An Electromagnetic Fault Injection Sensor using Hogge Phase-Detector

Jakub Breier, Shivam Bhasin
Temasek Laboratories
Nanyang Technological University
Singapore
Email: {jbreier, sbhasin}@ntu.edu.sg

Wei He*
Shield Lab, Central Research Institute
Huawei International Pte. Ltd.
Singapore
Email: hewei48@huawei.com

***Abstract*—Fault injection attack against embedded devices has attracted much attention in recent years. As a highly efficient fault injection, EM fault injection (EMFI) outperforms other injection means owing to its outstanding penetration capability in incurring local faults into security ICs. In this paper, we present an all digital countermeasure for detecting the on-the-fly EMFI attempts in silicon chips. The proposed logic consists of a watchdog ring-oscillator (RO), and a Hogge Phase Detector (PD) for sensing the frequency turbulence induced by the on-going EMFIs. Experimental validation on Xilinx FPGA Virtex-5 FPGA reports a fault detection rate of 93.15% and a failure rate of 0.0069, with negligible overhead. A significant security margin for alerting the injection attempt is also noticeable. The technique is versatile and can be integrated in any VLSI design for its lightweight and all digital architecture, especially for the security-critical scenarios, such as the endpoints of Internet-of-Things (IoT).**

***Keywords*—Fault Injection Attack, Hooge Phase Detector, Countermeasure, Electromagnetic**

I. Introduction

Embedded system has evolved to be irreplaceable in modern information society. It forms the backbone of the prevailing Internet-of-Things (IoT) which involve connecting a number of embedded endpoints to collect and process dedicated information, contributing to an intelligent and functional ecosystem. This framework has invoked several upcoming concepts like smart home, autonomous vehicle (AV), smart city etc. Depending on the application, these embedded devices are continuously interacting with data of personal (for ex. smart home) or sensitive (for ex. smart city). Coming with tremendous benefits and wide application spectrum, the security of these devices has become a critical issue.

Alongside several hardware and software attacks on embedded devices, side-channel attacks (SCA) [1] and fault attack (FA) [2] on embedded cryptographic primitives have evolved to be practical threats. Typically, SCA exploits the leaked physical information from the operating security devices for extracting secrets, such as secret keys of cryptographies [1], [3], [4], [5]. on the contrary, adversary in FA intentionally introduces data faults into critical computations. By analyzing the induced faulty outputs or behaviors, some confidential information can be practically extracted.

* This research was conducted when author was at Temasek Laboratories

There are two main approaches for inducing faults into modern ICs. The first is the global injection that is normally performed by disturbing the clock system or power line of the chip [6], [7]. For these injections, the equipment cost is low but lacking the ability to control the injection precision, since adversary does not know where and how many the fault/faults will appear. Therefore, normally a big number of perturbations need to be gathered, so as to find the usable faults for a specific fault attack that requires precise fault models. The advantage for global injection is in its low cost since it does not require an advanced injection equipment. The other method relies on customized fault perturbation solutions, like laser based fault injection (LFI) [8] or electromagnetic fault injection (EMFI) [9]. In this approach, the fault impact can be strictly constrained to the Point-of-Interest (POI) that is compatible with specific fault attack models. As the IC packages are getting more advanced and reliable, LFI becomes difficult due to the requirement for chip de-capsulation. EMFI often outperforms LFI since the package material and silicon substrate is transparent to the EM field. Without loss of generality, we focus on EMFI in this paper to present the proposed countermeasure, however, it is still viable against other fault attack methodologies.

Countermeasures against EMFI can be applied at two different levels. Information-based countermeasures, as the parity-based concurrent error detection (CED) [10], detect malicious modifications in underlying data. The pitfall of this strategy is that the circuit must be modified with heavy but unavoidable overhead (performance, hardware, power etc). Moreover, the system can only detect the faults that have already been successfully injected. Sensor-based countermeasures [11], [12] deploy sensors to detect injection/disturbance attempts by monitoring environmental parameters (induced EM field in this case). These countermeasures are relatively low cost, and can detect injection attempts even before the fault is injected and thus well suited for real-time applications.

