
Telsy
Defining Security Since 1971
Telsy

Aspetti implementativi della crittografia

Andrea Molino – *FPGA & Embedded Systems R&D Engineer @ TELSY*

Telsy

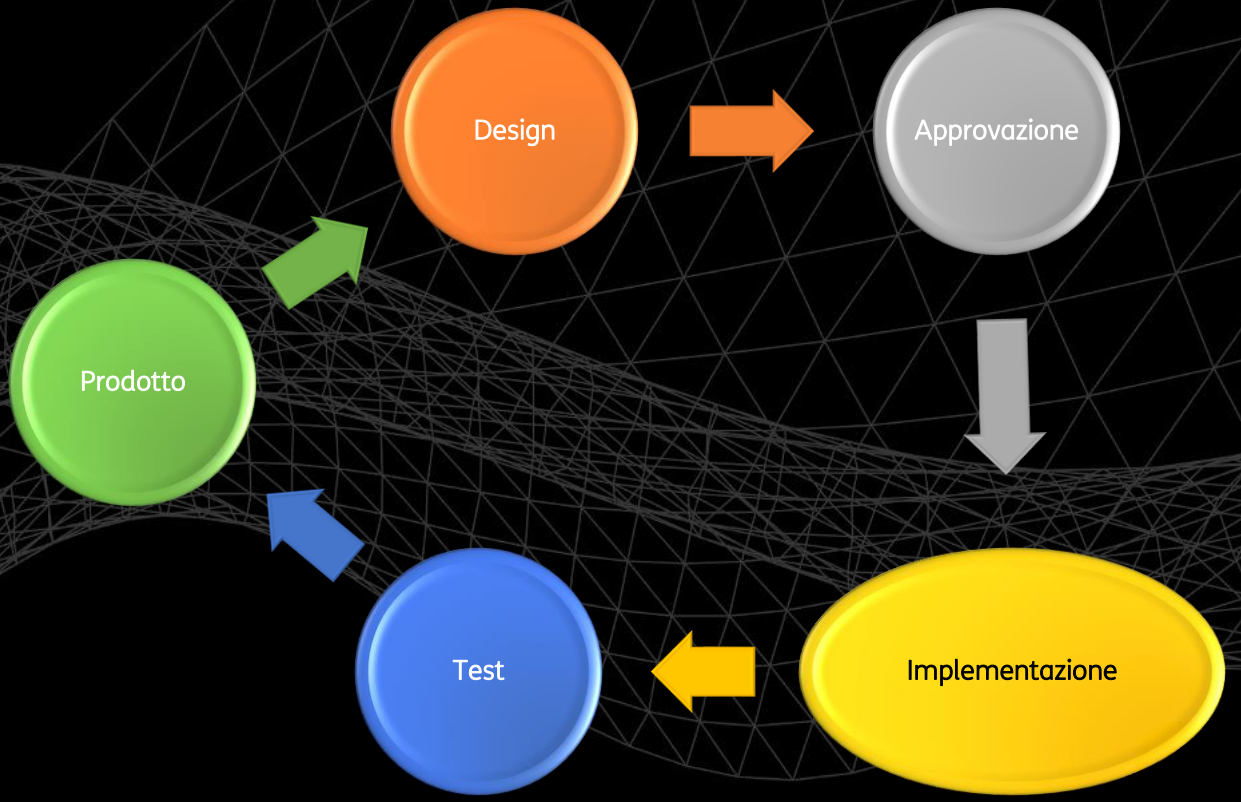
TELSY – profilo dell’azienda

- Fondata nel 1971
- Oggi 100% gruppo TIM
- Specializzata in crittografia e cybersecurity
- Implementazione di algoritmi sia SW che HW
- Applicazioni in ambito governativo e civile
- Sotto Golden Power
- Fortemente attiva nella ricerca

Telsy

Dall’idea al prodotto

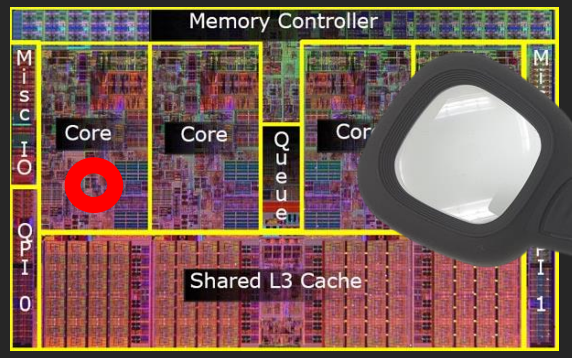
- Implementare algoritmi di cifratura e schemi di sicurezza pensati all’interno dell’azienda «*design thinking crittografico*»
- Design conscio delle opzioni e delle possibili difficoltà implementative

