Summary of Aghiles Thesis

Abstract

While software security has historically been the primary focus, hardware-level threats such as laser attacks, electromagnetic interference, X-rays, and thermal attacks underscore the need to secure electronic systems at the physical layer. PUFs are introduced as a promising solution for generating unique, secure identifiers by leveraging inherent manufacturing variations. PUFs are difficult to clone and are widely used for cryptographic key generation and device authentication, as they dynamically generate keys instead of storing them, reducing the risk of key extraction.

However, PUFs are sensitive to environmental factors like temperature and voltage fluctuations, which can compromise their reliability and the principle of "non-clonability." Thermal attacks, in particular, can be localized (targeting specific components like ring oscillators) or non-localized (affecting the entire circuit), with localized attacks offering more precise manipulation of PUF responses.

This thesis focuses on analyzing the effects of global and localized thermal attacks on RO-PUFs implemented in two semiconductor technologies: Bulk-65nm and FDSOI-28nm. These technologies were chosen due to their industry relevance and distinct characteristics. The study examines two attack scenarios:

- Uniform thermal attacks affecting all oscillators to assess the impact of homogeneous temperature increases.
- Localized thermal attacks targeting specific oscillators to analyze temperature-induced variations in PUF responses.

Simulations are conducted using Virtuoso and the Monte Carlo method to account for process variability. Unlike previous research, which focused on long-term thermal effects to induce aging, this study investigates real-time thermal attacks during PUF operation, assuming attackers can disable temperature sensors. The results reveal vulnerabilities to both global and localized thermal attacks, demonstrating how attackers can manipulate PUF responses. These findings pave the way for developing effective countermeasures to enhance PUF resilience under thermal stress.

Background

PUFs are hardware security primitives that leverage manufacturing variations to create unique, unclonable identifiers. PUFs, such as RO-PUFs, are widely used

due to their simplicity, generating CRPs by comparing frequencies of selected ROs. Key evaluation metrics include reliability, uniqueness, and uniformity, with the latter emphasized as it reflects the balance of '0's and '1's in responses and is critical for detecting thermal attack impacts.

PUFs are vulnerable to thermal and voltage variations, which attackers exploit to manipulate responses. For example, FPGA-based RO-PUFs can be compromised by overheating static transistors via malicious bitstreams, accelerating aging (e.g., NBTI/PBTI effects) to alter frequencies and CRP outcomes. While countermeasures like ARO-PUFs mitigate natural aging (e.g., stabilizing voltages during "freeze" mode to reduce NBTI in pMOS transistors), they are ineffective against intentional, real-time thermal attacks targeting both pMOS and nMOS degradation.

This highlights the need to analyze thermal attack resilience in two semiconductor technologies (Bulk-65nm and FDSOI-28nm), as existing solutions are insufficient against deliberate, high-temperature manipulation.

Threat model

For evaluating the impact of thermal attacks on RO-PUFs, we are going to compare two threat models.

Scenario A : Uniform Thermal Attack

- Objective: Analyze the effects of a uniform temperature increase across all ROs in the PUF.
- Relevance: Simulates conditions where the entire device is uniformly heated, potentially disrupting all ROs.
- Method: Digital simulations using SPICE for thermal modeling and Monte Carlo simulations to account for process variability.
- Advantage: Avoids the complexity and cost of physical experiments while providing detailed insights into PUF reliability under uniform thermal stress.

Scenario B : Localized Thermal Attack

- Objective: Study the impact of localized heating (e.g., via a laser beam) on specific ROs and its propagation to adjacent areas.
- Relevance: Explores how uneven thermal conditions can create vulnerabilities not evident under uniform heating.

- Method: SPICE simulations for detailed thermal modeling and Monte Carlo simulations to include process variations.
- Advantage: Enables testing of localized attack scenarios without the need for expensive physical setups, providing a deep understanding of thermal propagation effects.

Choice of the technology

Choosing the right technology is crucial in developing electronic circuits, especially to ensure reliability and security against thermal attacks.

Bulk-65nm

Advantages:

- Cost-Performance Efficiency: Balances cost and performance, ideal for diverse applications.
- Technological Maturity: Well-established processes reduce manufacturing risks and enhance reliability.
- Availability: Widely used in the industry, with readily available components and design tools.

Use Case: Suitable for applications requiring cost-effectiveness and proven reliability.

FSDOI-28nm

Advantages:

- Thermal Resilience: Performs better under thermal stress due to reduced leakage and improved electrostatic control.
- Energy Efficiency: Supports lower operating voltages and dynamic threshold control, enabling energy savings.
- High Performance: Offers higher speeds and superior performance metrics compared to traditional technologies.

Use Case: Ideal for high-speed, low-power applications requiring thermal resilience.

Thermal attack on Bulk-65nm

Transistor Level

Bulk transistors exhibit temperature-dependent behavior, with current and mobility decreasing at high temperatures due to increased lattice vibrations.

This impacts RO frequency, as higher temperatures reduce switching speed, leading to lower frequencies. A temperature threshold of 300°C is chosen to avoid circuit damage while achieving significant thermal effects.

Uniform Thermal Attack

Simulations show that increasing temperature narrows the frequency distribution of ROs, causing frequencies to converge.

