CDS: An Anti-Aging Calibratable Digital Sensor for Detecting Multiple Types of Fault Injection Attacks

Zhiyuan Chen, Kun Yang* and Kui Ren
The State Key Laboratory of Blockchain and Data Security, Zhejiang University
School of Cyber Science and Technology, Zhejiang University
ZJU-Hangzhou Global Scientific and Technological Innovation Center

ABSTRACT

Fault injection attacks (FIAs) are a class of active physical attacks that inject faults into computing devices to deliberately change their intended behaviors for malicious purposes such as security feature circumvention, privilege escalation, secret data extraction by analyzing the erroneous outputs, etc. Existing sensors that detect fault injection attacks are either susceptible to aging or suffer from complicated and costly calibration process. Worse still, most sensors will fail in the presence of dynamic voltage and frequency scaling (DVFS) because they are built upon fixed delay chains and cannot adapt to operating voltage and frequency variations. In this paper, we overcome these limitations by presenting CDS, a delay chain based digital sensor that exploits timing variations of both detector and protected object for detecting multiple types of fault injection attacks. CDS utilizes a calibration module to solve the accuracy degradation caused by aging phenomena and a dynamic adjustment module to acclimatize itself to the need of dynamically adjusting voltage according to operating frequency in the presence of DVFS. To demonstrate its capability, we use CDS to protect the hardware accelerator of PRESENT cryptographic algorithm against voltage and laser glitching attacks. Simulation results based on HSPICE show that (i) CDS can detect 100% of voltage and temperature coordinated glitching attacks with 4.1% early warning; (ii) CDS can detect 100% of laser glitching attacks with 9.1% early warning; (iii) CDS maintains outstanding aging resistance with only 1.1% false alarm rate increase after 7 years of use.

1 INTRODUCTION

Fault injection attacks (FIAs) can bypass security mechanisms, alter register contents, and disrupt the normal operations of integrated circuits (ICs) by manipulating the voltage and clock inputs, injecting electromagnetic glitches, etc. to gain higher security privileges [17] or execute malicious codes [16, 19]. With the increased use of field programmable gate array (FPGA) cloud services, attackers begin attempting to conduct remote FIAs. The authors in [9] successfully hammered AES hardware accelerator deployed on FPGA in the cloud by exploiting power consuming circuitry that is connected to the FPGA's power distribution network (PDN). Subsequently, the authors in [11] presented a successful attack against a deep neural network (DNN) running on a cloud FPGA by utilizing power failure injection. FIAs have been proven to be feasible and pose a threat to the secure operations of computing devices [3, 8]. Therefore, there is an urgent need to develop countermeasures for combating FIAs.

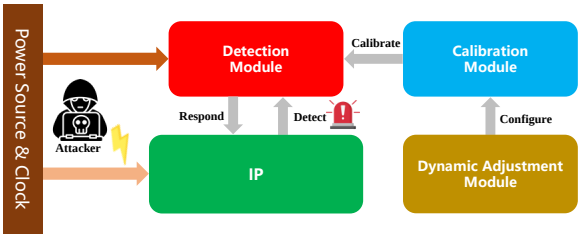

Figure 1: Our proposed counter strategy

There have been many studies proposing strategies to resist FIAs, which can be divided into two categories: (i) redundant computing based strategies and (ii) threshold detection based strategies. The strategies of adding redundancy are taking advantage of the strict requirements of FIAs towards injection timing and the difficulty of triggering multiple identical faults in different logic units or code segments. Redundant computing based countermeasures will either affect performance of computing devices or incur additional hardware overhead. Typical examples of threshold detection based countermeasures include digital [1, 5–7, 12, 14, 21, 22] or analog [4, 13, 15] sensors designed for anomaly detection. Digital sensors are usually designed for detecting abnormal behaviors with regards to circuitry timing given the fact that FIAs introduce faults to program execution mainly by creating timing violation in ICs [12, 20]. Analog sensors usually detect FIAs by directly checking the voltages of power rails, or capturing the voltage pulses induced by varying electromagnetic fields, and compare with the predefined thresholds. Analog sensors have poor portability and tend to consume more overhead in terms of area and power. Digital sensors are therefore becoming the primary choice in the fight against the FIAs.

