University of Pisa

Department of Information Engineering

Hardware and Embedded Security

Nicolò Mariano Fragale

March 2025

Contents

Information

These notes are intended for educational purposes only and cover essential concepts in the field of data systems and security. The aim is to provide a comprehensive understanding of topics such as system vulnerabilities, protection techniques, and defense strategies in cybersecurity.

This document includes topics related to access control, authentication mechanisms, database security, cryptographic methods, and advanced persistent threats, with a particular focus on practical applications in real-world scenarios.

1 Rossi

Esistono 3 tipi di Silicio:

1. Silicio puro;
2. Silicio di tipo Positivo (p-type) (eccesso di cariche positive);
3. Silicio di tipo Negativo (n-type) (eccesso di cariche negative).

Il silicio puro è poco conduttivo, quindi viene drogato con impurità per renderlo più conduttivo ed essere usato per dispositivi elettronici.

Positivo e Negativo poi deteminano il verso della corrente elettrica.

Il silicio drogato viene utilizzato per realizzare i MOSFET (Metal Oxide Semiconductor Field Effect Transistor) che sono i componenti base dei circuiti integrati.

1.1 MOSFET Struttura di un MOSFET

1. **VDD**: Tensione di alimentazione, rappresenta in logica digitale il valore 1;
2. **VSS, Ground**: Tensione di massa, rappresenta in logica digitale il valore 0;

Il Mosfet si divide in Mosfet di arricchimento e Mosfet di depauperamento.

Consideriamo solo il primo che è formato da 4 regioni: Sorgente, Drenaggio, Gate e Bulk.

MOSFET-N (NMOS):

- Sorgente e Drenaggio sono di tipo N;
- Gate è isolato e riceve il segnale di controllo;
- Bulk è collegato al GND ed è di tipo P.

A bassa tensione il transistor è spento, a tensione alta il transistor è acceso, quindi la corrente passa da Drain a Source quando viene applicata una tensione positiva **VDD** e tensione negativa **VSS** è 0V. Ma soprattutto quando esiste differenza di potenziale tra Drain e Source.

MOSFET-P (PMOS):

- Sorgente e Drenaggio sono di tipo P;
- Gate è isolato e riceve il segnale di controllo;
- Bulk è collegato a VDD ed è di tipo N.

A bassa tensione il transistor è acceso (VSS), a tensione alta il transistor è spento (VDD), quindi la corrente passa da Source a Drain.

NMOS è preferito di gran lunga al PMOS, visto che è piu veloce, resistenza minore e consuma meno energia.

Un circuito **CMOS** è formato da una coppia di MOSFET:

- Un MOSFET di tipo P (PMOS) con la sorgente collegata al VDD;
- Un MOSFET di tipo N (NMOS) con la sorgente collegata al GND (VSS).

I due transistor sono complementari, ovvero quando uno è acceso, l'altro è spento.

Assorbe corrente solo quando cambia stato.

CMOS è usato per realizzare porte logiche (AND, OR, XOR, NAND, ecc.), microprocessori, memorie (SRAM, Flash) e sensori di immagine nelle fotocamere.

1.2 Propagation delay

Il tempo di propagazione è il tempo necessario affinché l'uscita cambi stato dopo una variazione dell'ingresso.

Il ritardo di propagazione misura il tempo tra il cambiamento dell'ingresso e la risposta dell'uscita. Si definiscono due ritardi:

- t_{PLH} (Propagation Delay Low-to-High) → Tempo impiegato dall'uscita per passare da LOW (0V) a HIGH (V_{DD}).
- t_{PHL} (Propagation Delay High-to-Low) → Tempo impiegato dall'uscita per passare da HIGH (V_{DD}) a LOW (0V).

Il ritardo medio si calcola come:

$$t_p = \frac{t_{PLH} + t_{PHL}}{2}$$

Propagation delay

Il ritardo di propagazione è influenzato da 3 fattori:

- Resistenza equivalente dei MOSFET R_{eq};
- Capacità di carico C_L;
- Corrente di commutazione I.

Il ritardo di propagazione è inversamente proporzionale alla corrente di commutazione e alla capacità di carico, e direttamente proporzionale alla resistenza equivalente dei MOSFET.

1.3 Power consumption

- Consumo Statico: corrente assorbita quando il circuito è in stato statico (non cambia stato);
- Consumo Dinamico: corrente assorbita quando il circuito cambia stato.
- Consumo da corto circuito: corrente assorbita quando i transistor sono in stato di corto circuito sempre durante il cambio di stato.

Consumo statico

Il consumo statico si riferisce alla corrente assorbita quando il circuito si trova in uno stato stabile, ovvero senza transizioni logiche. In teoria, i circuiti CMOS hanno un consumo statico molto basso, poiché idealmente un percorso diretto tra V_{DD} e GND non dovrebbe esistere quando il circuito è stabile.

Cause del consumo statico:

1. **Subthreshold Leakage Current:** è la corrente che scorre attraverso un MOSFET anche quando è spento e dipende dalla temperatura e dalle dimensioni dei transistor.