At 300°C, 4% of PUF response bits flip, indicating vulnerability to uniform thermal stress. This level of bit flips can be corrected using ECC, but it highlights the need for robustness against thermal variations.

Localized Thermal Attack

Localized attacks exploit temperature gradients (ΔT) between ROs, with optimal attack temperatures between 50°C and 80°C.

A temperature difference of 30°C (e.g., 80°C vs. 50°C) biases PUF responses, with an 80% chance of flipping bits when frequencies differ by 3.5%.

This significantly reduces uniformity (distribution of '0's and '1's), making PUF responses predictable and compromising security.

Conclusion

Bulk-65nm RO-PUFs are vulnerable to both uniform and localized thermal attacks. While uniform attacks cause manageable bit flips, localized attacks can control PUF outputs by exploiting temperature differences.

This emphasize the need for countermeasures to protect PUFs from thermal manipulation, ensuring their reliability and security in real-world applications.

Thermal attack on FDSOI-28nm

Transistor level

At high temperatures, FDSOI transistors experience reduced current and mobility, leading to lower RO frequencies. This behavior is consistent across different RO sizes.

Uniform Thermal Attack

Simulations show that increasing temperature narrows the frequency distribution, causing frequencies to converge.

At 300°C, 14% of PUF response bits flip, indicating significant vulnerability to uniform thermal stress. This exceeds the correction capacity of ECC, posing a serious reliability issue.

Localized Thermal Attack

Localized attacks exploit temperature gradients (ΔT) between ROs, with the steepest frequency slope observed at 300°C.

A temperature difference of 30°C (e.g., 300°C vs. 270°C) biases PUF responses, with a 68% chance of flipping bits when frequencies differ by 0.8%.

This reduces uniformity from 50% to 32%, making PUF responses predictable and compromising security.

Conclusion

FDSOI-28nm RO-PUFs are highly vulnerable to both uniform and localized thermal attacks. Uniform attacks cause significant bit flips, while localized attacks can control PUF outputs by exploiting temperature differences.

This highlights the need for countermeasures to enhance PUF resilience against thermal manipulation, ensuring reliability and security in real-world applications.

FDSOI-28nm VS Bulk-65nm?

Uniform Thermal Attack

Both technologies show a decrease in RO frequency and a narrowing of frequency distributions at 300°C.

FDSOI-28nm exhibits less pronounced frequency shifts and standard deviation reduction compared to Bulk-65nm, suggesting greater thermal stability.

However, FDSOI-28nm experiences 14% bit flips at 300°C, significantly higher than Bulk-65nm's 4%, making FDSOI-28nm more vulnerable to uniform thermal attacks.

Localized Thermal Attack

Optimal attack temperatures differ: 50-80°C for Bulk-65nm and 270-300°C for FDSOI-28nm.

Bulk-65nm shows a faster and more pronounced bias in PUF responses (increase in '0's) with temperature differences (ΔT), while FDSOI-28nm is less sensitive to localized attacks.

Bulk-65nm is more vulnerable to localized attacks, whereas FDSOI-28nm demonstrates slightly better resilience in this scenario.

Conclusion

Bulk-65nm is highly sensitive to localized thermal attacks but more robust against uniform thermal attacks.

FDSOI-28nm is vulnerable to both uniform and localized attacks, with uniform attacks causing significant bit flips (14%) and localized attacks showing moderate bias.

This emphasizes the need for technology-specific countermeasures to enhance PUF resilience against thermal manipulation.

General Conclusion

Let's summarize this study's findings on the effects of thermal attacks on RO-PUFs implemented in Bulk-65nm and FDSOI-28nm technologies. Two attack scenarios

were analyzed: uniform thermal attacks (affecting the entire chip) and localized thermal attacks (targeting specific ROs). For Bulk-65nm, the Uniform Thermal Attack caused only 4% bit flips, posing minimal threat, while the Localized Thermal Attack brought up high vulnerability, with an 80% bias in PUF outputs when temperature differences (ΔT) are exploited.

Regarding FDSOI-28nm, the Uniform Thermal Attack had a significant impact, with 14% bit flips, exceeding the correction capacity of error-correcting codes (ECC), while the Localized Thermal Attack had moderate imapct, with a 68% bias in PUF outputs at a (ΔT) of 30°C.

FDSOI is more susceptible to uniform thermal attacks, while Bulk is more vulnerable to localized thermal attacks.

In the end, both technologies exhibit critical vulnerabilities, highlighting the need for robust countermeasures to protect PUFs from thermal manipulation in environments where such attacks are a threat.

This study underscores the importance of addressing thermal attack vulnerabilities in PUF designs to ensure their reliability and security in real-world applications.

Glossary

PUFs = Physically Unclonable Functions

RO-PUFs = Ring Oscillator-based PUFs

ARO-PUFs = Aging-Resistant RO-PUFs

FDSOI = Fully Depleted Silicon on Insulator

CRP = Challenge-Response Pairs

NBTI = Negative-bias temperature instability

PBTI = Positive-bias temperature instability

SPICE = Simulation Program with Integrated Circuit Emphasis

ECC = Error-Correcting Codes

ΔT = Temperature differences