electronics

MDPI

Article

Protecting Private Communications in Cyber-Physical Systems through Physical Unclonable Functions

Marina Pérez-Jiménez [1], Borja Bordel Sánchez [2,*], Andrea Migliorini [3] and Ramón Alcarria [2]

1 Instituto de Sistemas Optoelectrónicos y Microtecnología. Universidad Politécnica de Madrid, 28040 Madrid, Spain; marina.perez@isom.upm.es
2 Department of Geospatial Engineering. Universidad Politécnica de Madrid, 28031 Madrid, Spain; ramon.alcarria@upm.es
3 Max Planck Institute of Microstructure Physics, 06120 Halle, Germany; andrea.migliorini@mpi-halle.mpg.de
* Correspondence: bbordel@dit.upm.es; Tel.: +34-910672167

Received: 31 January 2019; Accepted: 27 March 2019; Published: 1 April 2019

Abstract: Cyber-physical systems (CPS) are envisioned to change the whole of society. New engineered systems joining physical and digital solutions are being employed in industry, education, etc. These new systems are networked by default, and private information is shared among the different components related to users, critical infrastructures, or business operations. In this context, it is essential to encrypt those communication links to protect such information. However, even most complicated schemes based on hybrid (asymmetric and symmetric) solutions, finally require physical devices to store a secret key. This approach is cryptographically weak, as any person with physical access to the device could obtain that key. Therefore, in this paper we propose the use of physical unclonable functions (PUF) to generate secret keys for lightweight encryption schemes. Using PUFs, any attempt to capture the key is changing the original secret stream, and even manufacturers are not able to build two identical PUFs. The proposed key generator is based on magnetic materials and lightweight pseudorandom number generators to meet the low-cost and small size requirements of CPS. In particular, materials with an activated exchange-bias effect are employed, together with simple copper coils. The encryption process can be based on a simple XOR gate because of the robustness of the proposed key generator. In order to evaluate the performance of the proposed technology, an experimental validation based on simulation scenarios is also provided.

Keywords: cyber-physical systems; physical unclonable functions; streaming communications; security; encryption

1. Introduction

Cyber-physical systems (CPS) [1] are defined as unions between physical and computational processes. This new approach has opened a new era in industry (Industry 4.0) [2], education, and engineering. In CPS, feedback control loops [3] are employed to make physical and cybernetic processes evolve together. Several heterogenous components are interconnected to create pervasive systems supporting these mechanisms. This new paradigm is particularly interesting to support real-time control systems, fed by an information stream (biological signals, data from sensors, etc.) [4].

However, these new systems are also vulnerable to new, innovative, and more aggressive attacks, known as 'cyber-physical attacks' [5]. In fact, as CPS are made of many interconnected components, attacks may affect a critical component when non-relevant (and often less secure) elements fail and the failure propagates due to a cascade effect. Besides, CPS are vulnerable not only to cybercrimes, but also to physical attacks. Thus, in these new systems, not only must attackers accessing to the

system through the communication networks be considered, but also people physically accessing and manipulating any device [6].

In this context, security for CPS is a critical issue. Many different schemes and solutions, then, have been proposed. Symmetric and asymmetric encryption schemes [7] or certificateless public key infrastructures [8] are probably some of the most common proposals. Nevertheless, those solutions and any other previously reported, finally require physical devices to store a secret key.

Software components can protect secret keys through cyber-protection technologies, as they have no physical existence, only logical. However, hardware devices must include memory (ROM memory) to store permanent information such as secret keys [9]. This configuration is vulnerable to physical attacks (i.e., people physically manipulating the device), as the key could be read from the memory by unauthorized people. This risk, moreover, is especially relevant in CPS, as many deployments are isolated, unmanaged, and unattended [10]. New mechanisms to create or protect keys against any cyber or physical attacker are, then, required.

Therefore, in this paper we propose a novel solution to protect communication links in CPS. The proposed encryption scheme is based on symmetric keys generated through physical unclonable functions (PUF) [11]. PUFs are systems whose response is unclonable, even if the manufacturing method of the system is known. They take advantage of certain naturally occurring physical properties (such as imperfections in dielectric materials) to create systems which are totally unrepeatable even by the original creator. In this paper, we are defining a new PUF based on magnetic materials which can suffer a spontaneous and unclonable modification of their properties thanks to the exchange-bias effect. This effect only needs an activation process that is done immediately after manufacturing the material. Modifications will depend on the room temperature and, probably (there is no conclusive evidence) on other environmental factors. Besides the activation process, the atomic structure of the material greatly affects the final behavior of this PUF. A unique sample of an activated material should be, then, divided into two elements to create the cipher and the receiver.

The objective of this paper is to provide a mathematical and engineering framework for this novel encryption scheme and key generator system. It is described the proposed architecture and the physical foundations of the electronic device supporting the designed PUF. Moreover, using simulation techniques, the performance of the proposed solution is evaluated.

The rest of the paper is organized as follows: Section 2 describes the state of the art on PUF and security techniques for CPS; Section 3 presents the proposed encryption solution, including the key generator and its mathematical foundations; Section 4 describes the proposed performance evaluation and experimental validation; and Section 5 concludes the paper.

2. State of the Art: Physical Unclonable Functions and Encryption in CPS

Although security and CPS is one of the most interesting and popular research topics nowadays, encryption and security schemes for CPS are pretty standard. In particular, as in most application scenarios, these solutions can be classified into two groups: symmetric and asymmetric key schemes.

Cyber-physical systems, in particular, are usually solutions exchanging information packets, not information streams. Thus, symmetric key schemes in CPS are usually focused on block ciphers [12] of cyclic redundancy checks (CRC) [13] which can detect and/or correct transmission errors caused by natural or intentional causes. This solution, nevertheless, is very inefficient as the amount of information to be exchanged grows. Nowadays, very large amounts of information need to be shared.

In order to improve efficiency in these symmetric key solutions, hardware-supported schemes have been reported [14]. Different sequential circuits focused on encryption may be also found. Nevertheless, in real-time applications, even hardware-based block ciphers are not enough, and stream ciphers are required. Different proposals may be found, although most authors agree the encryption system must be as simple as possible, and the engineering cost must be put on key generation. In this sense, different techniques and pseudo-random number generators (PRNG) [15] for key creation have been described.

These symmetric solutions, however, present a very well-known problem: key distribution. Although this is a problem in any system, in CPS where sparse and resource constrained devices must communication through very unsecure links and networks it is more critical if possible. To address this problem, asymmetric key solutions have been investigated.

Different proposals to adapt cryptography based on elliptic curves to cyber-physical systems may be found [16]. In some occasions, even these mathematical procedures are mixed with nondeterministic effects such as temperature measures to improve the encryption entropy [17]. Employed algorithms are standard solutions such as ElGamal encryption [18,19], although innovative public key infrastructure has also been reported to enable, for example, the transmission of signed information (using high-level data format as JSON) [20].

As a general problem of any of the previously described solutions, all of them require from devices to store a secret key in a ROM or non-volatile memory. A very risky situation in CPS.

Other works have considered a totally new approach based on innovative characteristics of CPS. In particular, taxonomies to classify and analyze the attacks to be suffered by CPS [21] have been proposed. Based on these taxonomies, some intelligent solutions to detect and react to cyber-physical attacks in the most appropriate manner have been studied [5]. Besides, some domain-specific solutions may be also found, especially in the area of Smart Grids [22], industrial control systems [23], or feedback control loops [24].

Nevertheless, these approaches are totally reactive, and only valid to detect and react to attacks that are already running. Although these solutions are needed, schemes to prevent those attacks and keep the private information as a secret are even more important.

In this work, we combine both approaches and define a preventive security scheme (a symmetric key encryption scheme), but which does not require to store a secret key in memory. This objective is reached thanks to physical unclonable functions (PUF).

PUFs [25] formalize the idea of one-way functions, later named 'physical random functions', which consist of the use of systems' random nature properties to identify them [26,27]. In particular, PUFs benefit from all these effects that are non-controllable or non-repeatable to create unique responses from systems to common excitations or challenges. Up to three different types of PUF have been reported: non-electric, electric, and intrinsic.

- Non-electronic PUFs [28] include all functions based on non-electric phenomena, although some electrical components are employed to create challenges or collect responses. These technologies are the oldest techniques in PUFs and are usually based on optical effects. Optical fibers, lasers, etc., present random and uncontrollable behaviors that may be employed to create a PUF. However, these mechanisms are expensive, complex, and require a very precise manipulation. These conditions do not fit CPS requirements, in general.
- Electronic PUFs [29] are those based on electric analog signals suffering random effects. For example, random and unclonable changes in the voltage threshold of solid-state devices such as diodes or transistors. These changes create a personal behavior for each device. The main problem of these PUFs is they may be difficult to measure.
- Intrinsic PUFs [25] are those that naturally arise when manufacturing a system, whose main function is usually different. For example, in logic circuits, time required by signals to go through different paths is slightly different and depends on the manufacturing conditions of each specific circuit (a type of PUF known as an 'arbitrary PUF'). 'Ring oscillator PUF' is also another example of intrinsic PUF.