However, there are many problems with existing digital sensors. Firstly, existing delay chain based digital sensors only use a single D flip-flop (DFF) to generate an alarm signal, which is susceptible to metastability due to setup time constraint. Secondly, digital sensors are prone to aging like analog sensors, which degrades detection accuracy. Lastly, most digital sensors are not designed to be adaptable to the presence of DVFS. To address these issues, we propose a FIA counter-strategy namely CDS as shown in Figure 1. CDS is designed to be an anti-aging digital sensor that can be automatically calibrated. The CDS detection module is designed based on a delay chain and uitilizes two complementary DFFs to generate an alarm

*Kun Yang is the Corresponding Author (Email: kuny@zju.edu.cn)

DAC '24, June 23–27, 2024, San Francisco, CA, USA

ACM ISBN 979-8-4007-0601-1/24/06
https://doi.org/10.1145/3649329.3657322

signal. CDS also includes a calibration module that mitigates aging effects and a dynamic adjustment module that acclimatizes CDS to varying operating voltages and frequecies in the presence of DVFS. The contributions of this paper are summarized as follows:

- To address the threat of fault injection faced by ICs, we propose CDS, an aging-resistant calibratable digital sensor to detect multiple types of FIAs (e.g., voltage glitching, laser glitching, etc.), and demonstrate its detection capability through simulation (100% detection coverage and 4.1% early warning).
- We study in detail the impact of aging phenomena on digital sensors and demonstrate the aging resistance of CDS detection module alone through simulation (only 1.93% false alarm rate after 7 years of use).
- To address the aging problem of digital sensors and to adapt to varying voltages and frequencies in the presence of DVFS, we design calibration module and dynamic adjustment module, which enable automated aging calibration as well as runtime configuration of the delay time of the delay chain. With calibration module and dynamic adjustment module introduced, the false alarm rate after 7 years of use is decreased from 1.93% to 1.1% (i.e., 43% improvement).

2 RELATED WORK

In recent years, there have been many studies proposing different kinds of sensors to detect FIAs, which can be mainly categorized into digital and analog sensors.

Digital Sensors: Digital sensors consist of two main types, delay based digital sensors [1, 6, 7, 12, 14, 21, 22] and impulse based digital sensors [5]. Delay based digital sensors need to design an delay chain. They usually use clock signal as the input to the delay chain and a DFF to capture timing variations caused by FIAs. Impulse based digital sensors are usually composed of several DFFs. Because studies have shown that DFFs are the most vulnerable units to attack and error. They are more like a trap circuit and have no direct timing relationship with the protected circuit. Therefore their detection accuracy is relatively low. Digital sensors usually face the aging problem. Even if the aging calibration function is considered in [2], the calibration cost is relatively high. Besides, most of the existing digital sensors does not take into account the DVFS requirements of the IC. So when the voltage and clock frequency are varying, the accuracy of these sensors will be reduced.

Analog Sensors: Analog sensors [4, 13, 15] usually directly detect certain information about the IC, such as temperature, voltage, etc, and then compare it to a predefined threshold. An analog sensor can only detect one physical quantity and therefore cannot detect multiple types of fault injection attacks at the same time. Analog sensors have to be altered to suit the different design environment and tend to take up more resources. Besides, analog sensors rely on costly calibration schemes, e.g., chip-by-chip laser trimming.

3 PRELIMINARIES

In this section, we will give a short overview of different types of FIAs and their working principles. The basic principles regarding IC aging will also be described.

3.1 Fault Injection Attacks

Typically, fault injection attacks can be categorized as non-intrusive fault attacks, semi-intrusive fault attacks and intrusive fault attacks.

Non-intrusive Fault Attacks: This type of attack does not require modification of the targeted device to induce a fault, making it highly probable that the victim will not recognize the attack. Additionally, these types of attacks do not require sophisticated equipment. Common methods include the use of electromagnetic pulses, positive or negative spikes in the power line, and adding additional clock edges.

Semi-intrusive Fault Attacks: To conduct a semi-intrusive fault injection, it is necessary to breach the attacked device. In optical fault attacks, this modification entails unpacking the chip to access the chip die without disrupting the passivation layer. Both laser and flash light can trigger a fault. Laser can precisely target specific memory or register bits, while flash lights cause global faults across larger regions of the chip.

