goorden, S.A.; Horstmann, M.; Mosk, A.P.; Škorić, B.; Pinkse, P.W. Quantum-secure authentication of a physical unclonable key. *Optica* **2014**, *1*, 421–424. [CrossRef]
23. Choi, J.; Hua, M.; Lee, S.Y.; Jo, W.; Lo, C.Y.; Kim, S.H.; Kim, H.T.; He, X. Hydrocipher: Bioinspired dynamic structural color-based cryptographic surface. *Adv. Opt. Mater.* **2020**, *8*, 1901259. [CrossRef]
24. Chen, F.; Li, Q.; Li, M.; Huang, F.; Zhang, H.; Kang, J.; Wang, P. Unclonable fluorescence behaviors of perovskite quantum dots/chaotic metasurfaces hybrid nanostructures for versatile security primitive. *Chem. Eng. J.* **2021**, *411*, 128350. [CrossRef]
25. Jacucci, G.; Schertel, L.; Zhang, Y.; Yang, H.; Vignolini, S. Light management with natural materials: From whiteness to transparency. *Adv. Mater.* **2021**, *33*, 2001215. [CrossRef]
26. Wan, Y.; Qiu, Z.; Hong, Y.; Wang, Y.; Zhang, J.; Liu, Q.; Wu, Z.; Guo, C.F. A highly sensitive flexible capacitive tactile sensor with sparse and high-aspect-ratio microstructures. *Adv. Electron. Mater.* **2018**, *4*, 1700586. [CrossRef]
27. Qiu, Z.; Wan, Y.; Zhou, W.; Yang, J.; Yang, J.; Huang, J.; Zhang, J.; Liu, Q.; Huang, S.; Bai, N.; et al. Ionic skin with biomimetic dielectric layer templated from calathea zebrine leaf. *Adv. Funct. Mater.* **2018**, *28*, 1802343. [CrossRef]
28. Horstmeyer, R.; Judkewitz, B.; Vellekoop, I.M.; Assawaworrarit, S.; Yang, C. Physical key-protected one-time pad. *Sci. Rep.* **2013**, *3*, 3543. [CrossRef] [PubMed]
29. Li, Y.; Lu, Z.; Zhu, C.; Niu, X. Robust image hashing based on random Gabor filtering and dithered lattice vector quantization. *IEEE Trans. Image Process.* **2011**, *21*, 1963–1980. [PubMed]
30. De Ru, W.G.; Eloff, J.H. Enhanced password authentication through fuzzy logic. *IEEE Expert* **1997**, *12*, 38–45. [CrossRef]
31. Levisohn, S.; Kleven, S. Avian mycoplasmosis (*Mycoplasma gallisepticum*). *Rev. Sci. Tech.* **2000**, *19*, 425–442. [CrossRef] [PubMed]
32. Turner, P.; Mamo, G.; Karlsson, E.N. Potential and utilization of thermophiles and thermostable enzymes in biorefining. *Microb. Cell Factories* **2007**, *6*, 1–23. [CrossRef]
33. Page, A.; Kulkarni, A.; Mohsenin, T. Utilizing deep neural nets for an embedded ECG-based biometric authentication system. In Proceedings of the 2015 IEEE Biomedical Circuits and Systems Conference (BioCAS), Atlanta, GA, USA, 22–24 October 2015; IEEE: New York, NY, USA, 2015; pp. 1–4.
34. Hussein, A.F.; AlZubaidi, A.K.; Al-Bayaty, A.; Habash, Q.A. An IoT real-time biometric authentication system based on ECG fiducial extracted features using discrete cosine transform. *arXiv* **2017**, arXiv: 1708.08189.
35. Yin, S.; Kim, M.; Kadetotad, D.; Liu, Y.; Bae, C.; Kim, S.J.; Cao, Y.; Seo, J.s. A 1.06 μW Smart ECG Processor in 65-nm CMOS for Real-Time Biometric Authentication and Personal Cardiac Monitoring. *IEEE J. Solid-State Circuits* **2019**, *54*, 2316–2326. [CrossRef]
36. Chang, J.S.; Facchetti, A.F.; Reuss, R. A circuits and systems perspective of organic/printed electronics: Review, challenges, and contemporary and emerging design approaches. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2017**, *7*, 7–26. [CrossRef]
37. Vines, B.; Rashid, M. Memristors: The fourth fundamental circuit element. In Proceedings of the 2009 International Conference on Electrical and Electronics Engineering—ELECO 2009 Bursa, Turkey, 5–8 November 2009; IEEE: New York, NY, USA, 2009; pp. II–37.
38. Chua, L. Memristor-the missing circuit element. *IEEE Trans. Circuit Theory* **1971**, *18*, 507–519. [CrossRef]
39. Snider, G.S. Self-organized computation with unreliable, memristive nanodevices. *Nanotechnology* **2007**, *18*, 365202. [CrossRef]
40. Gaol, D.; Zhang, G.L.; Yin, X.; Li, B.; Schlichtmann, U.; Zhuo, C. Reliable memristor-based neuromorphic design using variation- and defect-aware training. In Proceedings of the 2021 IEEE/ACM International Conference on Computer Aided Design (ICCAD), Munich, Germany, 1–4 November 2021; IEEE: New York, NY, USA, 2021; pp. 1–9.
