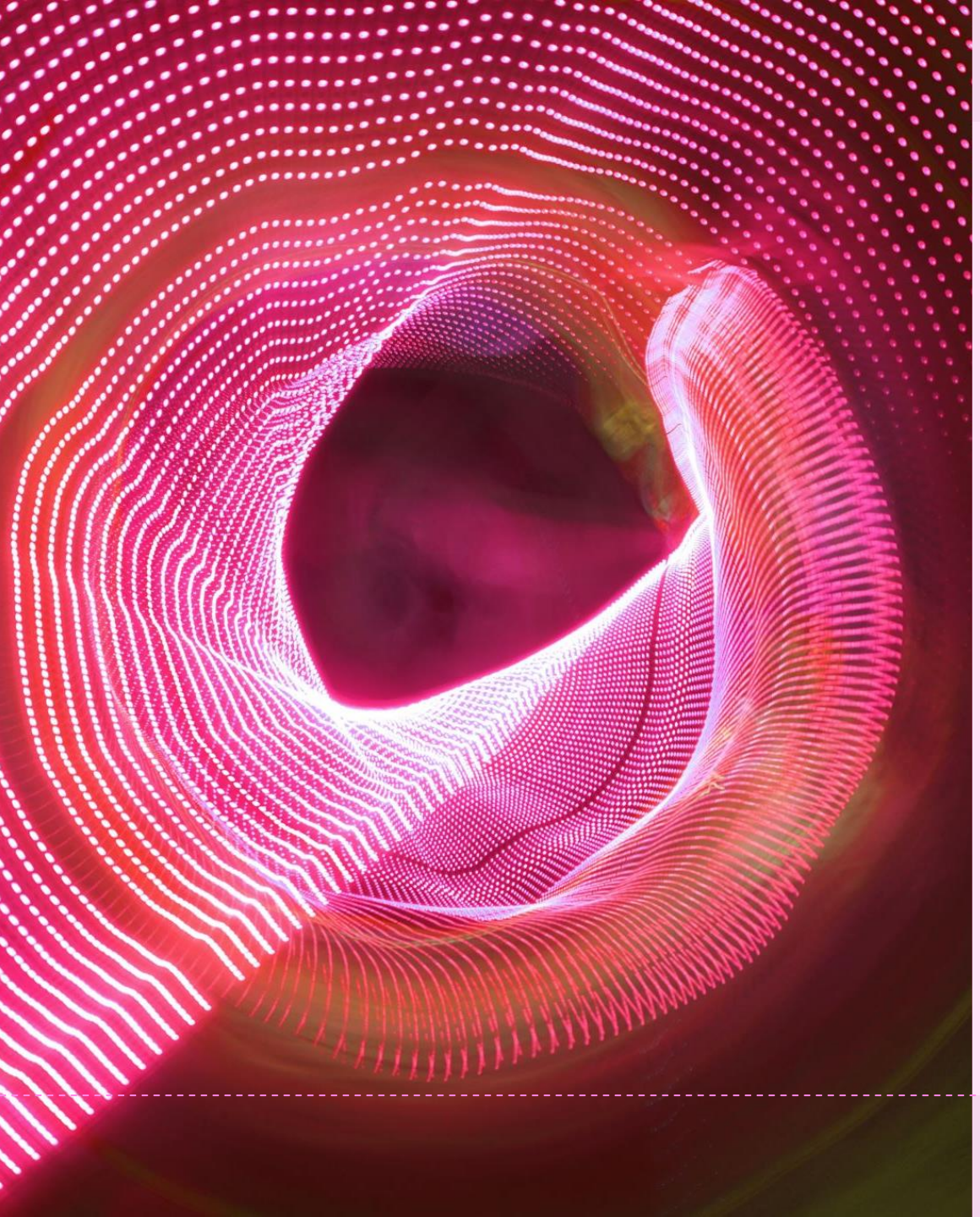
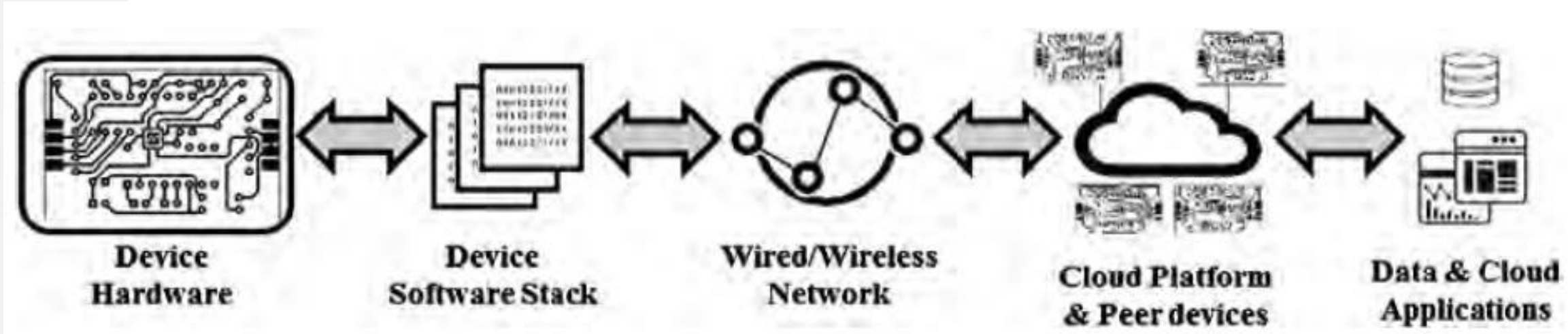