A sensor-based countermeasure, composed of a watchdog ring oscillator (RO) and a phase-locked-loop (PLL), was proposed recently to detect EMFI [12]. The PLL is able to detect a phase shift (PS) in RO frequency due to EM disturbance. A main shortcoming of the proposed countermeasure is the assumption of presence of PLL module, which is actually not

easily available in low-resource IoT devices.

In this paper, we propose an all-digital, lightweight digital sensor to detect the EMFI-induced phase shift in a watchdog RO. The detection is realized by sensing the phase shift change between two frequencies: (a) the original RO oscillation signal `CK`, and (b) a synchronized but delayed signal `Data` derived from `CK`. The all-digital low-cost nature makes it usable for a wide range of embedded devices.

The content of this paper is organized as follows: In Sec. II, relevant technical background is recalled. Sec. III details the proposed digital EMFI sensor. The FPGA implementation and the experiment to evaluate the effectiveness of the sensor system are presented in Sec. IV. Further application aspects of the proposed sensor and some possible reaction mechanisms are discussed in Sec. V. Sec. VI draws the work conclusions and future work.

II. Background

A. EMFI Impact on Ring Oscillator

As an efficient method for injecting faults into ICs [9], EMFI uses high voltage EM field in form of transient pulses or harmonics to disturb the chips. It can be performed without de-capsulation of the target chip, making it cost effective.

RO is basically a closed delay loop, cascaded by odd number of inverters for producing signal oscillation between two voltage levels, representing digital `0` and `1`. The signal delay is related to silicon temperature and voltage level, and the RO oscillation frequency is determined by the signal propagation delay in this logic chain. RO frequency has also been used as a watchdog for monitoring the real-time local voltage or temperature in silicon [13], [14]. It was previously shown that RO is sensitive to EM injections. This is because the generated EM field causes coupling with the circuit lines which may induce transient currents, and these currents can accelerate or delay the single propagation in RO loop, which consequently affects the RO frequency/phase [9].

B. Prior Countermeasures against EMFI

A delay-based glitch detector was proposed by Zussa *et al*, in [11] for detecting the EMFIs. It detects timing violation due to EM injection and subsequently raises an alarm flag. Several detectors are deployed over the chip to make sure that at least one detector captures local EM injection. However, the placement of detectors is chosen empirically.

A novel sensor system was proposed by Miura *et al*, in [12], for detecting the EM disturbance by monitoring the phase shift of a RO frequency relying on a PLL. In this circuit, the RO output is used as the clock input of PLL and the feedback of PLL loop is self-calibrating. In case ripple in frequency/phase on RO frequency, the PLL may enter an `unlocked` state and raise an alarm.

A primary requirement of the proposal in [12] is the presence of a PLL primitive. PLL is an analog component which consumes significant power that inevitably limits the applications on power-constrained devices, such as the wireless endpoints of Internet of Things (IoT) and cyber-physical systems (CPS) that are typically powered by batteries. To overcome this limitation, we propose an all-digital EMFI sensor in the following.

III. Low-Cost Digital EMFI Sensor

This section describes the proposed sensor followed by its timing characteristics which are used for EMFI detection.

A. Hogge based EMFI Detector

As a popular linear phase detector, Hogge Phase Detector (PD) was proposed in [15]. This PD consists of two D type Flip-Flops (FFs) and two Exclusive-Or (XOR) gates, for detecting the phase shift between two frequencies (Data and CK), as seen in Fig. 1. FF1 is clocked by the `rising` edge of the signal `CK`, FF2 is clocked by the `falling` edge of `CK`. Input and output from FF1 and FF2 are respectively `XORed` to produce two pulses, where Y is a proportional pulse in relation to the phase shift of `Data` and `CK`, and X is a reference pulse with CK/2 width. Given locked phase condition, pulses X and Y have the same width with opposite polarities. In this work, Hogge PD is deployed to detect the RO frequency disturbance induced by EMFI. The sensor system is depicted in Fig. 2, which consists of three functional modules.