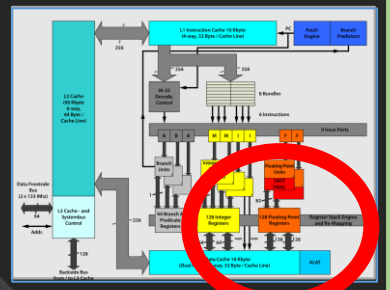


Telsy

Diverse opzioni a disposizione (1)

CPU

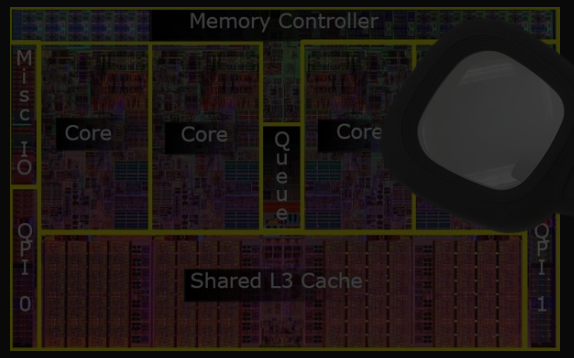


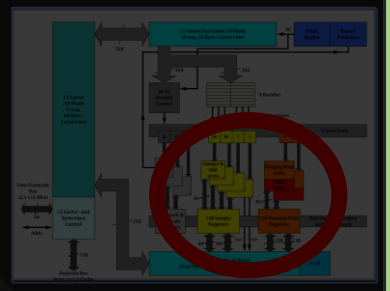


1-8 core

Diverse opzioni a disposizione (2)

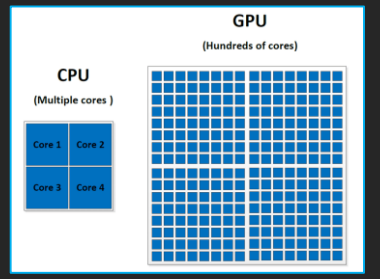
CPU





1-8 core

GPU

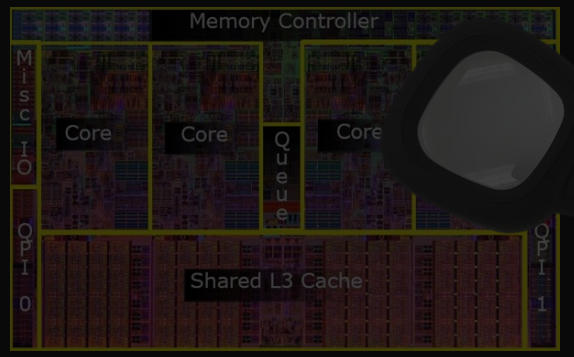


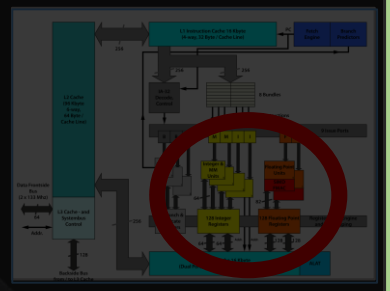
100-1k Processing Units

Telsy

Diverse opzioni a disposizione (3)