Intrusive Fault Attacks: Penetration of the attacked device is required for this type of attack. After de-packaging, the passivation layer must be removed to access the metal layer using microprobes. This method enables targeting individual bus lines on the chip and modifying their values. Intrusive fault attacks necessitate the most advanced equipment, with the benefit of minimal limitations for fault injections.

3.2 Timing Constraints

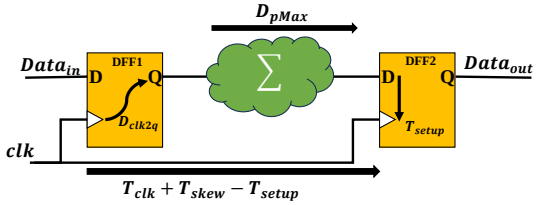

Figure 2: IC internal architecture

In ICs, clock signal is usually used to synchronize the overall operation. Figure 2 shows a brief architecture inside the IC. When the rising edge of the clock signal arrives, data is fed into the combinational logic (labeled $\sum$) from the upstream DFFs. After a series of logic operations, the results are latched to the downstream DFFs at the next rising edge. IC must satisfy timing constraints to work correctly. The exact writing of the timing constraint formula can be expressed as:

$$T_{clk} > D_{clk2q} + D_{pMax} + T_{setup} - T_{skew} \tag{1}$$

where T_{clk} and D_{pMax} are the clock period and the maximum data propagation time respectively, D_{clk2q} denotes the delay that elapses between the rising edge of the clock and the actual update of the DFF outputs, T_{skew} is the possible skew or small phase difference between the clock signals at the clock inputs of the two different DFFs, and T_{setup} indicates the setup time.

FIAs work by violating the timing constraints. One way to directly violate them is to overclock the circuit or inject a very short clock period, causing the circuit's clock period to decrease as formula (2). This will lead to DFF setup time violation or premature data latches. Another way to violate the timing constraints is to increase the processing time of the combinational logic to ensure

correct operation as formula (3). Injection voltage glitchings and electromagnetic pulses can all lead to increased processing times of combinational logic.

$$T_{clk_{dec}} < D_{clk2q} + D_{pMax} + T_{setup} - T_{skew} \quad (2)$$

$$T_{clk} < D_{clk2q} + D_{pMax_{inc}} + T_{setup} - T_{skew} \quad (3)$$

where $T_{clk_{dec}}$ denotes the shortened clock period, and $D_{pMax_{inc}}$ denotes the increased maximum propagation time due to the attack.

3.3 Integrated Circuits Aging

The two main factors of aging phenomenon in CMOS technology are negative bias temperature instability (NBTI) and hot carrier injection (HCI). They lead to increase in the delay of signal propagation in ICs.

NBTI Aging: Bias temperature instability (BTI) is a shift in threshold voltage with applied stress. For pMOS transistors, the threshold voltage corresponds to a negative gate bias. NBTI is a more serious concern than positive BTI. Transistors undergo two NBTI phases depending on their operating state. The stress phase happens when the transistor is on ($V_{gs} < V_{th}$). The threshold voltage of the transistor increases during this phase due to the $Si–SiO_2$ interface generating positive interface traps. The second recovery phase happens when the transistor is off ($V_{gs} > V_{th}$). The threshold voltage drift that occurs during the stress phase partially recovers in the recovery phase.

HCI Aging: HCI happens when carriers are injected into the gate dielectric during transistor switching, creating interface traps, oxide charges, and parasitic currents. HCI is linked to switching activity, leading to circuit degradation with shifting threshold voltage and drain current of stressed transistors. Typically, nMOS transistors face effects from HCI. The induced threshold voltage drift caused by HCI is sensitive to the number of gate input transitions of the transistor.

4 CDS SENSOR

The proposed CDS sensor is presented in this section. We first describe the overall architecture of CDS sensor, and then introduce the specific functionalities and design details of its building blocks.