   È più significativa nei NMOS, perché hanno una soglia di tensione inferiore rispetto ai PMOS.

2. **Reverse Bias Junction Leakage:** è la corrente che scorre attraverso la giunzione PN anche quando il transistor è spento ed è maggiore negli NMOS rispetto ai PMOS a causa della più alta mobilità degli elettroni.

Consumo dinamico

Il consumo dinamico è la potenza dissipata quando il circuito commuta tra stati logici, ovvero quando l'uscita cambia da 0 a 1 o viceversa.

$$P_{dynamic} = \alpha \cdot C_L \cdot V_{DD}^2 \cdot f$$

Dove:

- α è il fattore di attività, ovvero la probabilità che il circuito commuti stato;
- C_L è la capacità di carico;
- V_{DD} è la tensione di alimentazione;
- f è la frequenza di commutazione (frequenza del clock).

Durante la transizione LOW $\rightarrow$ HIGH, il PMOS si accende e carica la capacità di carico C_L.

Durante la transizione HIGH $\rightarrow$ LOW, l'NMOS si accende e scarica C_L verso GND.

Maggiore è la capacità di carico, maggiore è l'energia richiesta per la commutazione.

Quindi per ridurre il consumo dinamico si può ridurre la tensione di alimentazione V_{DD}, rifurre la capacità di carico C_L usando transistor più piccoli e ridurre l' attività di commutazione f.

Consumo da corto circuito

Il consumo da corto circuito avviene quando entrambi i transistor NMOS e PMOS sono temporaneamente accesi durante la transizione di stato, creando un percorso diretto tra V e GND.

$$P_{short-circuit} = I_{sc} \cdot V_{DD} \cdot t_{sc}$$

Dove:

- I_{sc} è la corrente di corto circuito;
- V_{DD} è la tensione di alimentazione;
- t_{sc} è il tempo durante il quale entrambi i transistor sono accesi;

1.4 Componenti riciclati e Invecchiamento Fenomeni dell'invecchiamento:

- Negative Bias Temperature Instability (NBTI);
- Positive Bias Temperature Instability (PBTI);
- Hot Carrier Injection (HCI);
- Time-Dependent Dielectric Breakdown (TDDB).

Negative Bias Temperature Instability (NBTI):

NBTI è un fenomeno che degrada le prestazioni dei transistor PMOS quando sono sottoposti a bias negativo prolungato (V_GS ¡ 0, quindi gate negativo rispetto a source). Questo porta a un aumento della tensione di soglia (V_T), riducendo la corrente che il transistor può fornire e rallentando il circuito. In questo modo il transistor chiederà una tensione maggiore per accendersi, maggiore resistenza interna e velocità di commutazione ridotta, infine il circuito risulterà rallentato.

Positive Bias Temperature Instability (PBTI):

Simile a NBTI, ma colpisce i transistor NMOS sotto bias positivo (V_GS ¿ 0) e le cariche tendono a rimanere intrappolate nei difetti dell'ossido di gate. A causa di ciò NMOS si accende più lentamente e gli elettroni si muovo pià lentamente.

Hot Carrier Injection (HCI):

HCI è un effetto di degrado che si verifica quando gli elettroni o i fori acquisiscono energia sufficiente per superare la barriera dell'ossido di gate e rimanere intrappolati all'interno, modificando le caratteristiche del transistor. Questo problema è più critico negli NMOS rispetto ai PMOS, perché gli elettroni hanno una maggiore mobilità rispetto ai fori. In questo caso si riduce la corrente di drain e la velocità di commutazione, facendo si che il transistor diventi meno efficiente.

Time-Dependent Dielectric Breakdown (TDDB):

TDDB è un meccanismo di guasto progressivo che porta alla rottura dell'ossido di gate nel tempo, a causa di uno stress elettrico prolungato. Una volta che il breakdown avviene, il transistor smette di funzionare correttamente. Quindi si perde la capacità isolante dell'ossido, aumentando la corrente di perdita e eventualmente il guasto irreversibile del dispositivo.

1.5 Process Variation Inter-Die Variations: due chip identici prodotti nello stesso o diversi wafer(disco di silicio) possono avere caratteristiche elettriche leggermente diverse.

Alcuni esempi di variazioni sono:

- Differenze nella tensione di soglia;
- Differenze nella corrente di perdita;
- Differenze nel tempo di propagazione.

Intra-Die Variations: variazioni intra-die sono differenze tra transistor all'interno dello stesso chip. Queste possono essere dovute a imperfezioni locali nel processo di fabbricazione.

Alcuni esempi di variazioni sono:

- Variazioni nelle frequenze di funzionamento tra diverse parti del chip.
- Variazioni nella tensione di soglia tra diversi transistor.
- Variazioni nella corrente di perdita tra diversi transistor.
- Degrado delle prestazioni nei percorsi critici.

A fine slide il professore consiglia dei video per approfondire il discorso.