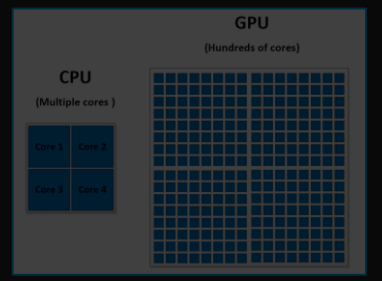
CPU





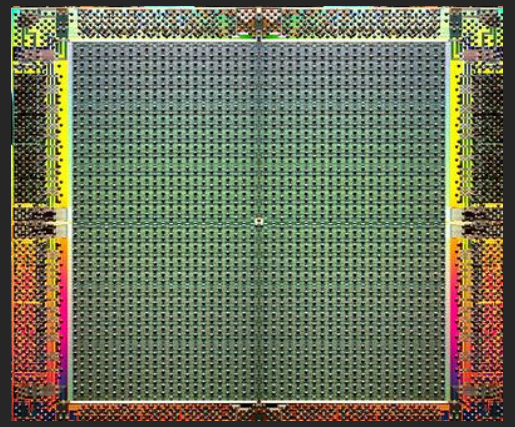
1-8 core

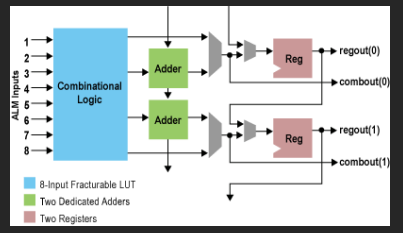
GPU



100-1k processing units

FPGA



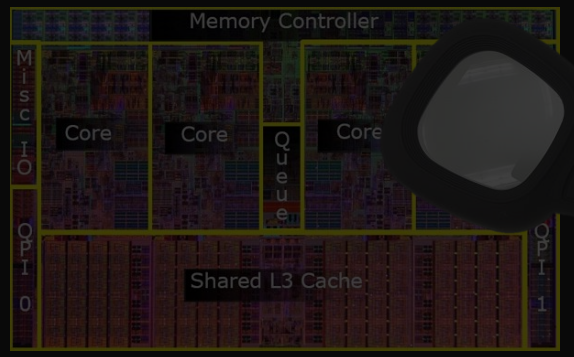


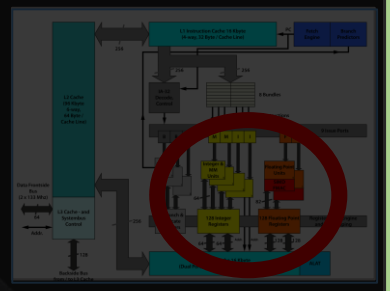
100k-1M Logic Blocks

Telsy

Diverse opzioni a disposizione (4+)

