This document is downloaded from DR-NTU (https://dr.ntu.edu.sg)
Nanyang Technological University, Singapore.

Cryptographically Secure Shield for Security IPs Protection

Ngo, Xuan Thuy; Danger, Jean-Luc; Guilley, Sylvain; Graba, Tarik; Mathieu, Yves; Najm, Zakaria; Bhasin, Shivam

2016

Ngo, X. T., Danger, J. -L., Guilley, S., Graba, T., Mathieu, Y., Najm, Z., et al. (2016). Cryptographically Secure Shield for Security IPs Protection. IEEE Transactions on Computers, 66(2), 354-360.

https://hdl.handle.net/10356/82948

https://doi.org/10.1109/TC.2016.2584041

© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [http://dx.doi.org/10.1109/TC.2016.2584041].

Downloaded on 26 Aug 2022 04:19:29 SGT

Cryptographically Secure Shield for Security IPs Protection

Xuan Thuy Ngo, Jean-Luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, Shivam Bhasin

***Abstract*—Probing attacks are serious threats on integrated circuits. Security products often include a protective layer called *shield* that acts like a digital fence. In this article, we demonstrate a new shield structure that is cryptographically secure. This shield is based on the lightweight block cipher and independent mesh lines to ensure the security against probing attacks of the hardware located behind the shield. Such structure can be proven secure against state-of-the-art invasive attacks. Then, we evaluate the impact of active shield on the performance of security IPs as PUF, TRNG, secure clock and AES using a set of fabricated ASICs with 65 nm CMOS technology of STMicroelectronics. Also, the impact of active shield on Side-Channel Attack (SCA) is evaluated.**

***Index Terms*—Hardware security, cryptographically secure shield, lightweight block ciphers, Focused Ion Beam (FIB), Physically Unclonable Function (PUF), True Random Number Generators, Side Channel Analysis, probing attack, SoC, AES.**

I. Introduction

A. Threats on Integrated Circuits

Nowadays, hardware trust and security play an important role because integrated circuits (ICs) are present in many critical infrastructures for sensitive markets like finance, identity, health, military affairs, etc. Many cryptographic intellectual property blocks (IPs) are integrated to assure the security of ICs. But, these cryptographic IPs can themselves be the target of attacks. In the state-of-the-art, there are two categories of attacks against IC security: *non-invasive* and *invasive* attacks. In this paper, we focus on the invasive attacks which can be performed either statically or dynamically.

- Static invasive attacks are attempts to modify/edit the circuit in a view to create malicious modifications allowing stealing or leaking sensitive information. For example, with a tool called Focused Ion Beam (FIB), attackers can draw artificial pads that conduct directly into the inner parts of the circuit, hence allowing the attacker to spy sensitive signals or secret data (such as keys). FIB attack is performed at power off.
- Dynamic invasive attacks are attempts to penetrate inside the circuit to read/monitor directly the sensitive data. For example, using a *probing station*, attackers can read data within the circuit, and in particular extract cryptographic keys, hence breaking the IC security. This kind of attack is performed at runtime, i.e when the circuit is powered and clocked.

These attacks are serious threats on ICs hence countermeasures are needed. A *metallic shield* is a protection aimed at thwarting these attacks. It consists in a mesh of metal lines on the top-most metal layer(s) of the IC, which prevents an adversary from reading (and writing) via a probing attack. However, with the progress in attack techniques, the shield protection can still be bypassed if improperly designed. Actually, we can classify the shields in two categories: either *passive* or *active*. Passive shielding consists in an analogue integrity check of the mesh. For instance, in [1], P. Laackmann and H. Taddiken present an analog passive shield based on a analog transmitter, an analog receiver, a drive and an evaluation device. The shield is associated with a capacitive measurement method to evaluate it. However, some alterations of the mesh can be undetected, if they are small or surgically-accurate enough to keep the mesh capacitance within acceptable bounds. Hence, digital (active) shielding aims at mitigating this problem. It consists in injecting random sequences of bits in the mesh, and subsequently in checking whether they arrive unaltered after their journey. An illustration is given in Figure 1. Such structures exist for the protection of both devices (e.g., FIPS-140 compliant security appliances [2]) and ICs. In this article, we focus on lines meshes suitable for ICs, that use only one metal layer, since they are really favored by the industry; using more than one metal layer is considered prohibitively expensive. Some ideas of architectures for active shields can be found in references [3], [4], [5]. Let us call them shield #1, #2 and #3. Shield #1 consists in sending a "*predetermined test data*" into a *small number of equipotentials* in the shield. Flylogic employees defeated this shield by identifying the equipotentials[1] in the mesh [7]: they found four of them, which they shorted together in order to make an opening in the shield, thanks to a FIB. Shields #2 and #3 consist in lines that

Xuan Thuy Ngo, Tarik Graba and Yves Mathieu are with the Department of COMELEC, Institut MINES-TELECOM, TELECOM-ParisTech, CNRS LTCI (UMR 5141) 46 rue Barrault, 75 634 Paris Cedex 13, France *and* 37/39 rue Dareau, 75 014 Paris, France. Email: {xngo, graba, mathieu}@telecom-paristech.fr

Jean-Luc Danger and Sylvain Guilley are with the Department of COMELEC, TELECOM-Paristech, Paris, France and Secure-IC S.A.S., 37/39 rue Dareau, 75 014 Paris, France *and* 80 avenue des Buttes de Coësmes, 35 700 Rennes, France. Email: {danger, guilley}@.telecom-paristech.fr or {jean-luc.danger, sylvain.guilley}@secure-ic.com

Zakaria Najm is with ST-Microelectronic, ROUSSET, France.

Shivam Bhasin is with Temasek Laboratories, NTU, Singapore.

This project has been funded by the French Government, under grant FUI #14 **HOMERE** 959 (**H**ardware tr**O**jans : **M**enaces et robust**E**sse des ci**R**cuits int**E**grés).