Different applications for PUFs have been described, including security applications. PUFs have been employed into two basic schemes: key generators and authentication mechanisms. The oldest PUF proposals are related to RFID systems, which include key generators based on PUFs [30]. Some hardware-supported algorithms also include PUFs to increase its entropy [31,32]; and PUF-based random number generators with high randomness levels have been also reported [33,34].

Authorization mechanisms [35] are based on challenge–response tables, which are employed to compare responses to authorization queries.

The proposed encryption mechanism in this work considers an encryption scheme with an electronic PUF embedded in a key generator, because of its low-cost character and reduced dimensions. Besides, only simple manufacturing processes are required to implement the proposed solution, which perfectly fits the characteristics of CPS.

3. Proposed Encryption Scheme

In this section, we described the proposed encryption scheme for CPS. The proposed scheme includes a simple encryption mechanism based on a XOR logic gate, and the PUF-based key generator.

3.1. Proposed Architecture and Global Overview

Figure 1 shows the proposed security solution for cyber-physical systems. In this figure, two different modules are presented: a transmitter and a receiver. In the transmitter, a certain discrete-time digital information $m[n]$ is collected to be transmitted. This information is injected in a symmetric encryption module, represented by $\varepsilon[\cdot]$ operator, together with a key stream $k[n]$. As a result, an encrypted message $e[n]$ is obtained (1).

$$\mathrm{e[n]} = \varepsilon(m[n],\, k[n]) \tag{1}$$

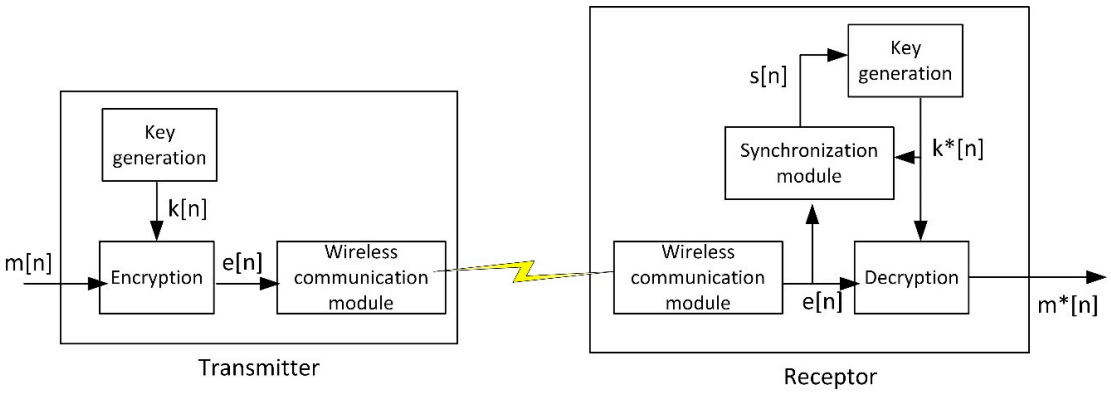

Figure 1. Global overview of the proposed solution.

This message is then transmitted through a wireless communication module. This module may be based on any existing technology such as Bluetooth, WiFi, or ZigBee. Hereinafter, we are assuming no errors are produced during the wireless transmission or, if produced, they are corrected by the native mechanisms considered by these technologies. For this analysis, thus, we are considering this module as a transparent component. The same solution could be applied to more complex scenarios, but additional mechanisms to manage data transmission should be considered (that are not the focus of this article).

Information is, then, recovered by the receiver. As a symmetric encryption scheme is being employed, the same encryption function may be employed to decrypt the original information (2). To this function, in this case, it is injected the encrypted message $e[n]$ and the key stream generated by the receiver $k^*[n]$. A clear information $m^*[n]$ is then obtained.

$$m^*[n] \;=\; \varepsilon(e[n],\, k^*[n]) \tag{2}$$

The recovered information $m^*[n]$ is only equivalent to the original information $m[n]$ only if encryption key $k[n]$ and decryption key $k^*[n]$ are equal. To guarantee both key streams have exactly the same sequence, a synchronization signal $s[n]$ is calculated and injected into the receiver's key generator.

This assumption may be hard to fulfill but different schemes have implemented this mechanism successfully [15,36]. In particular, in our work, we are employing physical unclonable functions. The key generator design based on PUF (see Section 3.3) guarantees the same sequence is generated in both the transmitter and the receiver (Sections 3.3 and 4 will provide evidence about this requirement). The described synchronization signal ensures, besides, both sequences present the same time base (as seen below).

This synchronization signal is calculated through a correlation algorithm in the synchronization module (3). In this algorithm, a simple correlation estimator $c[r]$ between both key streams is obtained. As the key generator guarantees both key streams (N bits length sequences in the transmitter and the receiver) are the same sequence, it is only necessary to analyze the delay r between both keys. The delay to be corrected in the receiver's key is the value for which $c[r]$ is maximum.

$$c[r] = \sum_{n=0}^{N-1-r} k[n+r] \cdot k^*[n] \tag{3}$$

With this synchronization correction, both stream keys are exactly the same sequence [37], and the symmetric encryption algorithm in the receiver may recover the original information.

3.2. Encryption Mechanism

Any existing or new symmetric encryption algorithm could be integrated in the proposed architecture. However, devices in CPSs tend to be resource constrained and, then, computationally low-cost algorithms are preferred. Thus, in this work we propose the use of the XOR (Exclusive OR) encryption. The XOR operation is also employed in some existing encryption solutions such as the Vernam cipher [37] or the one-time pad [38]. However, these mechanisms include some other configurations (such as the key structure or the data format) which are not valid in our proposal. Thus, we are referring the basic encryption technology supporting all these schemes: XOR operation.

This encryption scheme may be easily implemented using a logic gate, and the obtained security level is sufficiently high. Mathematical evaluations can prove this result depends on the randomness of the key stream. In fact, XOR-based encryption presents some vulnerabilities (such as the known-plaintext attack), but most of them are addressed below with the appropriate key generator and, in any case, the balance between the reached security level and the lightweight implementation in XOR encryption is adequate for CPSs [39].

Mathematically, the XOR encryption process may be represented by a simple binary operation (4). The XOR gate receives two data streams to perform the encryption. For this model, information signal $m[n]$ is composed of N bit samples. In that way, $m[n]$ takes values in the range $\{0, \ldots, 2^N - 1\}$. Figure 2 represents the encryption scheme.

$$e[n] = m[n] \oplus k[n] \tag{4}$$

Then, if the employed key stream $k[n]$ is a flow of random numbers, the resulting encrypted signal $e[n]$ has a discrete probability density function equal to the probability function describing the behavior of the key stream $k[n]$. In particular, all possible values have the same probability. Hereinafter, $P(\cdot)$ is the probability operator and $P(\cdot \mid \cdot)$ the conditional probability operator.

$$P(k[n] = \xi_i) = P(e[n] = \xi_i) = \varphi_1 = \frac{1}{2^N} \quad \forall \xi_i \tag{5}$$

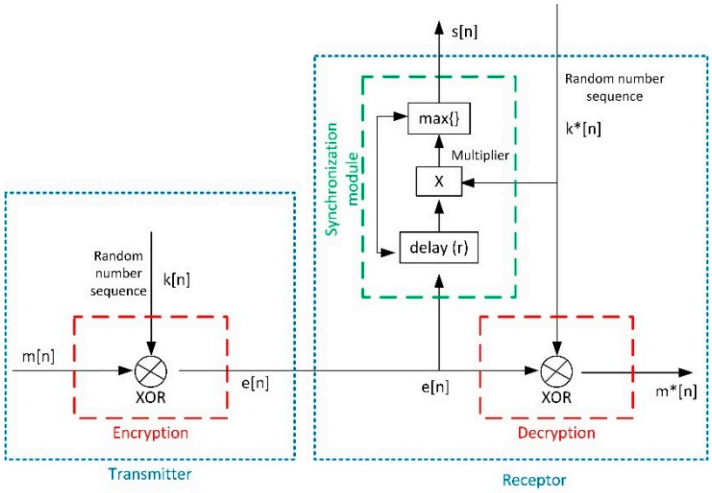

Figure 2. Encryption scheme.

Then, because of the structure of the XOR truth table, a known value from the encrypted signal $e[n]$ of all possible values in the range of the information signal $m[n]$ have the same probability of having generated that encrypted sample (6).

$$P\left(m[n] = \xi_j \mid e[n] = \xi_i\right) = \varphi_2 = \frac{1}{2^N} \quad \forall \xi_i, \xi_j \tag{6}$$

In order to determine how secure the proposed XOR encryption is, we employ Shannon's information theory. The mutual information between the encrypted and the original information flow $I(m;e)$ represents the residual information that remains in the encrypted signal about the original one (7). Considering expressions (5) and (6), it is easy to obtain this amount is zero; i.e., the encrypted signal does not provide any information about the original signal $m[n]$.

$$I(m;e) = \sum_{i=0}^{2^N-1} \sum_{j=0}^{2^N-1} P\left(m = \xi_j\ ,\ e = \xi_i\right) \cdot log\left(\frac{P\left(m = \xi_j \mid e = \xi_i\right)}{P(e = \xi_i)}\right) = 0 \tag{7}$$

This mathematical demonstration is only valid for continuous random key streams. However, random numerical flows are impossible to generate in practice. Then, only pseudorandom number sequences are possible to obtain. Experiments show that a pseudorandom sequence may replace a random flow with some considerations:

- REQ#1: The pseudorandom sequence (which is periodical) must present a long period; enough to encrypt each information message using only one key period
- REQ#2: The same sequence cannot be employed to encrypt an undefined number of messages. The pseudorandom sequences must be changed each certain operation time.
- REQ#3: The algorithm generating the number sequence must be secret.