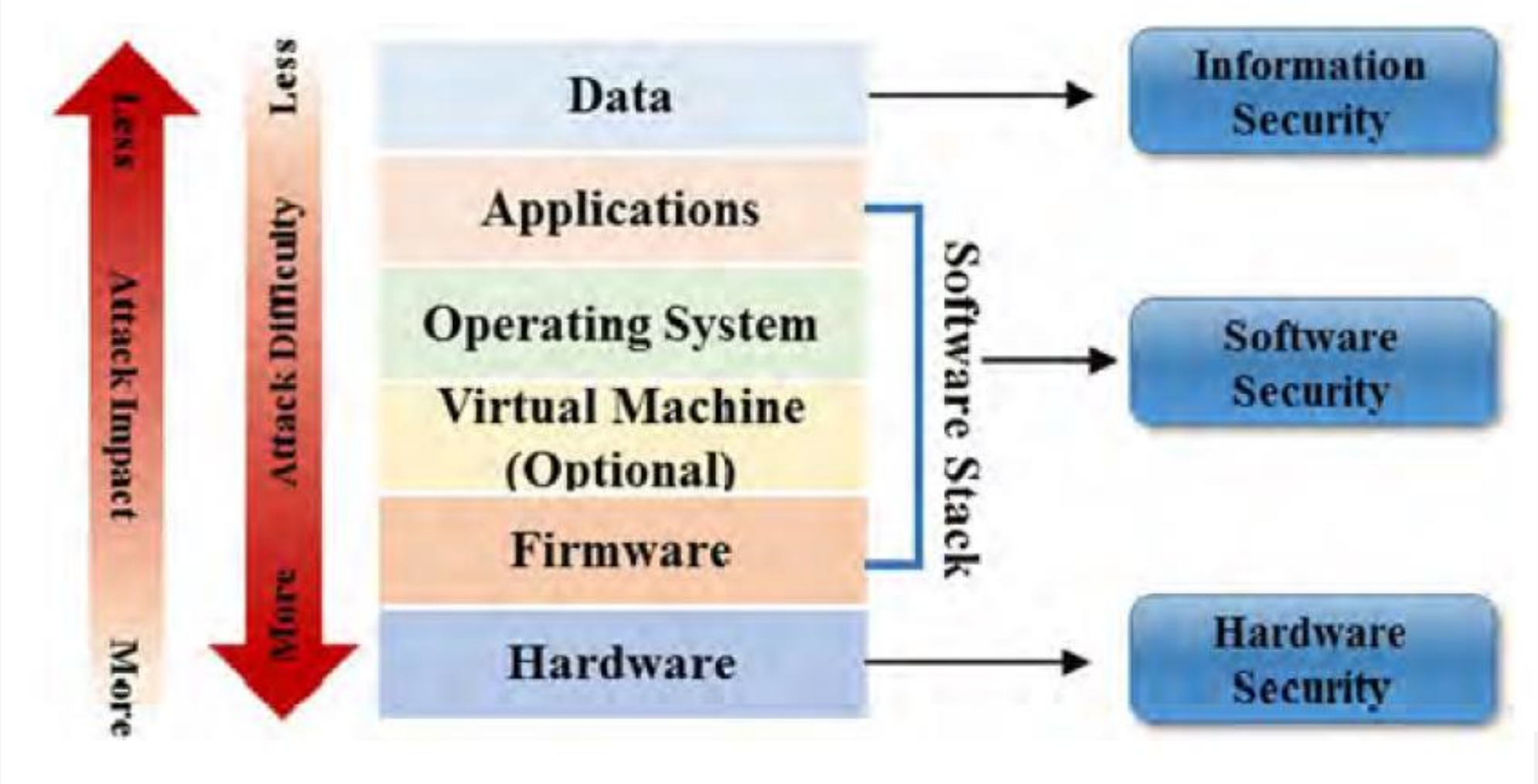
# Segurança em Hardware

Prof Maurício Acconcia Dias

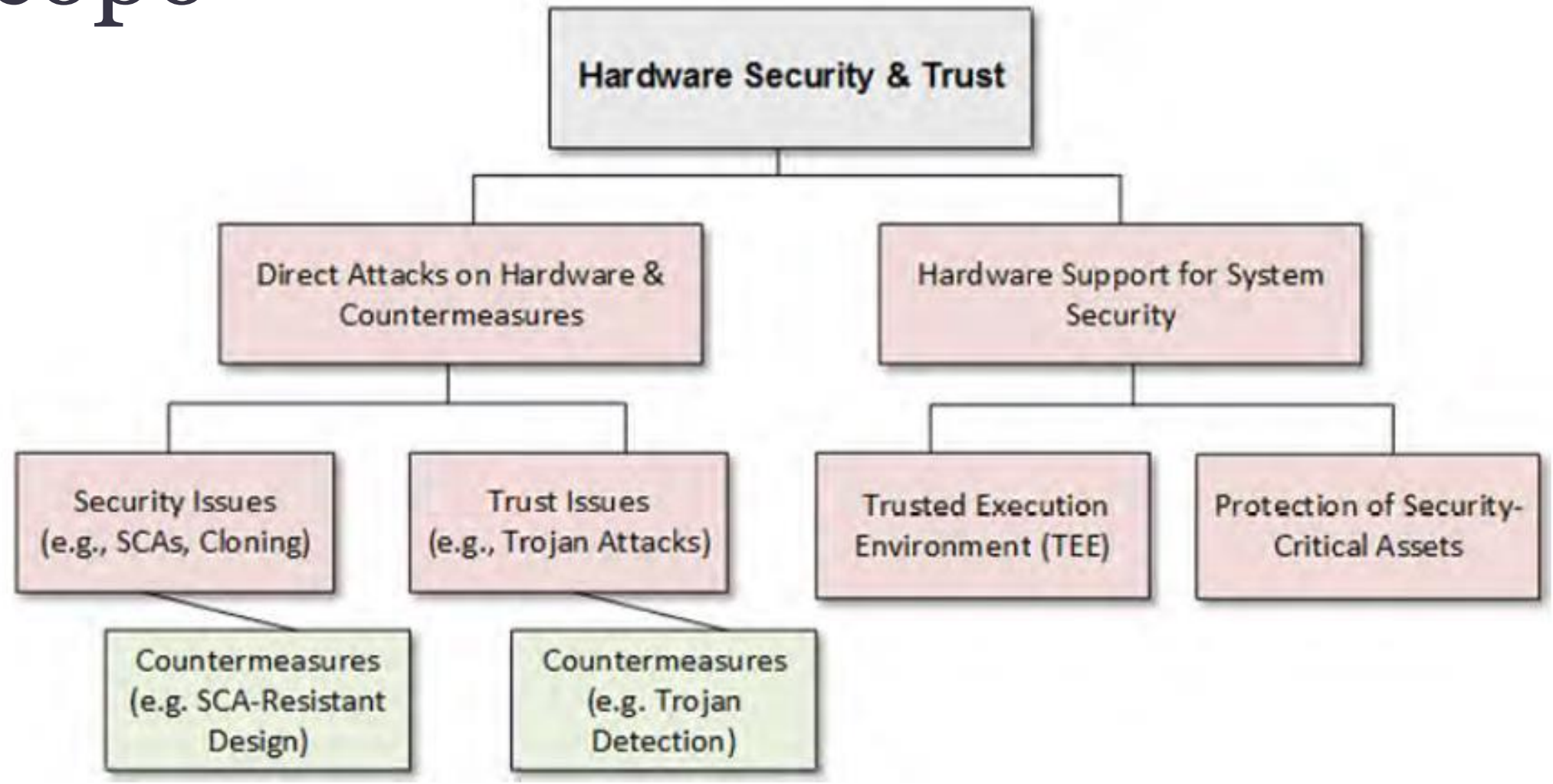
# Dispositivo de computação



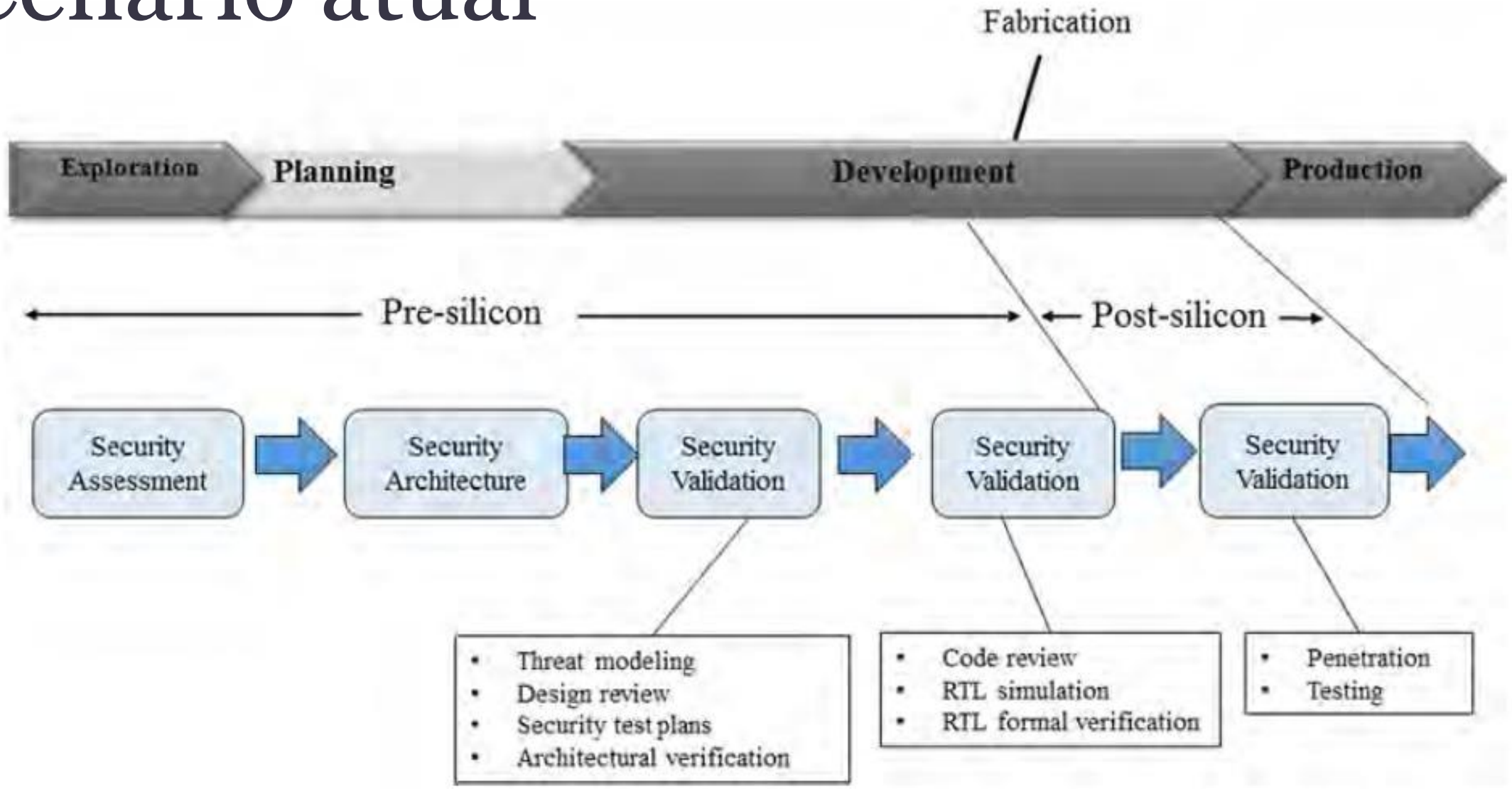
# Perfil do ataque



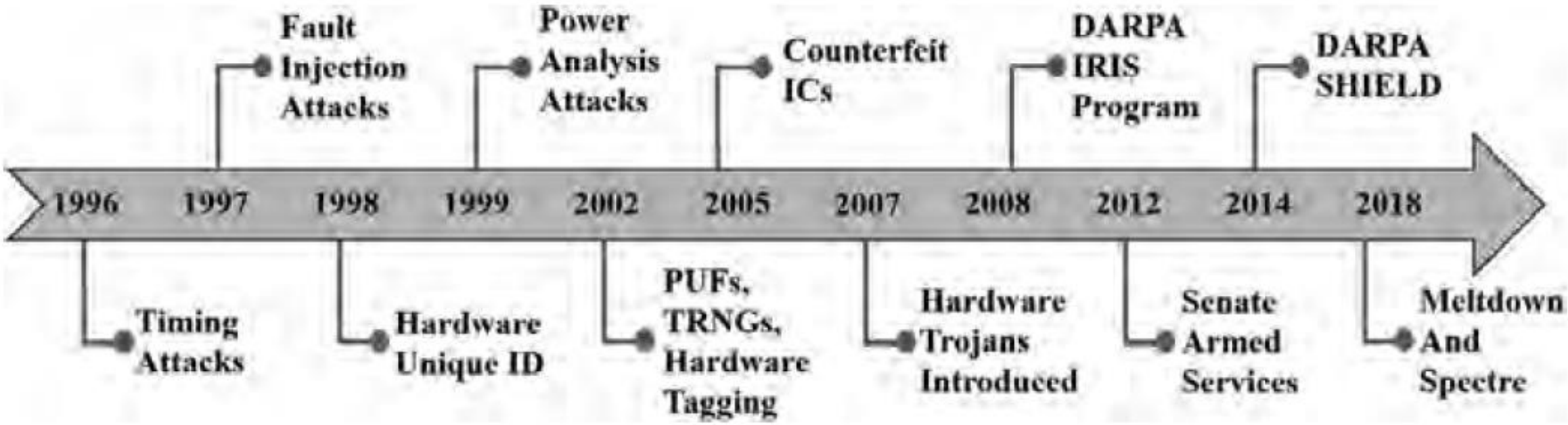
# Escopo


Hardware Security & Trust
Direct Attacks on Hardware & Countermeasures
Hardware Support for System Security
Security Issues (e.g., SCAs, Cloning)
Trust Issues (e.g., Trojan Attacks)
Trusted Execution Environment (TEE)
Protection of Security-Critical Assets
Countermeasures (e.g. SCA-Resistant Design)
Countermeasures (e.g. Trojan Detection)

# Cenário atual



# Histórico

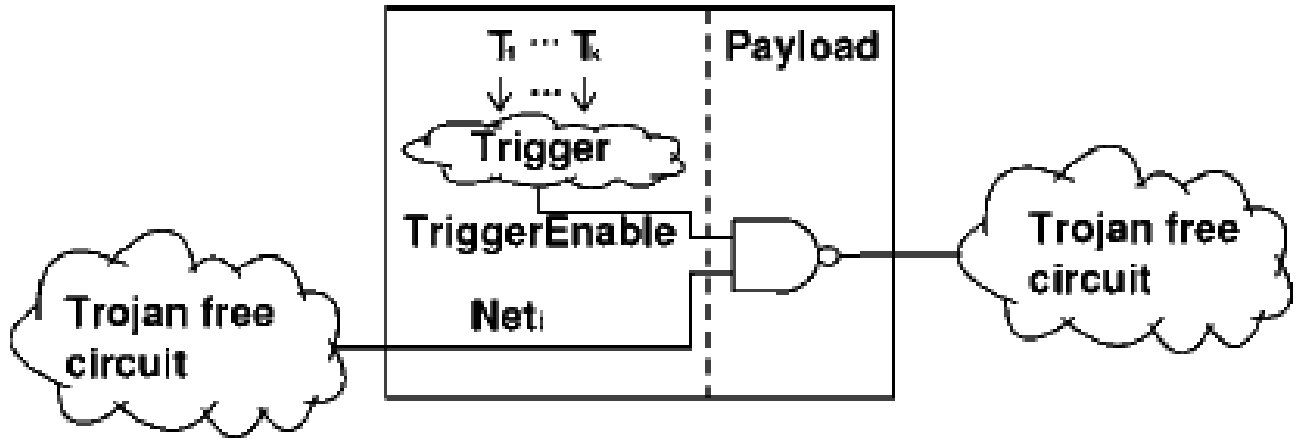

1996
1997
1998
1999
2002
2005
2007
2008
2012
2014
2018
Timing Attacks
Fault Injection Attacks
Hardware Unique ID
Power Analysis Attacks
PUFs, TRNGs, Hardware Tagging
Counterfeit ICs
Hardware Trojans Introduced
DARPA IRIS Program
Senate Armed Services
DARPA SHIELD
Meltdown And Spectre