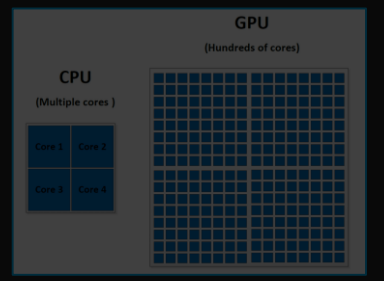
CPU





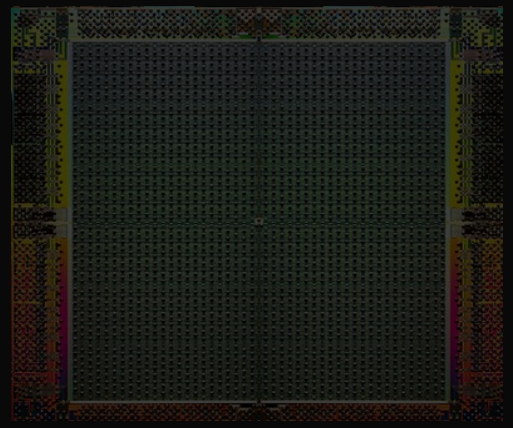
1-8 core

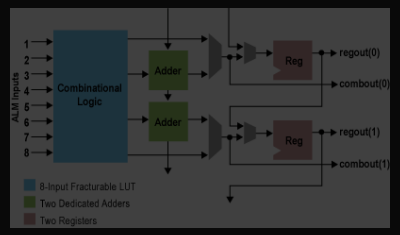
GPU



100-1k processing units

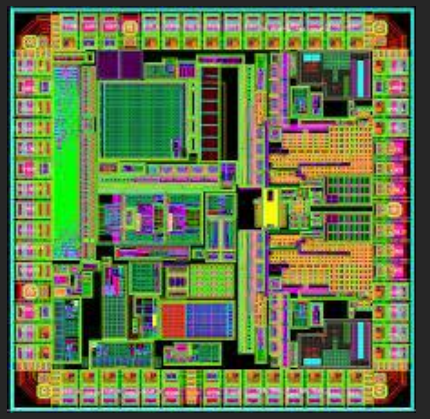
FPGA





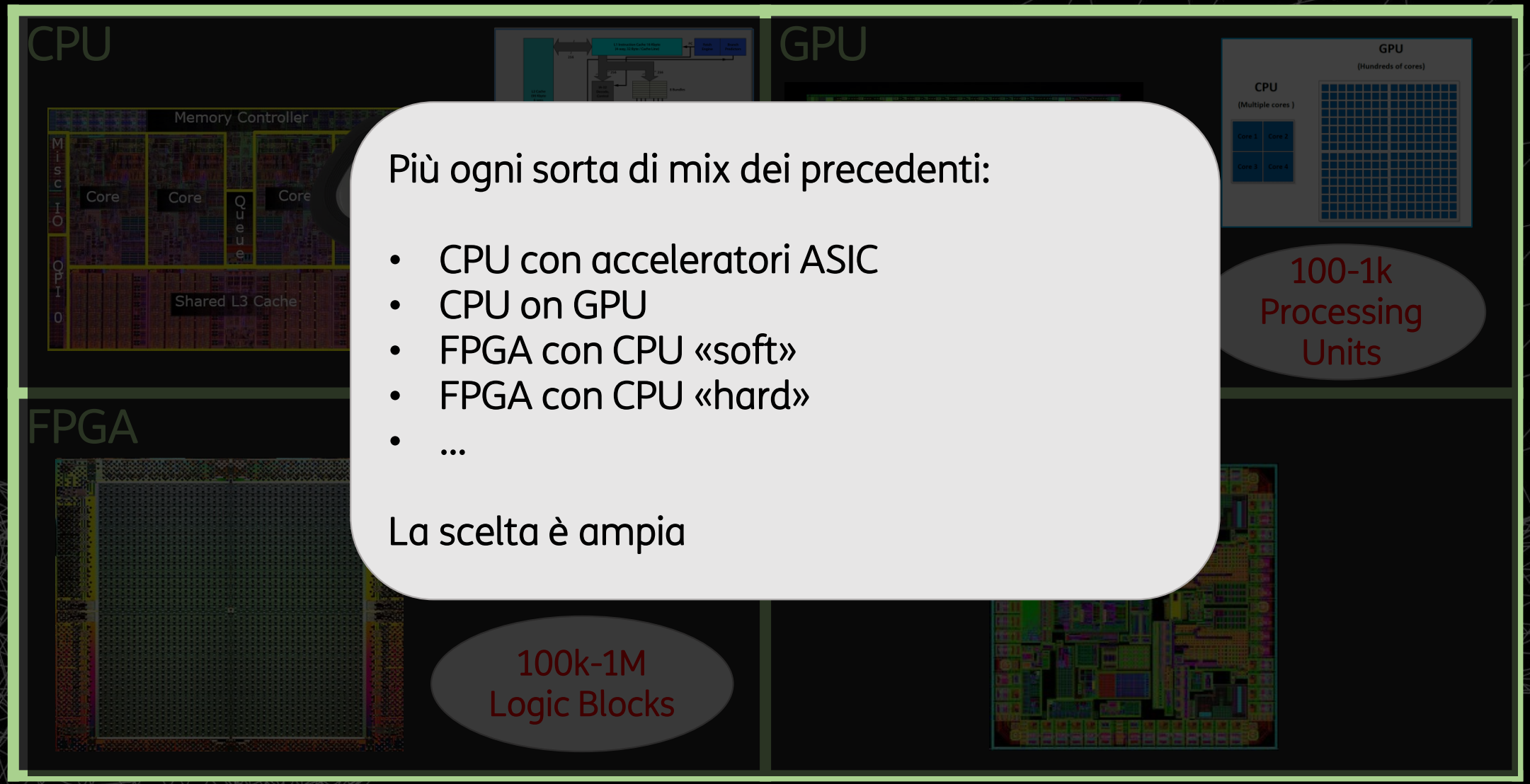
100k-1M Logic Elements

ASIC (fully custom)



Telsy

Diverse opzioni a disposizione



Più ogni sorta di mix dei precedenti:

- CPU con acceleratori ASIC
- CPU on GPU
- FPGA con CPU «soft»
- FPGA con CPU «hard»
- …

