SN Computer Science (2020) 1:259
https://doi.org/10.1007/s42979-020-00274-0

ORIGINAL RESEARCH

Conception and Evaluation of Secure Circuits for Strong Digital PUF

Johan Marconot[1,2] · David Hely[2] · Florian Pebay-Peyroula[1]

Received: 4 May 2020 / Accepted: 27 July 2020 / Published online: 11 August 2020

Abstract

Physical unclonable functions (PUFs) are efficient primitives to generate authentication signatures and security keys. However, PUFs may be sensitive to noise and environmental conditions inducing reliability issues. Digital PUFs (DPUFs), which are by design inherently robust, have recently been proposed in the literature. They rely on static source of entropy: random structures produced by specific manufacturing process. In this paper, we propose secure efficient circuits to extract responses from these structures and further develop strong DPUF model. We first review the existing DPUF fabrication processes and associate extraction circuits, and discuss possible optimization in terms of cost and security. We notably use substitution–permutation networks (SPN) as a logical scheme to extract the DPUF data. The SPN circuit performances depend not only on network parameters but also by dimension and randomness of DPUF structures. We modelize and evaluate diverse SPN circuit settings providing ideal configurations for security-cost trade-off. Finally, we measure the implementation cost, identifying the most optimized configuration which reduces the circuit area. Our final SPN circuit for strong DPUF model needs less than 12,000 um^2 circuit area (for a 45 nm technology node) and diffuseness is estimated to 0.5 ± 0.001. The results make SPN-based strong DPUF a pertinent alternative to classic PUF.

Keywords Physical unclonable function · Digital PUF · Diffuseness · Substitution–permutation network · Implementation cost

Introduction

Physical unclonable functions (PUF) are being known as a promising way to build efficient authentication mechanisms for integrated circuit (IC). Not reproducible and unpredictable fluctuations of IC manufacturing process ensure for each IC an unclonable physical disorder. A PUF measures a chosen physical parameter (e.g. time [1], frequency [2] …) to extract a unique chip signature. PUFs are based on challenge–response mechanisms which are classified in two categories: strong and weak. A rigorous definition is given in [3]: a PUF is classified as strong if it has a large challenge–response pairs (CRP) space, qualified as non-enumerable, and this CRP space scales exponentially with the PUF design size. As depicted on Fig. 1, in the strong PUF model a logical circuit receives a digital challenge and returns a response back depending on both the challenge and the physical disorder. On the contrary, a weak PUF just deals with a few challenge–response pairs with a linear or polynomial CRP space growth. Sometimes, as depicted in Fig. 1, a weak PUF implementation only consists of a stand-alone

This article is part of the topical collection “Hardware-Assisted Security Solutions for Electronic Systems” guest edited by Himanshu Thapliyal, Saraju P. Mohanty, Wujie Wen and Yiran Chen.

Electronic supplementary material The online version of this article (https://doi.org/10.1007/s42979-020-00274-0) contains supplementary material, which is available to authorized users.

✉ David Hely
david.hely@grenoble-inp.fr

Johan Marconot
Johan.marconot@grenoble-inp.fr

Florian Pebay-Peyroula
florian.pebay@cea.fr

[1] University of Grenoble Alpes, CEA, LETI, DSYS, Grenoble, France

[2] University of Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France

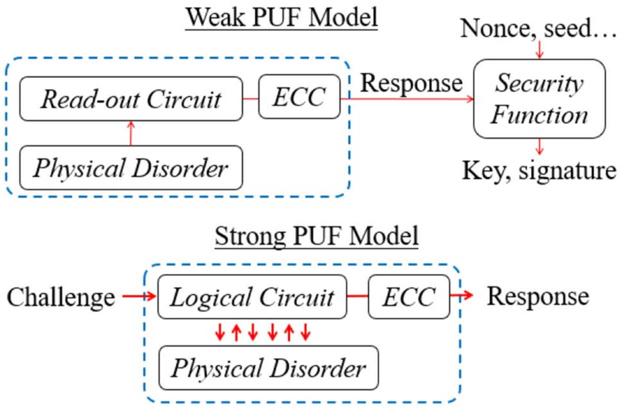

Fig. 1 The weak PUF and strong PUF models

response extracted by a simple read-out circuit. Strong and weak models differ in term of properties and utilization. A weak PUF is generally coupled with security functions; derivation process to generate key or signatures. For this purpose, it requires external nonce or seed and additional processes. At the opposite, a well-defined strong PUF with a large CRP space can be directly used in authentication protocols. Strong PUFs appear to be good candidate to enable authentication features and to optimize the tradeoff between cost and security [4].

PUFs are usually based on continuous physical or analogic measurements which are sensitive to external influence (temperature, humidity …) and also to aging. A PUF response could then not be correctly extracted and may lead to a wrong authentication. Such issues are usually solved by additional circuitry, including error correcting code (ECC) and reconstruction scheme [5, 6]. This extra hardware increases the cost of PUFs; strong ECC circuits exceed thousands of logic gates [5], and induce also a risk of information leakage [7]. The reproducibility of the response is a key factor when designing a PUF, it implies to focus on measurable robust parameters. However, the exhaustive and pertinent study realized by the University of Singapore [8] shows that, whatever random physical parameters is chosen as source of entropy, the PUF design still needs ECC. Thus, the current trends slightly step aside from the construction of high reliable PUF, and focus on other properties. At this point, a novel proposal for a reliable PUF is interesting only with a “perfect” stability. These last years, the most robust designs which have been proposed are the digital PUF (DPUF) [9–12]. These PUFs exploit structural variations—interconnections randomly interrupted—obtained by fluctuations of a customized fabrication process. Since the structures are inherently robust their evaluation by the logical circuit is reproducible. Such primitive is named as a “digital PUF” (i.e. DPUF) in [9], in reference to the digital nature of the disorder on which relies the response extraction.

The subfield related to digital PUF is still new, the literature contains few propositions covering both weak and strong model for DPUF implementation. Strong DPUFs are interesting for devices which need authentication functions with high entropy, and at the same time, have severe lifecycle and operating constraints which prohibit the use of conventional PUFs [13]. However, an adequate extraction circuit is required, with low implementation cost and secure scheme for the challenge–response mechanism generation to respect both performance and security objectives. In this paper, we present our work on DPUFs extending a previous contribution on the conception of strong DPUF circuits [14] focusing specifically on the extraction circuit. DPUF extraction circuits leverage the random DPUF structure to implement a challenge–response mechanism. The main motivations of this work are twofold, first, it aims at developing secure and efficient extraction circuits for Digital PUF primitives and second, it aims at providing evaluation results to help a designer to set-up the best configuration considering the DPUF primitive parameters and the security needs and the expected application security.

We first introduce the DPUF definition and review proposed DPUFs in the literature, presenting the primitive itself and the associated extraction circuit when available. We then investigate extraction circuits based on mathematic schemes which could fulfil the desired security properties of a strong DPUF primitive such as unpredictability, randomness and diffuseness. We propose a new extraction circuit based on substitution–permutation network (SPN) to implement a secure challenge–response mechanism leveraging DPUF primitive. We name this novel architecture SPN-DPUF and performed an analysis of circuit parameters taking account of both security metrics and implementation cost. The main contributions of this work are:

- The review of DPUF proposals in the literature and formalization of a DPUF model
- The usage of a SPN scheme for a secure and efficient DPUF extraction circuit.
- An evaluation and optimization of SPN circuit configurations for a security-cost trade-off.

In "Digital PUF Evaluation Criteria", we discuss the evaluation criteria for the DPUF conception, security metrics as well as performance indicators. In "State of Art of Digital PUF", we present similar works on DPUFs with both aspects of conception (i.e. method to generate random structure and extraction circuit). In "Substitution–Permutation Network Architecture for Strong DPUF", we describe our SPN-DPUF architecture and strategies to optimize the security-cost trade-off of the circuit. In "Optimization and Analysis of DPUF Circuit", we evaluate and optimize the SPN circuit, including previous listed metrics. In the final

"Perspective for the SPN-DPUF", we investigate not only the global cost and constraint to integrate a complete Strong DPUF picking up one of the randomization processes, before to conclude the paper by discussion on perspectives but also the limits of DPUFs.

Digital PUF Evaluation Criteria

Security Metrics for PUF Primitives

Given an adequate DPUF manufacturing process, the random structures (hardware primitive) must provide sufficient entropy for the responses returned by the extraction circuit. Standard requirements must be verified; basically, randomness tests are performed to prove that the state of the structures is non-biased. Moreover, the structure must be large enough to offer numerous combinations of random states and to avoid collision between the manufactured structures. In addition, the extracted response should respect the required length for security data (at least 80 bits as specified in the ISO/IEC standard on lightweight security techniques [15]). Both the structure dimensions and the extraction circuit configuration impact such requirements. In theory, if the randomization process is well designed, the unique and unclonable state of the randomized structure obtained during the fabrication ensure the uniqueness of the DPUF responses. The response properties also depend on the extraction circuit model. Indeed, the way the data issued by the hardware primitive are extracted considerably influence the DPUFs properties. If they are poorly extracted, they may not meet usual PUFs security requirements. The PUF responses (depending on both the randomized structure and the extraction process) should respect mathematical properties. These properties are thoroughly studied in the literature, including discussion on the adequate security model to evaluate a PUF [16-18]. The most important and common properties are clearly defined in [19], discussing the future standardization of PUF based security parameter features (ISO/IEC 20897). Table 1 gives the metrics on which we focus in this paper:

Uniqueness

For any pair of PUFs, it should not be possible to find a challenge for which both PUFs return the same response. The so-called Inter Hamming Distance metric is usually used to evaluate this parameter.