If these conditions are not fulfilled, then, simple cryptanalysis may break the encryption.

The proposed key generator in the next subsection employs a lightweight PRNG connected to a PUF in order to create pseudorandom sequences with a very large period, including also a dynamic mechanism to dynamically modify this sequence in a secret manner.

This encryption scheme also enables us to easily calculate the synchronization signal through the proposed correlation algorithm. As key streams have a random behavior, their correlation with any

other signal tends to be negligible (8). To prove that, we are obtaining a correlation estimator $c^*[r]$ between the receiver key stream $k^*[n]$ and the encrypted signal $e[n]$.

$$\begin{aligned} c^*[r] &= \sum_{n=0}^{N-1-r} e[n+r]\cdot k^*[n] = \sum_{n=0}^{N-1-r} (m[n+r] \oplus k[n+r])\cdot k^*[n] = \\ &= \sum_{n=0}^{N-1-r} (m[n+r]\cdot k^*[n]) \oplus (k[n+r]\cdot k^*[n]) \approx \sum_{n=0}^{N-1-r} k[n+r]\cdot k^*[n] = c[r] \end{aligned} \tag{8}$$

3.3. Key Generator

As said before, in order to guarantee a total protection level, the proposed key generator must generate a random key stream. Figure 3 shows the proposed design to reach that objective. In order to create a number sequence meeting the three basic requirements described in Section 3.2, in this key generator a simple lightweight pseudorandom number generator (PRNG) is considered to ensure a behavior as random as possible at low computational cost.

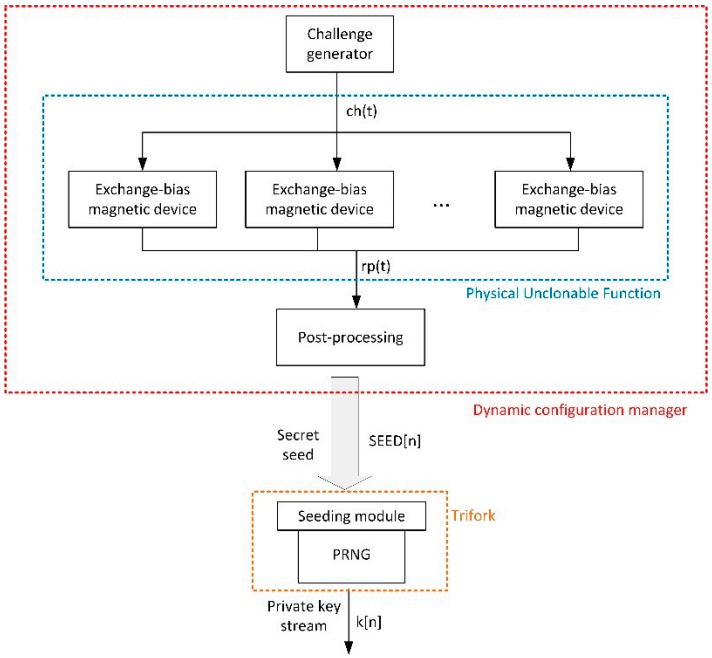

Figure 3. PUF-based key generator.

In particular, we propose the use of the Trifork PRNG [15,40]. This PRNG is based on three perturbed lagged Fibonacci generators (PLFGs), interconnected in such a manner that only using shift registers and OR logic gates make it possible to create a number sequence with a very long period (very random) and totally protected against cyberattacks (as proved by the NIST tests [40]). Then REQ#1 is met.

In order to create the key stream, Trifork must be configured with a secret seed $SEED[n]$. This seed includes three N-bit length values (9), $x_0[n]$, $y_0[n]$, and $z_0[n]$. This collection is employed by a seeding module to create the initial sequence (not included in the secret key stream) to trigger the key generation process.

$$SEED[n] = \{x_0[n],\ y_0[n],\ z_0[n]\} \tag{9}$$

This secret seed $SEED[n]$ also changes with time, in order to guarantee the same secret key stream is not used indefinitely. However, as the period of the sequences generated by Trifork is very long, the secret seed may change quite slowly.

This secret seed is usually stored in a ROM memory, calculated through a certain algorithm or received from remote servers, but all these options have been proven to be unsecure. Thus, in this work this secret seed is calculated using PUF. Figure 4 shows the proposed PUF for seed generation.

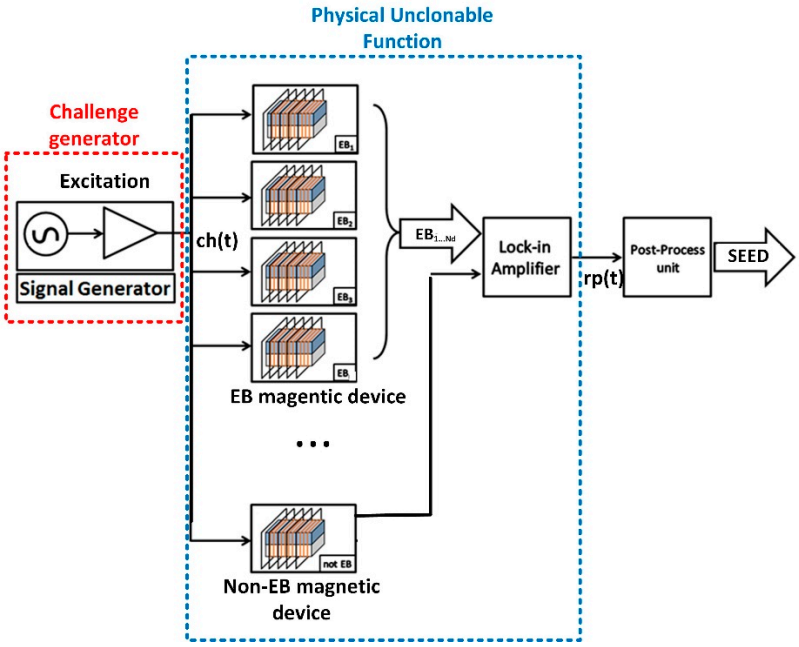

Figure 4. PUF schematics.

As can be seen, the proposed PUF is based on the parallel connection of N_d exchange-bias magnetic elemental devices; and one additional non-EB magnetic device. All these elemental devices are challenged using the same analog excitation. In order to get all magnetic materials (devices) to respond to the excitation (challenge) with an unclonable signal changing with time, we propose the material is activated to suffer the exchange-bias effect (EB).

3.3.1. Exchange-Bias Effect: Overview

Discovered by Meiklejohn and Bean [41] in 1956, they describe the EB as a process that occurs as a result of the interaction between two layers of magnetic material composing the magnetic device: a ferromagnetic (FM) and an antiferromagnetic (AFM) layer. The first (and simplest) consequence of this phenomenon is a displacement of the hysteresis cycle showed by magnetic materials affected by a magnetic field (because of the influence of the atomic spins of the FM on the AFM ions in the contact zone of the two materials, or interface). In a physical sense, an EB device is seen as a united set of magnetic domains that do not interact with each other but have an interface with a ferromagnetic layer, so that each one of the domains in the AFM has a magnetic moment [42].

However, in a more practical context, this effect causes the material magnetization to evolve and change when the material is left at room temperature after activation. It is then when the dependence of the (exchange-bias) magnetic field with $ln(t)$ (logarithm of time instant) becomes noticeable, as stated by O'Grady et al. [43] and Paetzold and Röll [44]. The importance of these results lies in the demonstration that a magnetic device composed of a FM and AFM bilayer behaves depending on the logarithm of time instant and without the intervention of any other variable.

In order to cause a magnetic bilayer to behave in that way, the material must be activated according to a specific process. The manufacturing methods of exchange-bias materials are not a subject of study in this work, but it is important to mention that the activation requires a distribution of the AF material in grains suitable to achieve this activation and thermal stability [43]. This manufacturing process, which will be called 'activation', consists of converting the behavior of the AFM from antiferromagnetic

to paramagnetic in such a way that the spins are oriented in a random manner. This is achieved by heating the material in a temperature range that is between the Néel temperature, T_N (above which an antiferromagnetic material becomes paramagnetic), and the Curie temperature, T_C (above which certain magnetic materials undergo a sharp change in their magnetic properties). This heating is done in the presence of a magnetic field H_{ext} high enough to saturate the ferromagnetic layer, as shown in Figure 5. Once the antiferromagnetic spins are aligned in a random manner, the sample is cooled below the Néel temperature, in what is called the alignment temperature, T_{AL}. If the presence of the saturation field is maintained, not only the spins of the ferromagnetic will be aligned but also those of the interface of the AFM, due to the influence of the spins of the interface of the FM, as seen in Figure 5.