[1]Notice that the identification of equipotential lines in the circuit can be achieved via a systematic test-and-trial pairwise probing of the mesh lines. However, a more simple technique called "voltage contrast" [6] is able to represent lines of different potential with different shades of gray. So, equipotential lines are those lines that constantly (in time) share the same color.

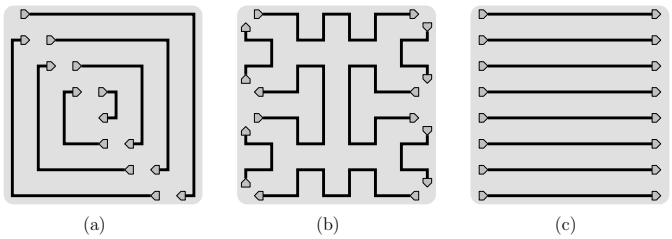


Fig. 1. Some mesh structures of metallic shields for $n = 8$ lines

carry the successive values of a linear feedback shift register (see shield #3 in Figure 1(a)). They are thus also easy to bypass: the value of all the lines can be guessed by solving a system of linear equations. So, in practice, these shields (and in general all the active shields of the state-of-the-art) manage to make probing attacks more difficult, but not impossible. Recently, a new active shield structure (based on a *maze*, called *random active shield*) has been proposed [8], [9]. This method achieves intricate spaghetti routing of a dense mesh of wires hence making the geometry of the shield difficult to recognize. However, the large scale generation of such a structure is admittedly complex (see Figure 1(b)). Moreover, the solution [8] can require several topmost metal layers for the creation of mesh wires: in a compact IC, this makes the routing of the legacy hardware to be protected (below the shield) very challenging. Last but not least, these articles do neither detail the nature of the random numbers, nor the actual cost (i.e., *area*, *power*) of the solution.

B. Shield Structure Studied in This Paper

In this article, we present a new shield structure named "cryptographically secure shield" that does not have the limitations of the state-of-the-art:

1) It resists rerouting attacks by FIB because there are no two identical lines: all the wires of the shield carry a different information;
2) The data sent over the shield lines are unpredictable, because they are the output of a (lightweight) block cipher operated in chained block cipher (CBC) mode;
3) The layout of the mesh is trivial: it simply consists in parallel lines, of minimal width and minimal spacing, as depicted in Figure 1(c). The input/output ports of our mesh are positioned with a regular spacing on two faces (left and right), which eases their connection. Notice that the term "mesh" is no longer suited for our shield, since the lines are not entangled. Nevertheless, we keep this term for consistency with previous structures.
4) Only the topmost metal layer is required.

Notice that all shield structures (including ours) protect only the frontside of the circuit; backside shall be protected by other means.

II. Cryptographically Secure Shield

A. Cryptographically Secure Shield Architecture

Our active shield consists of two parts, depicted in Figure 2:

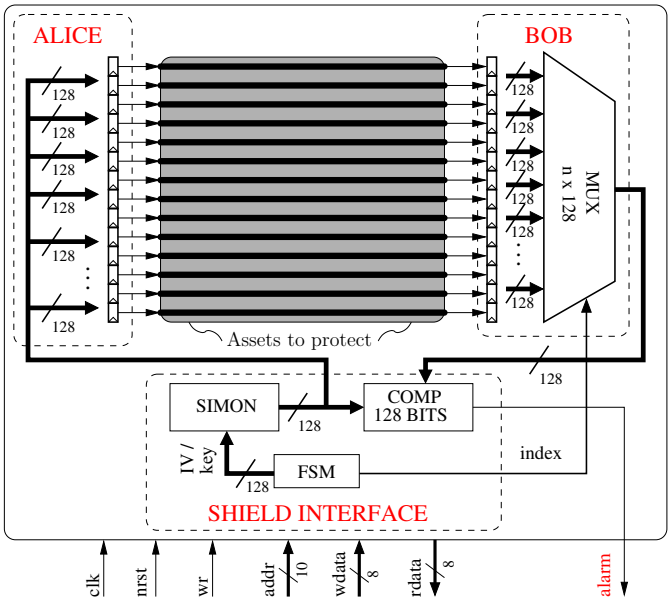


Fig. 2. Cryptographically secure shield structure

- **Control (logic) part**: which is composed of ALICE, BOB and SHIELD INTERFACE. This part is placed (hence protected) behind the shield mesh. It is used to generate and check the random bits which will circulate through the mesh. If the bits received by BOB are different than those sent by ALICE then control part generates an "alarm" signal.
- **Shield mesh**: which is composed of n lines on the last metal layer. It is used as a communication channel between ALICE and BOB, and achieves the anti-tamper protection of the integrated circuit located below it. This part is used to detect "remove-and-rewire" & "probing through the mesh" attacks.

The principle of our shield is to check the integrity of random bits sent by ALICE to BOB via the shield mesh. The rationale of our shield relies on a simple on-chip unidirectional encrypted communication through the mesh. The shield mesh is made up of $n > 128$ lines; Thus, ALICE sends to BOB its 128 bits through the first, second, etc. packet of 128 bit lines (called R1, R2, etc. in Figure 2). Enable signals e_1, e_2, etc. allow for such dispatching. If the exchanged 128 random bits match, we can deduce that the shield has probably not been altered. The alarm signal (output of the comparator) is kept is to low value "0"[2]. Indeed, an attacker can guess the value of each line with $1/2$ probability. However, after m exchanges between ALICE and BOB, the probability of an undetected attack is lowered to $1/2^m$, because the attacker has no a priori information: he can at best make independent guesses at random. So, within a short time span, any shield opening or forging (i.e., rerouting) will be detected. Otherwise, when the two 128 random bits sequences differ, the alarm signal is asserted to "1", to indicate that there is an integrity

[2]In practice, the alarm signal is a single point of failure hence must be redunded adequately.

problem with the shield lines.