Randomness

For a given challenge, it should not be possible for an adversary to predict the response. The uniformity (i.e. the rate of 1 and 0 in the response bit stream) is the first basic metric used to verify the randomness.

Second, there are standard test suits which aim at evaluating the level of randomness. The NIST provides software tools to determine if a security primitive is suitable for the security data generation, testing a wide range of diverse statistical properties [20]. Each test evaluates for a sample of numbers the p value, the probability under which the tested number is assumed to be not random and thus is rejected. The NIST proposes a threshold fixed to 0.001 for the *p* value and 96% of the numbers should pass the test as a condition to accept the source of randomness.

Third, some prefer to focus on the entropy which is commonly used in information security. For a given bit stream, it aims at estimating the true amount of entropy bit which corresponds to the equivalent security key level. As an example, from a response of size 128 bits if only 64 entropy bits can be extracted it means that the effective security key length is 64 bits*;* which could be broken by a well-conceived brute force attack. In the PUF literature the min-entropy is used as a metric to estimate the amount of entropy bit in a response; formal definition is given in [21].

Table 1 Security metrics for PUF evaluation

Properties	Metrics	Description	Ideal value
Uniqueness	Inter hamming distance	Average hamming distance of responses of distinct PUF Instances to the same challenge	0.50
Randomness	Uniformity	Ratio of 1 s and 0 s for the PUF responses	0.50
	NIST test	Ratio of success for each test given *p* value = 0.001	96% success rate
	Min-entropy	Equivalent security key size	At least 96 bits
Diffuseness	Avalanche effect	Average hamming distance of responses of a PUF instance for a pair of challenges which have only one bit of difference	0.50
	Strict Avalanche effect	Bit modification rate for each bit position in the responses	0.50 for each output bits

Diffuseness

For any PUF challenge/response pairs, it should not be possible for an adversary to distinguish at which challenge is corresponding a response (i.e. the response can hardly be linked to the challenge). It can be measured using the avalanche effect, such as for the SD-PUF evaluation in [9], which consists in measuring the Hamming distance of DPUF responses for two challenges which only have one different input bit. We compute the average of the metric for several response pairs to estimate the quality of the diffusion. This metric can be enhanced by analyzing the strict avalanche effect (SAE), a more accurate metric used in cryptology [22]: it consists in computing, for the previous set of response pairs, the bit modification rate for each bit position in the responses. We focus in this work on security metrics which evaluate the properties of the DPUF to be a good candidate to build secure cryptographic protocol. This study focuses only security properties of the data generated by the DPUF, other system level will need to be evaluate such as the resilience to modeling attack or side channel. It exists system level countermeasure which are independent of the circuit which can be implemented at the system level to prevent such attacks such as the one described in [30].

For a DPUF, such properties depend on the entropy provided by the randomized structures (i.e. the digital PUF primitive) and on the characteristics of the chosen interrogation circuit. To fulfil all these requirements, an adequate interrogation circuit is required to better exploit the PUF primitive, with low implementation cost but still providing the expected mathematic properties.

Indicators for Security-Cost Trade-Off

The implementation cost as well as performance are crucial for the interrogation circuitry. If the circuit lacks of efficiency it may be prohibitive in case of resource-constrained devices. Essential criteria lead the conception: used circuit area, power consumption, speed. Priority is given to one or the other depending on the objectives or constraints of the use case. Specific metrics have to be considered to fairly evaluate and compare the PUFs security level as well as their performance.

These last decades, numerous PUF have been proposed over the literature. It is challenging to establish an exhaustive and pertinent comparison of PUFs. A database is hosted by the Singapore University [8], enumerating the results of large set of PUFs; including classic PUF metrics such as instability rate or inter-PUF distance… The study details also the circuit area and consumed energy when they are provided by the authors of PUF proposals; it also includes normalization approaches based on computation of performance per bit (energy per bit, area per bit). Also, the standard ISO/IEC 29192 [23] formalizes the metrics to evaluate performance of lightweight cryptography primitives. The report has a huge focus on the requirements for hardware implementation of crypto-primitives which faces the same environment and use case constraints than the PUFs. Thanks to these references, we establish a set of indicators for the evaluation of PUF performance and compare the different proposals. Still, the ideal security-cost trade-off depends on objectives and constraints of use case.

Metrics for Chip Area

(1) The couple circuit area (um^2) and technology node (nm), a precized reference for a circuit surface. (2) The normalized technology-independent area per bit which allows a fair comparison between primitives.

Metrics for Power Consumption

(1) The total amount of consumed power (W) to produce a response. (2) The energy per bit (pJ/bit) which allows a fair comparison between primitives.

Metrics for the Speed Performance

(1) The operating frequency (MHz) of the circuit. (2) The latency (s) for the PUF to produce a response. (3) The throughput (kb/s) indicating the global speed performance.

In addition to security and performance criteria, as explained in the introduction, the PUF hardware primitive could be very sensitive to environment and aging. Consequently, a PUF response which was measured earlier in IC lifecycle may not be correctly extracted a 2nd time. The *robustness* of PUF is evaluated using the intra Hamming distance. The next section shows that recent DPUF proposals provide reliable response extractions which solve the instability issue. In this case, the evaluation objectives focus on security and cost requirements.

State of Art of Digital PUF

Presentation of the Digital PUF Model

The adjective “digital” to qualify the DPUF model was introduced in [9] where a pure digital structure is used as a static source of entropy. As depicted on Fig. 2, electrical contacts are randomly closed with a specific method during lithography, it generates a unique and random grid of closed/opened contacts for each chip. This is the so-called DPUF primitive which is robust by nature. An extraction circuit converts the electrical discontinuities of the structure into bit streams used as PUF responses. Other terms are used:

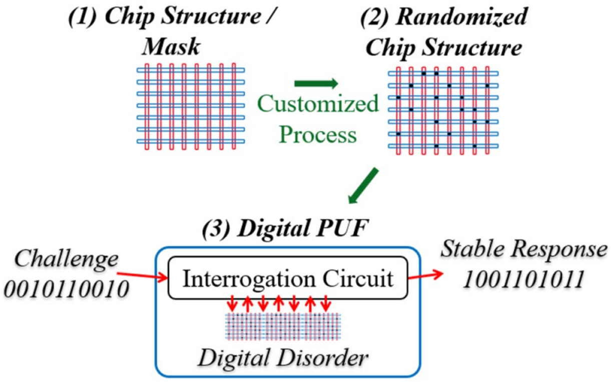

Fig. 2 The digital PUF model

"physical-based VIA-PUF" [10] or "self-assembly PUF" [11, 12] depending on the method to generate the random structure (i.e. the DPUF primitive). The recent survey [3] offers a well-clarified taxonomy, including a parametric-based PUF classification. In this scheme, the DPUFs are classified as PUFs using binary connectivity as evaluation parameter. In this paper, we use the term "digital PUF" (DPUF); and we define a DPUF as a PUF respecting these statements:

1. The evaluation parameter is a digital source of entropy strongly resistant to noise or aging, perfectly stable at the point there is no requirement for a correction code.
2. The response generation, from the evaluation parameter to the final extracted bit streams, is a purely digital process.
3. A DPUF is a robust and functional digital circuit, thus the DPUF implementation respects the integrated circuit conception flow and fits all design timing constraints.

The DPUFs are reliable by design, avoiding the need of noise extractor and error correction processes. This inherent property advantages the DPUFs over the classic sensitive PUFs, making them pertinent for use case as on-field devices facing harsh environmental conditions, and also devices concerned by the circuitry aging. This digital PUF paradigm can bring benefits for security features. The literature provides well-described proposals, in each of them the DPUF conception relies on the two already cited basic blocks, as seen in Fig. 2: (1) a customized process which produces random structures. (2) An extraction circuit which exploits the binary connectivity of the structure as a random digital parameter to produce a stable response.

Both of these basic blocks may be specified independently of each other; diverse processes may be used with the same circuitry, and vice versa. Also, the physical specifications of random structures can vary, even be arbitrary restricted. This wide range of choice for the DPUF conception offers a complex problematic when one wants to efficiently respect security and performance objectives. Both manufacturing process and extraction circuit have an impact on performance, cost and security of DPUFs. Here, the extraction circuit is a key element, it influences both the DPUFs costs parameters such as circuit area and the mathematic properties of the generated response. Several circuits have already been proposed in the literature: weak PUF model with not only simple read-out circuit [10] but also complex logical network [9] acting as a challenge–response mechanism and thus implementing a strong DPUF model. This DPUF offers a large space of CRPs useful for multiple authentications and with a high capacity of reproducibility due to its inherent robustness. In the next sections, we investigate the properties and results of DPUFs proposed in the literature; SD-PUF [9], VIA-PUF [10], LED-PUF [11] and CNT-PUF [24]. We consider separately the random structure fabrication method and the extraction circuit which can be virtually independent from each other.