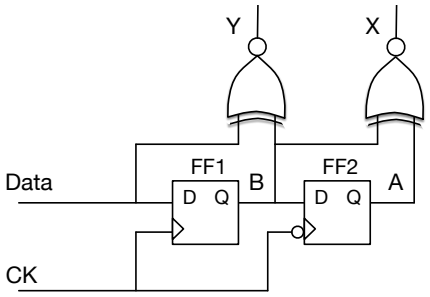

Fig. 1. Hogge phase detector.

- Ring Oscillator: The RO is used as the watchdog for sensing the transient frequency ripples induced by EMFI.
- Modulator: A 'D Flip-Flop with Synchronous Reset' (FDR) is used to derive a frequency `Data` with exactly half of the RO frequency f.
- Hogge PD: The generated `Data` $(f/2)$ and the original RO frequency `CK` (f) are used as the two inputs to the Hogge PD. A 1 bit **alarm** signal is generated, serving as the threat flag indicating the incoming EMFI injections.

As aforementioned, `Data` signal is derived from `CK`, so any frequency changes in RO (`CK` signal) result in corresponding changes in `Data`, which make the phase shift between the two signals still maintained. To purposely incur phase shift change, we introduced a **delay factor** (prolonged routing) on signal line of `Data` from Modulator to PD. Owing to the long propagation time, the disturbance on RO will **not** be immediately reflected on `Data` in PD. So, any ripple on either `Data` or `CK` will cause phase shift change that can be detected.

The duty cycle of the RO frequency f is 50%, and the modulated `Data` has a frequency of $f/2$, also in a 50% duty

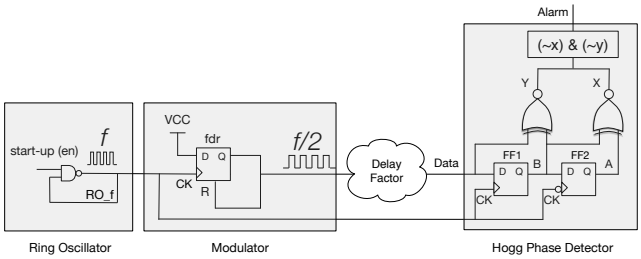

Fig. 2. Logic scheme of the low-cost digital EMFI detector.

cycle. Since the delay factor is determined by routing, `Data` has a fixed phase shift with `CK`. An alarm signal is generated by Equation (1) to alert the abnormality in phase shift of the two frequencies, which stays in low voltage level, e.g., binary '0', in absence of EM disturbance, as shown in the `vigilant state` of Fig. 3.

$$alarm = \overline{x} \cdot \overline{y} = \overline{(Data \oplus B)} \cdot \overline{(B \oplus A)} \tag{1}$$

B. Frequency Disturbance in Timing

1) **Low-Frequency Ripple:** The `low-frequency` disturbance on RO frequency is defined as the absence of one or more oscillation cycles. Relying on the duration of EM pulse and the RO frequency, the oscillation can slow down during multiple cycles. For simplicity, only the single oscillation disappearance is demonstrated. Because of the delay factor applied to `Data` signal line, the disappearance (delayed) of `CK` only affect the `Data` in PD after several `CK` cycles. So at the injection moment, signal `Data` is still oscillating normally in PD but clocks of FF1 and FF2 are affected immediately, which produces abnormalities in both register outputs of A and B, and subsequently triggers alarm, as shown by `low-frequency ripple` in Fig 3. The first rising edge of alarm is used for alerting the cipher to respond immediately towards the on-going injection attempts. The disturbance continues for a limited time period and automatically returns to `vigilant state`.

2) **High-Frequency Ripple:** High-frequency ripple is defined as the appearance of multiple oscillations into a single clock period of the original frequency. Similarly, due to the delayed ripple propagation on `Data` in PD, the disturbance on RO induced temporary phase shift changes between `CK` and `Data`, which can also be detected by PD by triggering the alarm signal, as illustrated in `high-frequency ripple` of Fig. 3.