This shield structure allows to detect invasive attacks using FIB or probing stations. The shield is activated on two occasions. Firstly, at chip boot, the shield allows to detect static attacks (by FIB) and dynamic attacks such as "linear memory dump" or " spy of ROM decryption in RAM". Indeed, these attacks need to modify or remove the shield mesh in order to penetrate inside the circuit. These modifications on the shield mesh will violate the integrity of random bits exchanged between ALICE and BOB hence activating the "alarm" signal. Second, the shield can be also activated episodically, so as to check whether an attack is performed at runtime. Alternatively, the shield can be activated only if critical operations are carried out where sensitive data need to be protected. Such selective shield activation allows to achieve significant power consumption savings.

B. Secure Operation of Shield

This section describes how to operate our active shield in a security application. The sequence of steps is given below:

- 1^{st} **step: secure boot**. Secure boot starts with builtin-self test (BIST) of vital physical co-processors, such as the True Random Numbers Generator (TRNG) used to generate the key used by the cipher of the shield which drives the mesh. Then integrity of the shield mesh is checked by generating a sequence of bits on ALICE registers (named R1, ..., R5 in Figure 2) and verifying their proper arrival at the corresponding registers of BOB. After that, the shield control logic part is checked using a scan-chain type of on-line test for example. At the end of this first step, the physical integrity of the circuit is guaranteed. In particular, attacks like *reset forced at active value* and *clock and/or voltage disconnection*, are detected right from the start, and the boot can stop dead.
- 2^{nd} **step: shield initialization**. In this step the active shield in initialized by seeding the lightweight cipher with a fresh random key generated by the TRNG. In our case study, we use SIMON block cipher with 128 bits of plaintext and key inputs, but any other lightweight block cipher would suit the need. Typically, the choice for the key in our test circuit is done during an enrollment phase (thanks to a privileged "`set_key`" command). The shield is now ready to be run.
- 3^{rd} **step: IPs operation**. When any critical IP (such as PUF, cryptographic operations, etc.) needs to be operated, the shield is activated. An example is the secure use of PUF which delivers a key to decrypt the boot code.
- 4^{th} **step: shield deactivation**. When critical application operations are no longer required, the shield can be clock gated hence reducing significantly its power consumption.

Obviously, secure boot shall be implemented carefully: typically, the key generation for the lightweight block cipher must be protected against corruption and the lightweight block cipher itself must not leak through side-channels.

III. Impact of the shield on the SoC

As discussed before, our shield is composed of two parts: control logic and metallic mesh parts. Each part can more or less impacted by other IPs of the circuit, especially the IPs placed beneath the metallic mesh.

A. Shield Control Part Impact on SoC

The shield control comprises three sub-parts:

- ALICE block: composed only of registers and buffers, to amplify the signals before they travel along the capacitive (since long) lines of the mesh.
- BOB block: composed of buffers and one n bit $\rightarrow$ 128 bit multiplexer.
- SHIELD INTERFACE: composed of a 128 bit block cipher, one 128 bit comparator, and a Finite-State Machine (FSM). The role of the FSM is to handle the connection with the CPU: the "shield", seen as an IP, is a slave on the system bus.

The size of the ALICE and BOB depend on the circuit size while the SHIELD INTERFACE part remains unchanged. For example the size of the active shield control logic, using SIMON block cipher to protect a 650×650 μm^2 circuit with STMicroelectronics 65 nm technology, is around 9% of the circuit [10]. When the shield is activated, the control part, which is an independant IP of circuit, has almost no impact on the other IPs such as RAM, processors, etc. Nevertheless, it can have an impact on some sensitive security IPs such as PUF and TRNG because their functions are based on the relative delay between signals which are renown to be very sensitive to noise. Nonetheless, a proper power planning clearly ensures a stable energy supply for these IPs, hence no malfunction is expected. However, the shield mesh can have a larger quantitative impact on the SoC.

B. Shield Mesh Impact on SoC

As described in Figure 2, the mesh is comprised of n lines on the last metal layer. These lines pass over the circuit on the top-most metal layer hence having some impact on the physical behavior of the circuit.

1) IR Drop: As shield mesh is composed of long metal lines, it can have an impact on the IR drop when random bits are updated on the mesh wires. Nevertheless, the mesh is not continuously changing, since random bits are not updated at every clock cycle. Actually, the random bits are changed only when the lightweight block cipher has finished its computation. For instance, in our case of study [10] where SIMON block cipher is used, the random bits are put on the mesh for a duration of 68 clock cycles. Moreover, we notice that, once against, IR drop can be mitigated by a properly dimensioned P/G (power/ground) network.

2) Inductive Coupling Phenomenon: Such inductive coupling is created between the mesh and underneath metal layers. In our case study [10] where the STMicroelectronics 65 nm technology is used, there are a total of 7 metal layers and the mesh is routed on the 7th metal layer. Therefore, the inductive coupling is expected between 7th and 6th metal layers. However, in any technology, the routing lines are orthogonal between two consecutive metal levels in order to comply with preferred routing directions. Therefore there is no parallel lines between 7th and 6th metal layers hence no inductive phenomenon.