Fabrication Process for the DPUF Structures

A few techniques have been proposed so far in the literature to introduce random disorder at fabrication time. These methods are described hereafter, all of them lead to reliable material ensuring the DPUF robustness.

The SD-PUF in [9] relies on specific sub-lithographic dimensions for the DPUF mask, fixing the interconnect layout line-ends close to each other. Thus, random discontinuities are produced in the metal layer due to unpredictable and uncontrollable variations during lithography. Evaluations were performed on data generated by a lithography simulation tool obtaining a perfect reliability. In this case, the connectivity rate depends on the layout split distance or the dose value which is applied during the lithography process.

The VIA-PUF in [10] is based on the random formation of Vertical Interconnect Access (VIA), metallic junction between two conductive layers. The etching mask patterns are specified with a hole size VIA for which the formation is uncertain. An experiment with 119 PUF devices and a 0.18 µm CMOS process technology resulted to 0% error rate. However, the authors precise that the formation VIA probability is slightly biased, thus a post-process is integrated to improve the randomness. It increases the DPUF area and reduces the entropy. This method still shows high potential for security-cost trade-off; only etching mask patterns are customized, and does not require to modify the equipment or materials of the lithography process.

The LED-PUF [11] exploits directed self-assembly (DSA) mechanism based on specific block copolymers. A specific guiding template is integrated on the circuit by lithography process or chemical treatment. Depending on the template dimension and chemical properties of copolymers, local defects are produced and a random structure is generated. Simulation and evaluation were performed, showing a strong reliability e.g. 0% error rate; but also biases in the forming probability: 0.46 uniformity.

The CNT-PUF [12] is based on carbon nanotubes (CNT), materials used as replacement of silicon for transistor channels. The deployment of this technology at an industrial level is still limited today due to assembly imperfection, but this phenomenon can be used as well to build random connection array. The authors show that high randomness is obtained for the nanotube placement given an optimized width of the carbon trench. A reliable PUF can be built with this random structure, coupled with a read-out circuit.

These methods are the main proposals in literature for the generation of reliable random structures used explicitly to build robust PUF primitives. In [25], the authors from the LETI institute present another technique: a chemical solution is used to on purpose degrade the VIAs, forming random electric discontinuities between the metal layers to produce a random hardware structure at fabrication. The LETI process consists in adding, during chip fabrication, a coating operation to spread the chemical solution on the wafer. This spreading is applied after a lithography step, and before etching, transfer and metallization. The adequate chemical solution is a composition of nano-particles made of polymers (polystyrene, methacrylate, hydroxystyrene). Figure 3 shows that these particles are coated on the silicium layers and randomly close the VIAs. When nano-spheres obstruct the VIA the etching is blocked and there is no metallization. Therefore, the interconnection is interrupted. In this case, the unformed VIA is qualified as closed. When the VIA is not affected by the nano-sphere, the interconnection is realized and the electrical signals will be transmitted. The formed VIA is called an opened VIA. A cleaning of the particles and the resin layer is performed after the etching process.

Such process requires to fulfill dedicated constraints with respect to the air-quality of the clean room or cleaning procedures. The coating also implies an adjustment of the manufacturing process; especially, the isolation of a diffusion annealing equipment. It also implies to have a certain level of trust to foundry in charge of the process. The chemical composition could be corrupted to degrade the entropy. However, if the correctness of the coating step is ensured, the movement of particle is unpredictable due to the complexity and the nanoscale of this process. The states of VIAs will remain unknown. Therefore, each produced chip has a specific, distinct and unpredictable grid of opened/closed VIA.

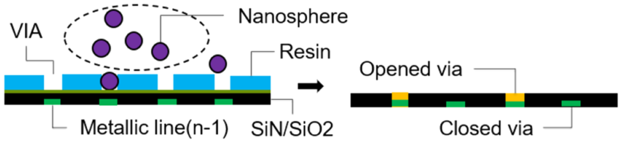

Fig. 3 Polystyrene nanosphere-based structure randomization

For all these methods, the process is customized so that the structure randomization is uncontrollable, unique and unpredictable to each chip. The result is the fabrication of unclonable instance-specific structures distinct from chip to chip, a digital random parameter used to generate random data. A specific amount of randomness may be needed for the DPUF structure, therefore, constraints can be imposed on the parameters of the chosen fabrication processes. The configuration of these parameters will impact the rate of closed versus opened connections, i.e. the structure randomness. As example, in the LETI-process, the density of nanospheres has as direct influence on the closure probability of VIAs, when for the VIA-PUF the crucial parameter is the size of the VIA hole specified in the etching mask. Thus, the structure randomness is one of the parameters which has to be studied during the conception and optimization of secure and efficient extraction circuit.

Logical Circuits for DPUF Response Extraction

In the previous works, there are extraction circuit proposals respectively covering the "Weak" and "Strong" PUF models. Generally, these circuits rely on specific logical cells which convert the random connections of the DPUF structure into a bit sequence; weak DPUF model as well as strong DPUF model require this conversion process. Such electronic structures are similar to memory cell; as depicted in Fig. 4, for the LED-PUF a basic logical cell (only three transistors) returns an output 1 or 0 traducing the connection status of the DSA via (Directly Self Assembly), an efficient way to implement a digital extraction circuit. Given a sufficient large structure, superposed with a grid of such logical cells for each random connection, several responses may be generated. We can consider that the PUF challenge is the address of a row of the grid of logical cells. The circuit converts the random connections of this row into a bit stream used as the

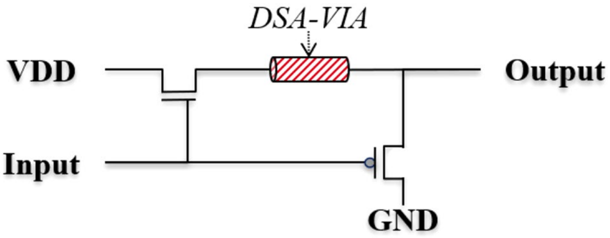

Fig. 4 Logical unit cell of the LED-PUF. Stable signal unit implementation. When input is high, the outputs either one or zero permanently depending on the state of DSA via

DPUF response (which basically corresponds to the status of connections). Thus, the simple and recurrent approach for a weak DPUF model is to deploy a basic logical read-out circuit which returns bit streams directly indicating the connection status of the random structure: 1 for established connection, 0 if interrupted. One advantage is a minimized surface, the response extraction needs only a read status cell. There is no additional circuitry or logical function. For the LED-PUF primitive [11], the required circuit area for a 128-bit output was estimated: 415 *um*^{2} with a technology node to 65 nm. Implementation cost have not been computed for other Weak DPUF (VIA-PUF or CNT-PUF).

As a drawback a weak *PUF* design needs an additional process to derivate security keys from the small CRP space; and protections for the read-out circuit against malicious accesses. Among the described solution, the VIA-PUF offers high potentials for security functions and is already commercialized by the ICTK Company. In their published work [10], the evaluation of this scheme shows good results, it also shows the issue to design a secure and efficient DPUF. An unavoidable bias in the fabrication process reduces the randomness of extracted bit streams. Therefore, an additional circuitry is integrated to compensate this loss of entropy and increases the circuit area. Using the LED-PUF process leads to the same issue (simulated structure hit 46% uniformity which not satisfy randomness requirements). For such weak DPUF, there is a severe requirement to rely on a well-random structure.

Customized processes have to be well precisely tuned, according to the fabrication parameters to gain sufficient randomness (uniformity up to the ideal value of 50%), and thus avoid post-process circuitry.

We further focus on the strong DPUF model requiring a more complex extraction circuit associated to the DPUF random structure. Instead of simply reading the connection status, the extraction circuit processes them with a challenge and returns a unique response. The system (extraction circuit associated to the DPUF primitive) should respect the strong PUF definition, i.e. providing a large challenge–response space which scales exponentially with the PUF size. Also, the circuit should respect the security properties previously discussed (unicity, randomness…) and should come at an acceptable cost (area overhead, power consumption, performance). Such goals depend on the chosen fabrication process which impacts the properties of the DPUF structure (physical constraints as well as amount of provided entropy) and consequently the extraction circuit constraints. These DPUF primitive properties need thus to be considered when specifying and designing the extraction circuit. The SD-PUF proposed in [9] briefly addresses on this point, a strong DPUF architecture is presented with a study of the effects of the random structure characteristics (connectivity rate and size) on the whole system.