3) **Complex Frequency Ripple:** In real-world EMFI, the induced frequency disturbance in RO can be more complicated than the situations demonstrated above. For instance, the disturbance can be a combined high-frequency and low-frequency ripples that expands over multiple `CK` cycles. However, owing to the delayed `Data` propagation to PD, the phase shift can be detected, resulting in alarm signal. By using a high frequency `CK` yielded from a smaller RO, and properly tuning the original phase shift (adjusting `Data` routing length), even a slight phase shift change can be detected.

C. Watchdog using Prolonged Routing of Data

As discussed before, the `Data` signal is derived from `CK` using a FDR. An important phenomenon observed is that the frequency ripple on `Data` does not affect the phase of `CK` frequency. So the EM injection on `Data` can as well cause phase shift between `CK` and `Data`. Therefore, this long routing can also be used as the EMFI watchdog. Since this routing can be long without decreasing its frequency, a large chip area can be protected using the long routing path of `Data` before PD, compared to the region covered by the small RO. This effect is experimentally validated in the next section.

D. Pre-Timing Characterization

In absence of EMFI, the alarm signal should be guaranteed to be logically low. This procedure must be done before the deployment for preventing any alarm glitches without EMFIs. The requirement is that the `rising edge` of `Data` signal in PD should only happen in the high voltage level of `CK`. This can be achieved by slightly adjusting the prolonged `Data` routing length to enforce a proper phase shift between the two signals.

IV. Practical Evaluation

A. FPGA Implementation

The proposed countermeasure was implemented in Xilinx Virtex-5 FPGA (VLX50T) to evaluate its detection sensitivity. To validate the effectiveness of the proposed countermeasure against EMFIs, we selected PRESENT block cipher [16] as the protection target. This cipher is a classic substitution permutation network (SPN), which consists of 64-bit `AddRoundKey`, 16 4-bit `S-box` and 64 bit pLayers, as sketched in Fig. 4. In this work, we target the `round data registers` for injecting the cipher faults.

First, the Ring Oscillator was implemented to encapsulate a group of CLBs by enforcing the routing path through the 4 CLB corners. The PRESENT cipher is implemented in the same CLB region. For the comparison, the PLL counterpart with similar placement was also implemented [12], where a PLL primitive in FPGA is used, instead of the Hogge PD, as the phase shift detector. The RO frequencies from PLL and Hogge sensors are $\approx$ 210 MHz and $\approx$ 203 MHz, respectively. The schematics of the two circuits are shown in Fig. 5.

B. EMFI Setup and Chip Scan

The setup of the experiment is depicted in Fig. 6, which is comprised of the FPGA system for implementing the cryptographic primitive, the EMFI sensors, and system for performing the EM injections. To prevent the EM interference to controller of the cryptography, another FPGA controller board is used to deploy the control logic. A 2D motorized stage is utilized to hold the crypto FPGA for conducting EMFI scanning over the chip surface. The PC serves for feeding the

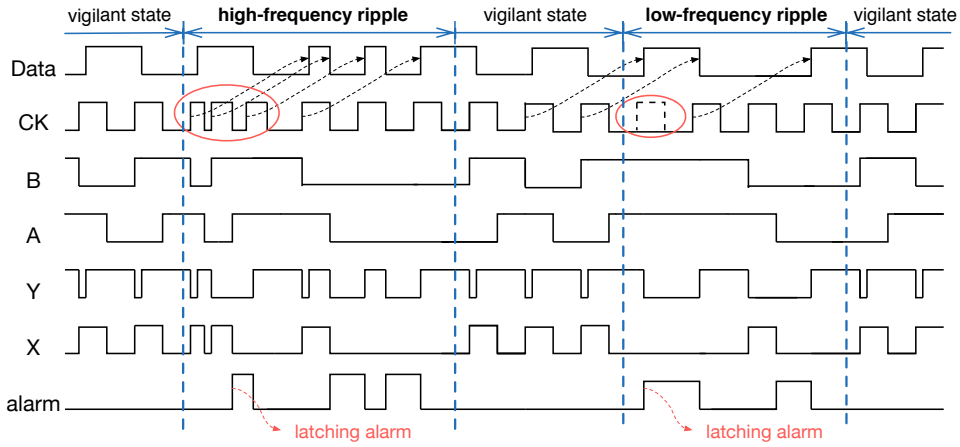

Fig. 3. Timing of low-/high- frequency ripples on CK induced by injections.