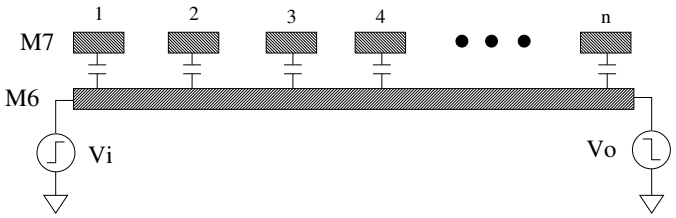


Fig. 3. Capacitive coupling of the active shield

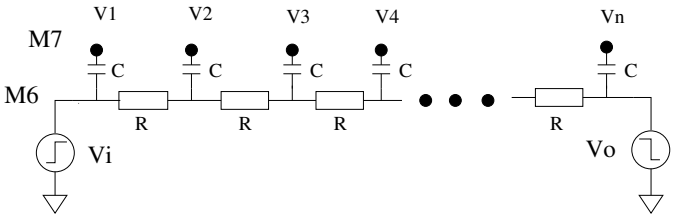


Fig. 4. Electrical coupling model created by shield mesh

3) Capacitive Coupling Phenomenon: The long lines of shield mesh can create capacitive coupling with the routing lines of the underneath metal layer. In our case study [10], there exists a capacitive coupling between the mesh (on 7th metal layer) and the routing lines on the 6th metal layer. The Figure 3 presents the principle of capacitive coupling model created by the shield mesh of n metal lines placed at 7th metal layer. This figure illustrates the critical case where a long routing line crosses the circuit at 6th metal layer (M6), thereby creating n coupling capacitors. The Figure 4 presents the corresponding electrical coupling model in this case. In this model, Vi is the output of one logic gate and Vo is the input of another logic gate of circuit. [V1,V2,...,Vn] is the voltage of mesh lines. Their values depend to the random bits exchanged between ALICE and BOB. Let C be the coupling capacitor between one mesh line and the long routing line at M6, an let R be the resistor of each part of long routing line at M6 with the shield lines at M7. This capacitive coupling impacts the circuit as well statically as dynamically. In the static case, the shield is deactivated and [V1,V2,...,Vn] are fixed. So the mesh adds an extra capacitor to the circuit. It will slow down signals exchanged on the M6 long wire. But in practice, such static effect is not so important. In the dynamic case, effects created by coupling capacitors are the most important. They can be called "intentional crosstalk" [11], [12]. This time, the value of [V1,V2,...,Vn] changes randomly hence creating a jitter in signals exchanged at M6 layer. The best case occurs when the potential of all lines of the shield go up when the line in M6 also has a rising edge. On the contrary, the worst case occurs when all the lines of the shield go down when the long M6 line has a rising edge. To attest this phenomenon, we perform SPICE simulation of our shield mesh presented in [10]. The shield mesh is composed of 640 metal lines, each being 650 μm long. The coupling capacitor C is approximatively equal to 1 fF and $R = 0.5\ \Omega$. The Figure 5 presents the Spice simulation result. We notice that the capacitive coupling impacts strongly the delay of driven M6 signal. Specifically, the delay depends on the random bits on the mesh. Therefore, the mesh creates a small albeit non-zero dynamic impact on the critical part of the circuit hence affecting security IP performance such as TRNG and PUF.

Now that the main factor of perturbation has been insulated as capacitive coupling, we study experimentally to which extend it should be considered harmful for IPs beneath the shield mesh.

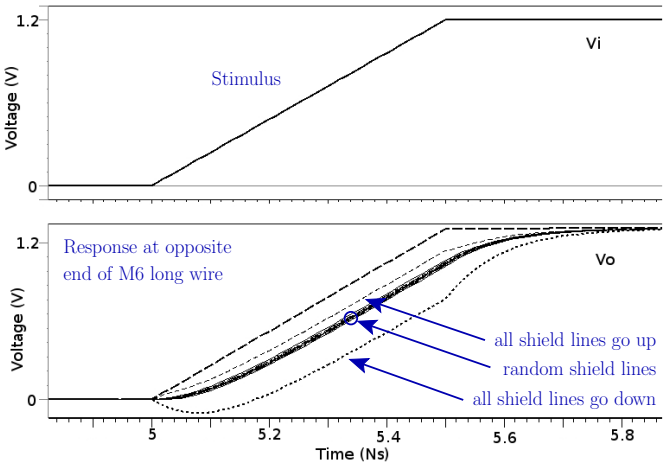


Fig. 5. Spice simulation result for capacitive coupling

IV. Case Study on a Test Chip

To evaluate the proposed shield, we designed an ASIC using `CMOS065`, the CMOS 65 nm technology from STMicroelectronics. It includes the following IPs:

- 4 Arbiter & Loop Physical Unclonable Function (A-PUF & L-PUF) [13];
- 2 Open-Loop True Random Number Generator (TRNG) [14];
- 1 AES 128 bits with Hardware Trojan (HT) [15];
- 2 SRAM blocks;
- 1 Secure Clock;

all placed beneath the cryptographic active shield. The core size is 560 μm $\times$ 560 μm. As detailed in [10], the area of the shield logic is 19394.4 μm^2, that is 9324 GE (Gate Equivalents), and its power consumption is 7.01 mW.

In this section we focus on evaluating the impact of active shield on SoC. We concentrate specifically on security IPs.

A. Impact of Active Shield on PUFs

Physical unclonable functions (PUFs) are used to generate the fingerprint of ICs or devices using the challenge-response mechanism. They exploit the difference of physical behavior between ICs created by process variations to generate one unique response for each IC. Therefore PUF structures are generally very sensible to environment changes such as voltage, temperature, frequency, etc. In this section, we test the impact of cryptographically active shield on two PUF structures: **SRAM PUF** [16] and **Loop PUF** [13].

1) Impact of Active Shied on SRAM PUF: Static Random Access Memory (SRAM) is an integrated volatile memory implemented in almost all integrated ICs. The SRAM initialisation values can be used as a PUF [16]. We noticed that the SRAM is immediately initialized when the circuit is powered up. On the contrary, the active shield needs a configuration step (clock activation, shield activation or shield key selection) before operation. Consequently the active shield is always operated after SRAM initialization. SRAM initialization state is preserved when the active shield is active. Thus the shield activity cannot modify the random initialization values of SRAM. So the SRAM PUF is robust even in conjunction with active shield integration. In conclusion, active shield has **no impact** on the SRAM PUF.

2) Impact of Active Shield on Loop PUF: The loop PUF is a delay based strong PUF presented by Cherif et al. [13]. Its structure is presented in Figure 6. It is composed of:

- A Ring-Oscillator Loop with N programmable delay chains.
- A signal named "En_signal" used to activate/deactivate the Loop.
- A N bit challenge C used to configure the delay chains.
- A frequency measurement module.