1.6 Testing Viene effettuato per verificare le funzionalità dei circuiti integrati e per individuare eventuali difetti dopo che sono stati fabbricati.

Un chip senza difetti è un good chip, altrimenti un bad chip; vengono testati tutti i chip e non tutti sono facili da verificare.

Queste verifiche possono essere sfruttate anche per scovare i chip contraffatti, che di solito sono chip vecchi, infatti piu dell' 80% di chip contraffatti sono chip vecchi.

Si effettuano principalmente 2 test:

1. Electrical test: testa le proprietà elettriche del chip sia in caso di corrente continua (comportamento statico) (DC) che in corrente alternata (comportamento dinamico) (AC):
    - Tensione di soglia dei transistor (DC);
    - Corrente di perdita (DC);
    - Tensione e Corrente di Alimentazione, quindi se il dispositivo opera con la tensione e corrente prevista (DC).
    - Frequenza di taglio, ovvero la banda che passa nel dispositivo (AC);
    - Propagation delay (AC);
    - Tempo di salita e discesa del segnale (AC).
    - Il livello di disturbo che può interferire con il segnale (AC).

2. Functional test: testa le funzionalità del chip, quindi se svolge correttamente il suo lavoro.
    - Logica digitale: verifica se le porte logiche funzionano correttamente;
    - Memorie: verifica se le memorie funzionano correttamente;
    - Interfacce: verifica se le interfacce funzionano correttamente;
    - Il codice viene eseguito senza errori.
3. Temperature test: verifica se il chip funziona correttamente a diverse temperature.
    - Militare: -65°C a 175°C; nel caso di chip militari con l'obiettivo di resistere a temperature estreme;
    - Industriale: -25°C a 85°C; per chip che devono resistere a temperature elevate;
    - Commerciale: -10°C a 70°C.

    Burn-In: testa il chip a temperature elevate per un lungo periodo di tempo per trovare infant mortality, ovvero i chip che si rompono subito dopo la fabbricazione.

    Temperature Cycling: testa il chip a temperature alte e basse per verificare se il chip funziona correttamente a diverse temperature.

Per verificare i risultati questi vengono comparati con i risultati attesi, se sono uguali il chip è buono, altrimenti è difettoso.

1.7 Hardware Metering Hardware metering (introdotto nel 2005) è un insieme di protocolli che permettono all'autore del prodotto di deterne i diritti successivamente alla produzione e distribuzione.

Questa tecnica quindi vale come un **Fingerprinting univoco** per identificare il prodotto.

Alcuni esempi di autenticazione hardware sono:

1. **On-Chip Aging Sensor:** misura l'invecchiamento del chip e quindi la sua vita utile;
2. **Physically Unclonable Functions (PUFs):** sono funzioni che generano un fingeprint univoco per ogni chip, quindi non clonabile;

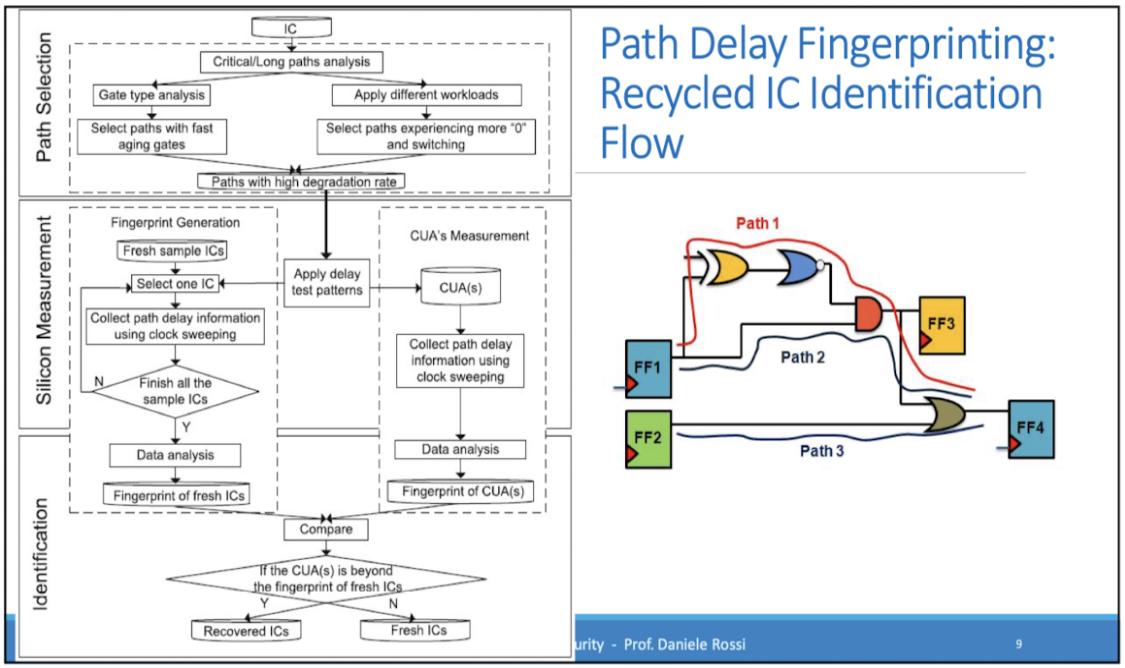
1.8 Path Delay Analysis Path Delay Fingerprinting è una tecnica che permette di identificare un chip tramite il degrado delle prestazioni senza usufruire di ulteriore hardware dedicato alla registrazione di aging.