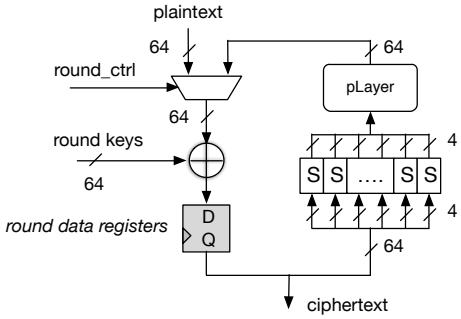

Fig. 4. PRESENT-80 block cipher.

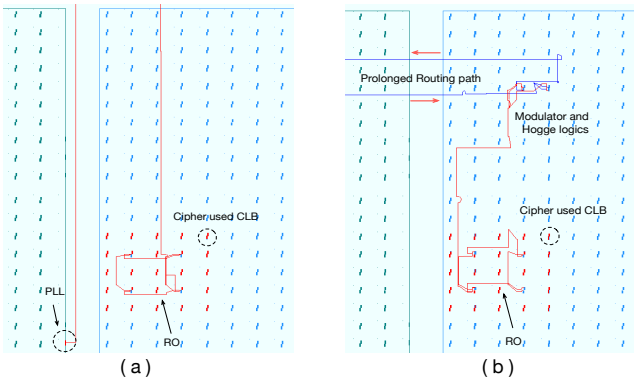

Fig. 5. Schematics of (a) PLL- and (b) Hogge- based EMFI sensors.

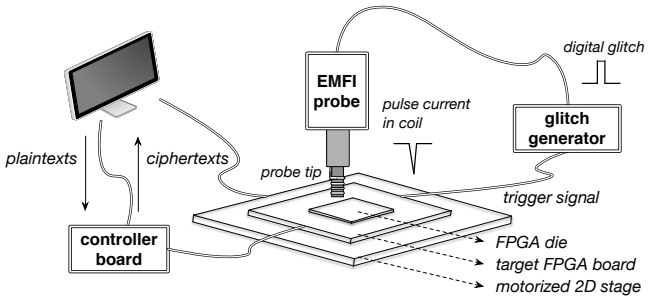

Fig. 6. EMFI setup for the experiments.

plaintext, meanwhile recording the ciphertext and the alarm bit together with the position coordinates for each injections.

The size of the chip is around 12×12 mm^2, and the probe tip we employed is a coil probe of 1.5 mm in diameter. The EM pulse was fixed to 20 ns. The generated EM field is perpendicular to the chip layer, which is capable of inducing *Eddy* current in circuit wires and causing data upset in registers. In the experiments, we launched the EMFIs targeted to the EMFI sensor deployed region, where the round data registers of PRESENT cipher are also implemented and protected by the RO watchdog. In the scanning campaign, the POI region is approximately targeted by a scan array of 100×100. The injection time is fixed to the last computation round of PRESENT cipher, and the transient injection voltage pulse of the coil is configured to be random, ranging between $40\%\sim100\%$ of its transient maximum 450 V in probe coil.

C. Experimental Results

The EMFI scan result for the detector is shown in Fig. 7. The different injection outcomes are highlighted by colour as explained in the legend, where (i) *Case_(1)*: "**Only Alarm**" represents the injections that only triggered the countermeasure; (ii) *Case_(2)*: "**Fault+Alarm**" represents the injections that injected cipher faults, meanwhile triggered the alarm; and (iii) *Case_(3)*: "**Only Fault**" presents the injections that injected cipher faults, while failed to be detected. In our scenarios, both *Case_(1)* and *Case_(2)* are assumed to be successful detections, since the sensor system responded to the injections can hence alert the cipher block to react to the threat by, for instance, temporarily suspending the ciphering computation. More reaction mechanism will be further discussion in Sec. V.