The operation principle of the Loop PUF is as follows:

- Choose a pair of challenge $C = (C_1, ..., C_N)$ and $C' = (C'_1, ..., C'_N)$.
- Measure the oscillation frequency of each challenge f_C and $f_{C'}$.
- Compute the difference of frequency $\delta f = f_C - f_{C'}$.
- Generate the bit output of Loop PUF depending on the sign of δf. If $\delta f > 0$ then the output is '1'. Otherwise the output is '0'.

To evaluate the impact of active shield on the Loop PUF, we generated 10000 times the 63 bit response corresponding to 63 pairs of challenges C and C' with and without activating the active shield. The results of the 1^{st} acquisition show that, for the Loop PUF without shield activated, there are:

- 6 unstable bits amongst 63.
- The unstable bits correspond to challenge pairs number 1, 16, 41, 43, 44 & 52.

When the shield is activated, then the Loop PUF features:

- 3 unstable bits amongst 63.
- The unstable bits correspond to challenge pairs number 1, 16 & 44.

Therefore, apparently, the Loop PUF has slightly more stable bits when the shield is activated. To better understand the results, we acquired 10000 times the δf for each challenge pair C and C' of Loop PUF with and without shield activated. Then we compute the mean and standard variation of δf for each challenge pair. Figure 7 (resp. Figure 8) shows the results of the δf mean (resp. standard deviation) for all 63 Loop PUF challenge pairs with and without shield in the 1^{st} acquisition. We notice that, for any challenge pair, the difference of frequency mean is almost the same for the Loop PUF with and without shield. Additionally, the standard deviation is also very similar except for some challenge pairs (Challenge pairs number 41, 43 and 52 for the 1^{st} acquisition) where the

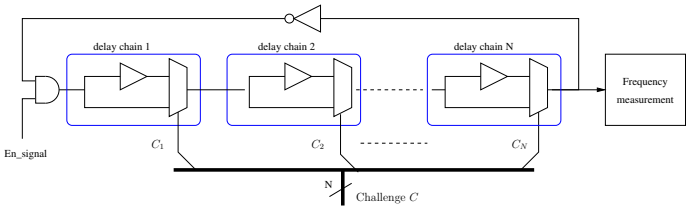


Fig. 6. Structure of the Loop PUF

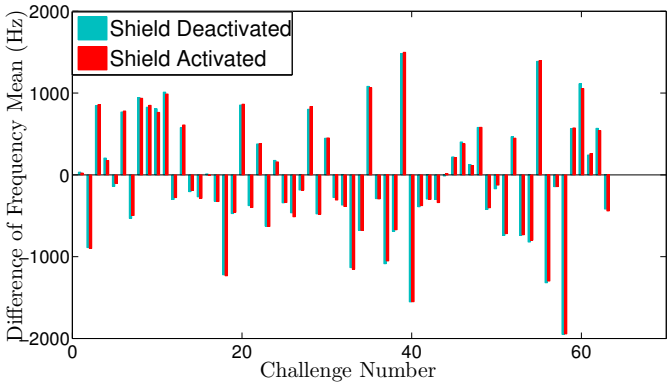


Fig. 7. Difference of Frequency (δf) Mean of Loop PUF for 63 challenges over 10000 measurements each

standard deviation of Loop PUF without the shield activated is much larger than the one with the shield. These results can be accounted by the capacitive crosstalk phenomenon presented in the previous section. The loop PUF is more reliable when the shield is activated than when it is not.

In conclusion, the Loop PUF response for all challenge pairs, without and with shield activated, are the same except some challenge pairs where δf are biased by environmental interferences. In reality, the shield has a tiny impact on δf measurements. It is natural because the shield activity, when the Loop PUF is configured with C and C', is not the same. Figure 9 explains this phenomena. This figure shows the distribution of frequency of Loop PUF for a challenge pair C and C' over 10000 measurements. We noticed that when the shield is activated, there is an important shift of f_C and $f_{C'}$. But the difference of frequency $\delta f = f_C - f_{C'}$ is almost the same. Therefore, impact of the cryptographically secure shield on Loop PUF structure is **negligible**.

B. Open-Loop TRNG

The Open-Loop TRNG is based on the difference of delays $\delta t_{DC} = t_d - t_c$ between data and clock of a D latch. If $\delta t_{DC} \gg 0$ or $\delta t_{DC} \ll 0$ then Q will be 0 or 1. However if $\delta t_{DC} \approx 0$ then the D latch is in a metastable state. Therefore, the main idea of Open-Loop TRNG is to adjust delays on data and clock to reduce the δt_{DC} hence reaching the metastable state of the D latch.

The complete structure of TRNG is presented in Figure 10. It is composed of:

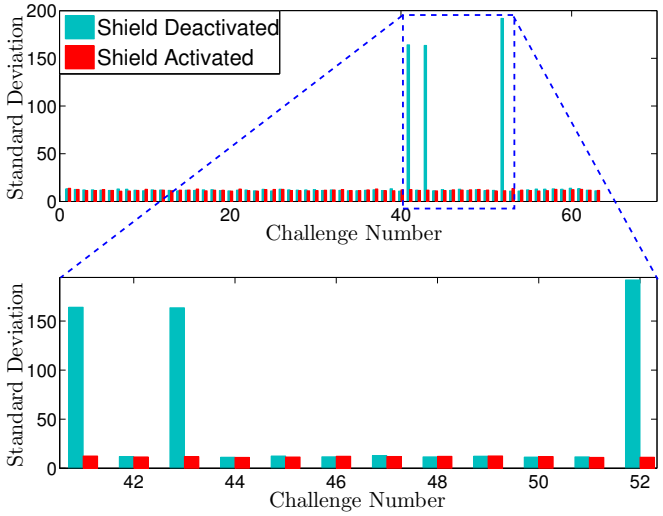


Fig. 8. Difference of Frequency (δf) Standard Deviation of Loop PUF for 63 challenges over 10000 measurements each (1^{st} acquisition)