Con degrado delle prestazioni ci si riferisce al tempo che i chip impiegano per eseguire operazioni funzionali $\rightarrow$ Ritardi più grandi $\leftrightarrow$ Uso prolungato.

(In generale) I test affermano che la più alta percentuale di degradazione si misura durante il primo anno (0%-10%), al termine del 4& anno si arriva circa al 17%.

Il grafico in slide mostra che le porte logiche XOR e NOR si degradano piu velocemente delle porte NAND, e gli inverter di taglia piu piccola si degradano piu velocemente di quelli di taglia piu grande.

L'immagine mostra il processo di identificazione dei circuiti integrati (IC) riciclati tramite Path Delay Fingerprinting.



Teniamo conto di 3 fattori principali:

1. **Proprietà delle porte logiche**
   (a) Analisi delle porte logiche, XOR degradando più velocemente;
   (b) Selezione dei percorsi che contengono maggior numero di pMOS (si degradano piu velocemente degli nMOS);
   (c) Selezione dei percorsi che contengono più switchings (cambi di stato).
   (d) Selezione dei percorsi che contengono più inverter di taglia più piccola (si degradano più velocemente di qulli di taglia più piccola).
2. **Misurazione di silicio e Clock Sweeping**
   (a) Si usa il clock del circuito per testare i percorsi, in questo modo si possono analizzare chip gia sul mercato senza che serva un design specifico.
   (b) Vengono comparate le misurazioni svolte durante il testing primario con quelle attuali (∀ paths), le misurazioni devono essere effettuate con le stesse condizioni (i.e Temperatura).

(c) Il clock viene fatto variare a diverse frequenze per determinare la frequenza limite alla quale il percorso smette di funzionare.

3. **Identificazione del path**

   Una volta misurati tutti i path si capisce se il chip è nuovo o riciclato.

   L'Analisi Statistica considera:

   (a) Simple Outlier Analysis (SOA): verifica se i ritardi misurati sono anomali rispetto al campione di riferimento (media di IC originali).

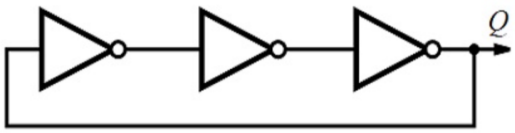
   (b) Principal Component Analysis (PCA): i dati raccolti vengono considerati come un set di variabili in uno spazio multidimensionale che generano dei componenti principali e cose varie, è complesso e articolato e il prof non l ha spiegato.

Se il ritardo del CUA è fuori dal range dei chip nuovi, è probabile che sia un IC riciclato.

1.9 Clock Sweeping Il clock sweeping è una tecnica che permette di identificare IC (circuiti integrati) riciclati basandosi sui risultati che forniscono quando vengono testati. Infatti gli IC devono rispondere in maniera specifica in base alla frequenza del clock e durante questo test gli IC vengono sottoposti a diverse frequenze di clock. Il punto è trovare la frequenza limite alla quale il percorso smette di funzionare, quindi non propaga alcun segnale. In questo modo possiamo misurare il **delay del path**.

I vari modi in cui possiamo performare questa tecnica dipende quindi dal controllo che abbiamo sul manovrare la frequenza di clock.

1.10 Ring Oscillator RO è una tecnica utilizzata per identificare IC contraffatti, in cosa consiste?
Un RO è un circuito costituito da un anello di porte logiche collegate in cascata (di numero disparo), il cui output è collegato all'input successivo.