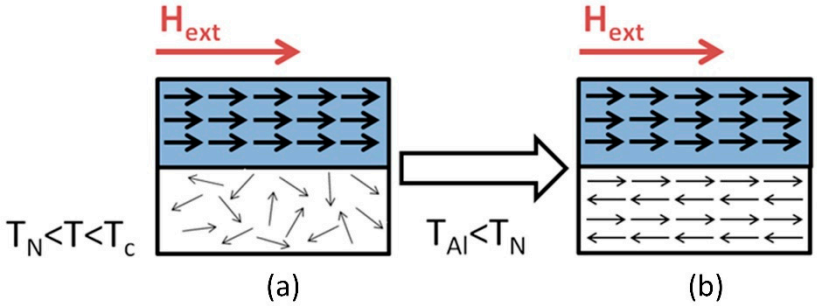

Figure 5. (**a**) Paramagnetic behavior of the AFM. (**b**) Reaching the alignment temperature.

Then, as a conclusion, an EB magnetic device presents a behavior that varies with time. This phenomenon enables us to create seeds also varying with time, so the entire secret key stream will dynamically and automatically change with time, as required (see Section 3.2). This dynamic evolution, besides, does not require any key distribution or communication; benefits from a natural phenomenon. Thus, the proposed scheme is more secure than any other previous proposal. REQ#2 is, therefore, fulfilled.

Although the evolution speed may be quite slow, a Trifork generator can produce very long-period number sequences, fulfilling REQ#1.

Any case, if any manufacturer or attacker could create an EB material behaving in the same manner as those materials employed in our PUF, no security will be provided by this mechanism (REQ#3 will not be met). Nevertheless, the next section describes how unclonable the behavior of these EB materials is; and how impossible it is in practice to either manufacture two identical or similar EB devices or to manipulate an existing EB-based PUF to be employed by cybercriminals.

3.3.2. Unclonable Behavior in EB devices

Only one last requirement (REQ#3) must be fulfilled. It must be guaranteed that the proposed PUF is secret; i.e., the PUF is unclonable and nobody could extract a magnetic device from a hardware node and employ it with unethical objectives.

Figure 6a shows a graphic schematic of an EB device. To create an elemental EB -PUF, two copper coils are associated to the EB material (bilayer). The first coil is a magnetic field generator, wound directly on top of the material. The second copper winding or sensing coil is also on top, to collect the response from the EB material. With this configuration, the proposed device presents a very reduced size.

To perform an electromagnetic analysis, this compact configuration may be expanded (see Figure 6b). In fact, at a short distance, the generator or field source, the magnetic material, and the signal receiving coil operate as if all them are put together.

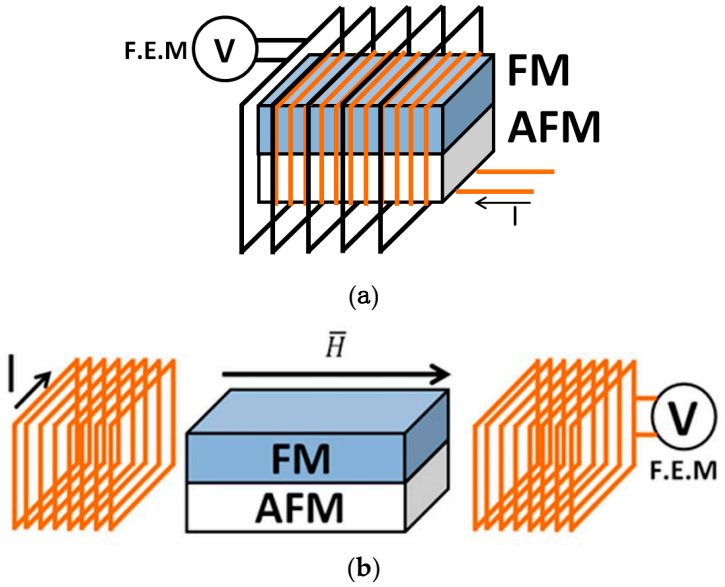

Figure 6. (**a**) Elemental EB device; (**b**) EB device with magnetic core (bilayer material) and separate field sensor.

In order to challenge (excite) the EB material, the field-generator coil produces a magnetic field $\overline{H}$ with two components: a great continuous component $\overline{H}_o$ and a variable field with time (10). The great continuous component is required by EB devices to operate, and the variable field is the challenge to the PUF.

$$\overline{H} = \overline{H}_o + \sum_k \overline{h}\, e^{j\omega_k t} \tag{10}$$

Generating controlled magnetic fields is quite complicated, especially in resource constrained nodes, but using an electrical (current) signal I (11) and the field-generator coil, the required magnetic field (10) may be produced.

$$I = I_o + \sum_k i\, e^{j\omega_k t} \tag{11}$$

The field that is generated in the coil will have a frequential composition that will be equal, as is evident, to the frequential composition of the signal in the excitation current. Thus, the material is subjected to a variable magnetic field and a variable magnetic flux will pass through it. This flow will induce an electromotive force in the sensing coil that will be measured and acquired to create the PUF response, as seen later.

This excitation will generate a magnetization (12) in the material, $\overline{\mathrm{M}}$, where $\overline{M}_o$ is the saturation magnetization at room temperature and $\overline{m}$ is the corresponding RF component. Hereinafter, in order to mathematically demonstrate the unclonable behavior of these EB devices, we are considering the superposition theorem to study each one of the frequential components ω_k in the magnetization and magnetic fields separately (13).

$$\overline{M} = \overline{M}_o + \sum_k \overline{m}\, e^{j\omega_k t} \tag{12}$$

$$\overline{M} = \overline{M}_o + \overline{m}\, e^{j\omega t} \tag{13}$$

The relation between the magnetic field and the magnetization may take different forms (14). However, in EB devices (see Section 3.3.1), the magnetic material (analyzed on a macroscopic scale) is divided around domains with a magnetization $\overline{M}$ when an external continuous magnetic field $\overline{H}_o$ is applied in such a way that it can be said that each domain precesses inside the material around the

axis of application of the magnetic field. Using the equation describing this movement, a new relation between the magnetic field and magnetization is deducted (15).

$$\overline{M} = \left(\frac{\mu}{\mu_0} - 1\right)\overline{H} \tag{14}$$

$$\frac{d\overline{M}}{dt} = -\gamma\mu_o\overline{M} \times \overline{H}_o \tag{15}$$

Where μ is the magnetic permeability in the material (considered isotropic), μ_0 is the magnetic permeability of free space, and γ is a gyromagnetic ratio. This ratio describes the relation between the spin magnetic moment in the material, $\overline{\mu}_B$, which is the moment that an electron spinning has on itself; and the kinetic moment that the electron has in the opposite direction, that will be named $\overline{p}$ (16).

$$\gamma = -\frac{\overline{\mu}_B}{\overline{p}} \tag{16}$$

In all of these expressions, the permeability and gyromagnetic parameters depend on the electronic configuration of the constituent atoms of the magnetic material, as well as on the interaction that exists between them. Both parameters are then, in practice, unclonable and are the basis for the proposed PUF.

In order to create a PUF, the EB devices must respond to the applied challenge or excitation. In magnetic material, this response is the magnetic induction (17); where $\overline{\overline{\mu}}$ is a tensor describing the magnetic permeability in the EB device (which is an anisotropic device, composed by two layers).

$$\overline{B} = \overline{\overline{\mu}}\overline{H} \tag{17}$$

In order to determine how variable the behavior of an EB device is, the value of this tensor must be studied. In particular, considering a second definition of the magnetic induction depending on the magnetic field and the magnetization vector (18), it can be deducted this tensor is the Polder tensor (19) and (20).

$$\overline{B} = \mu_0(\overline{H} + \overline{M}) \tag{18}$$

$$\overline{\overline{\mu}} = \mu_o \begin{bmatrix} \mu_p & -jK & 0 \\ jK & \mu_p & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{19}$$

$$\mu_p = 1 + \frac{\omega_o\omega_M}{\omega_o^2 - \omega^2} \quad K = -\frac{\omega - \omega_M}{\omega_o^2 - \omega^2} \tag{20}$$

The Polder tensor describes, in general, the magnetic permeability of ferrites, but in this case, it may be also employed for EB devices. Two relevant parameters are identified (21): the Larmor frequency ω_o and a new parameter ω_M dependent on the atomic structure of the material (i.e., the magnetization vector).

$$\begin{gathered} \gamma\mu_o H_o = \omega_o \\ \gamma\mu_o M = \omega_M \end{gathered} \tag{21}$$

Although the Lamor frequency may be controlled through the excitation current generating the excitation magnetic field $\overline{\mathrm{H}}_\mathrm{o}$; the 'natural frequency' ω_M (in fact, a resonance frequency, see Section 3.3.3) is uncontrollable and unclonable [45]. Besides, because of the EB effect (see Section 3.3.1) the magnetization vector induced in the device varies with time (depending on the logarithm of the time instant). Then, ω_M will also evolve with time in an autonomous, independent, and uncontrollable manner.