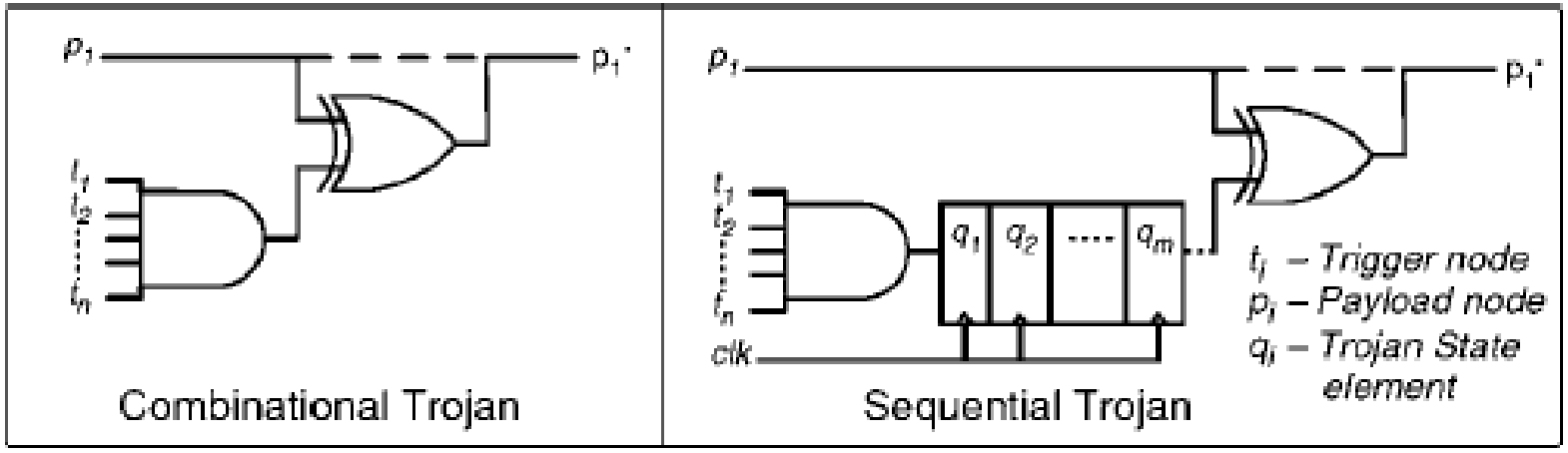
# DARPA Shield

- Supply Chain Hardware Integrity for Electronics Defense (SHIELD)

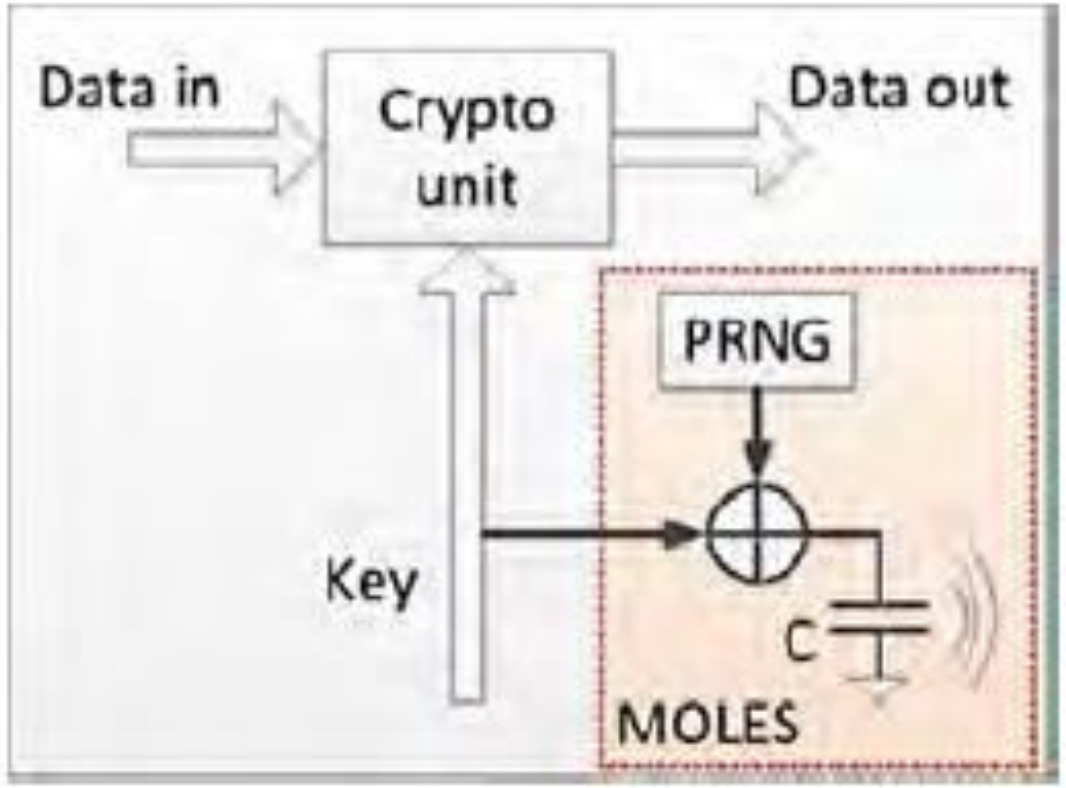
- The goal of DARPA's SHIELD program is to eliminate counterfeit integrated circuits from the electronics supply chain by making counterfeiting too complex and time-consuming to be cost effective.

