# Enhanced Processor Defence Against Physical and Software Threats by Securing DIFT Against Fault Injection Attacks

PhD Dissertation Defense

**William PENSEC**

Université Bretagne Sud, UMR 6285, Lab-STICC, Lorient, France

December 19, 2024

# Outline

1. Introduction
   - Context
   - Motivations
   - Information Flow Tracking
   - Physical Attacks
   - Objectives
2. D-RI5CY – Vulnerability Assessment
3. Proposed protections against FIAs
4. Experimental results
5. Conclusion and Perspectives
   - Conclusion
   - Perspectives

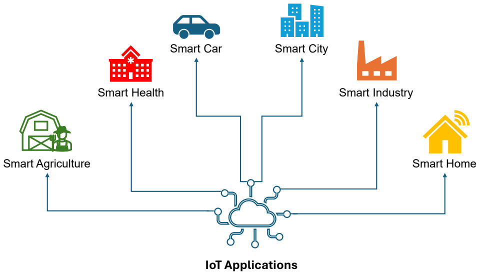
# Outline

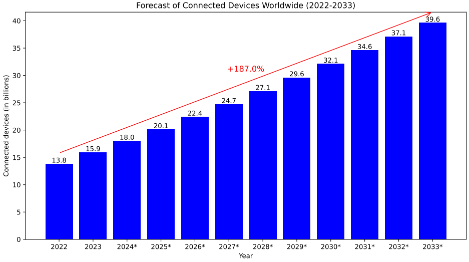
1. Introduction
   - Context
   - Motivations
   - Information Flow Tracking
   - Physical Attacks
   - Objectives
2. D-RI5CY – Vulnerability Assessment
3. Proposed protections against FIAs
4. Experimental results
5. Conclusion and Perspectives

# Context: Embedded Systems and IoT

## Internet of Things (IoT)

- Wide range of application
- Fast growing market with rapid expansion of use
- Rely on sensors depending on their usage
- Collect and share data
- Manipulation of critical data
- Increasingly vulnerable to multiple threats





* Years marked are forecasted values

# Motivations: IoT Under Threats

## Threats

- Software threats: malwares, memory overflow attacks, SQL injection, etc
- Network threats: DDoS, man-in-the-middle, jamming, etc
- Hardware threats: physical attacks such as reverse engineering, Side-Channel Attacks (SCA), Fault Injection Attacks (FIA)

## Vulnerabilities on critical systems

-

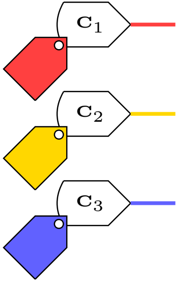
# Information Flow Tracking

- Protection against software attacks (e.g.: *buffer overflow*, *format string*, *SQL injections*, . . . ) [1, 2]

# Dynamic Information Flow Tracking

**Three** steps

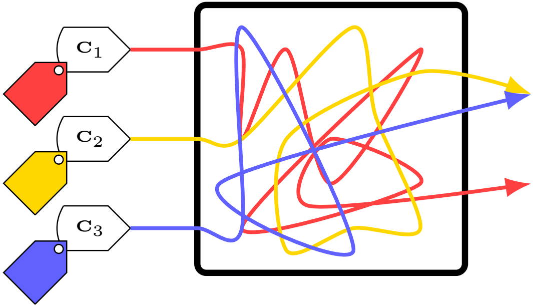
- Tag initialisation



# Dynamic Information Flow Tracking

**Three steps**

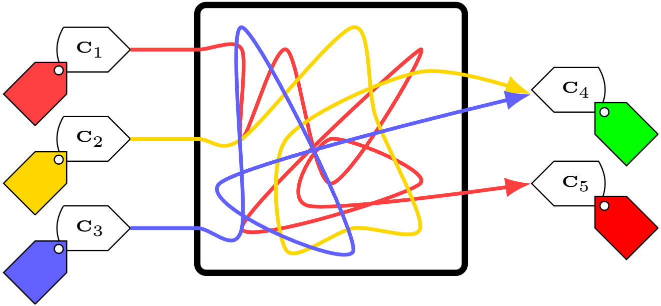
- Tag initialisation
- Tag propagation



# Dynamic Information Flow Tracking

## Three steps

- Tag initialisation
- Tag propagation
- Tag check



# Physical Attacks

-

# Objectives of this PhD Thesis

## Contributions

- Provide a robust security mechanism against software and hardware threats.
- Taking into account Fault Injection Attacks
- Propose lightweight countermeasures against FIA
- Take into account constraints, such as area and performance overhead

# Outline

1. Introduction
2. D-RI5CY – Vulnerability Assessment
3. Proposed protections against FIAs
4. Experimental results
5. Conclusion and Perspectives

# D-RI5CY

# Vulnerability Assessment

# Outline

1. Introduction
2. D-RI5CY – Vulnerability Assessment
3. Proposed protections against FIAs
4. Experimental results
5. Conclusion and Perspectives

# Introduction

# Parity codes

# Simple Parity

# Hamming Code

# SECDED

# Outline

1. Introduction
2. D-RI5CY – Vulnerability Assessment
3. Proposed protections against FIAs
4. Experimental results
5. Conclusion and Perspectives

# Experimental setup

# Outline

1 Introduction

2 D-RI5CY – Vulnerability Assessment

3 Proposed protections against FIAs

4 Experimental results

5 Conclusion and Perspectives
- Conclusion
- Perspectives

# Conclusion

# Perspectives

# Publications

# Publications

# Enhanced Processor Defence Against Physical and Software Threats by Securing DIFT Against Fault Injection Attacks

PhD Dissertation Defense

**William PENSEC**

Thank you for your attention.

# References

# References

[1] Christopher Brant et al. “Challenges and Opportunities for Practical and Effective Dynamic Information Flow Tracking”. In: *ACM Computing Surveys* 55.1 (Nov. 2021). ISSN: 0360-0300. DOI: 10.1145/3483790.

[2] Wei Hu, Armaiti Ardeshiricham, and Ryan Kastner. “Hardware Information Flow Tracking”. In: *ACM Computing Surveys* (2021). DOI: 10.1145/3447867.