Nowadays, however, there are no instruments or procedures to predict, manipulate, or clone the behavior of this 'natural frequency' ω_M or the EB devices (as it depends on atomic structures) [45].

In fact, in order to create two identical EB devices, a unique magnetic material must be firstly activated and, later, divided into two samples. Besides, any attempt to extract or manipulate the PUF from its casing and operation conditions will modify the magnetization vector and, in consequence, the system behavior, the generated seed and, finally, the secret key stream.

However, before ensuring REQ#3 is fulfilled, it must be evaluated how variations in ω_M affect the PUF responses. Figure 7 shows the evolution in μ_p and K depending on the excitation frequency for different possible values of ω_M.

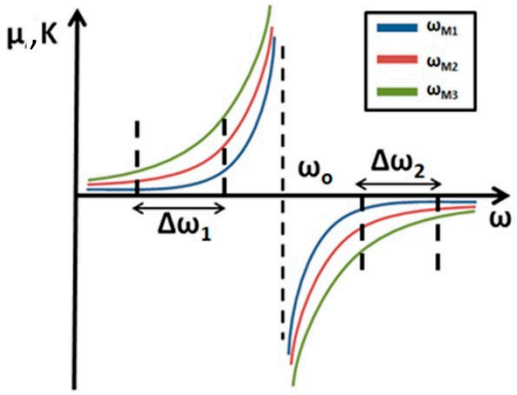

Figure 7. Schematic representation of two possible work zones for the presented EB device.

As can be seen, the response of μ_p and K is similar for all material around the Larmor frequency ω_o, regardless of the value of ω_M. Besides, the same situation occurs for very high or very low frequencies. Then, we will configure the device to work around high frequencies relatively far from the Larmor pulsation. This means that none of the previous terms tend to infinity and, in addition, the term ω_M influences the frequency behavior of the material (see Figure 7).

Finally, it is necessary to acquire or sense the magnetic induction to generate an analog electrical signal. As variable components are always considered in the fields, it is easy to generate that electrical (voltage) signal through an induced electromotive force in a second copper coil (22).

$$\varepsilon = \oint_C E \cdot dl = \int_S NB \cdot \hat{n} dA = \int_S NB_n dA = -\frac{d\phi_m}{dt} \tag{22}$$

With the previous expressions and discussions, it is demonstrated that there is a direct relationship between the magnetization of the material and its behavior as a transmission line for radio frequency signals. Then, as (nowadays) magnetization in EB devices is uncontrollable and unclonable (no work has reported a method to control the natural frequency ω_M) [45], the response of these devices as a transmission line to the applied excitation (challenge) will also be unclonable. REQ#3 is then met.

Then, to create a cipher and decipher pair, an EB material must be generated, divided into two identical samples; and using these samples, two EB devices are constructed. The same process must be repeated to build all required EB devices for both the cipher and the decipher.

3.3.3. Global Behavior and Seed Obtention

Previous equations establish a clear relationship between the components of the permeability tensor and the resonance frequencies of EB devices. In fact, a simple analysis shows that the EB device's resonance frequency (that for which all reactive or imaginary components in $\bar{\bar{\mu}}$ are vanish) is the 'natural frequency', ω_M.

As in any other resonant system, at this resonance frequency, an EB device stores (or consumes) all received energy, so no signal or magnetic induction is transmitted. Then, each one of the EB devices will have the resonance at $f_M = \frac{\omega_M}{2\pi}$ (the particular value will depend of the atomic structure of the material) and will filter any signal within this bandwidth, known as notch band (see Figure 8).

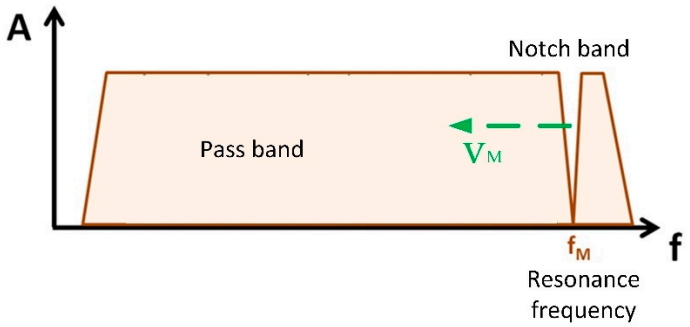

Figure 8. Frequential response of an EB device.

On the other hand, this resonance frequency will vary with time (as already said), with a speed v_M. Experimental studies [45], besides, prove this frequency evolves in downward direction (see Figure 8).

Then, the global PUF proposed in Figure 4 will present a global frequential response calculated as the superposition of N_d notch filters, one for each EB device (see Figure 9). Mathematically, then, when applying a challenge $ch(t)$, a response $rp(t)$ is obtained whose frequential structure is variable and unclonable (23), as the natural frequency ω_M cannot be controlled [45].

$$\begin{aligned} ch(t) &= \sum_{k} C_k \, e^{j\omega_k t} \\ rp(t) &= PUF\{ch(t)\} = \sum_{s=1}^{N_d} \sum_{k} A_s(t) C_k \, e^{j\omega_k t} \end{aligned} \tag{23}$$

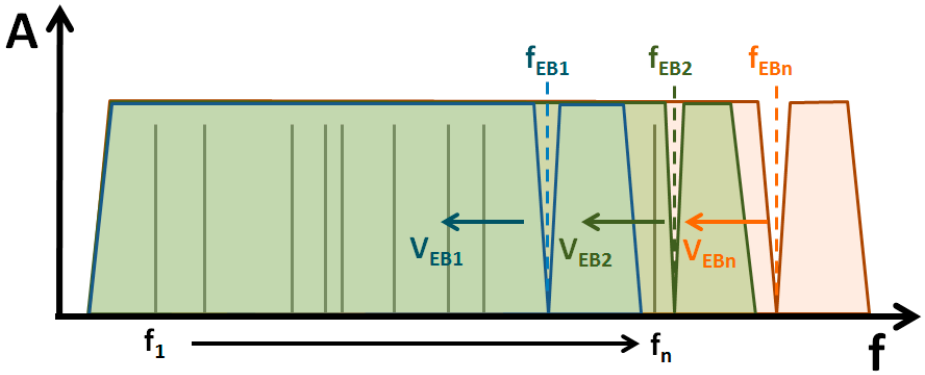

Figure 9. Operation of the complete PUF.

However, to maintain EB devices in the operation conditions, challenges must be mixed with great continuous signals, to create the required continuous magnetic fields. Then, the obtained response will also be mixed with the great signal which must be removed to extract the real PUF response. To perform this operation, in the proposed PUF (see Figure 4) a non-EB device and a lock-in are included.

The non-EB device has the two windings described above and the core is composed of either a bilayer material where the exchange-bias has not been activated and has the initial permeability value) or is an air core (vacuum). The objective of using this core is to isolate the effect on the phase shift of the signal due to the effect of the couplings that may exist in the windings and which, being identical to those that are mounted in the devices with the activated bilayer core, introduce a similar phase shift. In this way, the two signals that enter the lock-in are differentiated only due to the effect generated by the exchange-bias phenomenon.

The lock-in amplifier is often a device that returns a DC signal proportional to the phase shift between two signals and to the amplitude of both signals. Therefore, if the same signal flows through two different paths, the differences in the circuitry of these paths will be what cause the changes in the signal and the difference that the lock-in will measure.

At this point, then, an unclonable and dynamic PUF response to the applied challenge is obtained.

The output signal of the lock-in goes through a post-processing system that measures it and converts it into a valid seed. The output seed of that unit will be the result of a mathematical operation that relates the amplitude of the received signal and its frequency; and therefore, will depend as much on the state of the cores of material bilayer with the effect of exchange-bias developing over time, as the set of signal frequencies that will be introduced into the material (challenge).

Complex algorithms to control the challenge to be applied or the seed calculation could be employed in order to increase the global entropy of the key generator. However, for this initial work presenting the solution, we are considering as challenge a simple composition of N_c harmonics; and the seed calculation was based on a sampling scheme (a sigma-delta modulator) to extract from the analog signal three digital words with the appropriate length. Besides, in order to remove transitory responses and other exogenous effects affecting the seed calculation, the post-processing module was configured to only respond to long-term changes in PUF response. Moving average filters are implemented to perform this function. This technological feature might limit the randomness of the generated keys, but the use of PRNG prevents this problem.

4. Performance Evaluation and Results

In relation to the proposed solution, an evaluation focused on security analyses has no sense, as the final obtained security level is directly dependent on the Trifork PRNG, a technology that has already been validated [40]. On the other hand, a qualitative risk analysis is not relevant at this point, as previous discussions have already proved that most relevant security risks have been addressed. Therefore, for this work, we are proposing an experimental validation based on a performance evaluation and key performance indicators (KPI).

4.1. Experiment Description

Five different experiments were carried out in order to evaluate five basic indicators: (1) randomness level; (2) the bit error rate depending on the accumulated operation time; (3) the distance between key streams generated by a similar PUF; (4) the malfunction probability depending on the number of EB devices in the PUF; and (5) the resource consumption caused by the proposed encryption scheme.