41. Yang, Z.; Liu, K.; Duan, Y.; Fan, M.; Zhang, Q.; Jin, Z. Three Challenges in ReRAM-Based Process-In-Memory for Neural Network. In Proceedings of the 2023 IEEE 5th International Conference on Artificial Intelligence Circuits and Systems (AICAS), Hangzhou, China, 11–13 June 2023; IEEE: New York, NY, USA, 2023; pp. 1–5.
42. Lei, T.; Fu, H.; Zang, H.; Huang, L.; Sun, W. Adomian Decomposition, Firing Change Process Analysis and Synchronous Control of Fractional-Order Hindmarsh–Rose Neurons in Electromagnetic Field. *Processes* **2023**, *11*, 2568. [CrossRef]
43. Chen, W.; Song, L.; Wang, S.; Zhang, Z.; Wang, G.; Hu, G.; Gao, S. Essential Characteristics of Memristors for Neuromorphic Computing. *Adv. Electron. Mater.* **2023**, *9*, 2200833. [CrossRef]
44. Li, H.; Wang, S.; Zhang, X.; Wang, W.; Yang, R.; Sun, Z.; Feng, W.; Lin, P.; Wang, Z.; Sun, L.; et al. Memristive crossbar arrays for storage and computing applications. *Adv. Intell. Syst.* **2021**, *3*, 2100017. [CrossRef]
45. Liu, X.; Zeng, Z. Memristor crossbar architectures for implementing deep neural networks. *Complex Intell. Syst.* **2022**, *8*, 787–802. [CrossRef]

46. Rajendran, J.; Karri, R.; Wendt, J.B.; Potkonjak, M.; McDonald, N.; Rose, G.S.; Wysocki, B. Nano meets security: Exploring nanoelectronic devices for security applications. *Proc. IEEE* **2015**, *103*, 829–849. [CrossRef]
47. Zeitouni, S.; Stapf, E.; Fereidooni, H.; Sadeghi, A.R. On the security of strong memristor-based physically unclonable functions. In Proceedings of the 2020 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 20–24 July 2020; IEEE: New York, NY, USA, 2020; pp. 1–6.
48. Koeberl, P.; Kocabaş, Ü.; Sadeghi, A.R. Memristor PUFs: A new generation of memory-based physically unclonable functions. In Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 18–22 March 2013; IEEE: New York, NY, USA, 2013; pp. 428–431.
49. Choi, S.; Kim, D.; Choi, Y.; Sun, W.; Shin, H. Multibit-generating pulsewidth-based memristive-puf structure and circuit implementation. *Electronics* **2020**, *9*, 1446. [CrossRef]
50. Sun, W.; Lee, J.; Kim, D.; Choi, Y. A Hardware Security Architecture: PUFs (Physical Unclonable Functions) using memristor. In Proceedings of the 2021 IEEE Region 10 Symposium (TENSYMP), Jeju, Republic of Korea, 23–25 August 2021; IEEE: New York, NY, USA, 2021; pp. 1–4.
51. Kim, D.; Kim, T.H.; Choi, Y.; Lee, G.H.; Lee, J.; Sun, W.; Park, B.G.; Kim, H.; Shin, H. Selected Bit-Line Current PUF: Implementation of Hardware Security Primitive Based on a Memristor Crossbar Array. *IEEE Access* **2021**, *9*, 120901–120910. [CrossRef]
52. Rose, G.S.; Meade, C.A. Performance analysis of a memristive crossbar PUF design. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
53. Gao, Y.; Ranasinghe, D.C.; Al-Sarawi, S.F.; Kavehei, O.; Abbott, D. mrPUF: A novel memristive device based physical unclonable function. In Proceedings of the Applied Cryptography and Network Security: 13th International Conference, ACNS 2015, New York, NY, USA, 2–5 June 2015; Revised Selected Papers 13; Springer: Berlin/Heidelberg, Germany, 2015; pp. 595–615.
54. Kavehei, O.; Hosung, C.; Ranasinghe, D.; Skafidas, S. mrPUF: A memristive device based physical unclonable function. *arXiv* **2013**, arXiv: 1302.2191.
55. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; US Department of Commerce, Technology Administration, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001.
56. Maiti, A.; Gunreddy, V.; Schaumont, P. A systematic method to evaluate and compare the performance of physical unclonable functions. In *Embedded Systems Design with FPGAs*; Springer, New York, NY, USA, 2013; pp. 245–267.
57. Breiman, L. Bagging predictors. *Mach. Learn.* **1996**, *24*, 123–140. [CrossRef]
58. Friedman, J.H. Greedy function approximation: A gradient boosting machine. *Ann. Stat.* **2001**, *29*, 1189–1232. [CrossRef]
59. Carro-Temboury, M.R.; Arppe, R.; Vosch, T.; Sørensen, T.J. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* **2018**, *4*, e1701384. [CrossRef] [PubMed]