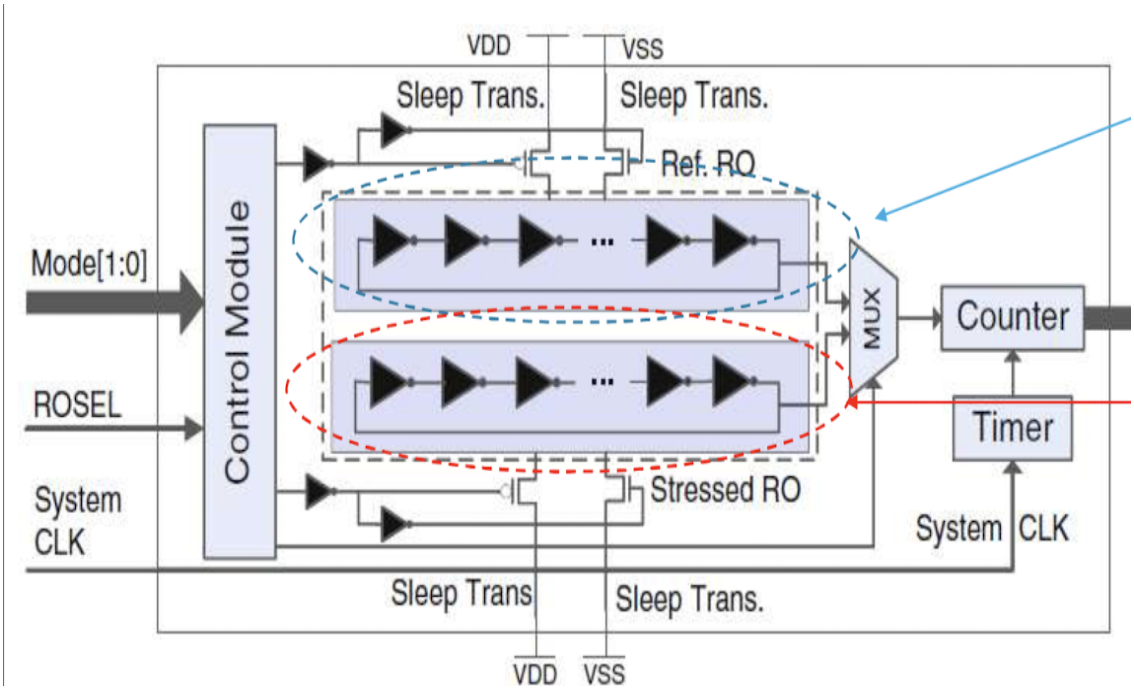


RO evaluate the intrinsic speed of a CMOS.
La frequenza del RO è inversamente proporzionale al numero di stage e alla velocità di commutazione delle porte logiche (propagation delay).

$$f_{osc} = \frac{1}{N(\tau_{LH} + \tau_{HL})} = \frac{1}{2N\tau_p}, \qquad \tau_p = \frac{\tau_{LH} + \tau_{HL}}{2}$$

La frequenza in un RO riciclato è inferiore rispetto a quella di un IC nuovo.
Temperatura e frequenza sono inversamente proporzionale, inoltre sostenere temperature elevate può causare un degrado delle prestazioni del chip.
Il suo comportamento deve essere tale che invecchi a un ritmo simile a quello del circuito integrato (IC) che sta monitorando.

1.11 RO as Sensor



1. Il primo RO (quello sopra) è chiamato il *Reference RO*, è un RO programmato per invecchiare molto lentamente;
2. Il secondo RO (quello sotto) è chiamato il *Sensor RO*, è un RO programmato per invecchiare al ritmo del chip che si sta monitorando.
3. **N.B:** Da chiedere prima al prof: numero inverter correlati a frequenza
4. **Counter:** conta il numero di cicli del RO, quindi il numero di oscillazioni in

a given time.

5. **System clock:** serve a compensare gli effetti negativi del degrado del circuito, mantenendo la precisione temporale costante nel tempo.
6. **MUX:** seleziona il RO da monitorare, è controllato dal **ROSEL** signal.
7. I transistor (pmos e nmos) collegati ai RO servono per attivarli e disattivarli. (se pmos=1 allora RO attivo perche controlla VDD, nmos controlla VSS)

Three mode of operation control:

1. **Manufacturing test mode:** both RO are disconnected to experience no aging;
2. **Functional mode:** Ref RO is disconnected (age a bit bit) and Stressed RO is connected to experience aging; (riflette lo stato di invecchimaneto del chip)
3. **Authentication mode:** both are connected to authenticate the chip.

These mode ensures:

1. The frequency beetwen the two RO will be larger over time;
2. Is impossible to modify RO based sensor during the recycling process.

1.12 Hardware Trojans A malicious addition or modification to the circuit used the change its beahavior, reduce the reliability, or leak sensitive information.

- **IP**: intellectual property, most little form of the three;
- **IC**: integrated circuit (i.e CPU);
- **SoC**: system on chip → set(IC) → CPU, GPU, RAM, ROM, etc.;

Hardware Trojans can be inserted in any of these three levels, but the most common is the IC level.
Detection of Hardware Trojans is difficult because they are often small and can be hidden in the design of the circuit and there is no known golden model to compare with. (Those who insert HT are the same who provide golden model (comparing both taint circuits)).
Detection is extremely difficult, both in hardware and software.
HT can be injected during each phase of the design process.