The first four parameters are going to be evaluated with experiments based on simulation scenarios and tools. The last and fifth KPI is evaluated using a real implementation.

Simulation scenarios were built using the MATLAB and SimuLink software tools, which also include mechanisms for electromagnetic and engineering simulations. It is a proprietary suite that employs a specific programming language based on C syntaxis. However, libraries based on other technologies such as C or Java may be employed. This suite was deployed in a Linux (Ubuntu 16.04) machine with 8GB of RAM memory and an Intel i7 processor.

The simulation scenario consisted of two nodes creating a bidirectional communication link between them (see Figure 1). Models for magnetic materials, radio channels, magnetization vectors, etc., were taken from standard existing libraries. The simulation model for the EB devices was configured and characterized through numerical functions fitted to follow and behave as the measures obtained by Migliorini and other authors [45] indicate. Apart from the magnetic components, each node was constructed with a relatively small amount of hardware: a general-purpose embedded processor with analog-digital converters, 5 kilobits of SRAM and 32 kilobytes of DRAM.

In order to pack and assign the described resources to the nodes, virtual containers were employed. In particular, Kernel-based Virtual Machine (KVM) technologies were employed with the libVirt Application Programming Interface (API). In that way, a simple C++ program may be employed to control virtual instances and they may be managed from the MATLAB suite.

With the objective of connecting the virtual instances and the MATLAB suite where the simulation scenario runs, the bridges provided by the MATLAB and Simulink libraries are deployed and executed.

These bridges forward the input traffic in the simulated nodes to the external virtual machine, so real algorithms, solutions, and protocols may be easily tested.

In the first four experiments, simulation tools are adequate to provide relevant results as the limitations due to hardware issues are not evaluated (we are considering nodes can easily implement the proposed cipher). In the last experiment, hardware limitations were considered and real devices were employed.

For the first experiment, the NIST SP 800-22 test suite [46] was considered. This suite includes 15 tests that are usually employed to evaluate the randomness of key generators, PUFs, and other similar proposals. These tests consider two parameters (usually known as α and p) to determine if the evaluated number sequence is random. Basically, the tests evaluate if a sequence is random with a confidence equal to $(1-\alpha)$. Tests obtain the p-value and they are successful (the sequence is random) if it is greater than α. In our experiment we are considering $\alpha = 0.01$. The simulation scenario consisted of the proposed key generator where 64 different EB devices where integrated.

For the second experiment, a collection of different simulations was carried out. For each different simulation, the number of EB devices in the proposed PUF was increased. A bidirectional secure communication link is stablished between both the transmitter and the receiver for each configuration. As a supporting wireless communication module, we have selected a Bluetooth 4.0 technology solution (available in the NS3 libraries). Communication links were configured to be 10Mbps links (Bluetooth 4.0 enables up to 32 Mbps connections). Using these links, 100 information packets per second were transmitted. Each packet was configured to have 100 information bits. Time was divided into 5-h slots. In this time period, $N_{packets} = 1.8 \times 10^6$ packets (or $N_{bits} = 1.8 \times 10^9$ information bits) are transmitted. Then, the resulting amounts are enough to evaluate the bit error rate (BER). Thus, the BER in the stablished communication link was evaluated and measured for each different slot.

The third experiment was performed using a simulation scenario similar to the previous one. Nevertheless, in this case, for each PUF configuration, cipher and decipher were built using 'cloned' PUF. The similarity level between PUF and the resulting key streams are measured and evaluated.

For these three initial experiments, simulations considering PRNG were configured as follows: $N = 16$ to represent a common current situation; and the applied excitation (challenge) to the PUF consisted of a composition of 100 harmonics whose frequencies were calculated using an automatic algorithm (24).

$$f_k = 1000 \cdot \frac{2k}{3} \tag{24}$$

Later, in the fourth experiment, some modifications in the scenario were applied. The cipher and decipher were reconsidered to implement two identical PUF (two samples from a unique EB activated material). The probability of the cipher and decipher not being able to operate correctly due to malfunctions in the PUF is then evaluated. Different configurations and numbers of EB devices in the PUF were considered. With this experiment, the probability of a magnetic material so anisotropic that two samples from the same material do not behave in the same manner is analyzed. The same configuration parameters were employed in this fourth experiment for the cipher and the decipher.

Simulations for these fourth initial experiments were repeated 12 times for each case. Each simulation was configured to represent 360 h of operation.

The fifth and last experiment was completely different from all already described. With the objective of evaluating the effect of hardware limitations, especially in the context of CPS where resource constrained devices are usually employed, in the proposed architecture; a real implementation of the proposed solution was executed. We evaluated the consumption in terms of RAM memory, program space, and computational time. The experiment was repeated for different values of N (the bit-length of number in the PRNG).

As a hardware platform, we employed an Arduino Nano board. It includes an AVR microcontroller, the ATmega328 microcontroller. It also has 32 KB of flash memory, 2 KB of SRAM memory, and 1 KB of EEPROM (which is rarely employed).

The implemented PUF for this experiment was manufactured as indicated by Migliorini [45]. Four different EB devices were employed in the designed PUF.

4.2. Results

In this section, results of the described experiments in the previous section are presented and discussed.

In order to remove from the simulation results (as much as possible) fluctuations in the simulation execution process caused by exogenous variables (e.g., delays operations performed by the operating systems), the average of all obtained results from the 12 performed simulation repetitions are employed to calculate the final results.

Table 1 shows the result from the first experiment.

Table 1. NIST test results. First experiment.

Test	*p*-Value	Result
Runs	0.973	Successful
Frequency Monobit	0.974	Successful
Overlapping Template Matching	0.319	Successful
Frequency Test within a Block	0.654	Successful
Longest Run of Ones in a Block	0.807	Successful
Universal	0.388	Successful
Linear Complexity	0.309	Successful
Binary Matrix Rank	0.419	Successful
Serial	0.999	Successful
Discrete Fourier Transform	0.215	Successful
Random Excursions Test *	0.461	Successful
Random Excursions Variant Test *	0.399	Successful
Approximate Entropy	0.921	Successful
Non-Overlapping Template Matching	0.979	Successful
Cumulative Sums	0.955	Successful

* Several different values for *p*-value where obtained. Result is the mean value.

As can be seen, all tests were successful guaranteeing the randomness of the proposal. Besides, obtained *p*-values are very high (in several tests around the unit), so the randomness level of the evaluated key generator output is also very high.

Figure 10 shows the results from the second experiment. The Bit Error Rate (BER) is evaluated according to the standard expression (25), being N_{error} the number of bit errors in each time period.

$$\text{BER } (\%) = \frac{N_{error}}{N_{bits}} \tag{25}$$

As can be seen, the bit error rate (BER) is always below 0.01%. BER evolution follows a sigmoid curve, where there is an initial period (around 150 h) when BER is stable. Later, BER starts going down until it reaches the value 5×10^{-6}% (approximately) and gets stable another time. This behavior is coherent with the PUF behavior. In fact, as the proposed PUF is not generating directly the key stream, but a seed for a PNRG (which only changes when long-term changes in the PUF response are detected), and as PUF evolves and changes quite slowly, BER may present very low values.

At first, PUF starts generating signals which may still present some very small fluctuations caused by the transitory period in the magnetic field and induction and PUF response. As time passes, and EB effect starts making the resonance frequency evolve, the small fluctuations tend to disappear and BER goes down. However, there is a minimum value for BER due to numerical processing, etc. This also explains why obtained values are very low, as only errors caused by the encryption mechanism are considered. Besides, only a few bits in packets are corrupted, when fluctuations in the magnetic fields caused very fast and transitory drifts in the PUF behavior. No structural errors are detected.

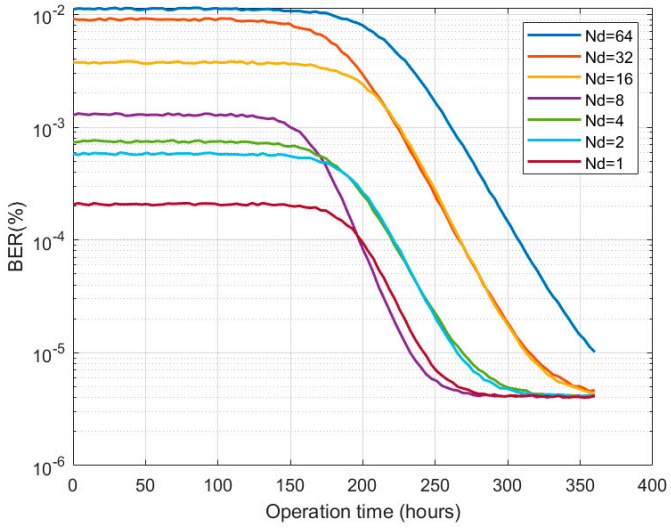

Figure 10. Results from the second experiment.

On the other hand, it can be also seen, as the number of EB devices in the PUF is increased, the initial BER is also higher. In fact, as more different magnetic materials are considered, the power and energy associated to fluctuations in magnetic materials are also higher. Consequently, more errors are induced. In any case, the obtained BER values are similar to those associated to traditional encryption and communication systems [47].