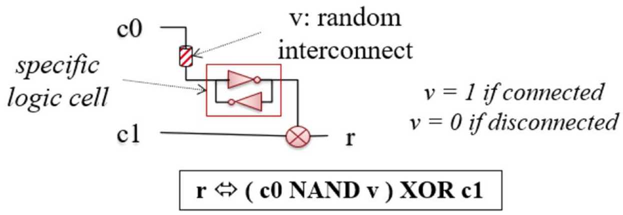

Fig. 5 Logical unit cell of the SD-PUF

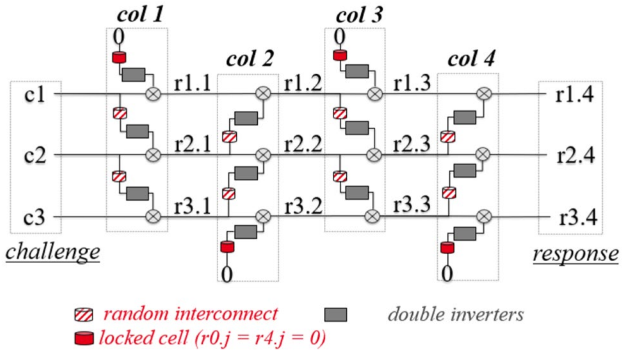

Fig. 6 XOR logic network based STRONG DPUF—3X4 grid

The digital disorder exploited in the SD-PUF architecture is coupled with a specific logical network which mixes the random interconnections with input bit streams. These bit sequences are thus considered as challenges and are diffused across the DPUF structure, a response is returned at the end of the network. The authors propose a grid of logical unit cells which is superposed to the random interconnect grid. As depicted in Fig. 5, each cell is composed by a two-input XOR gate and a customized double-inverter. To get a deterministic behavior of these inverters, the authors suggest to design the skewed-1 inverter larger which dominates at power-up, thus the structure acts as a regular inverter. When the connection is established, the inverters transmit and invert the bit C (1), when the connection is interrupted the output is locked to 1. It is equivalent to a *NAND* gate between input bits and the status of interconnects. Such logic structure is similar to the LED-PUF cell and has the same role: convert the connection status into bit streams. But in this architecture, the authors add two-input XOR gates to diffuse the challenge bit across the randomized structure.

On the example depicted on Fig. 6, random on/off connections are dispatched as a grid of three rows and four columns and coupled with a logical layer of inverters and XORs. A three-bit challenge is transmitted as an input to the PUF and is diffused across the grid and the logical layer. Each column of logical cells applies the previous specified logical operation (in Fig. 6) on the transmitted bits. At the end, a bit stream with same format—three-bit sequence—can be extracted and used as a PUF response. It is noted that the output cell is alternatively connected to upper and lower neighbors' input cell. As side effect: logic cells at the border are placed out of the network and their input are locked to 0. For such circuit, the generic and equivalent logical expression of the transmitted bit $r_{i,j}$ given the random state $v_{i,j}$ of the interconnect, at the ith row and jth column, for a grid of n rows, is:

$$r_{i,j} = \begin{cases} \left(v_{i,j}\mathrm{NAND}r_{i-1,j-1}\right)\mathrm{XOR}r_{i,j-1}, & \text{if } j \text{ odd} \\ \left(v_{i,j}\mathrm{NAND}r_{i+1,j-1}\right)\mathrm{XOR}r_{i,j-1}, & \text{if } j \text{ even} \end{cases}$$

with $r_{i,0} = c_i$ and $r_{0,j} = r_{n+1,j} = 0$

This DPUF circuit forms a challenge–response mechanism, the basis for a strong PUF model. At first, the authors performed PUF metrics evaluation on small DPUF design (dimension grid 8 × 8). Data were generated by HSPICE simulators and a perfect robustness was proved for diverse ranges of temperature and voltage. Then, the authors performed a study on higher DPUF structures (64 × 64) with a behavioral emulator, obtaining strong results for uniqueness and randomness. The respective metrics, inter hamming distance and uniformities, were estimated to 0.5 ± 0.0001, closed to the ideal value (0.5). In fact, the uniform output distribution of XOR gates ensure the required uniformity of the final response. This model of interrogation circuit provides a first pertinent solution for a strong DPUF model.

However, the proposal lacks both strong security schemes and optimization of the DPUF circuitry for a trade-off with the implementation cost. At first, the XOR operations of this circuit are only performed on the bits of two neighbored rows, which then restricts the diffusion of a challenge bit. Moreover, for an interrupted connection, the transmitted bit is locked to 1, reducing the diffusion. As a result, this logical network has a weak diffusion property. Uniqueness and randomness are sufficient for a restricted utilization of the PUF: the generation of a chip ID or a few signatures. However, for extended applications, diffuseness is also required to enforce the security scheme. Maiti et al. [7] describe this property as being required for the case of strong PUF using a large CRP space. Second, only one implementation cost has been estimated. A D-PUF structure with a grid 64 × 64 was synthetized with the NanGate a 45 nm technology node library, resulting to 13 000 um^2 for the required circuit area; it is equivalent to a normalize area of 203 um^2/bit. This value is a first reference to evaluate the implementation cost, but other configurations should be evaluated with higher row dimension (96, 128). Such dimensions are needed in this scheme to have a correct output length respecting the security data size (128 bits). A more detailed analysis on the optimization of circuit settings should be performed to identify an ideal grid size for a good security-cost trade-off (balancing security level and silicon area cost). The SD-PUF proposal still provides an interesting model for the extraction circuit, combining the DPUF random structure with a logical layer. It is an efficient way to implement a strong DPUF primitive and it offers flexibility: designers could easily work on the diverse parameters of this DPUF model, studying structure specificities as well as extraction circuit configuration enhancing the required PUF metrics, security or implementation cost depending on their objectives. However, in the literature, there is no deepened study of extraction circuit model which could be fully integrated into random structure and implement a strong DPUF primitive. Other proposals concern a weak PUF model and this only one real strong DPUF model shows an issue with the diffuseness on which further studies should be focused. The XOR logical network lacks also of implementation cost optimization. Thus, we propose in the next part alternatives design improving the diffusion properties of a DPUF interrogation circuit and also a study of the trade-off between DPUF parameters and PUF security metrics.

Substitution–Permutation Network Architecture for Strong DPUF

Mathematical Scheme for a Secure Network

The random hardware structure of a DPUF requires an appropriate challenge–response mechanism to exploit its entropy and to fulfil security requirements described in the previous section. A previous XOR network (the so-called XN model in the following) based logical layer [9] has already been evaluated on simulated DPUFs, proving uniqueness and uniformity. This proposal has low diffusion property and lacks of implementation cost analysis. The next "Security evaluation" provides results on simulated DPUF circuits with XOR logical networks. The evaluation shows that the diffusion metric (avalanche effect from "Security metrics for PUF primitives") is estimated under 0.3, far from the ideal value (0.5). The diffuseness increases only with higher but costlier grid dimension. Therefore, we propose to build more efficient circuits for challenge–response mechanism; novel circuitries for the transmission of the challenge to the digital structure, diffusing the challenge bits across the random structure and returning a bit sequence as a PUF response as like the first XOR logical network. With this approach, the random structure is modelized as a grid of random connections, as depicted on Fig. 7, such model is defined by physical parameters: (1) number of rows, (2) number of columns and (3) disconnection probability (i.e. the rate of opened versus closed connection).

Second, we optimize the structure parameters for the diverse proposed models to converge to the most efficient logical layer. The new circuit should limit the required

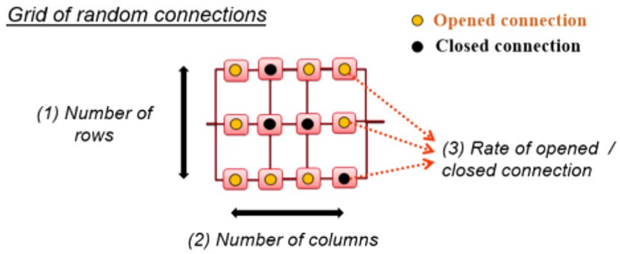

Fig. 7 Model for the DPUF random structure

silicon area; to be compatible with resource-constrained applications. We focus on the efficient logical mechanism used in lightweight cryptographic functions. This research field is already well developed and provides analyses of security-resource tradeoff of diverse cryptographic primitive. Among the standardized proposals, the encryption algorithm PRESENT [26] is one of the most efficient for hardware implementation. The algorithm relies on a SPN composed of small SBOXs (4 bits to 4 bits) and permutation; such operations improve diffusion and confusion. We propose to use this scheme in a novel circuit, along with the first XOR structure proposed in the previous work on SD-PUF [9]. The approach is to extend the circuitry between the columns of random interconnects, integrating wires for row permutation and interconnections to small SBOXs. The operations are performed between two columns of the XOR logical layer. The new circuitry, depicted on Fig. 8, embeds the randomized structure (as digital disorder), the XOR layer and the SPN.

In this design, the additional operations can be arbitrarily iterated i.e. integrated between only some of the columns of the grid of VIAs. We introduce the sampling parameter, *sp,* which is used to indicate the ratio of additional logic in the digital PUF structure**.** As an example, for a SPN circuit with a grid of 12 rows and 6 columns of random interconnects (detailed on Fig. 8), with a sampling set to 1/3, substitution and permutation operations are realized only one time for three columns of the grid. The *X*-layer is the same XOR logical layer previously described. *S*-layer and *P*-layer are, respectively, the substitution and permutation operations which are performed on a bit sequence as like in PRESENT. Their logical expression is completely described in [26].