Tab. I shows the results comparison of the two sensor systems. For the PLL based sensor, 264 out of 333 (*i.e.,*

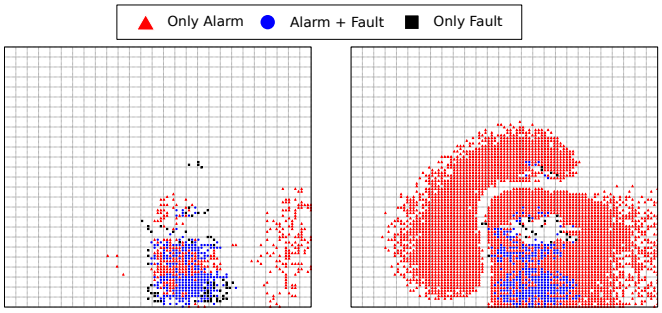

Fig. 7. Scan results for: (a) PLL EMFI sensor and (b) Hogge EMFI sensor, corresponding to the full area of the chip. Higher detection rate and larger detection coverage are seen using the proposed injection sensor.

264+69) injections that invoked cipher faults are detected by the sensor, giving a detection rate of cipher faults of 79.28%. Besides, another 348 injections triggered the alarm but without cipher faults, which gives failure rate of 1/8.87 or 0.1127, *i.e.,* ratio of undetected faults to detected injections. Intuitively, an effective countermeasure should minimize this failure rate as much as possible. For the proposed Hogge PD based sensor, the detection rate is 93.15% as compared to 79.28% for PLL counterpart. Similarly, the failure rate for the proposed countermeasure is significantly reduced to 1/143.96 or 0.0069, as indicated in Fig. 7b, which demonstrates significantly high sensitivity against EMFI.

TABLE I
THE EXPERIMENTAL RESULTS OF EMFI SCAN IN THE CIPHER REGION

		Only Alarm Case_(1)	Fault+Alarm Case_(2)	Only Fault Case_(3)	Scan Matrix	RO freq.
PLL EMFI Sensor	No.	348	264	69	100×100	$\approx$210 MHz
	Detection	Successful		Failed		
	Detection Rate	$\frac{Case\_(2)}{Case\_(2)+Case\_(3)} = \mathbf{79.28\%}$				
	Failure Rate	$\frac{Case\_(3)}{Case\_(1)+Case\_(2)} = \mathbf{0.1127}$				
Hogge EMFI Sensor	No.	3259	340	25	100×100	$\approx$203 MHz
	Detection	Successful		Failed		
	Detection Rate	$\frac{Case\_(2)}{Case\_(2)+Case\_(3)} = \mathbf{93.15\%}$				
	Failure Rate	$\frac{Case\_(3)}{Case\_(1)+Case\_(2)} = \mathbf{0.0069}$				

Compared to the PLL counterpart, the proposed Hogge sensor costs only 3 flip-flops and 2 LUTs for the entire system, without any analog component, as seen in Table. II. The RO and `Data` routings can both be used as the sensor watchdogs. The only extra requirement is its pre-timing delay adjustment in the `Data` signal line by a simple tuning on the routing length.

V. Complementing Discussions

A. Design Principles of Digital Detector

As aforementioned, fault injections are realized by impacting the circuitries in two different directions: a) to directly induce charging or discharging phenomena in storage element bits also known as single event upset (SEU), and b) to cause signal propagation change in combinatorial logic chain, and consequently resulting in timing violation also known as single event transient (SET). For SEU, sufficient energy should be transmitted in order to breach the threshold in storage bit between '0' and '1', hence it requires higher energy, *w.r.t.* impacting signal timing delays. In contrast, a sensitive injection sensor is preferably constructed over detecting the abnormality on signal propagation, so as to achieve better sensitivity. The RO used in this proposal is able to accumulate the impacts for each injection, since the signal oscillating along the RO loop is fast, so each injection can typically affect the signal propagation multiple times, hence amplifies its impacts, as illustrated in Fig. 8.