It is important to note that, contrary to other works where real implementations are employed to evaluate BER [34], in this case we are using a simulation scenario where only some effects are considered (in particular, only effects related to EB phenomenon are analyzed). For example, fluctuations in the electrical challenges are not considered. Thus, results with real devices might strongly change (BER may go up several magnitude orders) and advanced techniques, such as error correction modules, could be necessary.

Figure 11 shows the results of the third experiment. Distances between key streams are calculated using a statistical expression. In particular, this distance is defined as the mutual information between both key streams (a similar understating to which employed in context-tree weighting method [48]). Mutual information is null when both streams are statistically independent and equal to N (the number of bits per sample, see Section 3), when they are statistically equivalent. To normalize the mutual information, ranging between zero and N, and turn this function into a distance function a simple algebraic expression is employed (26). This definition guarantees two streams that are 100% different are statistically independent, contrary to traditional (Euclidean) distance definitions.

$$d(k;k^*) = \frac{N - I(k;k^*)}{N} \tag{26}$$

Distance between the manufacturing conditions of two PUF is evaluated using a Euclidean distance and the notion of mean square error. Being C_1 and C_2 vectors describing the manufacturing conditions (M variables), the distance between the two corresponding PUF may be directly obtained (27).

$$d(C_1;C_2) = \frac{1}{M}\sqrt{\sum_{i=1}^{M}(C_1(i) - C_2(i))^2} \tag{27}$$

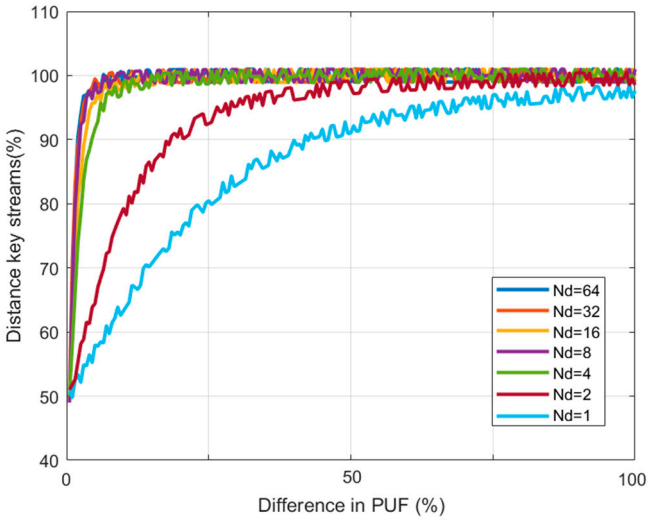

Figure 11. Results from the third experiment.

As can be seen, even two PUFs manufactured as 'clones' generate key streams that are 50% different. In other words, and considering the distance between key streams is evaluated using the mutual information, only half of bits per sample in the key streams are statistically independent. For configurations including more than two EB devices, even PUFs manufactured with only 10% difference generate statistically independent key streams (distance 100%). Configurations including only one or two EB devices also generate independent key streams and secure encryptions (as only identical key streams may grant access to the private information).

However, similar PUFs generate dependent key streams if fewer EB devices are included. Even if as more different PUFs are manufactured the distance between key streams also increases, one-device configurations only produce totally independent key streams for totally different PUFs; while two-device configuration required materials with at least 50% differences.

Any case, this experiment validates the unclonable behavior of the proposed PUF and encryption solution.

Figure 12 shows the results of the fourth experiment.

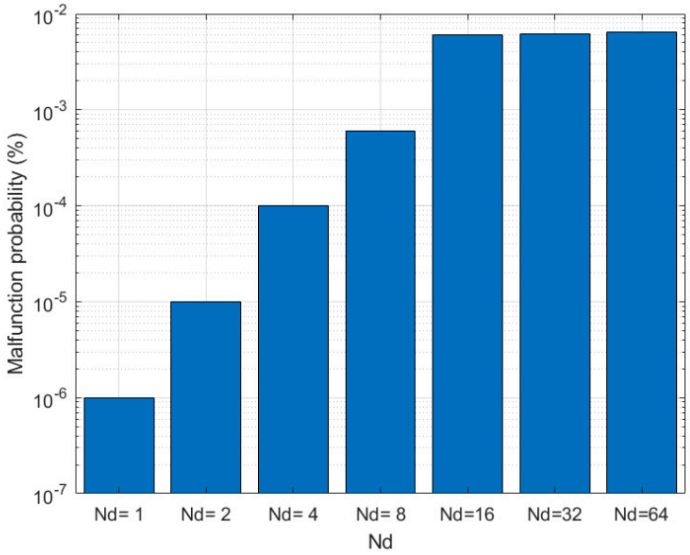

Figure 12. Results from the fourth experiment.

As Figure 12 shows, the malfunction probability is also higher as more EB devices are employed to build the PUF. In fact, as more identical EB devices must be manufactured, the malfunction probability

grows up. In any case, above $N_d = 16$, configurations present a stable malfunction probability around 0.01%. Between $N_d = 1$ and $N_d = 16$, the malfunction probability goes up exponentially, being 10^{-6}% the minimum probability (for a one EB device configuration).

With the four previously described experiments, the performance of the PUF is evaluated. However, one final experiment is required to evaluate indicators related to hardware nodes and limitations.

Table 2 shows the obtained results from the fifth experiment.

Table 2. Resource consumption. Results from the fifth experiment.

N	Use of RAM	Use of Program Space	Processing Time to Generate the First Key Sample
4	12%	65%	120 µs
8	14%	67%	3.9 ms
10	14%	67%	5 ms
12	14%	67%	5 ms
16	14%	67%	5 ms

As can be seen, results are almost independent from the sample length (N). In general, the proposed solution consumes around 70% of available program space in resource constrained nodes. Although this amount may seem too high, the remaining 30% is enough to implement sensing algorithms and other similar small software solutions.

On the other hand, the consumed processing time is quite low, so sampling algorithms can be easily implemented. Considering the required time to encrypt one sample, the fastest signal our nodes could sample is 200 KHz. Traditionally, an Arduino board may consider an analog signal with a maximum bandwidth up to 4.5 MHz. When using our cipher, this quantity is reduced to 200 KHz, but this speed is still enough for most applications.

Once the proposed solution is proven to be adequate for implementation in resource constrained nodes, we can compare resource consumption in our proposal to previously reported solutions. Table 3 shows that comparison.

Table 3. Resource consumption. Comparison to previous works.

Proposal	Memory Usage (ROM and RAM)	Processing Time
PUFKY [34]	3KB	5.62 ms
ROPUF [49]	2KB	4.6 ms
EB PUF (our proposal)	22KB	5 ms

As can be seen, required processing time is similar in all proposals (around 5 ms). However, hardware-supported algorithms present a much lower memory consumption, as they are totally optimized to perform a specific calculation, while implementations based on general purpose microcontrollers need more memory resources. In particular, bootloader, auxiliary variables, sampling routine, etc. mean our proposal consumes 22 KB in memory.

Any case, the proposed solution in this paper may be also implemented using simple logic gates and hardware technologies, so the memory consumption could be also reduced.

5. Conclusions

Cyber-physical systems (CPS) are networked by default, and private information is shared among the different components related to users, critical infrastructure, or business operations. In this context, it is essential to encrypt those communication links to protect such information. However, most solutions require physical devices to store a secret key, which is a very unsecure approach.

Therefore, in this paper, an encryption scheme based on keys generated through physical unclonable functions (PUFs). Using PUFs, any attempt to access to the key will immediately and

irreversibly change the key, and given one PUF, even the manufacturer cannot clone it into an identical one. The proposed key generator is based on magnetic materials to meet the low-cost and small size requirements of CPS. In particular, materials with an activated exchange-bias effect are employed, together with simple copper coils. The encryption process can be based on a simple XOR gate because of the robustness of the proposed key generator.

Results prove the unclonable behavior of the proposed PUF and the security level of the described encryption scheme. On the other hand, the described solution also meets the requirements of resource constrained nodes in a CPS.

Author Contributions: The contributions described in this work are distributed among the authors as follows: All authors wrote the paper; M.P.-J. and A.M. contributed to the theoretical formalization; R.A. contributed to the proposal of the different simulation paradigms; and B.B. developed the global architecture and application model.

Funding: The research leading to these results has received funding from the Ministry of Economy and Competitiveness through SEMOLA (TEC2015-68284-R) project and from the Ministry of Science, Innovation and Universities through VACADENA (RTC-2017-6031-2) project.