4.1 Architecture Overview

Figure 3 shows the overall architecture of CDS sensor, which consists of three main functional modules: (i) **Detection Module**: the detection module of CDS sensor is built upon a delay chain and is capable of detecting multiple types of fault injection attacks by capturing the timing variation of the delay chain; (ii) **Calibration Module**: the calibration module of CDS sensor also includes a delay chain and enables automated aging calibration with accuracy of one basic delay unit; (iii) **Dynamic Adjustment Module**: the dynamic adjustment module works together with the calibration module to acclimatize CDS to the need of dynamically adjusting voltage according to operating frequency in the presence of DVFS.

4.2 Detection Module

As shown in the upper half of Figure 3, the detection module of CDS sensor mainly consists of an artificial delay chain, two DFFs, and an OR gate. The artificial delay chain includes a series of series-connected basic delay units. Each basic delay unit is composed of a buffer and a 2-to-1 multiplexer. The length of the delay chain is configured on the basis of the critical path of the protected IP. The length of the delay chain $delay$ is usually set to be slightly larger than the maximum data propagation time through the logic D_{pMax} so as to play an early warning role.

The detection principle of CDS is shown in Figure 4, where clk and D_{clk} indicate the clock signal and the clock signal after the delay chain respectively. When the computing device works normally, the delay of the delay chain is larger than the maximum data propagation time through the logic and smaller than the clock period , in which case CDS will not issue an alarm. FIA will normally increase $delay$ and D_{pMAX}. When the clock period is larger than the maximum data propagation time through the logic and smaller than the delay of the delay chain , the protected device will not generate an erroneous output and CDS will issue an early warning. When the maximum data propagation time through the logic is larger than the clock period and smaller than the delay of the delay chain , the protected device will work incorrectly and CDS will issue an alarm. CDS uses two DFFs to capture timing variation. In some previous work [7, 21], often only one DFF is used for capturing timing variation and the capturing DFF itself will also be affected by timing violation, which will result in detection blind zone of the sensor. CDS solves this problem by making two DFFs work complementarily for capturing timing variation, and finally generates an alarm signal via an OR gate if FIA happens.

4.3 Calibration Module

The calibration module, as shown in the lower left of Figure 3, consists of a frequency division DFF, a delay chain, and a series of calibration DFFs. Each calibration DFF is serving for a corresponding basic delay unit in the detection module. When CDS is not aging, the delay chain length of the calibration module and the delay chain length of the detection module add up to one clock cycle. When the detection accuracy of CDS decreases due to aging, the calibration signal is set to 1. The frequency division DFF will first halve the clock frequency.

The CDS calibration principle is illustrated in Figure 5, where clk^* indicates to the clock signal after frequency division, and $D_{clk_1^*}$ and $D_{clk_2^*}$ respectively refer to the data inputs of the i_{th} calibration DFF in case A and case B. In case A, $delay < T_{clk}$, the i_{th} calibration DFF will select the buffer of the i_{th} basic delay unit. In case B, $delay > T_{clk}$, the i_{th} calibration DFF will abandon the buffer of the i_{th} basic delay unit. When aging occurs, the delay time of the delay chain in the detection module will increase. To compensate for the aging effect, the calibration module will automatically abandon a certain number of basic delay units of the detection module's delay chain so that the delay time of the actual active delay chain in the detection module can maintain its initial value. An NMOS sleep transistor and a PMOS sleep transistor are respectively connected to the power terminal and the ground terminal of every component in the calibration module so that the calibration module can be disconnected from the power supply during hibernation to minimize the aging effect. The calibration signal and its complementary signal are respectively connected to the gate terminals of NMOS

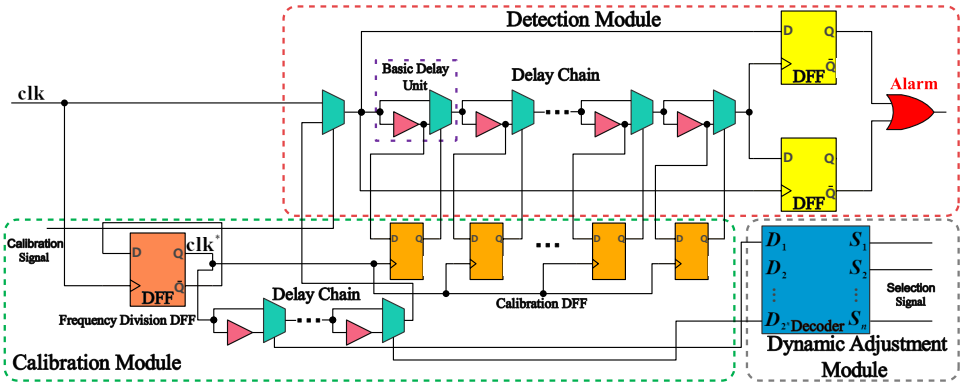

Figure 3: CDS architecture, including detection module, calibration module and dynamic adjustment module

