Summary of Aghiles Thesis - RO-PUFs

Abstract

PUFs have emerged as a cost-effective solution to establish a root of trust for electronic devices by leveraging intrinsic process variability. They generate unique identification signatures and cryptographic keys on demand, eliminating the need to store sensitive information in vulnerable memory.

Despite their advantages, PUFs are susceptible to environmental factors, particularly temperature, which can accelerate aging effects like BTI and HCI. This paper investigates the impact of externally induced heat on RO-PUFs, which rely on frequency comparisons of identically designed ROs.

The study also explores the feasibility of temperature-based attacks, such as localized heating via short circuits or laser injection, to manipulate PUF responses. Through Monte Carlo simulations on 65nm technology, the analysis reveals the significant influence of temperature on RO-PUF reliability. The findings contribute to understanding temperature vulnerabilities in PUFs and highlight the need for robust countermeasures.

Introduction

Device security is critical in modern electronics, especially as devices handle sensitive tasks like banking transactions and personal data storage. Despite advancements in hardware and software security, attackers continue to develop methods to bypass even the most secure systems.

PUFs have gained attention as a hardware-based security primitive that generates unique keys on demand by exploiting fabrication process variability, making them resistant to cloning. Among the various PUF designs, RO-PUFs are widely studied. These PUFs compare the frequencies of identically designed ROs, which are influenced by process variability, aging, and environmental conditions.

However, RO-PUFs are vulnerable to temperature variations, which can accelerate aging effects like BTI and HCI, altering transistor performance and enabling attacks. Recent research has demonstrated how localized heating, induced by techniques such as short circuits, can manipulate RO-PUFs and even clone them. This paper examines the effects of temperature on RO-PUFs, explores temperature-based attacks, and discusses broader challenges in hardware security. The study aims to improve understanding of temperature vulnerabilities in PUFs and proposes future research directions, including fault injection in power-off circuits.

Reliability and temperature effects on PUF

PUFs are designed for security applications, requiring consistent responses over time. However, high temperatures can significantly affect the behavior of ROs, leading to reliability and security issues.

Physical Unclonable Function

PUFs are evaluated using key metrics:

1. Uniqueness: Measures the ability to distinguish devices based on Hamming distance between responses.

$$\text{Uniqueness} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(P_i, P_j)}{n} \times 100\%$$

where k = number of PUFs

n = number of bits in each PUF response

P_i and P_j = the responses of the i-th or j-th PUF

$HD(P_i, P_j)$ = the Hamming Distance between these responses

2. Reliability: Assesses the consistency of PUF responses over time and under varying conditions.

$$\text{Reliability} = (1 - \frac{1}{x} \sum_{y=1}^{x} \frac{HD(R_i, R_{i,y})}{n}) \times 100\%$$

where x = number of samples taken from PUF responses

R_i = response extracted from the i-th board

n = number of response bits generated by the PUF

$HD(R_i, R_{i,y})$ = Hamming Distance between the response R_i and the y-th sampling

$R_{i,y}$ = the y-th sample of R_i

3. Uniformity: Evaluates the distribution of '0's and '1's in PUF responses, aiming for a balanced 50% distribution.

$$\text{Uniformity} = \frac{1}{n} \sum_{l=1}^{n} R_{i,l} \times 100\%$$

where $R_{i,l}$ is the l-th binary bit of an n-bit response from a chip i

4. Bit-aliasing: Identifies systematic biases in PUF responses on a per-challenge basis.

$$\text{Bit-aliasing} = \frac{1}{k} \sum_{l=1}^{k} R_{l,i} \times 100\%$$

where k = number of PUFs

l = index of the bit in the PUF identifier

$R_{l,i}$ = value of the l-th bit in the response of the i-th PUF

There are several types of PUFs, such as RO-PUFs, which generate keys by comparing the frequencies of identically designed ROs. These PUFs are sensitive to environmental factors like temperature, which can alter RO frequencies and compromise reliability.

Temperature effect on RO-based PUF reliability

Higher temperatures cause ROs to become unstable, increasing the likelihood of bit flips in PUF outputs, which compromises reliability.

Simulations on a 65nm technology RO with 5 inverters, conducted at temperatures of 27°C, 57°C, 107°C, and 207°C, reveal that frequency distributions narrow as temperature rises. This narrowing increases the risk of ROs having similar frequencies, leading to output flips and reduced reliability. The standard deviation of frequency distributions decreases with higher temperatures, indicating less variability and tighter clustering around the mean.

Experiments with a 25-inverter RO confirm that temperature similarly affects ROs regardless of the number of inverters. A normalized comparison of ROs with 5, 13, 25, and 49 inverters further demonstrates that temperature uniformly impacts the reliability of all RO architectures. These findings highlight the vulnerability of RO-PUFs to temperature variations, emphasizing the need for robust design strategies to mitigate these effects.

Temperature attacks on RO-PUF

By targeting specific ROs, an attacker can temporarily alter their frequencies, leading to changes in PUF outputs.

Experiments reveal that the oscillation frequency of ROs decreases with rising temperature, regardless of the number of inverters (5, 13, 25, or 49). The frequency drop is sharp up to 150°C, followed by stabilization or slight further decrease up to 250°C. This behavior is consistent across all RO configurations, making temperature a viable attack vector.

The frequency of ROs depends on parameters like threshold voltage and carrier mobility, both of which are temperature-sensitive. As temperature increases, the threshold voltages of NMOS and PMOS transistors decrease due to shifts in Fermi level and band gap energy. However, simulations show that the frequency

decrease cannot be solely attributed to threshold voltage changes. Instead, carrier mobility plays a dominant role, as higher temperatures increase carrier collisions, reducing mobility and drain current.

Controlled and localised aging

Aging effects, such as BTI and HCI, degrade circuit performance over time, increasing threshold voltages, reducing current, and raising leakage currents. These effects are typically gradual but can be accelerated by factors like high temperatures and power supply voltages.

While temperature sensors in modern chips can detect and mitigate high-temperature attacks, a new threat emerges: modifying circuit characteristics while the device is powered off. This approach could enable undetected fault injection into PUFs, bypassing traditional countermeasures. Future research will focus on exploring the feasibility of such attacks on powered-off circuits, which could pose significant challenges to electronic security.

Conclusions

ROs, critical to many electronic systems, are vulnerable to temperature-induced fault injection attacks, which can disrupt their operation and compromise security. While current countermeasures, such as hardware and software redundancy, can detect and mitigate these attacks when circuits are powered on, emerging threats target powered-off circuits. Future research will investigate the potential for fault injection in powered-off circuits, a challenging area that could redefine the security landscape for electronic systems.

Glossary

PUF = Physical Unclonable Functions

BTI = Bias Temperature Instability

HCI = Hot Carrier Injection

RO-PUF = Ring Oscillator-based Physical Unclonable Functions