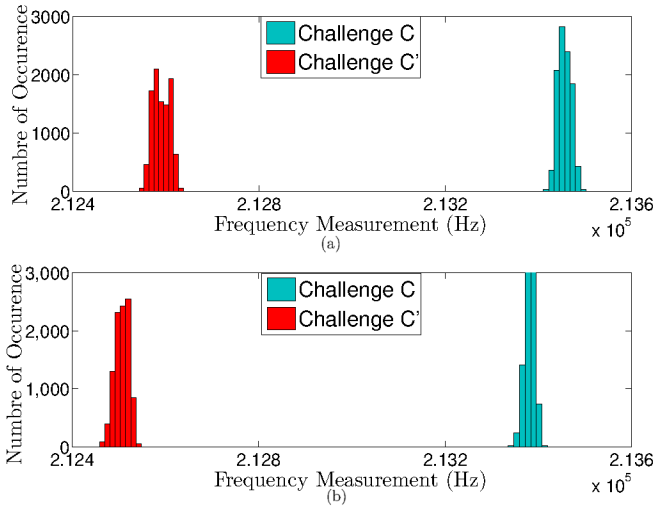


Fig. 9. Frequency distribution of Loop PUF for a pair of challenge C and C': (a) inactive shield, (b) active shield.

- A set of 16 D latches;
- Two programmable coarse delay chains (CC_1 and CC_2) and two programmable fine delay chains (FC_1 and FC_2). These chains are used as programmable delays on the data and clock lines of 16 latchs. They allow to control precisely and finely data and clock delays.

For evaluating the shield impact on this TRNG, we computed the randomness at all 16 D latch outputs with and without activating the shield for all possible combinations of 4 coarse and fine delay chains. We also computed the randomness of the sum of 16 D latch outputs by xoring them together. Figure 11 shows the results of this experiment. The x-axis is the output of 16 D latch. The y-axis is the combination of 4 programmable coarse and fine delay chains. The probability to have '1' at all 16 D latch outputs is represented by colors. We notice that the behavior of each latch output is different. For example the output of latch number $I5$ is always '0' for all combinations of delay chains while the output of other latchs can be always '1', '0' or unstable depending to the combination of delay chains. The Figure 11 shows that the Open Loop TRNG has more metastable state by adding all latch outputs together (XOR output). The experimental results also show that the Open-Loop TRNG with shield activated has more metastable states than the one without active shield. This seems reasonable, because the crosstalk created by the mesh is random (SIMON is computed in CBC). Therefore it can be considered as random noise for the TRNG. Moreover, the control part of the shield will also add another noise source for TRNG. So we can conclude that our shield has an **positive impact** on the Open-Loop TRNG.

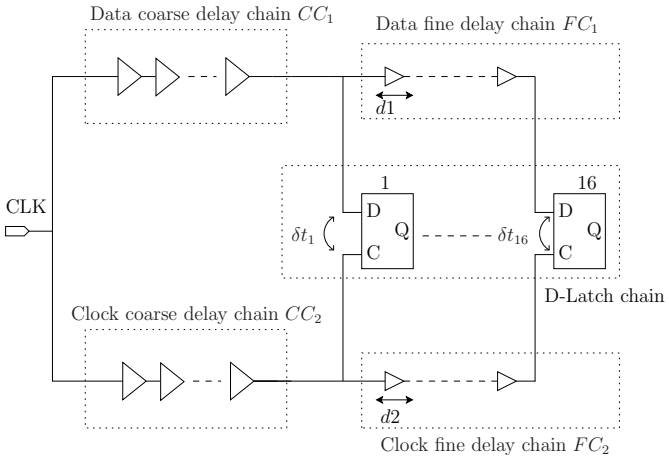


Fig. 10. Structure of the metastability-based TRNG

C. Impact of Active Shield on Secure Clock

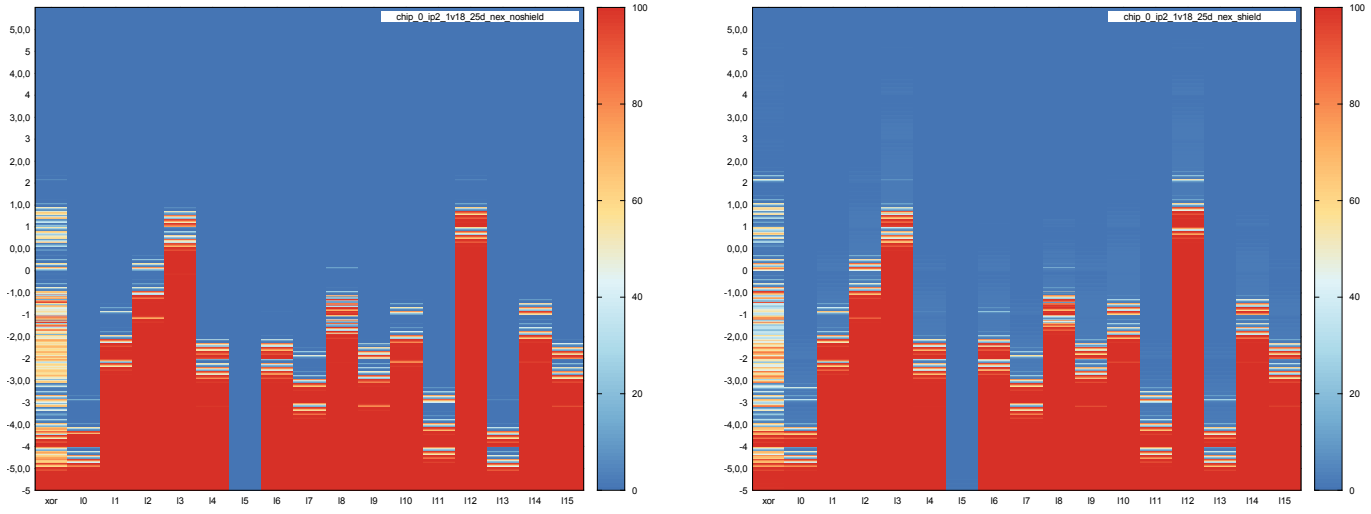
The secure clock is an IP which aims at adding random jitters in the clock cycles. Figure 12 presents the structure of secure clock implemented in the ASIC. It is composed of:

- A set of 31 buffers to create different clock delays.
- A 31 to 1 multiplexer to select different clock delays.
- A random number generator (RNG) block used as multiplexer control signals which allows to randomly select clock delays.