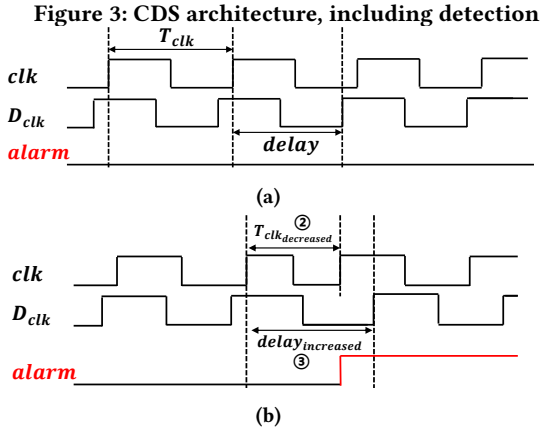

Figure 4: CDS detection principle : (a) normal operation (b) FIAs detection

sleep transistors and PMOS sleep transistors. When the calibration signal is set to 0, the calibration module goes to hibernate.

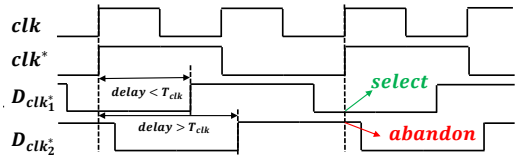

Figure 5: CDS calibration principle

4.4 Dynamic Adjustment Module

As shown in the lower right of Figure 3, the dynamic adjustment module in essence is a decoder, which allows for provisioning a set of selection signals so as to configure the length of the delay chain in the calibration module. The set of output signals of the decoder serve as the set of selection signals for the 2-to-1 multiplexers of the basic delay units in the calibration module, which enables the delay time adjustment of the calibration module's delay chain. After configuring the delay time of the delay chain in the calibration module, the calibration operation as described in Section 4.3 is subsequently performed to dynamically adjust the delay time of the delay chain in the detection module so as to acclimatize CDS to the need of dynamically adjusting voltage according to operating frequency in the presence of DVFS. Although some prior sensors [7] also allow for adjusting the delay time of delay chain, they do not support aging calibration and will fail in the presence of DVFS since they can no longer accurately determine the delay time of the basic delay unit after aging and thus cannot reconfigure the delay time of the delay chain as needed. The dynamic adjustment module also connects to sleep transistors in order to minimize aging effects.

5 EVALUATION AND SIMULATION RESULTS

In this section, we present the simulation setup and evaluation results regarding detection capability, aging resistance, and calibration effect. Afterwards, we compare CDS with prior work in terms of overhead. Lastly, we perform the attack analysis.

5.1 Simulation Setup

To evaluate the ability of CDS to detect FIA, we choose the PRESENT algorithm's substitution box (S-Box) as the protected object. CDS and the target S-Box are implemented in the transistor level using 45 nm NANGATE technology in HSPICE and simulated for voltage and temperature coordinated glitching attacks and laser glitching attacks [6]. The detailed simulation parameter settings are shown in Table 1. In order to test the effects of aging on the CDS, we use the HSPICE built-in MOSRA Level 3 model to assess the effect of NBTI and HCI aging, up to 7 years of operation in steps of four months.