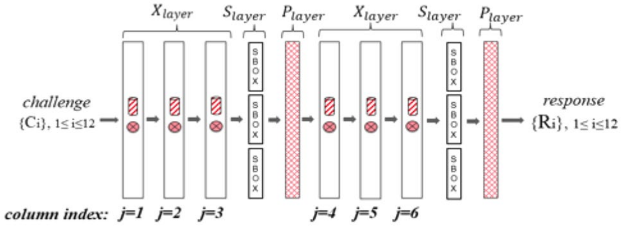

Fig. 8 Substitution–permutation network-based DPUF, grid dimension: 12 × 6 sampling parameter: 1/3

At the *j*th column of the SPN-DPUF circuit, the simplified expression of the sequence of transmitted bits is:

$$r_{*,j} = X_{\text{layer}}\left(r_{*,j-1}\right), \quad \text{if} \quad j \bmod sp \neq 0,$$

$$r_{*,j} = P_{\text{layer}}\left(S_{\text{layer}}\left(X_{\text{layer}}\left(r_{*,j-1}\right)\right)\right), \quad \text{if} \quad j \bmod sp = 0.$$

Flexibility and Variant of SPN Architecture

In the SPN architecture, the mathematical scheme on which relies the extraction circuit as well as the physical specificities of the structure are flexible. These parameters may vary and diverse DPUF configurations can be evaluated; even variants of mathematic scheme with different logical operations. Figure 9 describes this strong DPUF Model and its parameters which are grouped in two categories: the physical ones (1, 2, and 3), dependent to the digital PUF primitive itself, and the mathematical scheme parameters (4, 5) of the extraction circuit. If this work focuses on the extraction circuit design, it aims at considering the physical parameter of the primitive to have the more efficient strong digital PUF combing all the parameters.

The physical parameters which can be arbitrary fixed are: the size of the grid of random connections, e.g. (1) the number of rows and (2) the number of columns; also (3) the disconnection probability. There are no specific constraints on (2), but for (1) the number of rows it has to be noted that it is equal to the challenge–response length. The constraints on the size of bit streams will directly impact this parameter. First, due to the use of small SBOX (4 bits) in the mathematical scheme, it implies that challenge–response length must be a multiple of 4. Second, in case of requirements on data size, such as a 128-bit key size, it imposes the grid to a minimum of 128 rows. The third parameter, (3) the disconnection probability, can vary depending on the flexibility and properties of the chosen DPUF fabrication process. The random disconnections are produced by physical phenomena

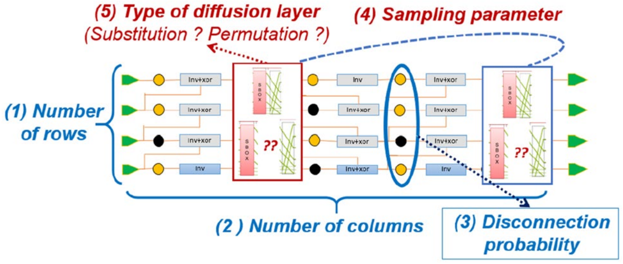

Fig. 9 Strong DPUF model and associated parameters

and involve complex parameters. But, the extraction circuit can still be defined and optimized considering that this disconnection probability is a simple only one variable.

The mathematical scheme used for the SPN architecture offers flexibility, two parameters can be specified: (4) the sampling parameter and (5) the type of diffusion layer. The sampling parameter is controllable, allowing us to densify the operation which strengthens the security. Variants of the schemes can be studied, especially simpler logical network only composed by one type of diffusion operation: permutation or substitution. These two variants are respectively named PN model (permutation-xor network) and SN model (substitution-xor network). They follow the same previous scheme of the SPN architecture but with only one type of diffusion layer.

Optimization of the Strong DPUF Architecture

It is necessary to consider all the earlier described parameters for the conception of DPUF extraction circuits. Their configuration will impact security properties as well as the implementation cost of the DPUF. One of our concerns is that the previous logical circuits based on xor-only network has weaknesses in term of diffusion. This weak-diffusion issue can be mitigated at some cost. The ratio of transmitted bit can be improved with a lower interruption probability of the connections. Previous work [9, 14] proved that more connectivity increases the randomness. But, it imposes constraints on the randomization process and may not be sufficient. This process may not be flexible or at some cost, or on the contrary by easily modified to get more or less randomness which, therefore, reduces constraints on the other parameters. It is also possible to configure the grid of random interconnections with a higher number of columns. It extends the diffusion of information but imply a larger structure at higher cost.

Such approaches with specific DPUF configuration hold for a XOR-only structure but also for the SPN architecture. If this novel SPN scheme can efficiently improve the diffusion, it still faces the question of the security-cost trade-off. How to limit the implementation of these schemes and still gain sufficient diffusion and randomness? In the SPN scheme, the substitution is a costly step in cryptographic function, around 70% of the required area of hardware implementations. Diverse studies have developed optimization strategy to limit the cost of SBOX, such as recent works in [27]. The alternative with the permutation-xor network (PN model) could reduce the surface of logical layer and still provide enough diffuseness. With an optimized configuration of diffusion parameters (sampling parameter and diffusion model) and physical parameters of structures, the extraction circuit could respect both security and cost objectives of the DPUF conception.

Before any further real design implementation, we argue that an evaluation on simulated digital PUFs should be performed. While avoiding costly and time-consuming ASIC development, this study can identify DPUF configurations for a first security-performance trade-off. The results will further lead to define constraints to the process stage to generate the random structure and the definition of an appropriate associated logical layer.

Optimization and Analysis of DPUF Circuit

Methodology and Targeted Metric

We study four models of logical layer. At first, the XOR-only network (XN) which is introduced in the literature for the SD-PUF and described in previous section. Second, our proposals: the substitution–permutation network (SPN) and both lightened variants, the permutation-xor network (PN) and the substitution-xor network (SN). We modelize strong digital PUF instances for different configurations of structure and mathematical scheme. We realize a structure optimization for these logical layers, combined with an evaluation of the security properties. The objectives are to verify if the logical structure fulfil—in theory—the security requirements and also to estimate a first trade-off with the required DPUF structure configuration. For such DPUF structures, the chosen CMOS and customization processes have an impact on the random structures. Here, we admit that it exists a process technology which allows us to produce random structures with a uniform distribution law for the disconnection probability. Thus, in the analysis of the random structure configuration, we only focus on the basic physical parameters which have been described: dimension (number of rows and columns) and disconnection probability. These structures can be considered as a pure digital information that we can model as a binary matrix for which its elements are the connection states: 1 for an established connection, 0 for a disconnection. The structures and the logical circuits can be implemented with mathematical tools such as Matlab and R. Figure 10 presents our evaluation platform and the process for the evaluation of strong DPUF models. At first, our platform can simulate DPUF structure (i.e. the hardware primitive)—random connection states—with our chosen physical parameters define in Fig. 9: (1) rows, (2) columns and (3) disconnection probabilities. We configure also our extraction circuit with the platform: (4) the sampling parameter and (5) the diffusion model. We apply random challenges to structures with these chosen circuit configurations and generate a set of responses which are further evaluate to measure the security of each DPUF configuration.

Then, we compute for these responses the basic security metrics presented in "Security metrics for PUF primitives":

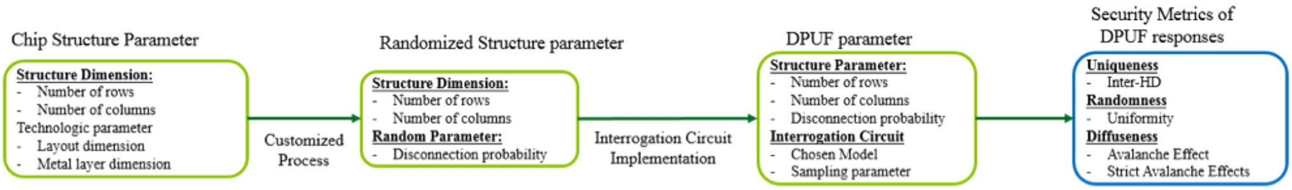

Fig. 10 Evaluation scheme of DPUF parameters and security metrics

Table 2 Inter-HD and uniformity of simulated XN, SPN, PN, and SN models

Metric (ideal)\model	XN	SPN	PN	SN
Inter HD (0.5)	0.4999 ~ 0.5001	0.4997 ~ 0.5001	0.4998 ~ 0.5002	0.4994 ~ 0.5003
Uniformity (0.5)	0.4988 ~ 0.5013	0.4990 ~ 0.5010	0.4990 ~ 0.5015	0.4991 ~ 0.5017

Response size: 128 bits. Grid size: 128 × (16–32–64). Disconnection probability: 0.25, 0.50, 0.75

inter-PUF and uniformity, which indicate the uniqueness and the randomness of a PUF [16, 18]; and also the avalanche effects, normal and strict, to estimate the diffuseness. For all these indicators, the ideal value is 0.5. The metrics are computed for DPUF parameters listed in Fig. 10: number of columns, disconnection probability, sampling parameter and diffusion model. In this first evaluation we fix the number of rows to 128, obtaining PUF responses of 128 bits which is the usual requirement for a size of security data. For the other parameters, we studied a wide range of configurations, for the physical structure as well as for the extraction scheme:

- Number of columns: 16, 32, 64, 128, 256
- Disconnection probability: 25%, 50%, 75%
- Sampling parameter: 1/2, 1/4, 1/8, 1/16, 1/32
- Diffusion model: XN, SN, PN and SPN

The main reason to work on power of two for the dimensions is that the same scale is used in the evaluation on other strong DPUF models [9], it allows a better comparison with these results. Moreover, this is also a current standard for the size parameter in cryptography and process information which justifies this choice. We choose also a power of two for the sampling parameter to scale coherently the diffusion operation on the columns. We limit the disconnection probabilities to the quartiles which is enough to estimate the trend effects on security metrics. This approach still implies a large number of possible parameter combinations. We performed a first analysis to optimize the physical parameters (size of circuit and needed structure randomness) and still have good PUF security metrics (i.e. unicity, diffusion…). The first identified configurations for adequate trade-off will guide the second phase of evaluation which aims at estimating the implementation cost. VHDL implementation and synthesis of extraction circuits are then realized with the given structure dimension and sampling level. These configurations will impact the performance indicators.