TABLE II
COMPARISON WITH STATE OF THE ART

Sensor	Analog Component	FF	LUTs	Buffers	Watchdog	Pre-Timing Charaterization
PLL Sensor [12]	Required	$1^{\ddagger}$	2^{*}	$3^{\$}$	RO Routing	None
Hogge Sensor [This Work]	None	$3^{\bullet}$	$2^{\dagger}$	0	RO + Data Routing	Required

‡ Alarm latching: 1 FF. * RO: 1 LUT, Alarm latching: 1 LUT.
$^{\bullet}$ Modulator: 1 FF, Hogge PD: 2 FFs. † RO: 1 LUT, Hogge: 1 LUT.
$^{\$}$ I/O of PLLs must be buffered to ensure less signal skew.

The second principle is that the sensor should be able to detect both accelerated and decelerated signal propagation, *i.e.,* it should be a **bi-directional** sensor, to have full detection coverage. The glitch-detector proposed in [11] is able to detect the decelerated signal due to the underpower, while lacking the capability to detect the accelerated signal in case the power supply is temporarily overpowered.

Besides, the disturbance should be easily captured by a storage element to raise the alarm flag. This is because the induced ripple is temporary and can disappear immediately. So it is optimal to apply the disturbance-induced glitches as the trigger input of storable element for raising the alarm bit. Based on these principles, different digital sensor architectures can be schemed, adapting to varying application scenarios.

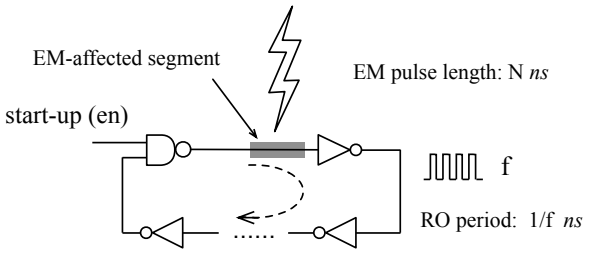

Fig. 8. Accumulated EM injection disturbance in RO watchdog.

B. Detection Capability against other Fault Injection Attacks

This sensor system can also be used for detecting other injection methods. Although LFI has a harder chip preparation requirement, it operates by inducing high-energy optical pulses to cause the disturbance. The impact of LFI on PLL based sensor was demonstrated in [17]. The present sensor also uses

the same watchdog RO as the detector with a different alarm circuitry. Thus, the proposed sensor would also detect LFI. Global fault injection remains out of the scope. However, by monitoring clock signal with the proposed detector instead of the RO, a clock glitch can also be detected. Similarly, a power glitch affecting the oscillation frequency in RO can also be monitored.

C. Reaction Mechanisms

The sensor presented in this paper aims at detecting the incoming fault injection threats, however, a typical concern of security designers is the design of appropriate reaction mechanism. In other words, when the proposed sensor in place detects an attack, how should the circuit react in order to not leak any sensitive information is a typical question to be answered. The reaction should be carefully planned as an optimistic reaction can lead to potential security flaws while a pessimistic reaction can lead to unnecessary denial-of-service (DoS). Typical reaction mechanisms can be schemed as follows:

- temporarily resetting the whole chip, to avoid sending the fault-affected outputs. This is the most direct reaction that can be applied. However, resetting the chip can be easily sensed by the adversaries, which will motivate them to employ further solutions to make the attacks.
- outputting garbage data, to cheat the adversaries. The garbage data can be produced by a random number generator (RNG). This is a more active countering solution.
- a kill switch, to erase the critical logic or the entire circuit. This option suits to the very security-sensitive applications.