Table 1: Simulation parameter settings

Parameter	Section 5.2	Section 5.3
Clock Cycle	0.25 ns	5 ns
Temperature*	$-10 - 150\,^{\circ}C$	$-10 - 150\,^{\circ}C$
Voltage*	$0.8 - 1.2\,V$	$1.0 - 1.4\,V$
Voltage Glitching Cycle*	0.25 ns	5 ns
Working Environment Point$^{\triangle}$	$(1\,V, 50\,^{\circ}C)$	$(1.2\,V, 55\,^{\circ}C)$
PGN Resistance$^{\triangle}$	$1 - 100\,\Omega$	$1 - 100\,\Omega$
PGN Capacitance$^{\triangle}$	$100 - 1000\,fF$	$100 - 1000\,fF$
Laser Glitching Cycle$^{\triangle}$	0.5 ns	60 ns
PGN Induced Current$^{\triangle}$	1 mA	1 mA

* voltage and temperature coordinated glitching attack
$^{\triangle}$ laser glitching attack

5.2 Detection Capability Evaluation

The FIA detection capability of CDS is illustrated in Figure 6. First, we performed two types of FIAs on the target at the same time (i.e., temperature and voltage fault injection). From Figure 6a, the erroneous operation of the S-Box increases with rising temperature and decreasing value of voltage glitching. The S-Box has completely failed to operate properly when the value of voltage glitching is 0.8 V. The simulation results show that the CDS can detect 100% FIAs when the S-Box generates an error output. CDS gives an early warning (33 of 805 attacks) because *delay* of the detection module is slightly longer than D_{pMax}. Figure 6b demonstrates CDS's detection capability of laser fault injection.When $R_{PGN} \geq 40\Omega$, the S-Box works incorrectly, while the CDS can detect 100% of the attacks. When $R_{PGN} = 30\Omega$, the S-Box operating normally and the CDS will issue an early warning signal. It is important to note that CDS does not issue alarm signals when FIAs are not performed. Therefore, according to the simulation results, CDS has great FIA detection accuracy and have a certain degree of early warning function.

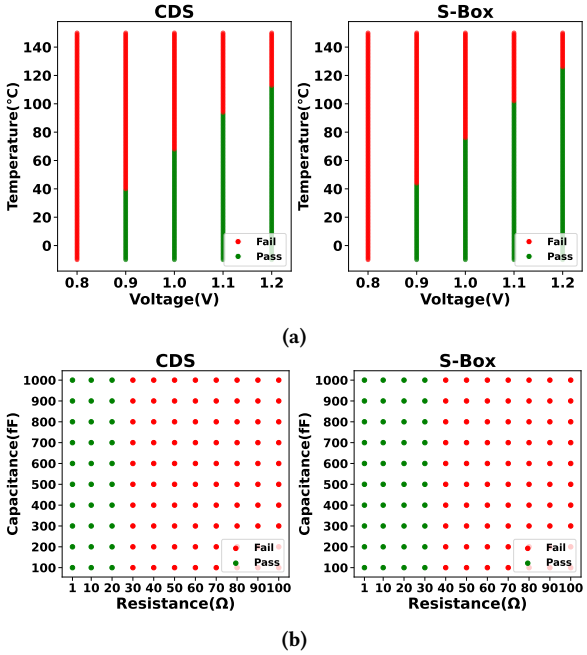

Figure 6: CDS detection capability evaluation: (a) voltage and temperature injection attack detection (b) laser injection attack detection

5.3 Aging Resistence Evaluation

According to [10, 18], the effects of NBTI and HCI on the circuit are mainly related to voltage and temperature. As shown in Figure 7, the delay time of the delay chain increases with time of use. It is about 15 ps after one year of use and about 45 ps after seven years. However, the effect of different operating voltages on the delay time is not as large as expected. Since the detection principle of CDS is by detecting the variations of delay time, the aging phenomena will have some influence on the detection accuracy of CDS. Figure 8 illustrates the degradation in CDS's accuracy for voltage and temperature coordinated glitching attack detection after 7 years of use. The increase in delay time of the delay chain due to aging is superimposed on the increase in delay time due to FIAs. So CDS generates alarm signals in situations where it otherwise would not. However CDS false alram rate is only 0.83% after one year of use and 1.93% after seven years of use. As a comparison, we