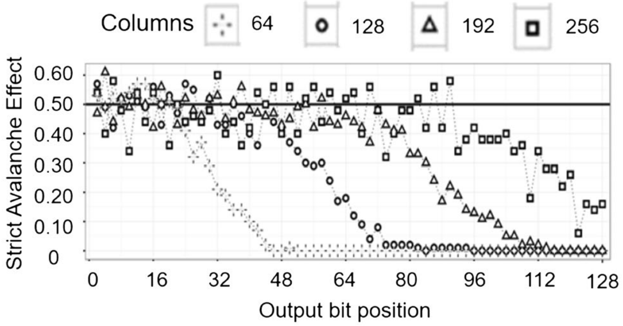

Fig. 11 Strict avalanche effect for the XN model for a modification of the 1st input bit

Security Evaluation

We computed the average of Inter-HD and uniformity for the diverse configurations which have been listed, to evaluate both uniqueness and randomness. Table 2 presents the interval of results for the entire set of configurations, the results are mostly around 0.50 ± 0.0015 even for the smallest circuit dimension (128 × 8). SN, PN and SPN models have strong results, close to ideal value. The metrics are acceptable from a security point of view for the XN model as it is claimed in [9]. Thus, an acceptable randomness level could be obtained with a simple XN model and smaller dimension; limiting the chip area dedicated to a DPUF. This solution can be pertinent for a limited security function (Unique—ID generation) which only requires uniqueness and randomness.

We computed the avalanche effect for each circuit to evaluate the diffuseness. We first focus on the XOR-only network: Fig. 11 shows the strict avalanche effect for the

XN model given a disconnection probability of 0.25 and diverse column dimensions (64, 128, 192 and 256). It requires at least 256 columns to have the metric near 0.50 which is a larger structure configuration. At lower dimension (16–32–64 columns), the average avalanche effects decreases completely, staying under 0.3. It confirms the weak diffusion issue and the needs to expand the PUF structure. Thus, we focus on the novel extraction circuit models and we compare the diffusion of SN, PN and SPN models to XN model presented in [1] for same configurations to enlighten the issue.

Table 3 shows the average avalanche effects, given structure dimension of grid 128 × 64, the three targeted disconnection probabilities and sampling 1/8 for the diffusion layer. The metric for SPN models is close to 0.5 ± 0.002, strongly higher than the XN model. PN shows also good results which still may decrease at lower disconnection probabilities. Therefore, we conclude that unlike to PN and SPN models, a XOR-only network based DPUF is not suitable for a security function which need a strong diffuseness. In comparison, substitution and permutation in the mathematical scheme strongly increases the diffusion.

Also, the SN model with only substitution as diffusion layer does not enforce the metric. For all the simulated configuration, its average avalanche effect is below 0.22 which is not acceptable from a security point of view. As a result, SN circuits have been left out for the rest of the study.

We extend the evaluation of diffuseness for SPN and PN models, especially for lower structure dimensions which should help to reduce the circuit area and therefore their implementation cost. Tables 4 and 5 present the average avalanche effects for 16 and 32 columns, respectively, for SPN models and PN models. The SPN model presents a stronger diffusion, which slightly decreases only for a high disconnection probability and low sampling parameter. The metric falls under 0.40 for the following configurations (dimensions, sampling level): (128 × 16, 1/8) and (128 × 32, 1/16). With higher sampling level, (128 × 16, 1/2) and (128 × 32, 1/4), the avalanche effect reaches 0.49 whatever the disconnection probabilities. SPN model may be interesting if sever security requirements are imposed to the chip with no possible trade-off with the disconnection probability configuration. At this point, the final choice between the configurations (16 or 32 columns) will depend on the constraints of circuitry integration and fabrication cost of random structure. For the PN model, the diffusion is more influenced by the rate of interrupted connections; the result points out that the ideal avalanche effect is obtained for a low disconnection probability around 0.25 and higher sampling parameter. This outcome may be also pertinent; with only additional permutations the PN model limits the use of chip area contrary to the case with substitutions. If the disconnection probability can be lower as required, a PN model for the DPUF interrogation circuit is adequate for a trade-off between the implementation cost of the logical structure and the diffusion requirement. An optimized configuration for PN models, limiting the required chip area of the DPUF is (128 × 32, 1/2, disconnection probability: 0.50 at most). With this setting, the PN model provides both security requirements and smaller circuit area for strong DPUF.

These results still show that the combination of both substitution and permutation as a diffusion layer is the strongest way to increase the diffuseness. In case of severe constraints on the surface or on the process stage, SPN model can be used to reach the required security metric. Given a constraint on the structure randomness due to process fabrication, Table 5 can return the needed sampling parameter and number of rows for a configuration which respect the diffuseness requirement. At this point, the results show different possible

Table 3 Avalanche effects on simulated XN, SPN and PN models

Metric (DP)\model	XN	SN	PN	SPN
DP = 0.25	0.1668	0.2173	0.4968	0.4991
DP = 0.50	0.0980	0.1645	0.4915	0.5002
DP = 0.75	0.0480	0.1106	0.4540	0.5019

Response size: 128 bits, Grid size: 128 × 64. Sampling parameter: 1/8. Disconnection probability (DP): 0.25, 0.5, 0.75

Table 4 Means of Avalanche effects on SPN models

Sampling level	Disconnection probability		
	75%	50%	25%
Dimension 128 × 16			
1/2	0.4999	0.5008	0.4999
1/4	0.4328	0.4675	0.4920
1/8	0.1532	0.2274	0.3393
Dimension 128 × 32			
1/4	0.4994	0.5000	0.4993
1/8	0.4457	0.4836	0.4993
1/16	0.1933	0.3307	0.4408

Table 5 Means of Avalanche Effects on PN models

Sampling level	Disconnection probability		
	75%	50%	25%
Dimension 128 × 16			
1/1	0.1613	0.4745	0.5059
1/2	0.1253	0.3509	0.4545
1/4	0.0693	0.2090	0.3159
Dimension 128 × 32			
1/2	0.4110	0.4944	0.5016
1/4	0.2962	0.4823	0.4991
1/8	0.1439	0.3383	0.4752

combinations of network parameters (sampling, columns) which can provide diffuseness. According to our study, ideal circuit settings are:

- SPN model—grid 128 × 16—sampling level 1/2
- SPN model—grid 128 × 32—sampling level 1/4
- PN model—grid 128 × 32—sampling level 1/2

Finally, we run also min-entropy formula and NIST test suite for random number. We obtained the required metrics, 127 entropy bits and success rate up to 98%, validating our circuit settings. An evaluation of the implementation cost of these circuits has to be performed, associating to these given configurations an estimation of the occupied area of the circuit. Such evaluation is necessary to precise the security-cost trade-off.

Implementation Cost of SPN Circuits

We study the implementation cost of SPN and PN models with the identified parameter configurations. VHDL architectures of circuits are implemented with the Design Compiler software from Synopsys. The software provides estimations of the occupied circuit area after a circuit synthesis; these results are used to evaluate and to compare the cost of SPN and PN models. As like the SD-PUF implementation [9], we use the open-source library NanGate 45 nm, thus the surface analyses of our design can be fairly compared with the SD-PUF results.

Several parameters can influence the synthesis process: clock frequency, supply voltage, clock uncertainty, and also optimization requests. In this first performance evaluation, we mainly focus on the required circuit area and the operative frequency which will define the running speed of the DPUF circuit. We synthetize our circuits with 45 nm technology node and evaluate the results for operative frequencies and area. Here, the operative frequency is specified at the synthesis configuration. Then, thanks to the synthesis software detailed reports are generated on the performances of the implemented designs: required surface, timing violations and energy consumption. It should be note that our VHDL architecture is purely combinatory, i.e. the logical network is fully integrated as a combinatory block with no internal registers. With this approach, the circuit extracts the response in one clock cycle.

The SPN and PN circuitries are implemented and synthetized with generic attributes for the DPUF circuit parameters (grid dimension, sampling parameter). The surface estimations are listed given these parameters and the operative frequency which can be arbitrary specified. We remove data for which time violations were detected, this defect appears when frequency is too high. Figure 12 presents these results for SPN and PN configurations for operative frequencies between 25 and 200 MHz and for circuit configurations this defect appear when frequency is too high. Figure 12 presents these results for SPN and PN configurations for operative frequencies between 25 and 200 MHz and for circuit configurations which were identified in the security analysis:

- Grid dimensions 128 × 16 and 128 × 32.
- Sampling parameter 1/2, 1/4 and 1/8

The areas vary between 6000 um^2 and 35000 um^2 depending on cases. The three parameters (columns, sampling, and frequency) influence the results, and limits appear on the maximum operative frequency. Hereafter, several conclusions are discussed, the main questions concern the constraints and effects related to the operative frequencies, the impact of grid dimensions on the required area and finally, the comparison between the most efficient SPN and PN configurations.