1.13 Implementation HT consists of:

1. Trojan Trigger: a condition that must be satisfied to activate the HT;
2. Trojan Payload: the action that the HT performs when activated;

Type of Trojan:

- **Functional Trojan:** takes as input nets of the main circuit and restitches (ricuce) with some other nets of the main circuit modifying its functionality;

- **Combinational Trojan:** trigger is activated when is performed (from the main circuit) a specific set of conditions (rare to append);
- **Sequential Trojan:** trigger is activated when a specific sequence of conditions/state is performed/transitions (more common);

1.14 HT Taxonomy:

- Physical characteristics:
  - Distribution: Defines how the Trojan is spread across the IC, whether localized or widely distributed. (Depend by the dead space available on the layout)
    - Tight: when components are topologically close in the layout;
    - Loose: when components are dispersed across the layout of a chip;
  - Structure:
    - Layout Change: The Trojan introduces modifications to the physical layout of the circuit.
    - Layout Same: The Trojan does not alter the overall physical layout but instead exploits existing structures.
  - Size: The relative footprint of the Trojan, which can range from a few gates to a significant portion of the circuit.
  - Type:
    - Functional: HTs realized through the addition or deletion of transistor or gates;
    - Parametric: HTs realized through the modification of existing gates;
- Activation characteristics:
  - Internally Triggered: The Trojan is activated by internal circuit conditions.
    - Always On: The Trojan continuously operates without requiring a specific trigger, is always activate and can disrupt the chip's function at any time.
    - Conditional: The Trojan activates only when specific internal conditions are met.
      - Logic: Triggered by a specific logic state or sequence.
      - Sensor: Activated by environmental conditions (e.g., temperature, voltage).
  - Externally Triggered: The Trojan is activated by external signals or influences as Antenna or sensor...

        - Antenna: Triggered via wireless signals (e.g., RF, electromagnetic waves).
        - Sensor: Activated by detecting external environmental changes (e.g., light, temperature).

- Action characteristics:
    - Transmit Information: The Trojan leaks sensitive data to an external entity.
    - Modify Specification: Alters the design parameters, such as timing or power characteristics such as delay.
    - Modify Functionality: Changes the intended behavior of the circuit.
        - Change: The Trojan modifies the circuit's normal operation.
        - Disable: The Trojan disrupts or completely disables certain functionalities.
- Moles: MOLES is a type of hardware Trojan that leaks sensitive information by exploiting side-channels such as:
    - Power consumption;
    - electromagnetic radiation;
    - Path delay.

    MOLES circuits are designed to subtly modify power consumption in a way that depends on secret data (e.g., cryptographic keys). This creates a side-channel that attackers can measure externally to reconstruct sensitive information.

    A critical feature of MOLES is the signal-to-noise ratio (SNR), defined as the power level of side-channel leakage to that of the host IC. An effective MOLES requires a low SNR to evade evaluators' detection, but a high enough SNR for the attacker to extract the secret key bits

Side-Channel Attack exploit the implementations of cryptographic algorithms or software: When performing a side-channel attack, some observable behaviour of the additional information that allows the attacker to decode some cipher text, calculate the cryptographic keys or obtain details of the executed instructions and data within the system

(altri esempi con immagini le trovi nella slide 4)

2 Saponara

2.1 The role of HW in cybersecurity: HW security and trust and HW-based security. Slide 1

1. **HW security:** Per ottenere un un hardware sicuro bisogna analizzare le sue vulnearbilità: identification, detection, prevention (of exploitation), patching.
   Analizzare i modi in cui l'hardware può essere compromesso e implementare tecniche di prevenzione e mitigazione.
   Implementare solutzioni di protezione.
   Examples: To prevent insert malicious code in OTA updates, authenticate who is updating, authenticate the software, check the integrity of update.
   Hardware security issue can be faced during the production phases, which is better when the hardware ia already operating in the field (recall).

2. **HW trust:** A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, virus, and a given level or physical interference.
   Hardware trust mainly concerns Authenticity, that can be verified statically checking for counterfeiting and dynamically using intrusion detection system, IDS, to verify that during the life cycle a virus/malware has not taken the control of an hardware
   Hardware trust is related to hardware counterfeiting.

3. **HW-based security:** Refers to all those solutions aimed at resorting to hardware devices to protect the whole system from attacks that exploit vulnerabilities of other components of the system itself.
   it does provide a "chain of trust" rooted in silicon that makes the device and extended network more trustworthy and secure.
   Hardware-baseed implementations:

   (a) System level solutions: TPM & TEE; (vedi domande seguenti per approfondire)

   (b) Architectural level solutions: to improve the security of the CPUs and of the involved memories, i.e MPU (da approfondire in questo paragrafo);

   (c) Security-oriented components: special purpose components used for performing specific security-oriented operations such as: hardware cuphers, SIM cards, Random number generator ...;

   (d) Proprietary Solutions vs. Open Security Platforms: Intel, AMD, ARM vs SECUBE, USB armory, OpenTitan (strong cybersecurity features available as open hw (HW acceleretors for cripography, secure boot process ...)).