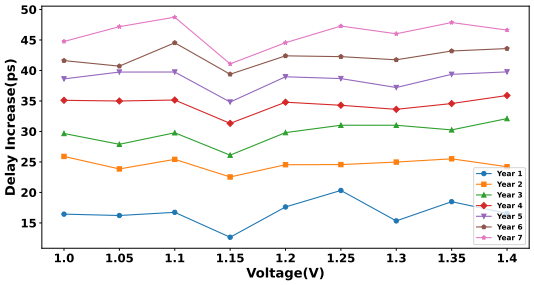

Figure 7: Increased delay of the delay chain

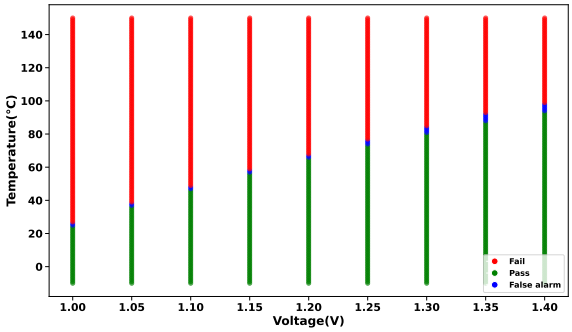

Figure 8: CDS detection capability after 7 years of use

studied the state-of-the-art digital sensor [1] subjected to the aging phenomenon. Since its detection principle is based on detecting changes in environmental parameters, we used the value of the limiting environmental parameter variations as its point of false alarm. The experimental results, as shown in Table 2, show that CDS clearly has better anti-aging properties.

Table 2: Error rate comparison

Time (years)	1	2	3	4	5	6	7
CDS (%)	0.83	1.10	1.17	1.52	1.59	1.79	1.93
[1] (%)	1.17	2.69	4.07	5.66	6.97	7.87	9.67

5.4 Calibration Effect Evaluation

Although our proposed sensors have good aging resistance, we still propose a CDS calibration module to further minimize the effect of aging phenomenon. And the calibration module also serves the dynamic regulation module to meet the DVFS requirement of the IC. The increase in delay due to aging is not significant when the usage time is short, so we choose to calibrate the sensor from the 60th month. The experimental results in Table 3 show that the false alarm rate of the calibrated sensor decreases to a certain extent, and the decrease is more obvious with the increase of the usage time.

Table 3: Error rate comparison between pre-calibrated CDS and post-calibrated CDS

Time (months)	60	64	68	72	76	80	84
Before (%)	1.59	1.66	1.73	1.79	1.79	1.79	1.93
After (%)	1.38	1.31	1.24	1.24	1.17	1.10	1.10

5.5 Overhead Comparison

Table 4 compares CDS with prior work [1, 6, 22] in terms of consumed equivalent gate counts. According to our design, the sum of the delay time of delay chain in the CDS detection module and the delay time of delay chain in the CDS calibration module is always equal to one clock cycle. Therefore, as shown in Table 4, the actual active equivalent gate counts consumed by the CDS detection module as well as the CDS sensor will vary with the clock frequency. When the normal operating frequency of protected computing device is high, the area overhead of CDS sensor is much smaller than prior sensors. The advantage in terms of area overhead will be much more significant if we only count the equivalent gate count consumed by the detection module given most prior sensors do not provide aging calibration or dynamic adjustment functionality.

Table 4: Overhead comparison

Sensor	$CDS_{0.25ns}$	CDS_{5ns}	[1]	[6]	[22]
Equivalent gate count	95 (47*)	505 (197*)	384	292	184

count*: equivalent gate count consumed by the CDS detection module

5.6 Attack Analysis

Many studies [13, 22] have shown that almost all FIAs make the target device malfunction by causing timing violations. The CDS proposed in this paper is a digital sensor based on timing variations detection and can defend against most of the FIAs. CDS cannot defend against one type of attacks that directly tamper with the OR gate which generates the alarm signal, which will be addressed in our future work. However, since CDS only occupies a very small area, attackers would have to use very sophisticated equipment and a significant amount of time to reverse engineer the IC layout and further determine the specific location of the OR gate.

6 CONCLUSION AND FUTURE WORK

In this work, we proposed CDS, a calibratable and dynamically adjustable digital sensor that detects multiply types of fault injection attacks including laser and voltage glitching. Compared with most existing FIA detectors that only exploit timing variation of detectors themselves, CDS has better aging resistance because of the following two merits: (i) CDS makes decisions based on timing variation of both detector and protected object; (ii) calibration module and dynamic adjustment module of CDS will only work during calibration phase and will hibernate during detection phase by being disconnected from power using sleep transistors. Furthermore, CDS can automatically calibrate and dynamically adjust itself to adapt to varing operating voltages and frequencies in the presence of DVFS. Simulation results based on HSPICE has demonstrated its detection capability, self-calibration and self-adjusting abilities, and aging resistance. In future work, we plan to tape out a security chip with CDS integrated and test it in a laboratory environment.

