A Lightweight Security Primitive using Laser-based Fault Injection

Teng Xu and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{xuteng, miodrag}@cs.ucla.edu

***Abstract*— Security and low power are essential requirements for sensor networks. In order to meet these requirements we have proposed a new type of lightweight security primitive using laser-based fault injection. The essential idea is to use lasers to cut the wires in the circuit layouts, thus to intentionally introduce faults in circuits. We have the following key observations: (1) Large VLSI ICs with partial faults can produce highly unpredictable outputs. (2) Faults in different positions in circuits can cause huge difference in outputs alternation. Therefore, we take advantage of the excellent output randomness of the circuit after fault-injection and directly use it as a security primitive. Compared to the traditional security primitive, e.g., PUF, our proposed laser-based security primitive is robust and resiliency against conditions of operations. More importantly, it employs very low power consumption, therefore providing an ideal platform for sensor networks. We compare the fault injection on standard modules, such as adders, multipliers, and XOR networks and further propose the best architecture. Our statistical tests indicate that by using the laser-based fault injection, lightweight security primitives for sensor networks with small footprint and low energy can be created.**

I. Introduction

Wireless sensor networks are widely used in modern technology. Due to the fact that wireless sensor networks are often exposed in open and hostile environments, the security and privacy has become an important issue. However, traditional cryptographic approaches have the problem of low speed and high energy consumption which is not suitable for the high speed and low energy constrained sensor networks. Therefore, to design lightweight security primitive for wireless sensor networks has become an important issue.

PUFs are low power physical hardware systems that have very complex but stable input to output mappings. In general, a PUF is effectively a very complex mathematical function that is easy to evaluate but impossible to predict. As the name suggests, the device is also impossible to physically replicate. Therefore, PUF, as a security primitive has the advantage of low-power, low-cost, and unclonability.

However, PUFs and their hardware security descendants still suffer of a number of security, design, and operational problems which impede them to become an ideal platform for the wireless sensor networks. For instance, they are susceptible to attacks enabled by pending implementation technologies, they sometimes require very accurate and expensive measurements. Most of all, they lack of stability in the presence of variations in environmental and operational conditions, such as supply voltage and localized temperature.

On the other hand, a well-known wisdom that is widely and strongly established is that integrated circuit (IC) defects and their functional faults are intrinsically a phenomenon that should be detected, diagnosed and, if possible, eliminated. In summary, faults in circuits are unwanted. Our objective is to rebut exactly the above well established postulate. Specifically, we intentionally use laser to introduce faults in circuit. Three key observations are that (i) faults can be intentionally produced. For example, increase the critical area by intentional routing. (ii) large VLSI ICs with partial faults can produce highly unpredictable outputs. The first one indicates the feasibility to introduce random faults in circuits. The second observation can prevent a large family of security attacks from statistical level. Based on the above observations, we claim that the faulty circuit can serve as a natural PUF and be used as a security primitive for wireless sensor networks. We call our proposed PUF the laser-based PUF.

In the following sections, we introduce the concept of faulty circuits and further evaluate the security properties of our laser-based PUF. When a circuit has one fault or very few number of faults, the fault detection is still possible. However, as the number of the faults increases, the detection becomes exceptionally hard, consequently, unclonable. An essential step in exploiting faults is the creation of structures so that the faults in circuits can maximize the output randomness. By applying the simulation of faulty circuits in digital domain, we analyse commonly used adders, multipliers and xor networks based laser-based PUFs in terms of their security properties. Our results indicate that the laser-based PUF shows excellent security properties. In order to establish this claim, we use both standard PUF tests as well as looking into their resistance against different types of attacks. For example, we demonstrate that there is very small correlation between results produced by faulty and fault-free common arithmetic units.

II. Related Work

We now briefly survey the most directly related literature on the physical unclonable function, and fault injection.

A. PUF

Pappu et al. demonstrated the first active physical unclonable function using optical mesoscopic systems in 2001[1]. Devadas and members of his research group observed that

978-1-4799-0162-3/14/$31.00 ©2014 IEEE

intrinsic deep submicron process variation in silicon is an ideal practical and economical starting point to fabricate a large amount of PUFs[2][3]. Two types of approaches, PPUF and SIMPL, enabled transition from secret key to public key hardware cryptography. PPUFs were introduced by Beckmann[4]. SIMPL was proposed by Rührmair[5]. Both approaches employed the gap between simulation and execution to accomplish various security tasks. Device-ageing based PUF introduces techniques that completely eliminate any need for simulation by exploiting mechanisms that allow the creation of exactly a specified number of identical devices[6]. The use of PUFs in conjunction with standard pseudorandom generators and von Neuman data post-processing was analyzed by the Devadas group[7]. More recently, the concept of digital PUF is proposed by Xu. [8][9]. To apply PUF in the domain of sensor network security is proposed in [10][11][12].