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

References

1. Bordel, B.; Alcarria, R.; Robles, T.; Martín, D. Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things. *Pervasive Mob. Comput.* **2017**, *40*, 156–184. [CrossRef]
2. Sánchez, B.B.; Alcarria, R.; de Rivera, D.S.; Sánchez-Picot, A. Enhancing Process Control in Industry 4.0 Scenarios using Cyber-Physical Systems. *JoWUA* **2016**, *7*, 41–64.
3. Lee, E.A. Cyber-physical systems-are computing foundations adequate. In Proceedings of the Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, TX, USA, 16–17 October 2006; Volume 2, pp. 1–9.
4. Bordel, B.; Alcarria, R.; Jara, A. Process execution in humanized Cyber-physical systems: Soft processes. In Proceedings of the 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21–24 June 2017; pp. 1–7.
5. Bordel, B.; Alcarria, R.; Sánchez-de-Rivera, D.; Robles, T. Protecting industry 4.0 systems against the malicious effects of cyber-physical attacks. In Proceedings of the International Conference on Ubiquitous Computing and Ambient Intelligence, Philadelphia, PA, USA, 7–10 November 2017; pp. 161–171.
6. Bordel, B.; Alcarria, R.; Robles, T.; Sánchez-Picot, Á. Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in Ambient Intelligence Environments. *IEEE Access* **2018**, *6*, 34896–34910. [CrossRef]
7. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
8. Xu, Z.; Liu, X.; Zhang, G.; He, W.; Dai, G.; Shu, W. A certificateless signature scheme for mobile wireless cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, ICDCS'08, Beijing, China, 17–20 June 2008; pp. 489–494.
9. Robles, T.; Bordel, B.; Alcarria, R.; Sánchez-de-Rivera, D. Blockchain Technologies for Private Data Management in AmI Environments. *Proceedings* **2018**, *2*, 1230. [CrossRef]
10. Sánchez-de-Rivera, D.; Martín, D.; Alcarria, R.; Bordel, B.; Robles, T. Towards a Wireless and Low-Power Infrastructure for Representing Information Based on E-Paper Displays. *Sustainability* **2017**, *9*, 76. [CrossRef]
11. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
12. Lai, X. *On the Design and Security of Block Ciphers*; Eidgenössische Technische Hochschule Zürich: Zürich, Switzerland, 1992.
13. Koopman, P.; Chakravarty, T. Cyclic redundancy code (CRC) polynomial selection for embedded networks. In Proceedings of the International Conference on Dependable Systems and Networks (DNS'04), Florence, Italy, 28 June–1 July 2004; pp. 145–154.
14. Martin, H.; Peris-Lopez, P.; Tapiador, J.E.; San Millan, E. An Estimator for the ASIC Footprint Area of Lightweight Cryptographic Algorithms. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1216–1225. [CrossRef]

15. Bordel, B.; Orue, A.B.; Alcarria, R.; Sanchez-De-Rivera, D. An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators. *IEEE Access* **2018**, *6*, 16149–16164. [CrossRef]
16. Miller, V.S. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology—CRYPTO '85 Proceedings*; Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, 1985; Volume 218.
17. Porambage, P.; Schmitt, C.; Kumar, P.; Gurtov, A.; Ylianttila, M. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In Proceedings of the 2014 IEEEWireless Communications and Networking Conference (WCNC'14), Istanbul, Turkey, 6–9 April 2014; pp. 2728–2733.
18. Vegh, L.; Miclea, L. Enhancing security in cyber-physical systems through cryptographic and steganographic techniques. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–6.
19. Kogiso, K.; Fujita, T. Cyber-security enhancement of networked control systems using homomorphic encryption. In Proceedings of the 54th Annual Conference on Decision and Control (CDC), Osaka, Japan, 15–18 December 2015; pp. 6836–6843.
20. Pohls, H.C. JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application. In Proceedings of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15), Blumenau, Brazil, 8–10 July 2015; pp. 306–312.
21. Yampolskiy, M.; Horváth, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. A language for describing attacks on cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 40–52. [CrossRef]
22. Mo, Y.; Kim, T.H.-J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber–Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* **2012**, *100*, 195–209.
23. Pasqualetti, F.; Dorfler, F.; Bullo, F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Proceedings of the 50th IEEE Conference on Decision and Control, a European Control Conference (CDC-ECC'11), Orlando, FL, USA, 12–15 December 2011; pp. 2195–2201.
24. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–Physical System Security for the Electric Power Grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]
25. Maes, R.; Verbauwhede, I. *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*; Springer: Berlin, Heidelberg, 2010.
26. Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, 18–22 November 2002; pp. 148–160.
27. Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Controlled physical random functions. In Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 9–13 December 2002; pp. 149–160.
28. Chen, Q.; Csaba, G.; Lugli, P.; Schlichtmann, U.; Ruhrmair, U. The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions. In Proceedings of the 2011 IEEE International Symposium on Hardware- Oriented Security and Trust (HOST'11), San Diego, CA, USA, 5–6 June 2011; pp. 134–141.
29. Bohm, C.; Hofer, M. *Physical Unclonable Functions in Theory and Practice*; Springer: New York, NY, USA, 2013.
30. Devadas, S.; Suh, E.; Paral, S.; Sowell, R.; Ziola, T.; Khandelwal, V. Design and Implementation of PUFBased "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In Proceedings of the 2008 IEEE International Conference on RFID (IEEE RFID'08), Las Vegas, NV, USA, 16–17 April 2008; pp. 58–64.
31. Guajardo, J.; Kumar, S.S.; Schrijen, G.-J.; Tuyls, P. Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection. In Proceedings of the 2007 International Conference on Field Programmable Logic and Applications (FPL'07), Amsterdam, The Netherlands, 27–29 August 2007; pp. 189–195.
32. Kumar, S.S.; Guajardo, J.; Maes, R.; Schrijen, G.-J.; Tuyls, P. Extended abstract: The butterfly PUF protecting IP on every FPGA. In Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), Anaheim, CA, USA, 9 June 2008; pp. 67–70.
33. Yu, M.-D.; Sowell, R.; Singh, A.; M'Raihi, D.; Devadas, S. Performance metrics and empirical results of a PUF cryptographic key generation ASIC. In Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'12), San Francisco, CA, USA, 3–4 June 2012; pp. 108–115.
34. Maes, R.; Van Herrewege, A.; Verbauwhede, I. PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES'12), Leuven, Belgium, 9–12 September 2012; Springer: Berlin, Heidelberg, 2012; Volume 7428, pp. 302–319.

35. Suh, G.E.; Devadas, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceedings of the 44th ACM/IEEE Design Automation Conference, San Diego, CA, USA, 4–8 June 2007; pp. 9–14.
36. Mareca, P.; Bordel, B. Robust hardware-supported chaotic cryptosystems for streaming commutations among reduced computing power nodes. *Analog Integr. Circuits Signal Process.* **2019**, *98*, 11–26. [CrossRef]
37. Ryabko, B.Y. The Vernam cipher is robust to small deviations from randomness. *Probl. Inf. Trans.* **2015**, *51*, 82–86. [CrossRef]
38. Dodis, Y.; Spencer, J. On the (non) universality of the one-time pad. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, BC, Canada, 16–19 November 2002; pp. 376–385.
39. Buchanan, W.J.; Li, S.; Asif, R. Lightweight cryptography methods. *J. Cyber Secur. Technol.* **2017**, *1*, 187–201. [CrossRef]
40. Orue, A.B.; Montoya, F.; Hernández Encinas, L. Trifork, a new pseudorandom number generator based on lagged fibonacci maps. *J. Comput. Sci. Eng.* **2010**, *2*, 46–51.
41. Meiklejohn, W.H.P.; Bean, C.P. New Magnetic Anisotropy. *Phys. Rev.* **1956**, *102*, 1413–1414. [CrossRef]
42. Fulcomer, E.; Charap, S.H. Temperature and frequency dependence of exchange anisotropy effects in oxidized NiFe films. *J. Appl. Phys.* **1972**, *43*, 4184–4190. [CrossRef]
43. O'Grady, K.; Fernandez-Outon, L.E.; Vallejo-Fernandez, G. A new paradigm for exchange bias polycrystalline thin films. *J. Magn. Magn. Mater.* **2010**, *322*, 883–889. [CrossRef]
44. Paetzold, A.; Röll, K. Thermally activated self-alignment of exchange coupling in NiO/NiFe bilayers. *J. Appl. Phys.* **2002**, *91*, 7748. [CrossRef]
45. Migliorini, A.; Kuerbanjiang, B.; Huminiuc, T.; Kepaptsoglou, D.; Muñoz, M.; Cuñado, J.L.F.; Camarero, J.; Aroca, C.; Vallejo-Fernández, G.; Lazarov, V.K.; et al. Spontaneous exchange bias formation driven by a structural phase transition in the antiferromagnetic material. *Nat. Mater.* **2018**, *17*, 28. [CrossRef] [PubMed]
46. NIST Special Publication 800-22 (2001). Available online: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final (accessed on 30 March 2019).
47. Argyris, A.; Syvridis, D.; Larger, L.; Annovazzi-Lodi, V.; Colet, P.; Fischer, I.; García-Ojalvo, J.; Mirasso, C.R.; Pesquera, L.; Shore, K.A. Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature* **2005**, *438*, 343–346. [CrossRef] [PubMed]
48. Schrijen, G.J.; Van Der Leest, V. Comparative analysis of SRAM memories used as PUF primitives. In Proceedings of the 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 12–16 March 2012; pp. 1319–1324.
49. Günlü, O.; Kernetzky, T.; İşcan, O.; Sidorenko, V.; Kramer, G.; Schaefer, R. Secure and Reliable Key Agreement with Physical Unclonable Functions. *Entropy* **2018**, *20*, 340. [CrossRef]