ACKNOWLEDGMENTS

This work was supported in part by the National Key Research and Development Program of China (Grant No. 2023YFB3105900), the National Natural Science Foundation of China (Grant No. 62372407) and the Fundamental Research Funds for the Central Universities (Grant No. 226-2023-00030).

REFERENCES

[1] Anik Md Toufiq Hasan et al. 2020. Detecting Failures and Attacks via Digital Sensors. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40, 7 (2020), 1315–1326.
[2] Anik Md Toufiq Hasan et al. 2021. Reducing Aging Impacts in Digital Sensors via Run-Time Calibration. *Journal of Electronic Testing* 37, 5-6 (2021), 653–673.
[3] Breier Jakub et al. 2022. How Practical Are Fault Injection Attacks, Really? *IEEE Access* 10 (2022), 113122–113130.
[4] Bastos R Possamai et al. 2013. A Bulk Built-In Sensor for Detection of Fault Attacks. In *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 51–54.
[5] El-Baze David et al. 2016. A Fully-Digital EM Pulse Detector. In *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 439–444.
[6] Ebrahimabadi Mohammad et al. 2022. Detecting Laser Fault Injection Attacks via Time-to-Digital Converter Sensors. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 97–100.
[7] Endo Sho et al. 2012. An Efficient Countermeasure Against Fault Sensitivity Analysis Using Configurable Delay Blocks. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 95–102.
[8] Gangolli Aakash et al. 2022. A Systematic Review of Fault Injection Attacks on IoT Systems. *Electronics* 11, 13 (2022), 2023.
[9] Krautter Jonas et al. 2018. FPGAhammer: Remote Voltage Fault Attacks on Shared FPGAs, Suitable for DFA on AES. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018), 44–68.
[10] Lahbib Insaf et al. 2015. Hot Carrier Injection Effect on Threshold Voltage of NMOSFETs. In *2015 11th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*. IEEE, 164–167.
[11] Luo Yukui et al. 2021. DeepStrike: Remotely-Guided Fault Injection Attacks on DNN Accelerator in Cloud-FPGA. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*. IEEE, 295–300.
[12] Muttaki Md Rafid et al. 2022. FTC: A Universal Sensor for Fault Injection Attack Detection. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 117–120.
[13] Miura Noriyuki et al. 2016. PLL to the Rescue: A Novel EM Fault Countermeasure. In *Proceedings of the 53rd Annual Design Automation Conference*. 1–6.
[14] Pundir Nitin et al. 2022. Security Properties Driven Pre-Silicon Laser Fault Injection Assessment. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 9–12.
[15] Sim Jae-Yoon et al. 2003. A 1.8-V 128-Mb Mobile DRAM with Double Boosting Pump, Hybrid Current Sense Amplifier, and Dual-Referenced Adjustment Scheme for Temperature Sensor. *IEEE Journal of Solid-State Circuits* 38, 4 (2003), 631–640.
[16] Timmers Niek et al. 2016. Controlling PC on ARM Using Fault Injection. In *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 25–35.
[17] Timmers Niek et al. 2017. Escalating Privileges in Linux Using Voltage Fault Injection. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 1–8.
[18] Wang Wenping et al. 2009. The Impact of NBTI Effect on Combinational Circuit: Modeling, Simulation, and Analysis. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 18, 2 (2009), 173–183.
[19] Zhang Fan et al. 2022. DARPT: Defense Against Remote Physical Attack Based on TDC in Multi-Tenant Scenario. In *Proceedings of the 59th ACM/IEEE Design Automation Conference*. 559–564.
[20] Zussa Loic et al. 2013. Power Supply Glitch Induced Faults on FPGA: An In-Depth Analysis of the Injection Mechanism. In *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*. IEEE, 110–115.
[21] Zussa Loic et al. 2014. Efficiency of a Glitch Detector Against Electromagnetic Fault Injection. In *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 1–6.
[22] Zhang Maoshen et al. 2021. A Digital and Lightweight Delay-Based Detector Against Fault Injection Attacks. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 1–5.