We test the impact of the shield on the secure clock by measuring the maximal frequency of secure clock with and without shield. In both cases, the maximal frequency of secure clock is around 350 MHz. Therefore there is **no impact** of active shield on the secure clock. Moreover, the crosstalk created by the shield can add more random jitter on the secure clock, which is beneficial security-wise.

D. Impact of Active Shield on Side-Channel Analysis

Side-Channel Analysis (SCA) is an attack which exploits the information gained from the leakage of a physical im-



(a) (b)

Fig. 11. TRNG outputs probability to be equal to 1 (in %): (a) With active shield disabled. (b) With active shield active.

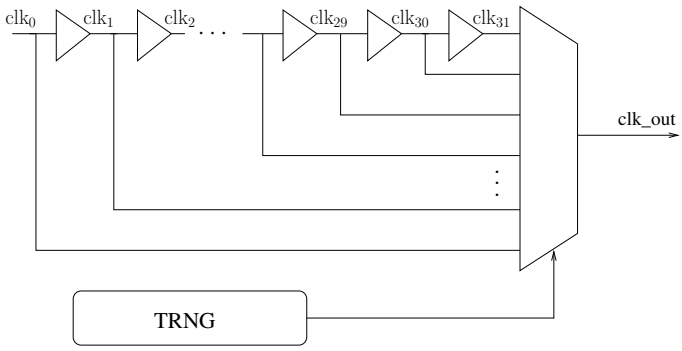


Fig. 12. Secure clock structure

plementation of a cryptosystem, rather than by brute force or exploitation of mathematical weaknesses in the algorithms (i.e., cryptanalysis). The SCA can be simple or complex depending on the target circuit. We perform the same SCA attack using Correlation Power Analysis (CPA [17]) technique on the AES with and without activating the shield. For the purpose of the experiment, 200,000 ElectroMagnetic (EM) traces are acquired for different plaintexts. The results show that for AES without active shield, CPA is successful with around 115,000 EM traces. when shield is active, CPA is successful with around 120,000 traces. For a better evaluation of shield's impact on SCA, we computed the Normalized Inter-Class Variance (NICV) for detection of Side-Channel Leakage [18]. NICV allows to evaluate the leakage level of Side-Channel traces. The NICV results are shown in Figure 13(b). We notice that, EM traces of AES with active shield have less leakage than those of AES without active shield. This result can be easily accounted for: the shield activity provides an additional noise on the EM traces hence reducing the Signal Noise Ratio (which is proportional with the NICV value). We also computed the guessing entropy for AES with and without shield in Figure 13(a). The guessing entropy defines the average rank of the good key depending on the number of SCA traces. More details about guessing entropy can be found in [19]. Figure 13(a) shows that the guessing entropy of AES with active shield converges to 0 faster than AES with deactivated shield. It means that the AES with the active shield is more difficult to break than the one without active shield. Therefore, the active shield has a **positive impact** on the cryptographic IPs against SCA attacks.

TABLE I
SUMMARY OF SHIELD IMPACT ON PROTOTYPE ASIC

	PUF	TRNG	Secure Clock	EMA	Critical Path
Active Shield	+	+++	+	+++	- - -

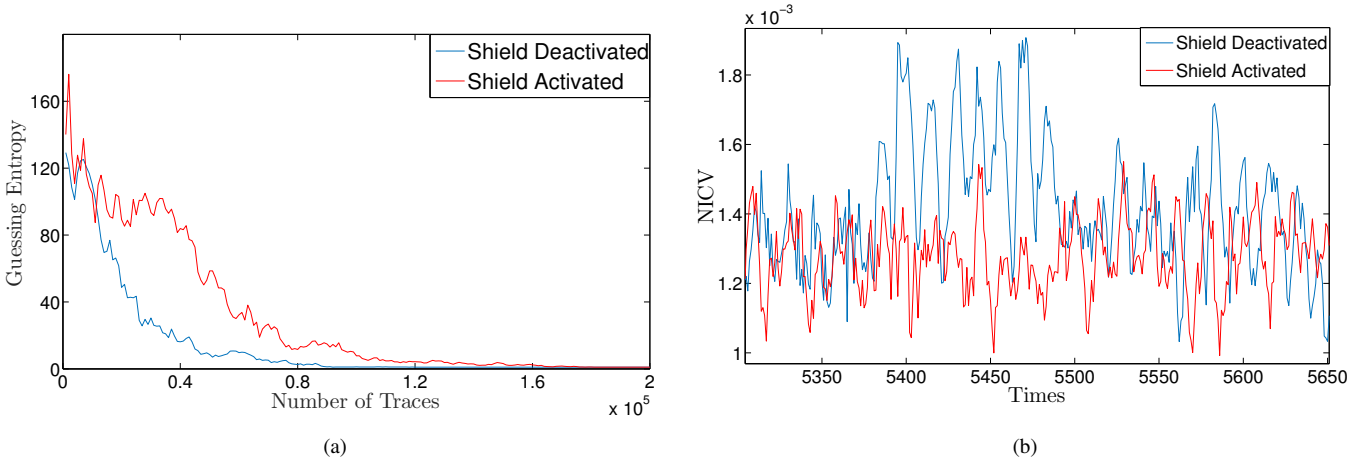
E. Impact of Active Shield on the IC Critical Path

The critical path is defined as the path between an input and an output with the maximum delay. It is an important criteria of integrated circuits, which determines their maximum operating frequency. Therefore, we evaluate the shield impact on the critical path of some IPs. The experiment is performed on Advanced Encryption Standard (AES) 128 bit IP, which is slow (the critical path is long). We measured the maximum frequency of AES with and without activating the active shield. For the AES without the shield, its maximum frequency is around 300 MHz. For the AES with the shield, its maximum frequency is around 270 MHz. Therefore, when the shield is activated, the critical path delay is **increased by 10%**.