B. Fault Injection

Since at least 1998, laser-based fault injection has been recognized and demonstrated as a powerful security attack on cryptographic devices [13]. Numerous fault injection-based security attacks have also been reported and surprisingly successful. A comprehensive survey on fault injection techniques as tools for compromising security devices and protocols was recently presented by Barenghi etc. [14]. The key difference between the surveyed research and our efforts is that for the first time we intentionally introduce faults in circuits and advocate positive use of faults for security.

III. Concepts

A. Motivational Example

We start with the simple one bit adder circuit represented by logical gates. We assume that the type of fault in the circuit is a gate-level stuck at fault which means that the output of a gate is tied to logical 1 or 0 regardless of the inputs. Note that when using laser to cut in the circuit, if we connect the position being cut to Vdd, it is equal to stuck at 1, and if we connect to ground, it is equal to stuck at 0. Figure 1 shows the five potential fault positions in a one bit adder. For each position, the output can be stuck at either 1 or 0. Table I compares the corresponding outputs of a one bit adder circuit with different fault positions with the outputs of a fault-free one bit adder. We define faulty outputs as the outputs generated by circuits with faults while fault-free outputs are defined as outputs generated by fault-free circuits. The results in Table I show that even if there is only a single stuck at fault in the circuit, the impact on the outputs is huge. This provides the intuition that the faulty outputs may show excellent randomness and unpredictability after appropriate configuration.

B. Laser-based PUFs

In order to create the laser-based PUF, we have two key operations. The first is to randomly use laser to introduce faults in circuits. As a result, for different implementations, the position and type of the faults would be different due to process variation. The second is that since the faults are randomly created due to intrinsic process variation, it is only by gate level characterization that the position and the type of the faults can be measured and, thus, potentially enable an attacker to clone the device. We eliminate this possibility by physically removing (e.g. burning) those pins on the circuit which enable gate level characterization. Therefore, the physical unclonablity of the faulty circuit is guaranteed.

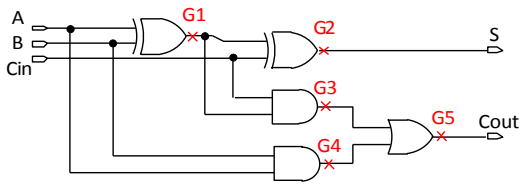


Fig. 1: Stuck at faults in a one bit adder. Gi indicates different positions of faults.

Now consider an attacker who attempts to clone our PUF. He is not able to execute a hardware level attack to look into the structure of laser-based PUF due to the burning of the pins. What he can do is to test all the possible input vectors on the faulty circuit to get the corresponding outputs and further create a mapping between the inputs and outputs. Due to the difficulty of reverse engineering, he can not reverse engineer the corresponding hardware architecture just by acquiring this mapping.

IV. Architecture

In this section, we propose the architecture of our laser-based PUF based on a few common circuits. The desiderata is that although our laser-based PUF can be applied in any type of circuit, we define an architecture to have "good performance" only when it guarantees excellent security properties under the constraint of small area and low energy consumption. We first propose the laser-based PUF architecture based on commonly used adders and multipliers. Then we propose a customized XOR network that can potentially show "better performance".

A. Adders

The adder is one of the most commonly used circuits. An example of the full adder based laser-based PUF is already shown in Figure 1.

B. Multipliers

Multipliers can also be found in many circuits, but generally take more area and power than adders. For the sake of security, when the faults in a particular architecture can significantly change the outputs, the architecture is regarded as "good" since the outputs would be hard to predict. Our intuition is that the faults in multipliers are easier to propagate and consequently alter the outputs more as compared to adders because of the increased circuit depth.

A / B / Cin	Cout / S										
	Fault-Free	$G1 \rightarrow 1$	$G1 \rightarrow 0$	$G2 \rightarrow 1$	$G2 \rightarrow 0$	$G3 \rightarrow 1$	$G3 \rightarrow 0$	$G4 \rightarrow 1$	$G4 \rightarrow 0$	$G5 \rightarrow 1$	$G5 \rightarrow 0$
0 0 0	0 0	0 1	0 0	0 1	0 0	1 0	0 0	1 0	0 0	1 0	0 0
0 0 1	0 1	1 0	0 1	0 1	0 0	1 1	0 1	1 1	0 1	1 1	0 1
0 1 0	0 1	0 1	0 0	0 1	0 0	1 1	0 1	1 1	0 1	1 1	0 1
0 1 1	1 0	1 0	0 1	1 1	1 0	1 0	0 0	1 0	1 0	1 0	0 0
1 0 0	0 1	0 1	0 0	0 1	0 0	1 1	0 1	1 1	0 1	1 1	0 1
1 0 1	1 0	1 0	0 1	1 1	1 0	1 0	0 0	1 0	1 0	1 0	0 0
1 1 0	1 0	1 1	1 0	1 1	1 0	1 0	1 0	1 0	0 0	1 0	0 0
1 1 1	1 1	1 0	1 1	1 1	1 0	1 1	1 1	1 1	0 1	1 1	0 1

TABLE I: Single stuck at fault impacts on the outputs of a one bit adder. Values in red indicate the different bits in faulty outputs compared to fault-free outputs.

