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 Saponara

2 Nannipieri

3 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.

3.1 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.

3.2 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.

3.3 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;

3.4 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.

3.5 Process Variation Inter-Die Variations: due chip identici prodotti nello stesso lotto possono avere caratteristiche elettriche leggermente diverse.

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.

3.6 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.

3.7 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;

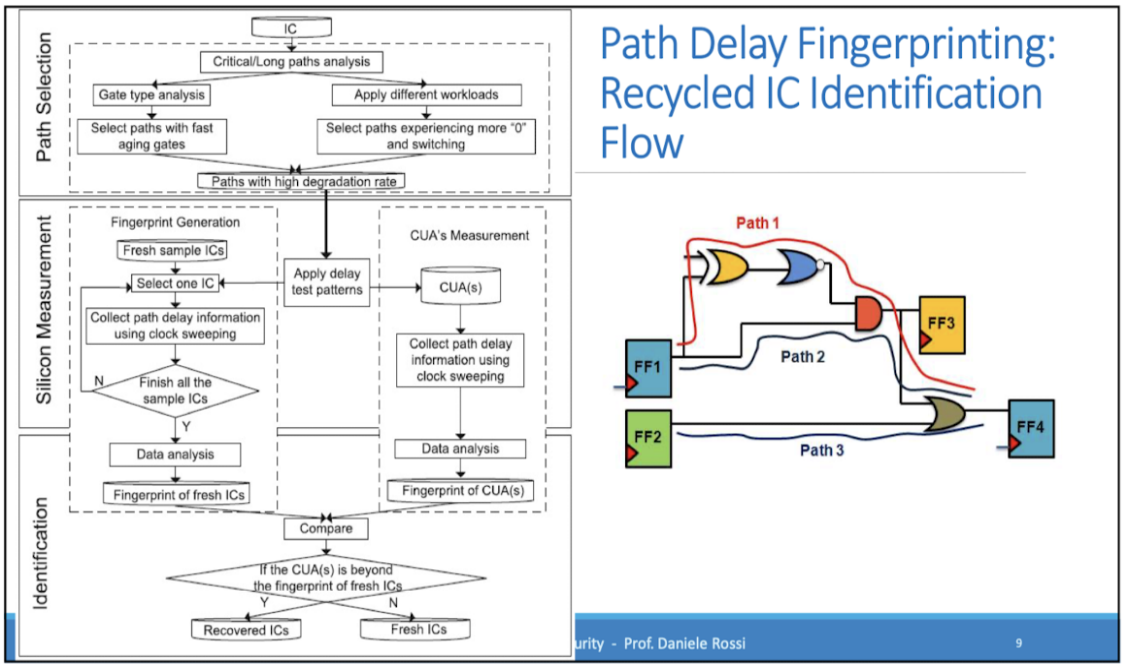
3.8 Path Delay Analysis Path Delay Fingerprinting è una tecnica che permette di identificare un chip tramite il degrado delle prestazioni senza usufruire di ulteriore hardware dedicato alla registrazione di aging.

Con degrado delle prestazioni ci si riferisce al tempo che i chip impiegano per eseguire operazioni funzionali → Ritardi più grandi ↔ 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 ($\forall$ 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.

3.9 Clock Sweeping