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.

3.3 Power consumption

- Static power consumption: corrente assorbita quando il circuito è in stato statico (non cambia stato);
- Dynamic power consumption: corrente assorbita quando il circuito cambia stato.
- Short-circuit power consumption: corrente assorbita quando i transistor sono in stato di corto circuito sempre durante il cambio di stato.

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).

3.5 Process Variation

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.