The Table I summarizes of shield impacts on the test chip.

V. CONCLUSION

In this article, we have presented a new cryptographically-secure active shield architecture. This shield, based on a lightweight lightweight block cipher, ensures hardware security against probing and FIB attacks. Still, we identify that the shield has a capacitive impact on the IPs it covers.



(a) (b)

Fig. 13. (a) **Guessing Entropy** computation for AES with activated/deactivate shield. (b) **NICV** computation for AES with activated/deactivate shield.

A characterization on the fabricated ASIC shows that the critical path delay is increased by no more than 10% because of extra capacitive load added by the active shield. Several tests are also performed to evaluate the impact of the active shield on other security aspects. The results demonstrate that active shield has a positive impact against the SCA analyses: the noise added by active shield increases the number of traces needed for a successful SCA attack. The test on Loop PUF shows that active shield has also no (or even a slightly positive) impact on the Loop PUF. The results of test on the Open-Loop TRNG shown that the active shield has a positive impact on the delay TRNG. The active shield, which can be consider as a random noise, improves the TRNG entropy. The same conclusion applies to the secure clock. So, in conclusion, not only the shield protects against attacks aiming at modifying and probing at the circuit beneath its mesh, but it also has a positive impact on PUF, TRNG, secure-clock, and SCA resistance. In summary, the only drawback is a slight decrease of the maximal operating frequency for the IPs it covers.

REFERENCES

[1] P. Laackmann and H. Taddiken, "Apparatus for Protecting an Integrated Circuit formed in a Substrate and Method for Protecting the Circuit against Reverse Engineering," February 19 2003, United States Patent number 6,798,234.

[2] J. Liddle, "Robust Hardware Security Devices made Possible by Laser Direct Structuring," December 2012, ECN (Electronic Component News) Magazine; Online: http://www.ecnmag.com/articles/2012/04/robust-hardware-security-devices-made-possible-laser-direct-structuring.

[3] A. Beit-Grogger and J. Riegebauer, "Integrated Circuit Having an Active Shield," November 8 2005, United States Patent number 6,962,294.

[4] M. Janke and K. Engl, "Integrated Circuit and Method of Protecting a Circuit Part to be Protected of an Integrated Circuit," Jan. 7 2010, uS Patent App. 12/166,906. [Online]. Available: http://www.google.com/patents/US20100001757

[5] INVIA, "Active Shield IP (*digital IP and analog IP that detects invasive attacks*)," http://invia.fr/detectors/active-shield.aspx.

[6] A. H. Olney, *Characterization of Integrated Circuits by Qualitative Voltage Contrast Imaging in the Scanning Electron Microscope*. Boston University, 1988. [Online]. Available: http://books.google.fr/books?id=k2QrOAAACAAJ

[7] C. Tarnovsky, "Infineon / ST Mesh Comparison," February 14th 2010, http://blog.ioactive.com/2010/02/infineon-st-mesh-comparison.html.

[8] S. Guilley, S. Briais, T. Porteboeuf, J.-L. Danger, J.-M. Cioranesco, and D. Naccache, "Random Active Shield," in *FDTC*, September 9 2012, Leuven, Belgium.

[9] J.-M. Cioranesco and D. Naccache, "Protection of an Integrated Circuit against Invasive Attacks," August 7 2013, Patent EP 2624296 A1.

[10] J. Cioranesco, J. Danger, T. Graba, S. Guilley, Y. Mathieu, D. Naccache, and X. T. Ngo, "Cryptographically Secure Shields," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014*, 2014, pp. 25–31. [Online]. Available: http://dx.doi.org/10.1109/HST.2014.6855563

[11] H. Ootera, K. Nishikawa, S. Yamakawa, T. Oomori, and S. Tanabe, "Reduction of Crosstalk Noise Between Interconnect Lines in CMOS RF Integrated Circuits," in *Electromagnetic Compatibility, 2002. EMC 2002. IEEE International Symposium on*, vol. 2, Aug 2002, pp. 866–870 vol.2.

[12] J. P. Z. Lee, F. Wang, A. Phanse, and L. C. Smith, "Substrate Cross Talk Noise Characterization and Prevention in 0.35 μm CMOS Technology," in *Custom Integrated Circuits, 1999. Proceedings of the IEEE 1999*, 1999, pp. 479–482.

[13] Z. Cherif, J.-L. Danger, F. Lozac'h, Y. Mathieu, and L. Bossuet, "Evaluation of Delay PUFs on CMOS 65 nm Technology: ASIC vs FPGA," in *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, ser. HASP '13. New York, NY, USA: ACM, 2013, pp. 4:1–4:8. [Online]. Available: http://doi.acm.org/10.1145/2487726.2487730

[14] J.-L. Danger, S. Guilley, and P. Hoogvorst, "High Speed True Random Number Generator based on Open Loop Structures in FPGAs," *Microelectronics Journal*, vol. 40, no. 11, pp. 1650–1656, November 2009.

[15] S. Bhasin, J.-L. Danger, S. Guilley, X. T. Ngo, and L. Sauvage, "Hardware Trojan Horses in Cryptographic IP Cores," in *Proceedings of the 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, ser. FDTC '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 15–29. [Online]. Available: http://dx.doi.org/10.1109/FDTC.2013.15

[16] S. Katzenbeisser, U. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon," ser. CHES'12. Springer, 2012, pp. 283–301. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-33027-8_17

[17] É. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *CHES*, ser. LNCS, vol. 3156. Springer, August 11–13 2004, pp. 16–29, Cambridge, MA, USA.

[18] S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage," in *International Symposium on Electromagnetic Compatibility (EMC '14 / Tokyo)*. IEEE, May 12-16 2014.

[19] F.-X. Standaert, T. Malkin, and M. Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," in *EUROCRYPT*, ser. LNCS, vol. 5479. Springer, April 26-30 2009, pp. 443–461, Cologne, Germany.