Summary of Maryam Thesis

Abstract

This thesis investigates a novel type of FIA called POTA, which targets embedded systems when they are powered off. By exploiting heating (via laser or environmental temperature manipulation), attackers can alter the characteristics of security sensors or detectors, rendering them less effective when the system is powered back on. The research evaluates the robustness of delay-based digital detectors and ROs implemented on Xilinx Artix-7 FPGAs under various power states (power-off, power-on, and inactive modes like clock-freezing) and temperature conditions. The findings reveal that heating during power-off or inactive modes degrades detector accuracy, increasing the risk of undetected attacks due to false negatives.

Related Work

Digital and Analog Fault Injection Attacks Detectors

There are several methods to counter FIAs. The first would be Redundancy-based methods, that detect faults by comparing redundant computations but fail to catch all fault types, especially localized attacks. The second would be sensor-based detectors, that are categorized into analog (time-to-digital converters) and digital. Analog detectors are sensitive but harder to calibrate, while digital detectors are widely adopted due to lower complexity and power use. Delay-based detectors monitor timing constraints (clock vs. propagation delays) to detect attacks like clock glitching or overheating. However, they struggle with localized attacks (such as laser/EM faults) and cannot detect clock period reductions. Detectors based on ROs use inverter chains to generate frequency signals. By counting oscillations during clock phases, they detect deviations caused by FIAs. These detectors outperform delay-based ones by identifying both clock increases and decreases but are more complex to implement. Studies show detectors can be bypassed (via glitching attacks), highlighting vulnerabilities dependent on internal parameters and attack techniques.

Aging effects

There are four main aging effects that degrade transistor performance over time, and impact detector reliability.

- BTIs, which increase transistor threshold voltage during electrical stress, with partial recovery when stress stops.
- HCIs, which damage transistor gates, worsening in smaller, high-voltage transistors.
- TDDB, which increase electrical leakage and dielectric defects.
- EM, which weaken interconnects, leading to opening of electrical interruptions.

This thesis links aging to temperature attacks (such as laser fault injection), using controlled heating to emulate both attack-induced heating and accelerated aging. This approach evaluates how power-off temperature attacks (POTAs) compromise detectors by altering their characteristics when inactive.

Methodology

This thesis evaluates two DUTs :

1. Delay-based detectors, which compare a delayed clock signal with the original clock to detect timing violations. If the buffer chain delay exceeds the clock period, an alarm triggers.
2. Ring Oscillators (ROs), which are a closed loop of inverters generates a frequency sensitive to environmental changes (temperature for example).

Three temperature conditions were tested, constant (chips heated continuously at 95°C), temperature cycling (daily heating/cooling cycles), and room temperature.

Three power conditions were combined with temperature scenarios, Power-off (no power supplied), Power-on (normal operation), Clock-freezing (Power-on but clock signal halted).

The attacker model assumes physical access to the system, with heating applied during power-off or inactive states to induce permanent detector degradation.

Experimental Results

Delay-Based Detectors

Under normal operation, heating (constant or cyclic) caused a 1.98% degradation in alarm activation thresholds during temperature cycling. This means detec-

tors required slightly longer delays to trigger alarms, increasing false negatives. Heating during power-off led to small but measurable degradation (0.31-0.36%). Though subtle, this could accumulate over repeated attacks. The most significant degradation occurred here (2.53%), as transistors remained in a static state, accelerating BTI effects. Temperature cycling worsened this effect compared to constant heating.

Ring Oscillators (ROs)

Higher-frequency ROs (around 60 MHz) degraded more (2.03%) than lower-frequency ones (4 MHz at 0.26%) under clock-freezing and temperature cycling. Heating altered propagation delays in inverters, directly impacting oscillation frequency. A 70°C internal temperature rise caused 7.98% frequency degradation in high-frequency ROs, highlighting their sensitivity to thermal stress.

General conclusion

Clock-freezing had the most severe impact due to BTI aging, as transistors held in a static state (no switching) experienced prolonged electrical stress, worsening threshold voltage shifts. Furthermore, temperature cycling caused more degradation than constant heating, likely due to thermal expansion/contraction stressing materials. FInally, POTA showed measurable effects, proving that detectors are vulnerable even when inactive.

Discussion

The results confirm that POTA is a credible threat. Heating during power-off or inactive states permanently alters detector thresholds and RO frequencies, reducing their accuracy. For example, a detector calibrated to trigger at a 17.2 MHz clock glitch might fail to activate after POTA, allowing undetected attacks. Even small threshold shifts (here, 0.3%) could allow attackers to bypass detection by staying just below the degraded threshold. Heating mimics long-term aging effects (here, BTI) in a short time, demonstrating how attackers could "age" detectors intentionally to weaken them. ROs and detectors operating at higher frequencies are more sensitive to thermal stress, making them priority targets.

Conclusion

This thesis demonstrates that POTAs can compromise embedded system security by degrading detector performance. When systems are powered off or inactive, heating

induces permanent changes in timing thresholds and RO frequencies, leading to increased false negatives. Clock-freezing scenarios, where inactive detectors are simulated, showed the most severe degradation due to BTI aging. Moreover, temperature cycling proved more harmful than constant heating.

Some futures directions would include testing localized heating (laser attacks) to mimic real-world POTA scenarios, developing self-testing mechanisms to detect detector degradation after power cycles, and evaluating countermeasures like redundancy or adaptive threshold calibration to mitigate POTA risks.

Glossary

BTI = Bias Temperature Instability

HCI = Hot Carrier Injection

EM = Electromigration

TDDB = Time-Dependent Dielectric Breakdown

FIA = Fault Injection Attacks

POTA = Power-Off Temperature Attacks

DUT = Devices Under Test

RO = Ring Oscillators