C. XOR networks

The XOR network architecture shown in Figure 2 has w inputs, u outputs and h stages of XOR gates. Each stage is comprised of u XOR gates. Between two stages, the outputs of previous stage are randomly shuffled and used as the inputs for the next stage of XOR gates. The total number of XOR gates used in this design is $u * h$.

In this architecture, on average, an output from a previous stage needs to be used as the input of 2 gates in the next stage, e.g., the red line connection in Figure 2. Now suppose a fault occurs at the first stage of this XOR network. As a result, in stage 1, the output of one gate is potentially changed. In stage 2, since the wire of the faulty output from previous stage is connecting to two gates in this stage, the outputs of two gates in stage 2 are influenced. In the final stage (stage h), on average, 2^{h-1} outputs are influenced. Therefore, we conclude that a fault in XOR network propagates exponentially as the stage grows.

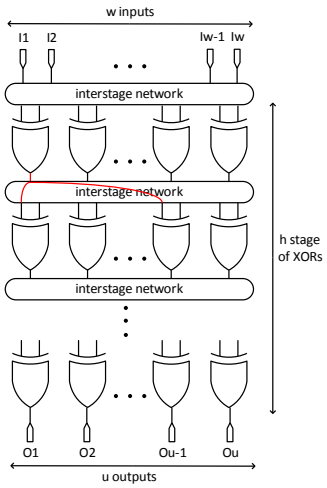


Fig. 2: XOR network architecture with w inputs, u outputs and h stages of XOR gates. Interstage network interconnects only the cells between neighbouring layers of gates. The red line shows an example of interstage connection.

V. Security Attacks and Evaluation

In this section, we analysis the security properties of the laser-based PUF based on adders, multipliers, and XOR networks respectively. The basic approach is to identify their resistance against statistical attacks. In the attacks, the attacker observes a polynomial number of challenge-response pairs and tries to statistically analyze them in order to predict the answer to an unseen challenge.

For each type of attack, we conducted comprehensive tests using 64-bit carry-ripple adder, 32-bit array multiplier and XOR network with $w = 64$, $u = 64$, and $h = 8$. All of these circuits have 64 outputs which facilitate comparison (we do not consider carry bit in the case of adder and multiplier). For each simulation, we present the results using 10,000 input vectors. In each type of circuit, we suppose 2 percent of the gates have faults.

A. Guessing with Statistical Model

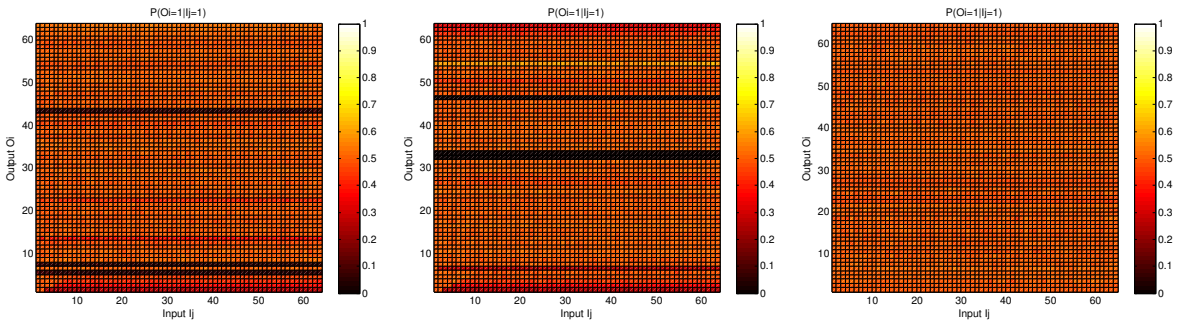
1) Predictions using fault-free circuits: In this type of attack, the attacker tries to predict the outputs of a laser-based PUF by using the outputs of the corresponding fault-free circuit given the same inputs. We simulate to analyse their average output hamming distance on adders, multipliers and XOR gates respectively. Ideally, the results should be around half of the number of outputs. Table II shows the average output hamming distance across the three circuits. It is obvious that XOR network has best performance, followed by multiplier and adder has worst performance.

	Adder	Multiplier	XOR network
Avg. Distance	2.7 ± 1.8	22.9 ± 4.3	31.92 ± 4.56

TABLE II: Average output hamming distance between 2% faulty circuit and fault free circuit. The uncertainties correspond to standard deviations in faults characterisation. The ideal hamming distance should be 32.