As we observe in Fig. 12, for each circuits the estimated area is stable at low frequency until a threshold is exceeded after which the area grows rapidly to almost the double.

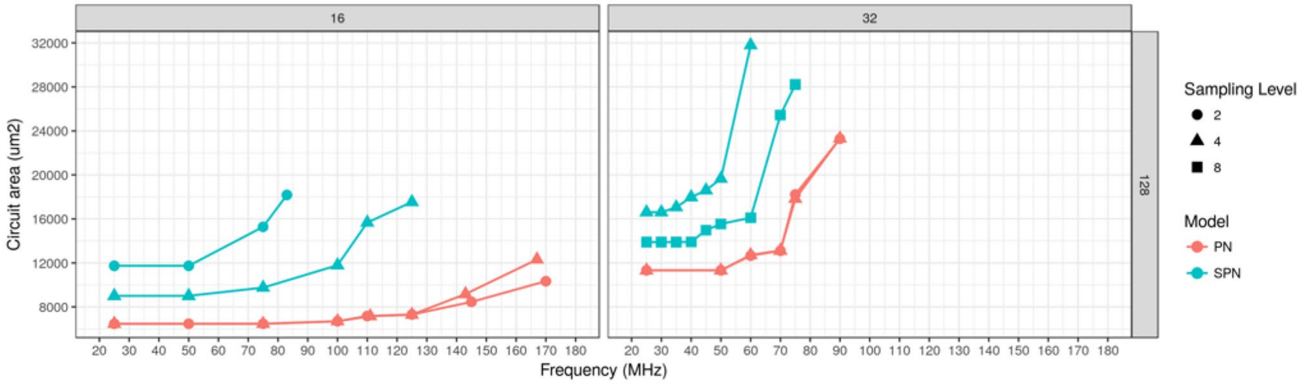

Fig. 12 SPN and PN area estimation, given frequency

As example, for a PN circuit with a 128 × 32 grid (Fig. 11, graph on the right, red color), the area is estimated around 12,000 um^2 until 50 MHz and then it goes up to 24,000 um^2 for a maximum operative frequency of 90 MHz. Curves with similar paces have been observed for the other parameter settings. At this point, the designer should choose between area and performance. The decision depends on requirements of the security use case and is out of scope of the study. In our evaluation, we evaluate the two frequencies which we consider interesting for such dilemma: (Fth) the frequency threshold under which area is stable and minimize, and (Fmax) the maximum operative frequency after which time violations appear. Table 6 gives the area evaluation for both frequencies Fth and Fmax, highlighting the frequency influence.

Concerning the grid dimension, one could easily anticipate that the number of columns severely influences the occupied area. Table 6 shows a proportional growth factor between both variables. Under Fth and at the same sampling level, the area of the PN circuits increases from 6450 um^2 for a 128 × 16 grid to 11,300 um^2 for a 128 × 32 grid. The same trend is observed for the SPN circuits, 9000 um^2 to 16,500 um^2 with 1/4 sampling level. Also, as expected from the discussion in "Optimization of the strong DPUF architecture", the substitution operation clearly increases the area cost. Figure 12 and Table 6 show that the SPN circuits are costlier than the PNs. Moreover, the SPN area overhead is much more impacted by the sampling level. As shown in Fig. 12, the influence of sampling level is negligible on the PN surfaces while the SPN circuits expose different results depending on sampling levels. In Table 6, at Fth and at the same size of grid (128 × 16), for, respectively, 1/4 and 1/2 as sampling level the SPN areas are 9000 um^2 and 11,750 um^2 ; a 20% growth. For the PN model, higher sampling levels may be specified with low impact on the occupied area. As presented in the previous section, higher sampling levels enhance the DPUF diffuseness. Therefore, PN circuits can be implemented with the highest sampling parameters to ensure the diffusion property with no area overhead. With the smaller grid, 128 × 16, the PN surface is reduced at 6450um^2. However, with this number of columns, diffusion is not sufficient; as illustrated by Table 5, the avalanche effect metric is limited and reaches the ideal value only with very low disconnection probability.

We thus focus on the circuit settings that meet the security constraints after this analysis:

- SPN model—grid 128 × 16—sampling level 1/2
- SPN model—grid 128 × 32—sampling level 1/4
- PN model—grid 128 × 32—sampling level 1/2

The three configurations are listed in Table 6. The SPN circuit with 128 × 32 grid and 1/4 sampling level is costly. Its occupied area is 16,600 um^2 while both other circuit settings have lower surface estimation. The 128 × 32 PN circuit and the 128 × 16 SPN circuit, with 1/2 sampling level, have close area results, respectively 11,300 um^2 and 11,750 um^2. Moreover, the threshold and maximum operative frequencies are equivalent and thus not discriminant (respectively, 50 and 90 MHz for both models). At this point, only their security metric can allow to decide which one should be deployed for a better security-cost trade-off. Table 7 allows to better compare these two configurations (which exposed the better area results) avalanche effects. The diffusion is strong with the SPN circuit, around 0.50 ± 0.01 for the three targeted disconnection probabilities. The PN model metric is slightly weaker, a higher disconnection probability is needed for better diffuseness. Thus, we conclude that the ideal circuit setting is SPN—128 × 16—1/2. The mathematic properties of the SPN diffusion layer and the high sampling level ensure a strong diffuseness. At the same time, the low

Table 7 Means of Avalanche effects for circuit settings with SPN—128 × 16—1/2 and PN—128 × 32—1/2

Configuration	Disconnection probability		
	75%	50%	25%
SPN—128 × 16—1/2	0.4999	0.5008	0.4999
PN—128 × 32—1/2	0.4110	0.4944	0.5016

Synthesis at 45 nm technology node under threshold frequency (50 MHz) and operative voltage: 0.95 V

Table 6 Circuit area for SPN and PN configurations at threshold and maximum operative frequency

Circuit settings (model—dimension—sampling level)	Synthesis at the threshold frequency (Fth)		Synthesis at the maximum frequency (Fmax)	
	Circuit area (um^2)	Fth (MHz)	Circuit area (um^2)	Fmax (MHz)
PN—128 × 32—1/2	11,300	50	23,300	90
PN—128 × 16—1/2	6450	100	10,300	170
SPN—128 × 32—1/4	16,500	30	32,000	60
SPN—128 × 16—1/4	9000	60	17,500	125
SPN—128 × 16—1/2	11,750	50	18,200	85

Number of columns: (left) 128 × 16 (right) 128 × 32 number of columns reduces the area overhead in comparison with the results of other configurations. Also, an acceptable security level is reached with much more relaxed constraints on the disconnection probability (between 25 and 75%). This is important since it makes the system more tolerant with the DPUF random structure properties which simplifies the DPUF fabrication process and reduces its cost.

Perspective for the SPN-DPUF

Global Cost and Constraints for SPN-DPUF

With the previous evaluation, we can conclude that the ideal configuration for a DPUF extraction circuit based on a 128-bit challenge–response mechanism is the SPN model with a 128 × 16 grid and a sampling level to 1/2. These circuit settings minimize the area overhead and maximize at the same time the security metrics. In addition to the surface estimation obtained after synthesis, we provide in Table 8 the results for other performance indicators defined in "Indicators for security-cost trade-off". For the final SPN—128 × 16—1/2 configuration, the normalized area is estimated to 91.8 um^2/bit. Also, at the threshold frequency (50 MHz), the corresponding throughput is around 6.25 Gbits/s and the normalized energy is 0.355 pJ/bit. These results can later be used by system architects when considering the integration of SPN-DPUF for on-chip security services. These results need then to be analyzed considering the use case and its associated constraints in term of area, speed and energy consumption. At this point, further studies on the use case will be needed to take the decision. It should be noted that several PUF implementations may overcome the SPN-DPUF as seen in the database of the Singapore University [8]. However, it concerns traditional PUFs which are concerned by robustness issues. In the literature, the only pertinent DPUF reference which can be compared with our proposition is the SD-PUF [9], a strong DPUF circuit based on xor-network. As described in "Logical Circuits for DPUF Response Extraction", the authors analyze the security metrics and the area overhead for 64 × 64 grids; in this case the surface is closed to 13,000 um^2. With 64 rows, the response size is 64 bits which implies a normalized area of 203.6 um^2/bit, costlier than the implemented SPN circuit (91.8 um^2/bit). We provide additional results in our evaluation in "Security evaluation", showing that for this xor logical network, a bigger grid is needed to ensure an acceptable diffuseness. A 128 × 256 grid is necessary which increases the area by a factor 8 (thus a final estimated area around 100,000 um^2). Our proposition of SPN model configuration for a strong DPUF extraction circuit is more efficient and adequate for a better security-cost trade-off. At this point, there are no other proposals for logical network based extraction circuit in the literature; most of the existing solutions are weak PUF model using simple read-out circuit.