# Hardware Trojans

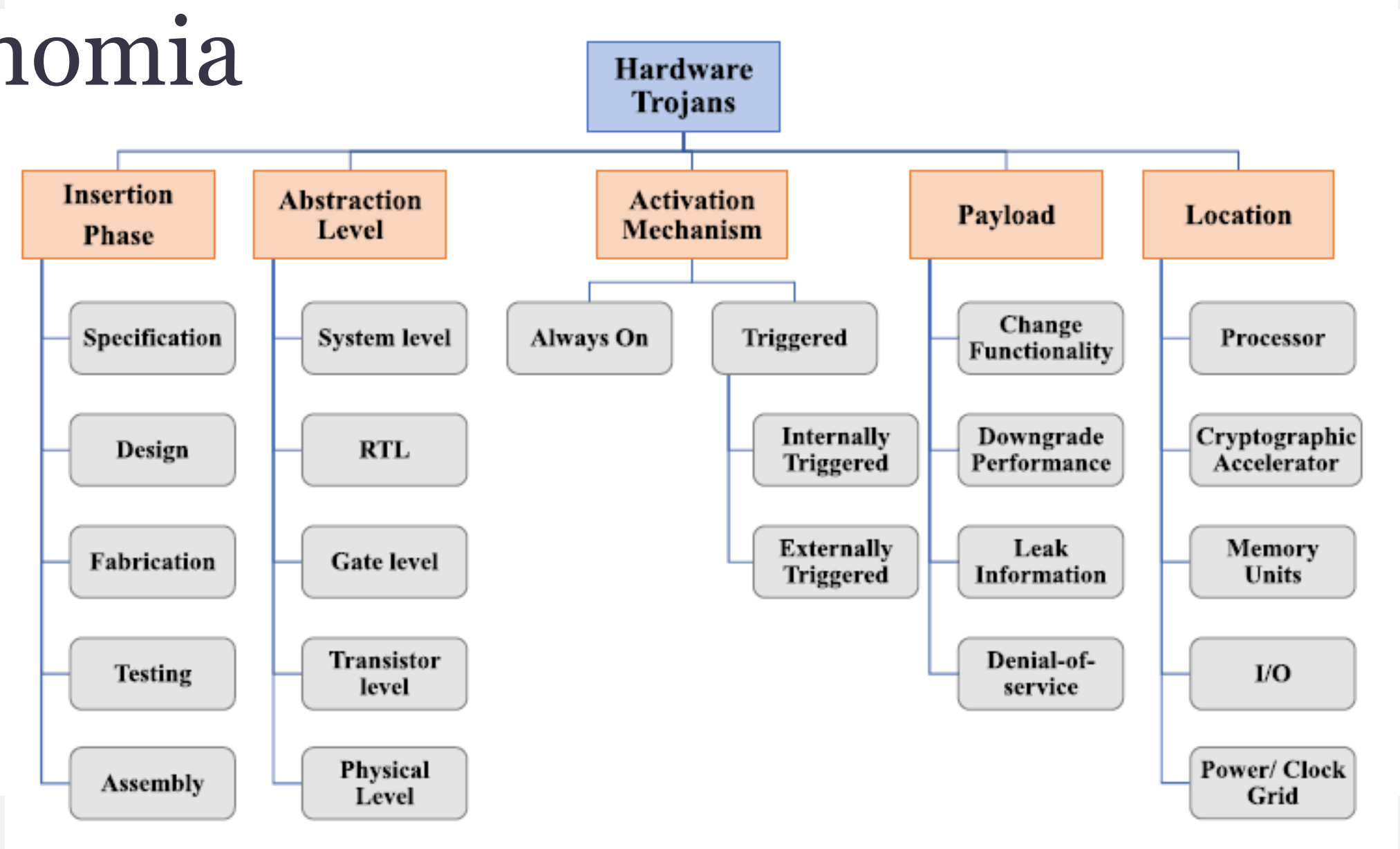


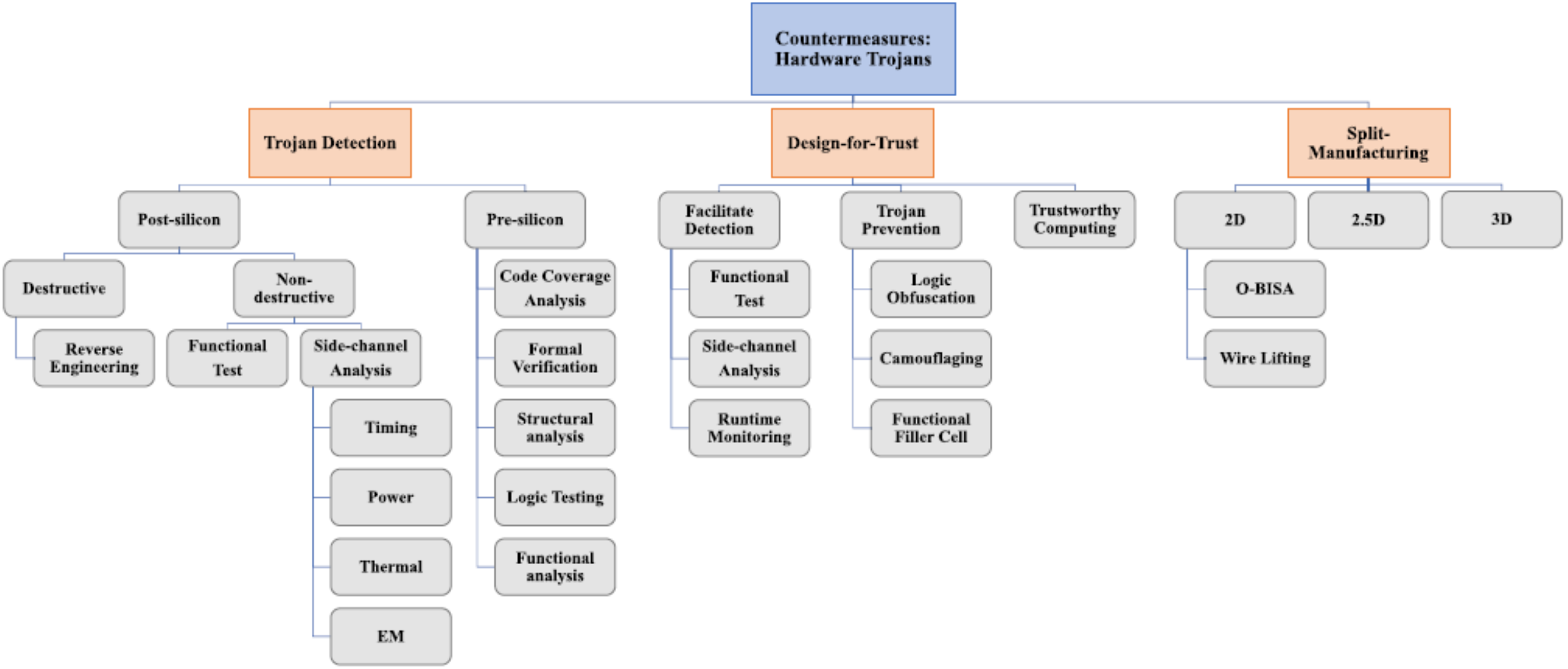
# Sistemas de Criptografia



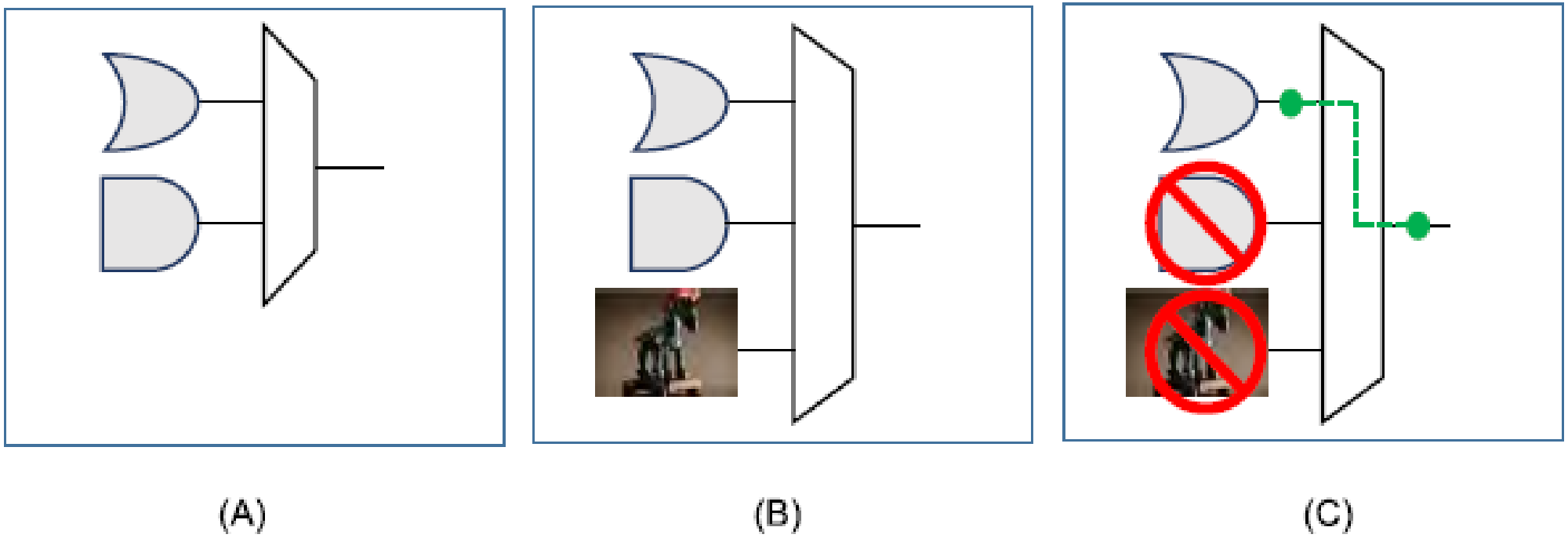
# Taxnomia


Hardware Trojans
Insertion Phase
Specification
Design
Fabrication
Testing
Assembly
Abstraction Level
System level
RTL
Gate level
Transistor level
Physical Level
Activation Mechanism
Always On
Triggered
Internally Triggered
Externally Triggered
Payload
Change Functionality
Downgrade Performance
Leak Information
Denial-of-service
Location
Processor
Cryptographic Accelerator
Memory Units
I/O
Power/ Clock Grid