To balance the reaction intensity, a watchdog counter is typically integrated, which remains separate from the sensitive circuit.

VI. Conclusions

This paper presented an EMFI countermeasure. The proposed circuit is composed of (1) a watchdog RO to sense disturbance in RO frequency `CK`, induced by EMFIs; (2) a modulator to generate a synchronized oscillation signal `Data` derived from `CK` with intentionally prolonged routing path; and (3) a phase detector for detecting the change of phase shift between `CK` and `Data`. The main merits of the developed countermeasure reside in its extremely low cost, all-digital architecture that is compatible with any digital IC environments, and suitability for resource-constrained devices. The countermeasure is compared against a state of the art PLL based counterpart proposed in [12] on Xilinx Virtex-5 FPGA with similar placement. Experimental results report fault detection rate of 93.15% for the proposed sensor against 79.28% for the PLL based one. Similarly, the failure rate of the proposed sensor is as low as 0.0069, compared to 0.1127 failure rate of the PLL based counterpart. The results confirm that the presented sensor proposal can provide outstanding sensitivity against EMFI injections on security-critical ICs. Based on the adopted structure, the proposed sensor should also resist LFI as well as some global injection attacks.

Future work will center to developing the lightweight digital sensor against passive EM measurement for generic EM side-channel attacks.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[2] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in *CRYPTO '97*, ser. LNCS, 1997, vol. 1294, pp. 513–525.

[3] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em sidechannel (s)," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 29–45.

[4] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers." in *USENIX Security symposium*, 2010, pp. 307–322.

[5] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *Cryptographic Hardware and Embedded Systems–CHES 2012*. Springer, 2012, pp. 41–57.

[6] L. Zussa, J.-M. Dutertre, J. Clédiere, B. Robisson, A. Tria *et al.*, "Investigation of timing constraints violation as a fault injection means," in *27th Conference on Design of Circuits and Integrated Systems (DCIS), Avignon, France*, 2012.

[7] J. Balasch, B. Gierlichs, and I. Verbauwhede, "An in-depth and black-box characterization of the effects of clock glitches on 8-bit mcus," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*. IEEE, 2011, pp. 105–114.

[8] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Cryptographic Hardware and Embedded Systems-CHES 2002*. Springer, 2002, pp. 2–12.

[9] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *Constructive Side-Channel Analysis and Secure Design*. Springer, 2012, pp. 151–166.

[10] X. Guo, D. Mukhopadhyay, and R. Karri, "Provably secure concurrent error detection against differential fault analysis." *IACR Cryptology ePrint Archive*, vol. 2012, p. 552, 2012.

[11] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *Proceedings of the conference on Design, Automation & Test in Europe*, 2014, p. 203.

[12] N. Miura, Z. Najm, W. He, S. Bhasin, X.-T. Ngo, M. Nagata, and J.-L. Danger, "Pll to the rescue: A novel em fault countermeasure," in *To Appear in Proceedings of the 53rd ACM Design Automation Conference*, Austin, TX, USA, 2016.

[13] B. Datta and D. Kumar, "Analysis of a ring oscillator based on chip thermal sensor in 65nm technology," *retrieved from Internet: http//www. unix. ecs. umas. edu/-dkumar/lab4*, vol. 658, 2005.

[14] W. He, M. Stottinger, E. de la Torre, and V. Diaz, "A self-tuned thermal compensation system for reducing process variation influence in side-channel attack resistant dual-rail logic," in *Design of Circuits and Integrated Systems (DCIS), 2015 Conference on*. IEEE, 2015, pp. 1–6.

[15] C. R. Hogge Jr, "A self correcting clock recovery curcuit," *Lightwave Technology, Journal of*, vol. 3, no. 6, pp. 1312–1314, 1985.

[16] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*. Springer, 2007.

[17] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata, "Ring oscillator under laser: Potential of pll based countermeasure against laser fault injection," in *International Workshop on Fault Diagnosis and Tolerance in Cryptography 2016*. IEEE, Aug 2016, pp. 1–12.