2) Avalanche effect predication: If the avalanche criterion is evident in a cryptographic system, then there is an ultra low probability that an attacker can predict any subsequent outputs using knowledge of outputs for similar inputs. The avalanche criterion can be measured by observing the corresponding outputs for two inputs who differ by a minimal amount. In the case of our laser-based PUF, the smallest amount that an input can change is by one bit.

Thus, we measure the hamming distance between output vectors when changing one bit of our input vector over 10,000 inputs. Ideally, the average hamming distance should be 32.



(a) Adder (b) Multiplier (c) XOR network

Fig. 3: Conditional probabilities between Input bits I_j and output bits O_i: $P(O_i = 1|I_j = 1)$.

Table III presents the results on the three architecture, still, XOR network performs best, then the multiplier and the adder.

	Adder	Multiplier	XOR network
Avg. Distance	1.54 ± 0.51	16.41 ± 3.15	31.24 ± 4.02

TABLE III: Average output hamming distance for avalanche effect of the 2% faulty circuit. The uncertainties correspond to standard deviations in faults characterisation. The ideal hamming distance should be 32.

3) Conditional probability: Another type of attack is the bitwise correlation modeling via the construction of per-bit input-output conditional probability distribution. The goal of the attacker is to predict $P(O_i = c_1|I_j = c_2)$, c_1, c_2=1 or 0. The ideal secure system will have a probability of 0.5 for all conditionals. Figure 3 depicts the conditional probability $P(O_i = 1|I_j = 1)$ across adders, multipliers and xor networks respectively. Despite the fact that some output bits in adders and multipliers are always 0 because of the positions of the faults, the overall performance of the three architecture is excellent. Note that most conditional probabilities are around 0.5 and for the few "black lines" in Figure 3a and Figure 3b, we simply do not use the corresponding outputs.

VI. Conclusion

We have developed techniques for the creation of the laser-based physical unclonable function for wireless sensor networks by intentionally use laser to introduce faults in circuits. In addition to complete elimination of standard PUF vulnerabilities such as susceptibility to operational and environmental variations, the tests on simple model (adders, multipliers and xor network) indicate excellent outputs randomness under the circumstance of small hardware footprint and low energy consumption. Among which, we find that the xor network shows best security properties compared to adders and multipliers. Our laser-based PUF is small footprint and low power, therefore ideal for wireless sensor networks.

VII. Acknowledgement

This work was supported by the NSF under Award CNS-0958369, Award CNS-1059435, and Award CCF-0926127.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *ACM Conference on Computer and Communications Security*, pp. 148–160, 2002.

[3] S. Devadas, V. Khandelwal, S. Paral, R. Sowell, E. Suh, and T. Ziola, "Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications," *IEEE RFID*, 2008.

[4] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," *Information Hiding Conference*, pp. 206–220, 2009.

[5] U. Rührmair, "SIMPL systems, or: can we design cryptographic hardware without secret key information?" *International Conference on Current Trends in Theory and Practice of Computer Science*, vol. 6543, pp. 26–45, 2011.

[6] S. Meguerdichian and M. Potkonjak, "Matched public PUF: ultra low energy security platform," *IEEE/ACM ISLPED*, pp. 45-50, 2011.

[7] C. W. O'Donnell, G. E. Suh, and S. Devadas, "PUF-based random number generation," *MIT CSAIL CSG Technical Memo 481*, 2004.

[8] T. Xu, J. B. Wendt, M. Potkonjak, "Digital Bimodal Function: An Ultra-Low Energy Security Primitive," *IEEE/ACM ISLPED*, pp. 292-297, 2013.

[9] T. Xu, M. Potkonjak, "Robust and Flexible FPGA-based Digital PUF, to appear in *International Conference on Field Programmable Logic and Applications (FPL)*, 2014.

[10] T. Xu, M. Potkonjak, "Lightweight digital hardware random number generators," *IEEE SENSORS*, pp. 1-4, 2013.

[11] T. Xu, J. B. Wendt, and M. Potkonjak, "Matched Digital PUFs for Low Power Security in Implantable Medical Devices" to appear in *IEEE International Conference on Healthcare Informatics (ICHI)*, 2014.

[12] R. Yan, V. C. Shah, T. Xu and M. Potkonjak, "Security Defenses for Vulnerable Medical Sensor Network, to appear in *International Conference on Healthcare Informatics (ICHI)*, 2014.

[13] J. Samson, W. Moreno, and F. Falquez, "A Technique for Automated Validation of Fault Tolerant Designs Using Laser Fault Injection, *Proc. Intl Symp. Fault-Tolerant Computing (FTCS-28)*, 1998.

[14] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056-3076, 2012.