# Contramedidas para trojans

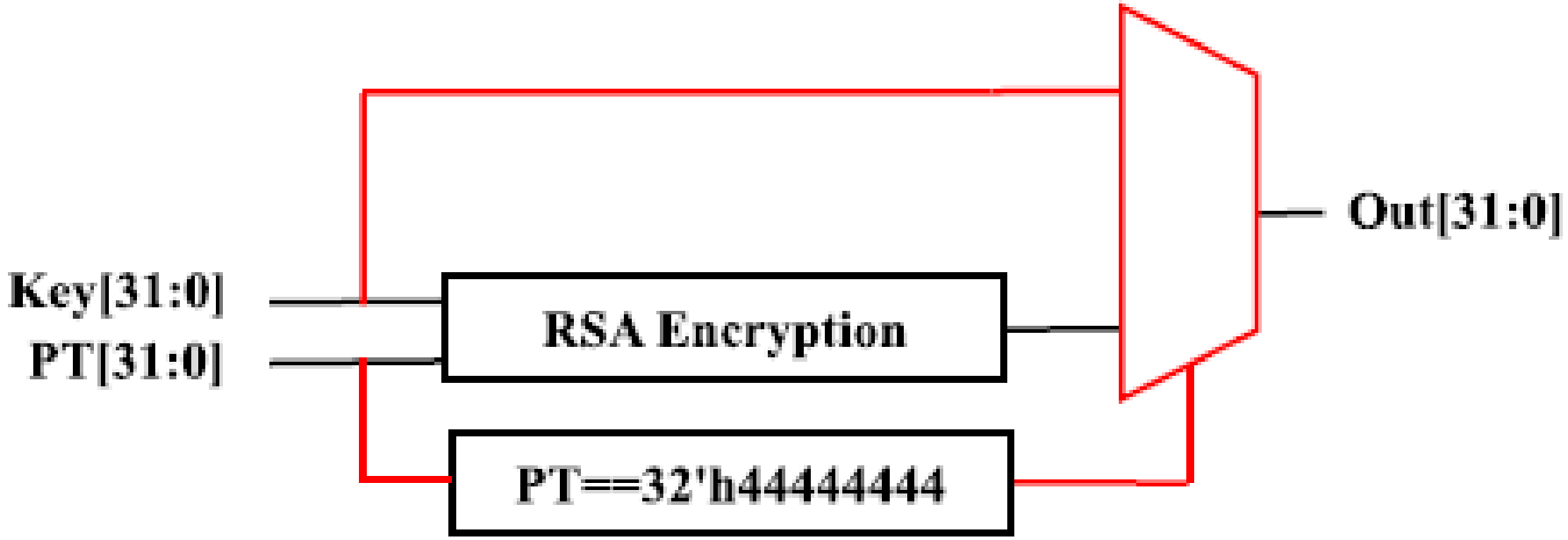


# UCI

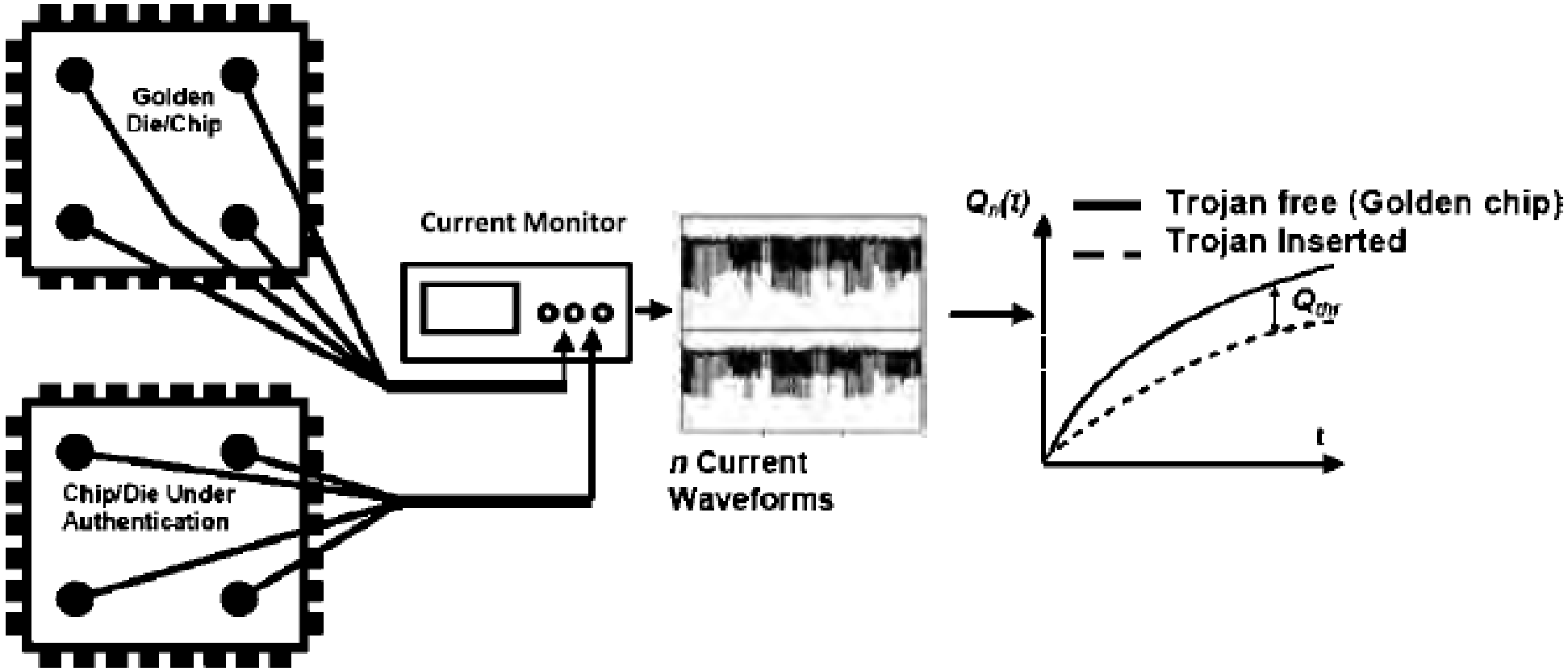


(A) (B) (C)