2.2 Difference between HW security and HW trustworthiness. Slide 1

2.3 Difference between secure HW and trusted HW. Slide 1 Slide 2 per esempi su hardware non sicuro

2.4 Counterfeiting in electronics: types, sources, consequences and threats. Slide 1 Slide 2

2.5 HW-based security: discuss TPM and TEE. Slide 1 Slide 4a per TPM approfondimenti

2.6 Discuss chip design & fabrication flow and sources of threats in the flow. Slide 2

2.7 How to detect chip counterfeiting and its limits. Slide 2

2.8 Make examples of security issues due to unsecure hardware in defence, energy, medical and automotive domains. Slide 2 slide 4a e 4b per automotive

2.9 HW solutions to implement secure update of the SW/FW. slide 4a

2.10 Discuss the TPM specifications for HW security. Slide 1 ma penso sia 4a

2.11 Discuss the SHE specifications for HW security. slide 4a, 5

2.12 Discuss the Evita (small, medium, full) specifications for HW security. slide 4a, 5

2.13 Discuss the typical HW security units that can be found in the HSM of a chip. slide 4a e 4b

2.14 Discuss limits of current cryptographic technologies (AES, SHA, ECC, RSA) in the new post-quantum era. slide 4b

2.15 Discuss the main secure-architectural solutions adopted in the European Processor Initiative. slide 4b

2.16 What is the Panic mechanism and when is it useful? slide 4b

2.17 Side channel attacks: what are they? Ways of implementing side channel attacks? slide 4b

2.18 Discuss the HW for SIM (Subscriber Identity Module). slide 4b

2.19 Briefly review what IEC 62443 is. slide 5

2.20 Hard IP macro and soft IP macro: definition, differences in database organization, licensing costs, in protection of the IP value.

2.20.1 IP Macro

IP macro is a block of logic that can be used in a IC or SOC. It could be a CPU, cryptographic unit, USB o HDMI interface ....

2.20.2 Hard IP macro definition

Hard IP macro is a physical block implemented in our SoC already programmed, having a functional behavior defined and immutable.
Hard IP macro is optimized for a specific technology node and is not reconfigurable. Ready to be integreted in a specific chip and technology. It is a block ready to use like plug and play
Hard IP macro could be a processor or a bluetooth module ...
Hard IP macro are added directly in the layout of the chip.

- Pros: Efficient in prestazioni e consumo, testato e sicuro e sai perfettamente come funziona.
- Cons: Flessibilità pressocche assente e se cambi technology could not work anymore.

2.20.3 Soft IP macro definition

Soft IP Macro is a description od the block, structural e beahavioral description written in HDL.
In this point IP is customizable e portable on many techonologies or FPGA. This code is translated in a netlist of logic elements (logic port, flip-flp, ...) and later on phisically mapped in the layout. cryptographic modulus are Soft IP examples.

1. Write HDL;
2. Logic sysntesis → flip-flop ...
3. Place and Route → phisically mapping
4. Now it is physical circuit like Hard IP.

2.20.4 Differences in database organization

2.20.5 Differences in licensing costs

- Hard IP macro:
    1. Higher costs;
    2. Licensing payment;
    3. Licensing available for a single project or defined number of usage;
    4. Need Non Disclosure Agreement (NDA) to use it;

5. From decine to hundreds of thousands of euros;
6. High commercial value assets;
7. Without source code;

- Soft IP macro:
  1. Lower costs;
  2. The license is often perpetual or site-wide, less binding, more "open".
  3. Vendors also sell soft IP with accessible source code, so it can be easily modified and integrated.

2.20.6 Differences in protection of the IP value.

1. **Technical Value**
   (a) **Soft IP**: Flexible, portable across different devices and technologies. Quality depends on the RTL code. Moderate technical value, but highly reusable and adaptable.
   (b) **Hard IP**: Fully optimized for power, performance, and area. Not modifiable. Used for complex functions (e.g., SerDes, DDR PHY, PCIe). Very high technical value, but context-specific.
2. **Economic Value**
   (a) **Soft IP**: Lower cost, often free or included with EDA tools. Value increases with documentation and reusability. Open-source IPs may have no commercial value but are still technically useful.
   (b) **Hard IP**: Very expensive to develop or license. Can cost tens or hundreds of thousands of euros. High economic value because it reduces project risks and accelerates time-to-market.
3. **Strategic Value**
   (a) **Soft IP**: Useful for prototyping, testing, or educational purposes. Strategic if it can be modified to create proprietary derivatives.
   (b) **Hard IP**: Critical asset in commercial ASICs. Often key to a company's competitive advantage. Very high strategic value in domains like telecom, automotive, AI, etc.

2.21 Discuss if a pure synchronous design is a good solution vs side channel attacks and the possible countermeasures in HW.

2.22 Difference between a True RNG and a CSPRNG in terms of security and throughput.

2.23 What are the trusted zones in a multi-processor system on chip?

2.24 Security mechanisms for memories (MPU, HW protection in SD memory card).

2.25 Difference between a chip for security and an IP macrocell for security.

2.26 Difference between ASICs and FPGAs for security.

2.27 Discuss the acronyms COTS, SoC, MPSoC, FPGA, FPSoC and ASICs.

2.28 Difference between front-end and back-end in the chip design flow.

2.29 What's a Fabless company? Make some examples.

2.30 HW solutions to implement secure boot.

2.31 HW solutions to uniquely identify the HW.

2.32 Discuss correlation among safety and security and needs for confidentiality, integrity, authenticity, traceability (non-repudiation), availability, reliability.