Table 8 Security-cost metrics for SPN—128 × 16—1/2 *

Security metric	
Unicity	0.4997–0.5001
Uniformity	0.4990–0.5010
Diffusion	0.4999–0.5008
Entropy	> 127 bits
Success rate for NIST test	> 98%
Total circuit area	11,750 um^2
Normalized area	91.8 um^2/bit
Threshold frequency (Fth)	50 MHz
Maximum frequency (Fmax)	85 MHz
Throughput	6.25 Gbits/s (Fth)
Total power	2.27 mW
Normalized energy	0.355 pJ/bit

Our evaluation focuses on the extraction circuit, this of course should be completed by potential costs induced by the chosen fabrication process of the DPUF random structure. The chosen process may induce an extra area overhead and integration constraints during the manufacturing. Second, the entity in charge of the DPUF fabrication will have the responsibility to guarantee the process parameters. Also, during manufacturing, it should guarantee the integrity of the DPUF structure; insurances have to be established on security of the fabrication step. This is the case for most of implementation steps of hardware security primitives. Third, well-defined security protocols have to be deployed for DPUF and users authentication; an exhaustive and pertinent survey was realized in [28] and can be used to investigating which protocol is the more pertinent for a given use case. Finally, the protection of the CRP database is crucial, eavesdropping of response may be used for usurpation. This issue implies to secure the network architecture and the CRP storage. This issue, common to all the PUF use cases, is addressed at the system level and is out of the scope of this work.

Finally, we should note that for a digital PUF sensitive information are present in digital form. The states of interconnections, “established” or “interrupted”, is a critical information: an adversary who retrieves these data can easily mathematically clone the digital PUF. The randomized interconnections should be deeply integrated into the first metal layer which obfuscates the information; and without direct access to the state of connections. In this case, an external adversary should perform a physical intrusion to get the secret. A retro-imagery, by chip un-processing and imagery, could reveal and identify the electric discontinuities but at high-cost. These vulnerabilities have to be mitigated if the primitive is integrated into a device used for security critical application. Nevertheless, depending on the required security level, such structures may particularly be suitable for applications with an adversary model not considering high-costly physical attacks. DPUFs are notably very good candidate for safety critical applications thanks to their inherent robustness.

Future Work and Conclusion

We have presented a substitution–permutation network-based secure circuit for Digital PUF (SPN-DPUF). The circuit relies on secure mathematic schemes to efficiently extract responses from the digital disorder of DPUFs. DPUFs are based on specific fabrication processes which produce for each chip an instance-specific grid of interconnection. Due to the digital nature of this source of entropy, resistant to noise and environmental perturbation, a reliable PUF model can be implemented. Some previous works already proposed DPUFs [9–12] including novel process for the fabrication of random structures as well as diverse extraction circuits for both current PUF models: weak and strong PUF. This literature points the high reliability of DPUFs and proves by evaluations on simulated instance or real-devices their uniqueness and randomness. The SD-PUF [9] structure is a "strong PUF model", providing a large space of responses and respecting unicity and randomness requirements. However, this first model is based on a XOR logic network for the interrogation circuit which shows low diffusion property. Therefore, we investigated a new approach relying on substitution and permutation network as a mathematic scheme for the DPUF extraction circuit. We simulated the challenge–response mechanism for diverse range of parameters; evaluating adequate disconnection probabilities and operation samplings to optimize the circuit configuration. We completed the analysis by the estimation of implementation cost, leading to a final SPN circuit with a circuit area of 11,750 um^2 with a 128×16 grid dimension and 1/2 as sampling level of the diffusion operations (for a 45 nm technology node). The results show that with this setting the SPN-DPUF can easily meet the classic security metrics; and offers a good trade-off between security and the circuit area. Our proposition is more efficient and secure than the first one from the literature (SD-PUF [9]). The future work will focus on analysis of real-data of random structure (i.e. Digital PUF primitives), with evaluation based on silicium measurements for both security and performance. New security metrics may be studied; indicators from future PUF standardization [19] or the prediction rate of machine learning attacks [29] which may reveal unexpected information from the data on the real random structures. Also, thanks to this study, the parameter analysis will be used to specify the global cost and constraints of the SPN-DPUF fabrication. If there is an opportunity to design a competitive hardware security primitive, one should not forget the security issue which concern all PUF: the requirements for well-defined secure schemes for the authentication protocols and the security of CRPs storage.

Acknowledgements This work was founded by the French program Investissement d'Avenir ANR-10-AIRT-05.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Lim D. Extracting secret keys from integrated circuits. Boston: Massachusetts Institute of Technology; 2004.
2. B. Gassend. Physical random functions. M.S. thesis, Massachusetts Institute of Technology, 2003.
3. McGrath T, Bagci I, Wang Z, Roedig U, Young R. A PUF taxonomy. Appl Phys Rev. 2019;6(11):011303.
4. Böhm C, Hofer M. Chapter 2: Use cases and Chapter 3: Applications. Physical unclonable functions in theory and practice, Graz University of Technology, Austria. Wien: Springer; 2013. p. 39–68.
5. Halak B. Chapter 4: reliability enhancement techniques for physically unclonable functions. Physically unclonable functions. Southampton: Springer; 2018. p. 73–128.
6. Colombier B, Bossuet L, Fischer V, Hély D. Key reconcialiation protocols for error correction of silicon PUF responses. IEEE Trans Inform Forensics Secur. 2017;12(18):1988–2002.
7. Delvaux J., Verbauwhede I. Attacking PUF-based pattern matching key generators via helper data manipulation. In: Conference on Cryptographer's Track at the RSA, San Francisco, 2014.
8. National University of Singapore, Department of Electrical and Computer Engineering. Database of Physically Unclonable Functions. [En ligne]. [Accès le 14 11 2018].
9. Miao J, Li M, Roy S, Ma Y, Yu B. SD-PUF: spliced digital physical unclonable function. IEEE Trans Comput-Aided Design Integr Circuits Syst. 2017;37(15):927–40.
10. Jeon D, Choi B.-D. Circuit design of physical unclonable function for security applications in standard CMOS technology. In: IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC), 2016.
11. Wang W-C, Yona Y, Diggavi S, Gupta P. Design and analysis of stability-guaranteed PUFs. IEEE Trans Inform Forensics Secur. 2018;13(14):978–92.
12. Hu Z, Lobez-Comeras J, Park H, Tang J, Afzali A, Tulevski G, Hannon J, Liehr M, Han S-J. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. Nat Nanotechnol. 2016;11:559–65.
13. Marconot J, Pebay-Peyroula F, Hély D. IoT Components LifeCycle Based Security Analysis. In: Euromicro Conference on Digital System Design (DSD), Vienne, 2017.
14. Marconot J, Hély D, Pebay-Peyroula F. SPN-DPUF: substitution-permutation network based secure circuit for digital PUF. In: IEEE Symposium on Very Large Scale Integrated, ISVLSI 2019, 2019.
15. ISO/IEC 29192-1:2012. Information technology—securitytechniques—lightweight cryptography—part 1: General. International organization for standardization, Gen`eve, Switzerland, 2012.

16. Maiti, A., Gunreddy, V., & Schaumont, P. (2013). A systematic method to evaluate and compare the performance of physical unclonable functions. In Embedded systems design with FPGAs (pp. 245–267). Springer, New York, NY.
17. Armknecht F, Moriyama D, Sadeghi AR, Yung M. Towards a unified security model for physically unclonable functions. In: Cryptographers' Track at the RSA Conference, 2016.
18. Halak B. Section 5.4: security evaluation metrics for PUF. Physically unclonable functions. Southampton: Springer; 2018. p. 134–142.
19. Danger J-L, Guilley S, Nguyen P, Rioul O. PUFs: standardization and evaluation. In: Mobile Systems Technologies Workshop, 2016, pp 12–18
20. NIST National Institute of Standards and Technology. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg: NIST; 2010.
21. Van Herrewege A. Section 2.6: quality metrics. In: Lightweight PUF-based key and random number generation. PhD thesis, KU Leuven, Arenberg Doctoral School, Faculty of Engineering Science, 2015, pp. 37–46.
22. A. F. Webster, S. E. Tavares. On the design of S-BOXES. In: Advances in Cryptology—Crypto '85. Lecture Notes in Computer Science, vol. 218, pp. 523–534, 1985.
23. ISO/IEC 29192-2:2012, Information technology—securitytechniques—lightweight cryptography—part 2: Block ci-phers. International organization for standardization, Gen`eve, Switzerland, 2012.
24. Hu Z, Han SJ. Creating security primitive by nanoscale manipulation of carbon nanotubes. In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 29–34, 2017.
25. May M, Pebay-Peyroula F. Method for securing an integrated circuit during production. US Brevet 2018358310 A1, 13 12 2018.
26. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. PRESENT: an ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp. 450–466, 2007.
27. Bui D-H, Puschini D, Bacles-Min S, Beigné E, Tran X-T. AES datapath optimization strategies for low-power low-energy multisecurity-level internet-of-things applications. IEEE Trans Very Large Scale Integr Syst. 2017;25(112):3281–90.
28. Delvaux J. Chapter 5: A Survey on PUF-Based Entity Authentication. In: Security analysis of PUF-based key generation and entity authentication. PhD thesis, KU Leuven and Shanghai Jiao Tong University, 2017, pp. 133–203.
29. Rührmair U, Sölter J, Sehnke F, Xu X, Mahmoud A, Stoyva V, Dror G, Schmidhuber J, Burleson W, Devadas S. PUF modeling attacks on simulated and silicon data. IEEE Trans Inform Forensics Secur. 2013;8(111):186–1.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.