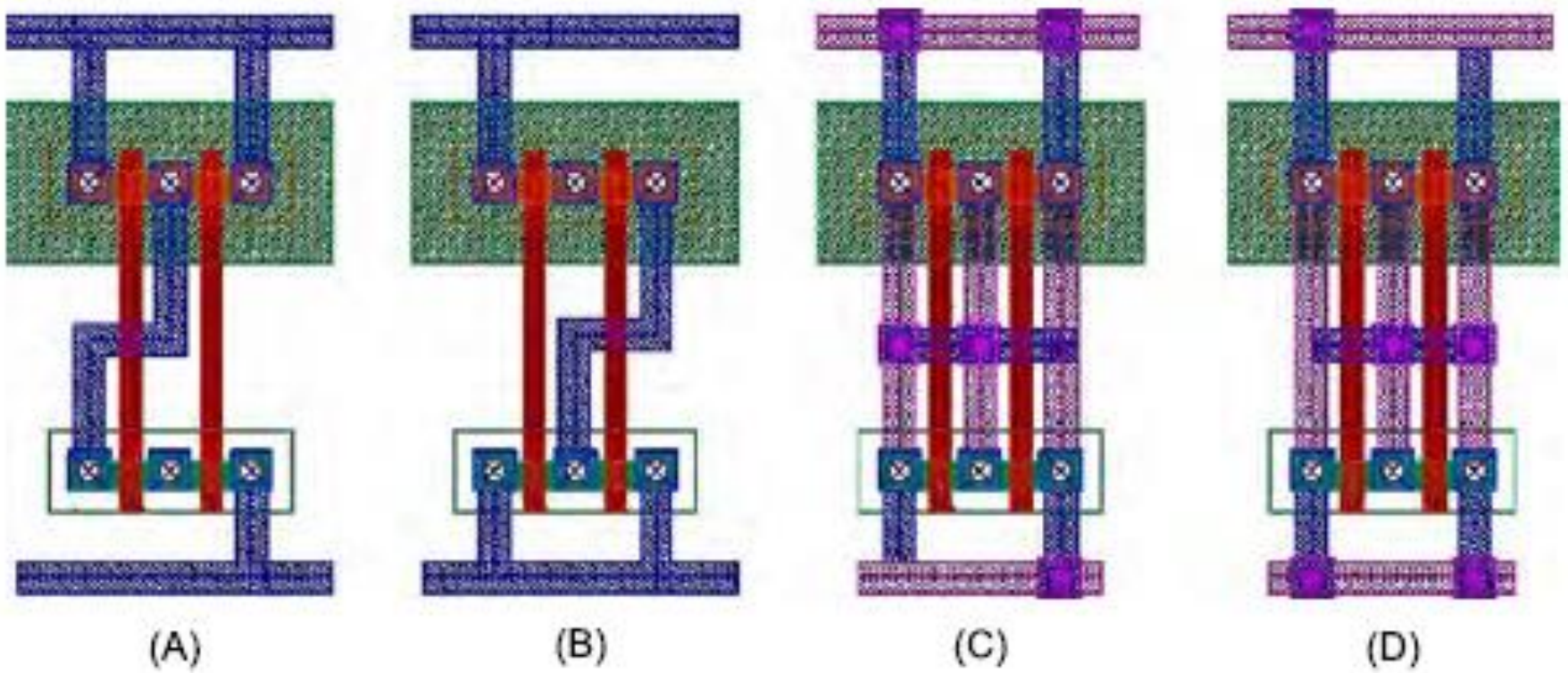
# Treshold



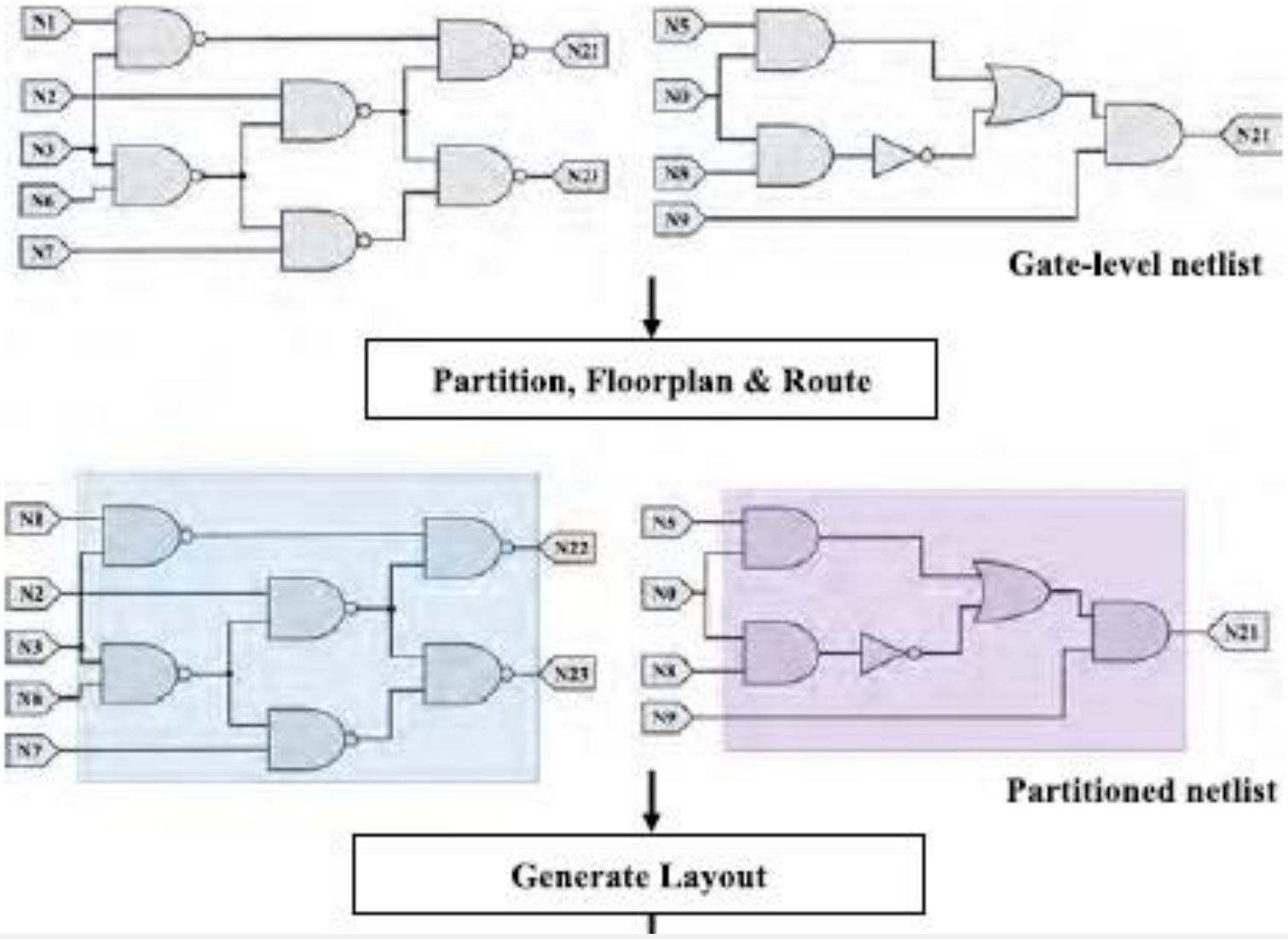
# Teste de Corrente



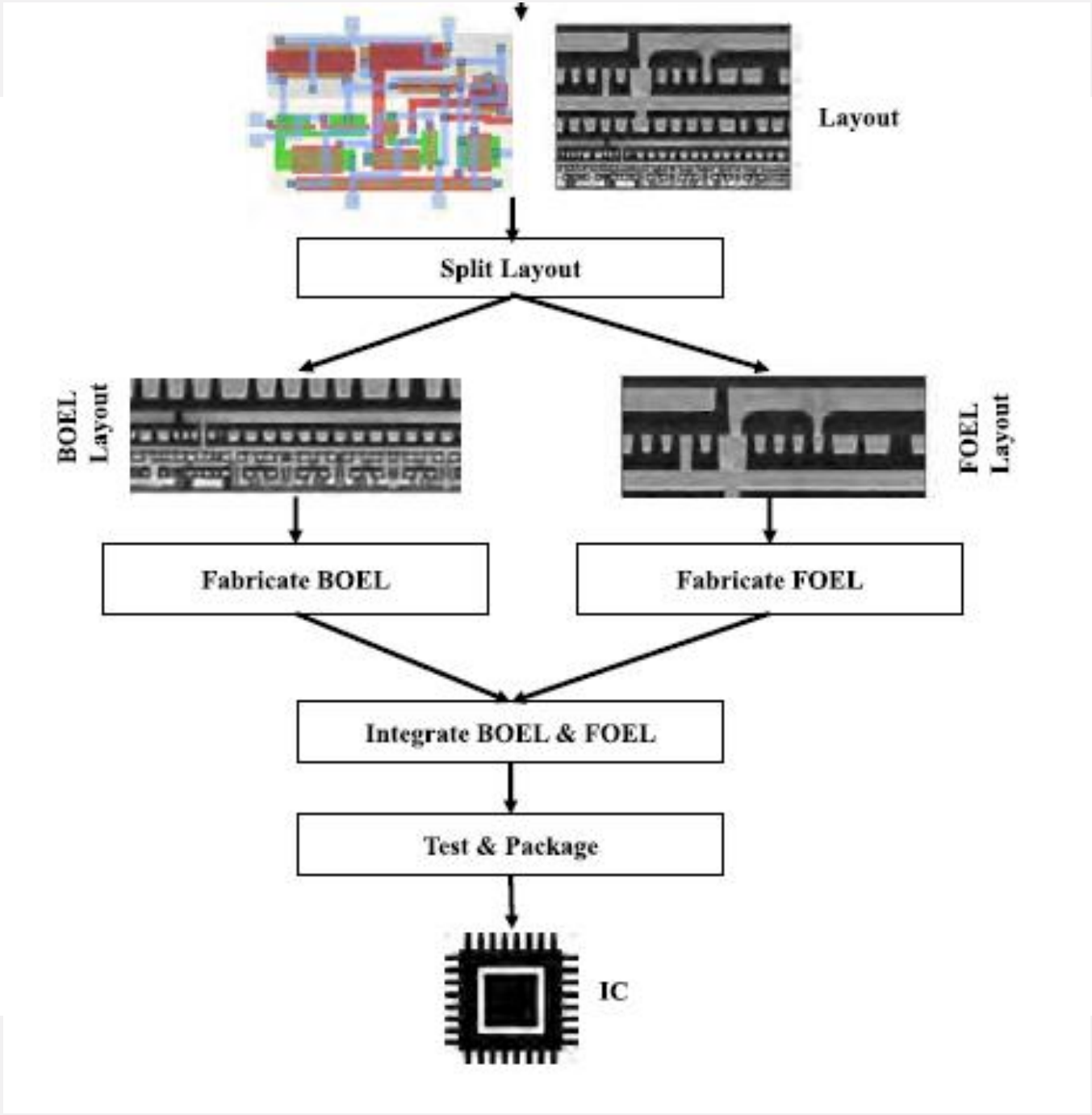
# Camuflagem de circuito



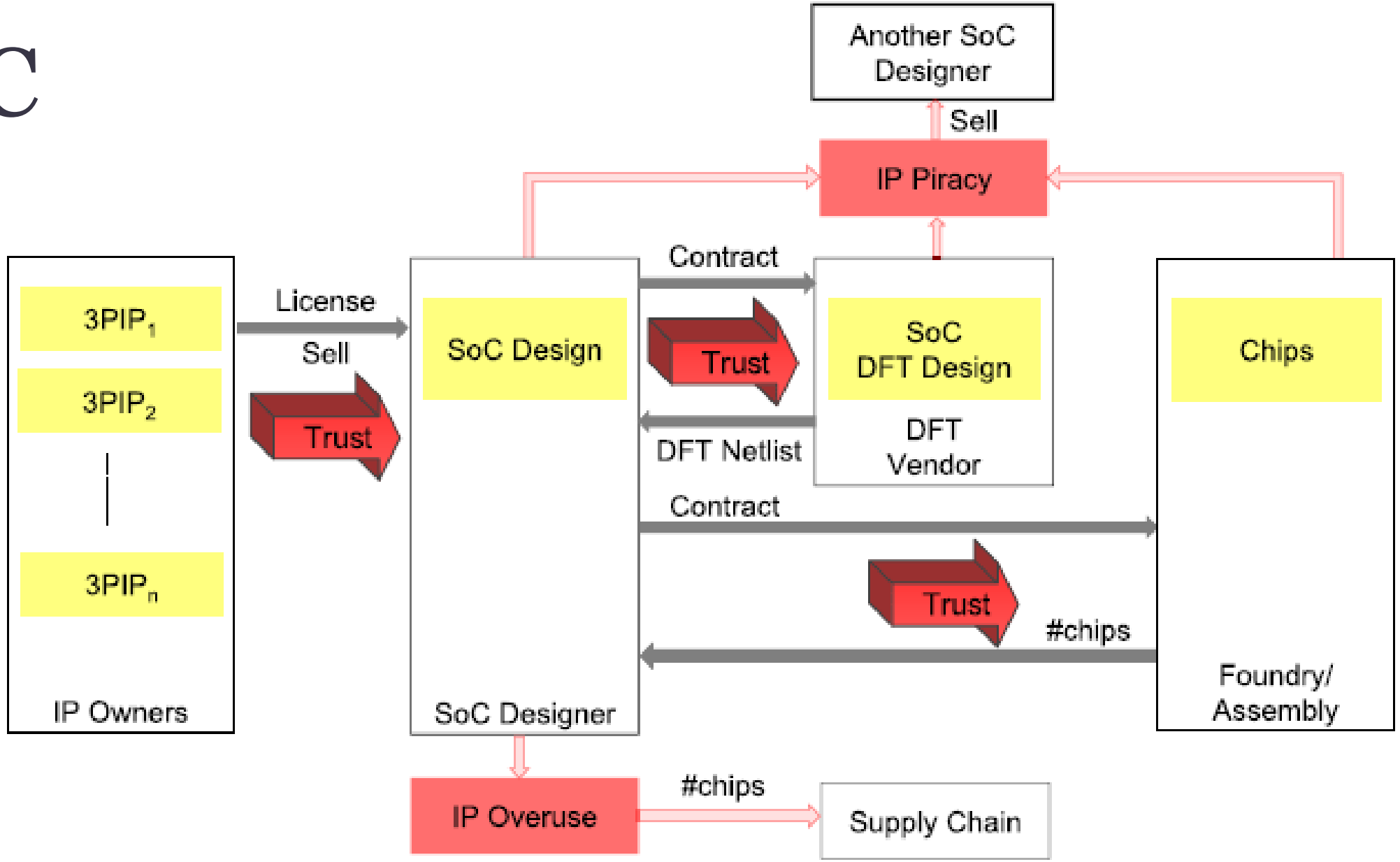
# Split Fabrication



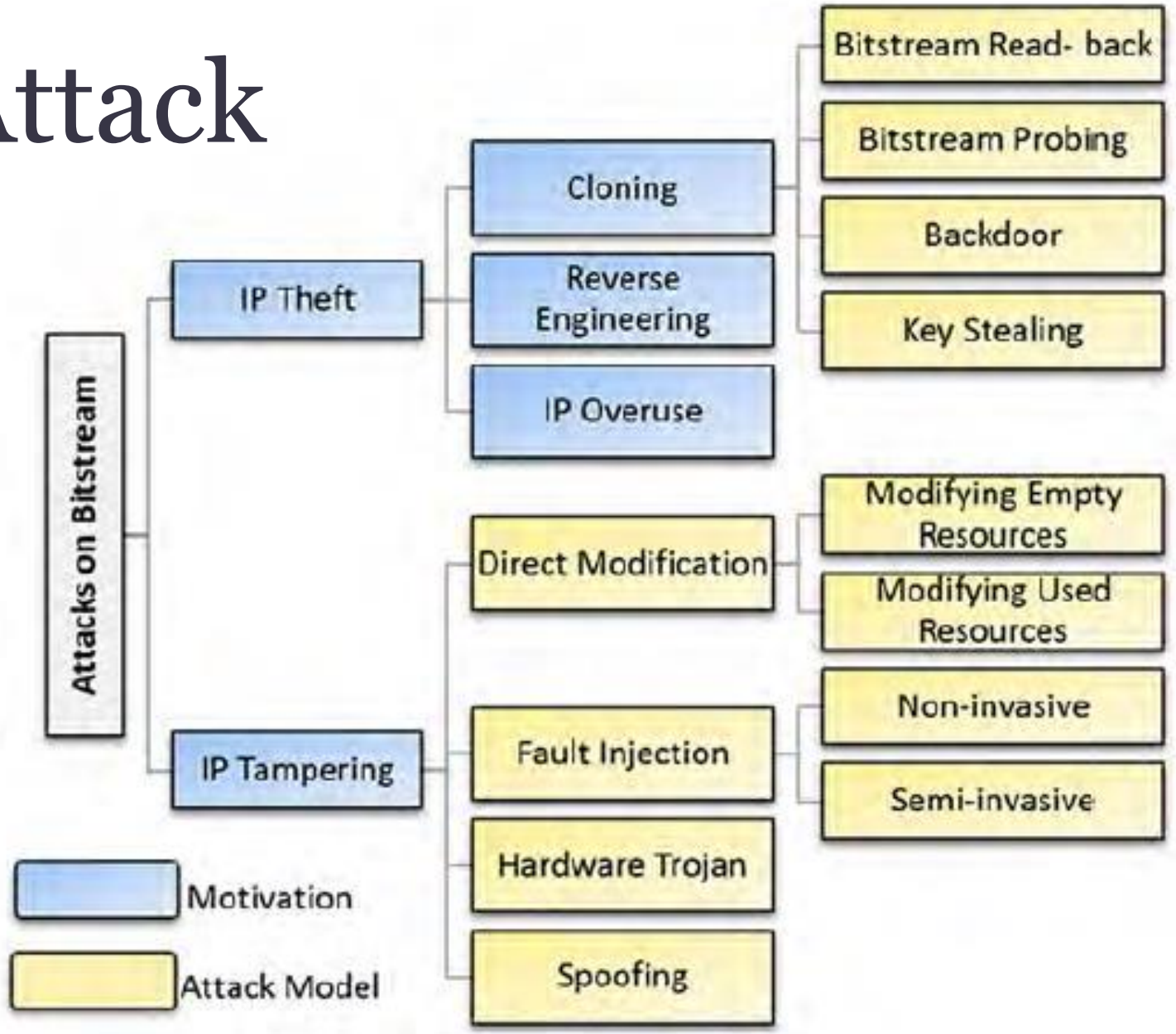