2.33 Why multiple AES modes are typically available in HW?

2.34 Briefly review what UN R155, ISO 21434 and NIS2 directive are.

2.35 What is an anomaly/intrusion detection system and the difference between HW fingerprinting and rule-based IDS.

2.36 Trash, but useful The European Processor Initiative (EPI) is one of the most ambitious projects in the EU to design sovereign, high-performance, and secure processors, especially targeting HPC (High Performance Computing) and automotive markets.

Solutions:

1. **Hardware Root of Trust (HRoT)** Pensa all HRot come il blocco di bedrock di Minecraft.

   Infatti è quel componente hardware sicuro e fidato da cui vengono avviate tutte le operazioni di sicurezza (dovrebbe essere non modificabile da nessuno).

   Se compromesso, allora tutto ciò che ne consegue è a rischio.

   Spesso è un chip dedicato con le funzionalità di verificare crittograficamente il firmware UEFI prima dell'esecuzione, gestione delle chiavi sicure, integrità del sistema e protezione da malware.

2. **Secure Boot e Measured Boot**

   All'accensione del computer, l'Hardware Root of Trust (HRoT) esegue il firmware UEFI. Questo, a sua volta:

   (a) Inizializza l'hardware di base (CPU, RAM, dispositivi I/O ...)

   (b) Avvia il bootloader, che poi carica il sistema operativo in RAM

   Prima di avviare il bootloader, entra in gioco la funzionalità di **Secure Boot**, che ha il compito di **verificare la firma digitale** dei componenti che stanno per essere eseguiti (es. il bootloader stesso). Se la firma non corrisponde a una delle chiavi fidate presenti nel firmware, l'esecuzione viene bloccata.

   Secure Boot può fallire o essere inefficace se:

   - La chiave privata è stata compromessa
   - Secure Boot è stato disattivato o modificato dall'utente
   - Il firmware UEFI stesso è stato compromesso → viene meno la Root of Trust

   In parallelo al Secure Boot viene avviato anche il **Measured Boot**, che **calcola e registra gli hash** dei componenti caricati durante la fase di avvio. Questi hash vengono salvati nel TPM (Trusted Platform Module) per poter essere **analizzati successivamente** (es. in ambiente aziendale, per rilevare modifiche sospette).

   Measured Boot non blocca l'avvio, ma fornisce una traccia affidabile dello stato del sistema al momento dell'accensione.

   HRoT → avvia firmware UEFI → Secure Boot and Measured Boot

3. **Memory Protection and Encryption**

L'architettura del sistema prevede l'utilizzo di **Memory Management Unit (MMU)** avanzate, che implementano controlli di accesso granulari per isolare i diversi processi e livelli di privilegio.

In aggiunta, è supportata la **crittografia della RAM in tempo reale**, una misura fondamentale in scenari dove è plausibile un attacco con accesso fisico al dispositivo (es. dispositivi edge, sistemi automotive, ambienti IoT).

Questa protezione contribuisce a garantire sia la **confidenzialità** che l'**integrità** dei dati in uso, contrastando attacchi come cold boot, DMA attacks, o dump della memoria.

La **Memory Management Unit (MMU)** è un componente dell'architettura della CPU che gestisce:

- la traduzione degli indirizzi virtuali in indirizzi fisici (*paging*);
- i controlli di accesso alla memoria (lettura, scrittura, esecuzione).
- impedisce a un processo in *user mode* di accedere alla memoria del *kernel*;
- impedisce a un processo di accedere alla memoria di altri processi.

Durante l'esecuzione, i dati sensibili (es. password, chiavi crittografiche) risiedono in chiaro nella RAM. Chi ha accesso fisico al dispositivo può eseguire attacchi come:

- **Cold Boot Attack**: congelamento e lettura fisica della RAM;
- **DMA Attack**: accesso diretto alla memoria tramite interfacce ad alta velocità (es. Thunderbolt, PCIe).

Per contrastare questi attacchi, alcune architetture prevedono la **crittografia automatica della RAM** in tempo reale. In questo schema:

- Il controller di memoria cifra/decripta i dati in ingresso e uscita dalla RAM;
- La chiave crittografica viene generata all'avvio tramite un *True Random Number Generator* (TRNG);
- La chiave non è mai esposta al sistema operativo né all'utente;
- Se il sistema si spegne o riavvia, la chiave va persa, rendendo i dati in RAM illeggibili.

Implementazioni reali di questa tecnologia includono:

- **AMD SME (Secure Memory Encryption)**: crittografia trasparente dell'intera RAM con una chiave hardware;
- **Intel TME (Total Memory Encryption)**: approccio analogo con chiave crittografica gestita internamente dalla CPU.

4. **Hardware Isolation & Secure Execution Environments**

5. **Secure Interconnects and I/O Protection**
6. **Support for Post-Quantum Cryptography (PQC)**
7. **Side-Channel Attack Mitigation**
8. **Secure Debug and Update Mechanisms**