# Split Fabrication



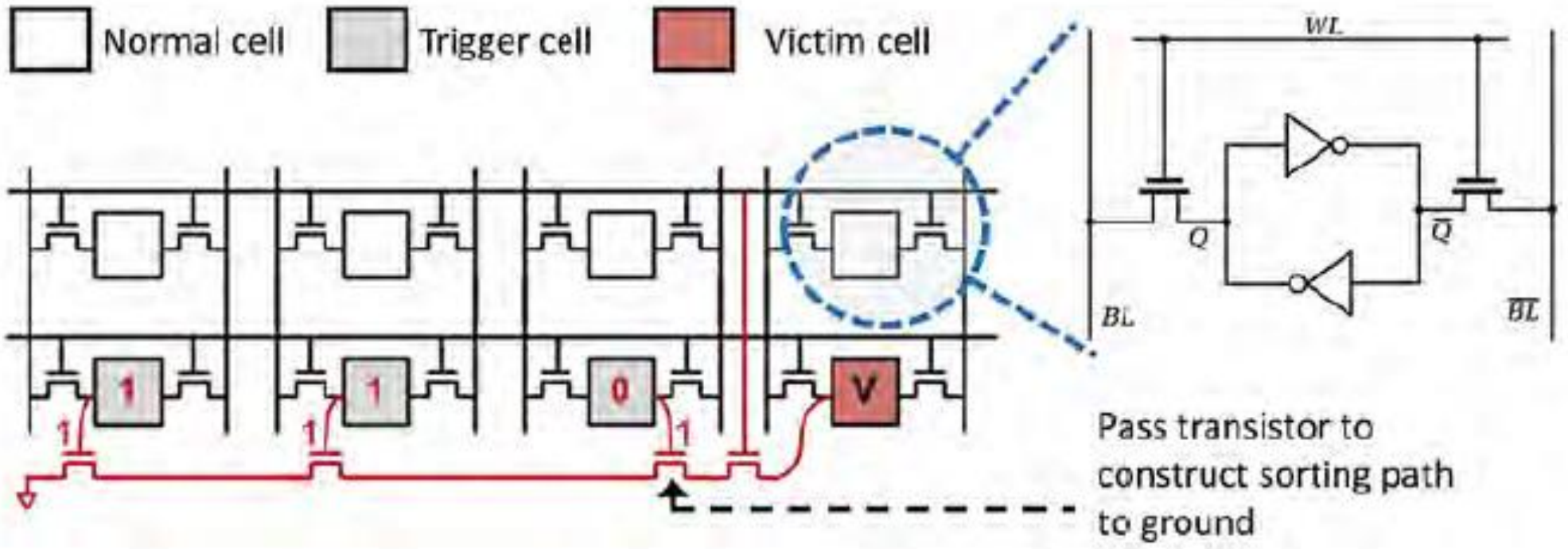
# ESC


Another SoC Designer
Sell
IP Piracy
3PIP1
3PIP2
3PIPn
IP Owners
License
Sell
Trust
SoC Design
SoC Designer
Contract
Trust
DFT Netlist
SoC DFT Design
DFT Vendor
Contract
Trust
#chips
Chips
Foundry/ Assembly
IP Overuse
#chips
Supply Chain

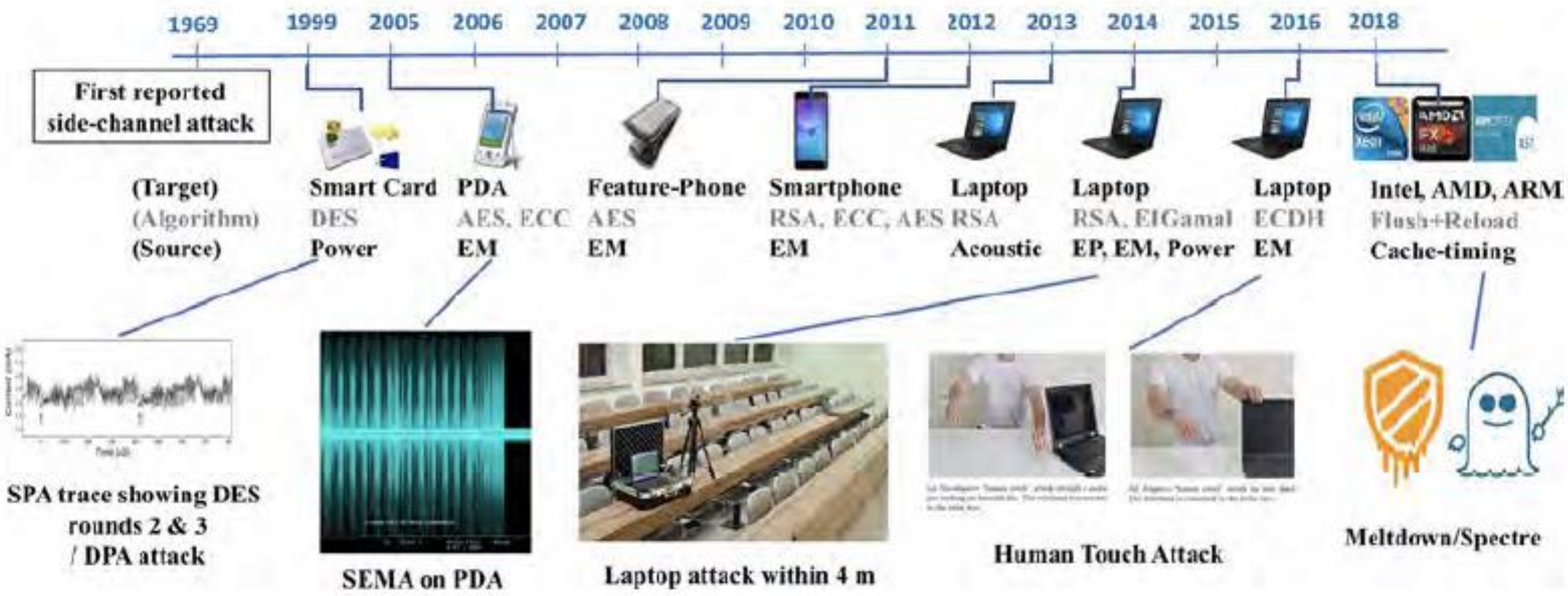
# Bitstream Attack



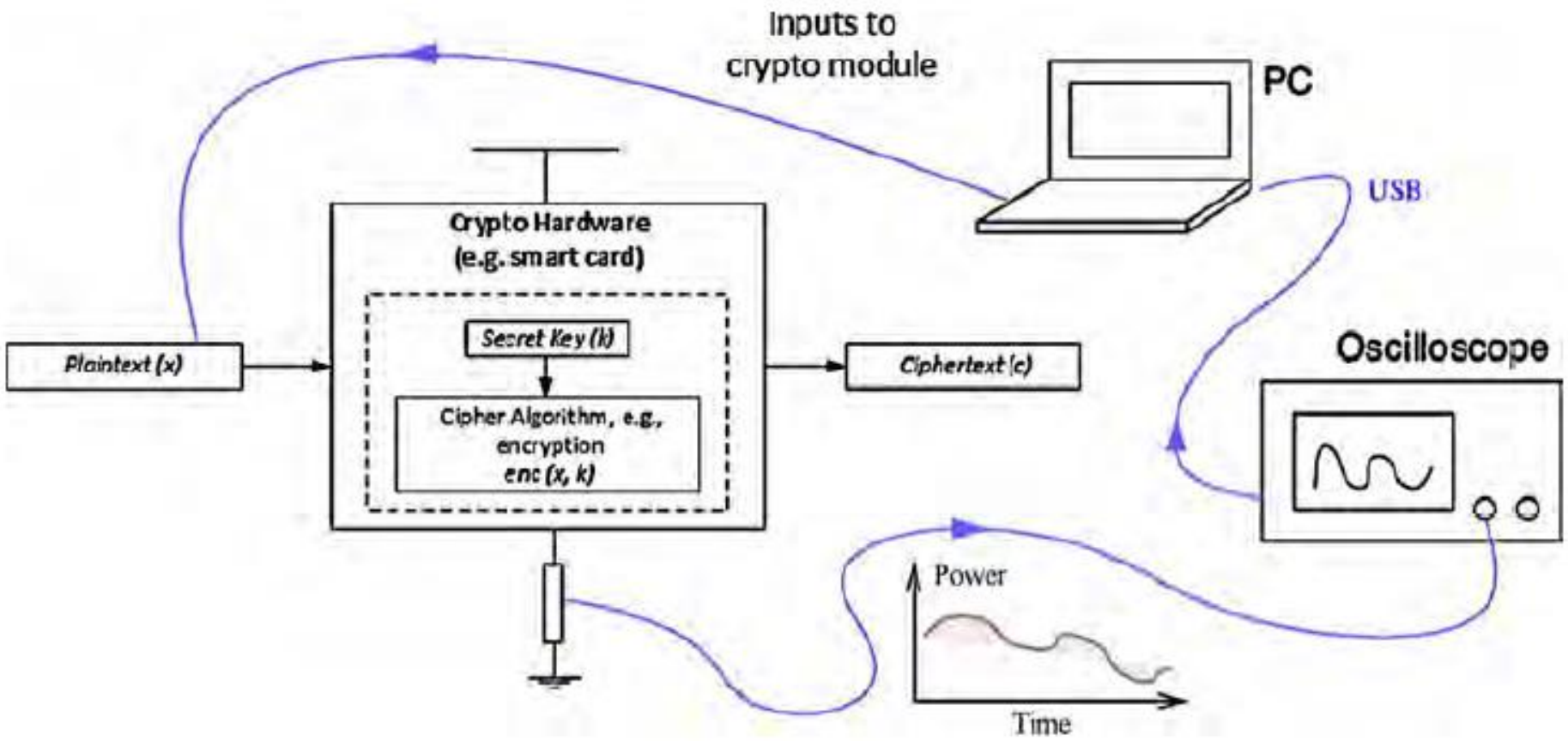
# Hardware trojan



# Sem Fio/ Ng

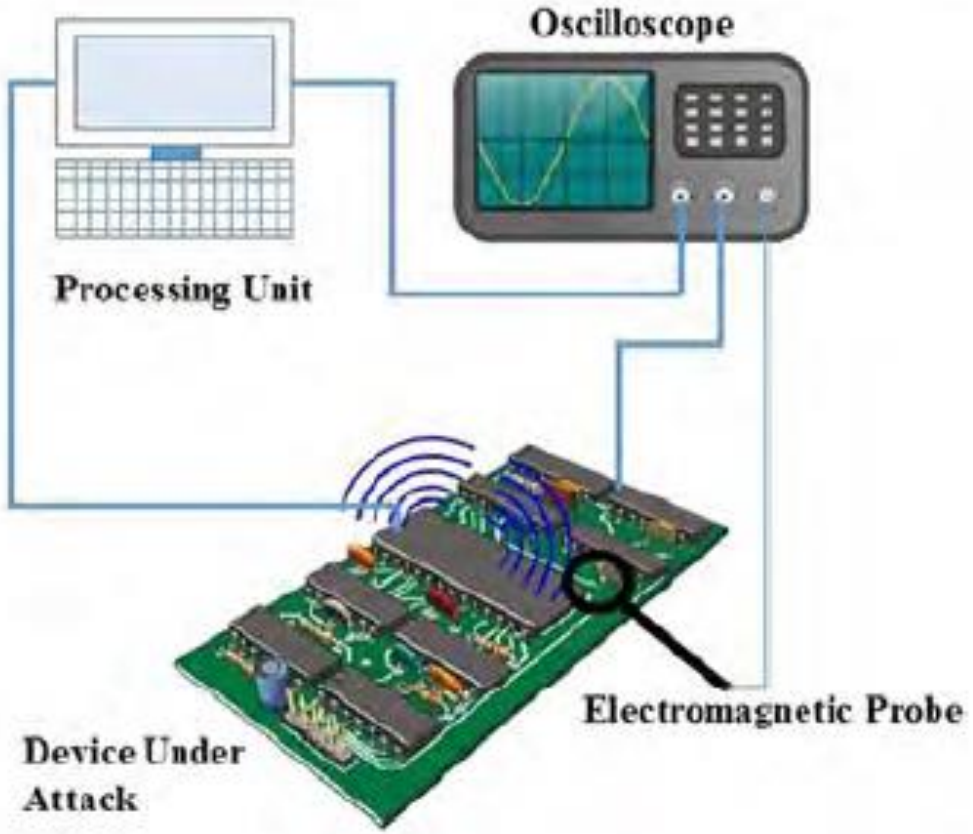

1969
1999
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2018
First reported side-channel attack
(Target)
(Algorithm)
(Source)
Smart Card
DES
Power
PDA
AES, ECC
EM
Feature-Phone
AES
EM
Smartphone
RSA, ECC, AES
EM
Laptop
RSA
Acoustic
Laptop
RSA, ElGamal
EP, EM, Power
Laptop
ECDH
EM
Intel, AMD, ARM
Flush+Reload
Cache-timing
SPA trace showing DES rounds 2 & 3 / DPA attack
SEMA on PDA
Laptop attack within 4 m
Human Touch Attack
Meltdown/Spectre

# Análise de potência



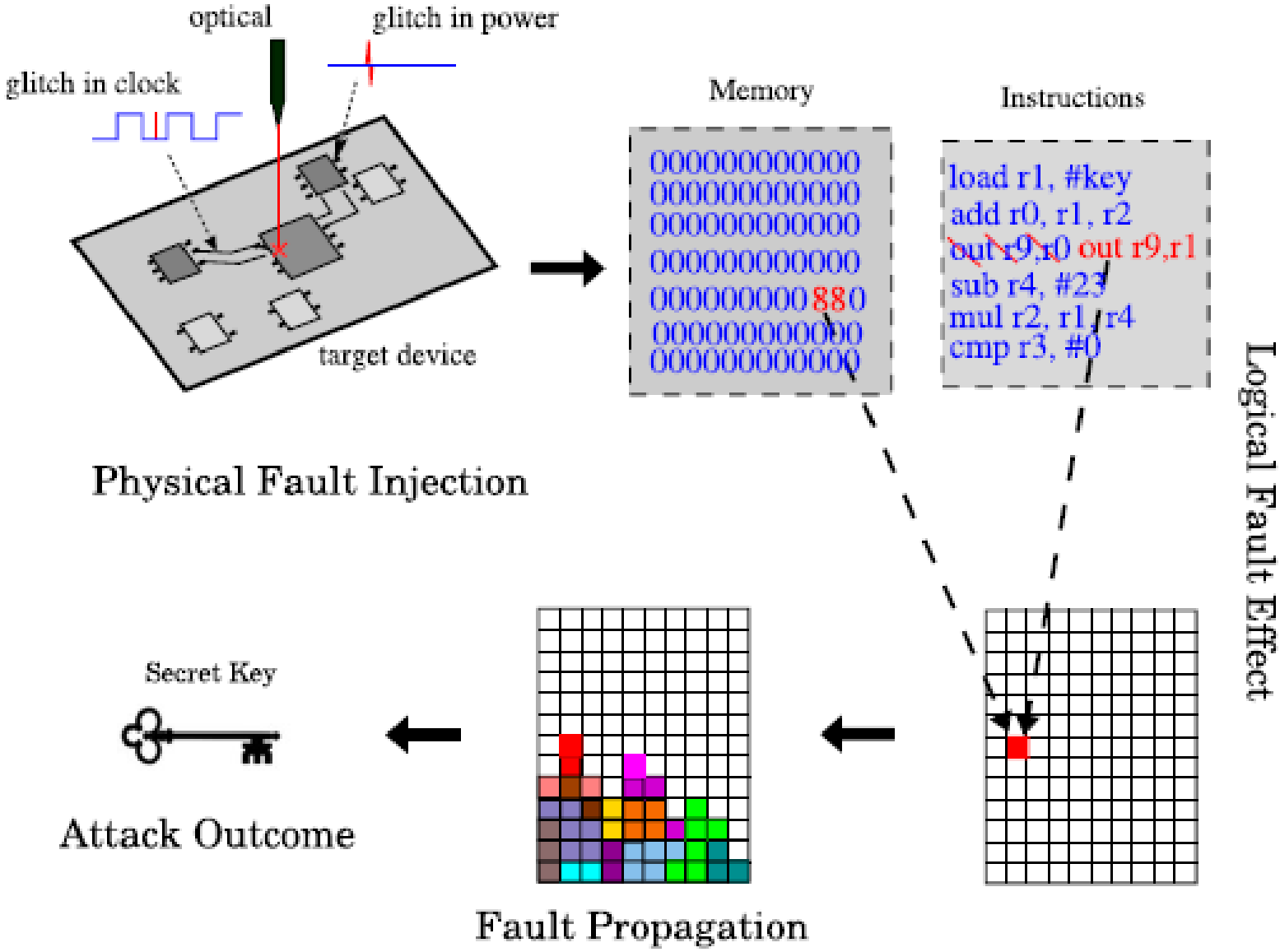
# Sonda eletromagnética

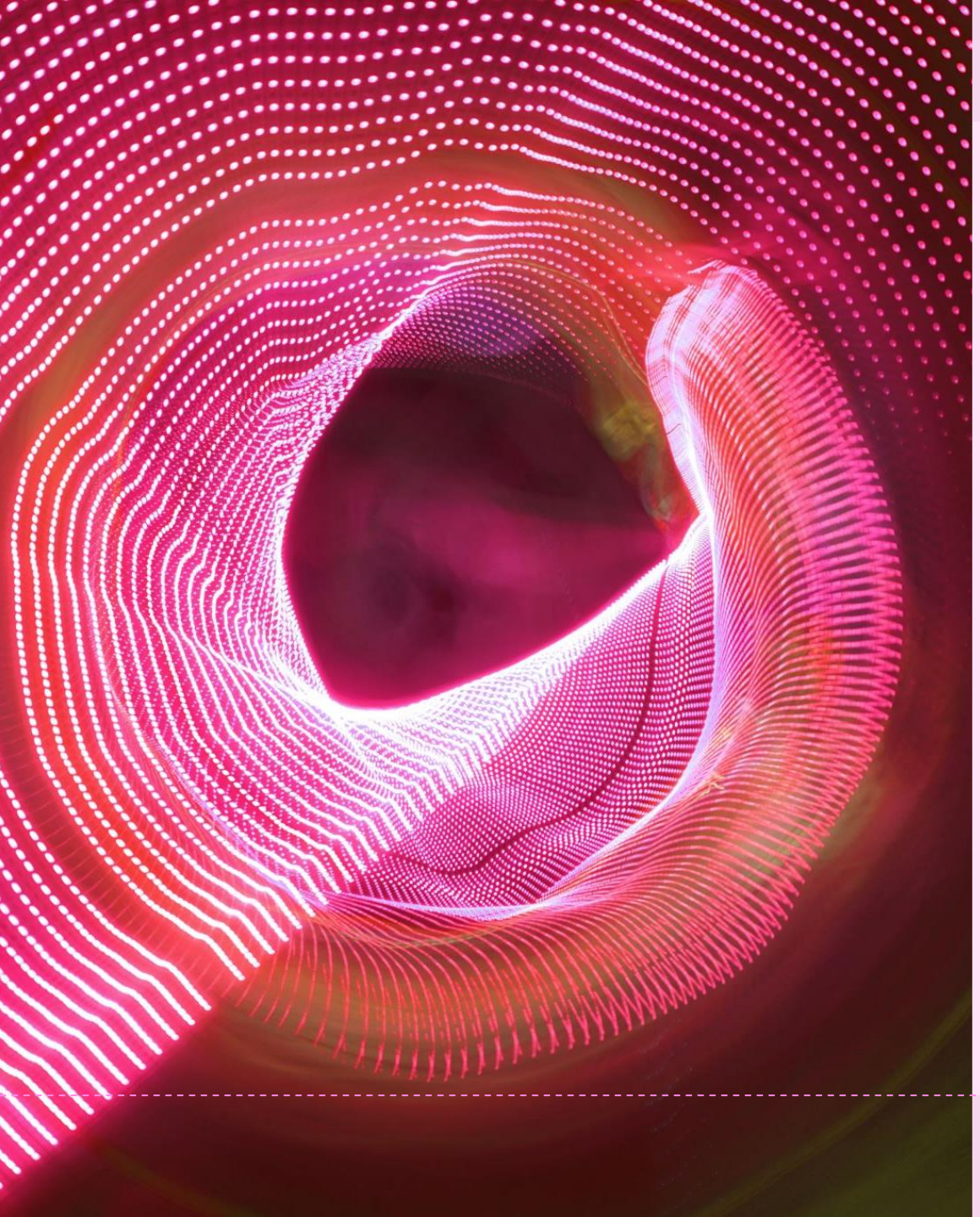
(A)




(B)

# Injeção de falhas física





# Obrigado!

Prof Maurício Acconcia Dias