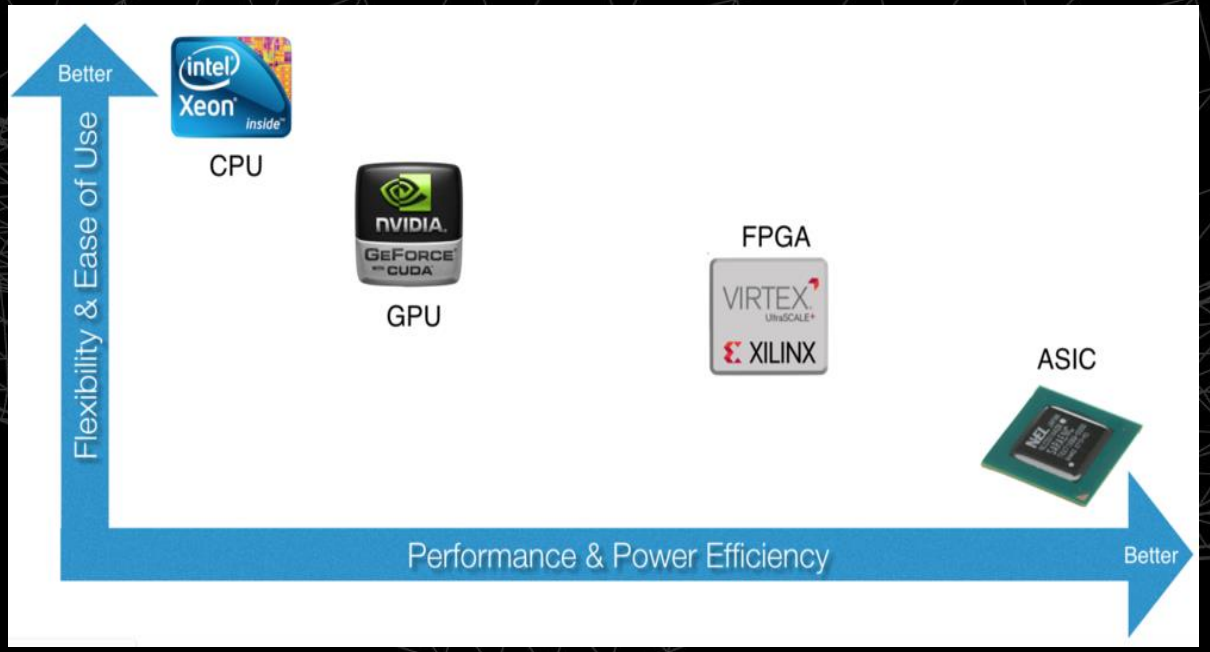
La scelta è ampia

Telsy

Prestazioni a confronto

- E’ molto difficile estrarre dei dati assoluti
- L’ordine di grandezza come velocità di elaborazione è il seguente (caso di studio AES256) :

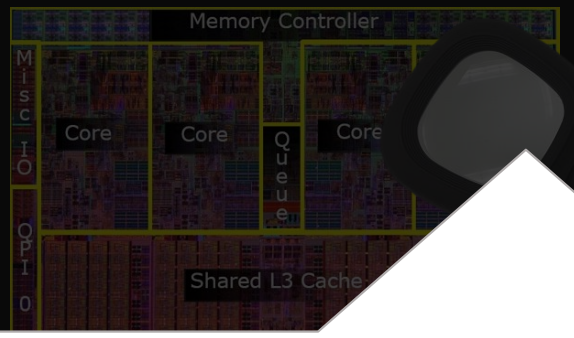
  - CPU smartphone : 1 → 10 Mbit/s
  - CPU workstation : 10 → 100 Mbit/s
  - GPU : 100Mbit/s → 1Gbit/s
  - FPGA/ASIC : 1Gbit/s → 10Gbit/s

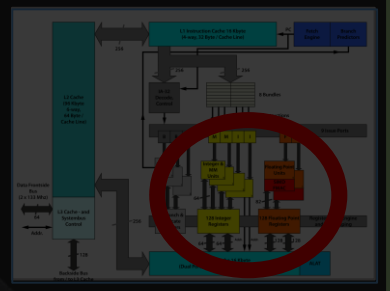


Telsy

Diverse opzioni a disposizione

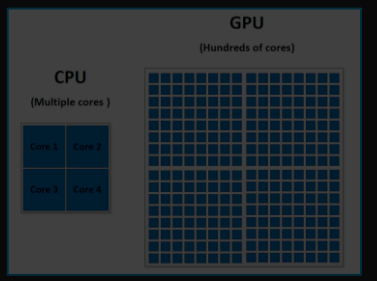
CPU





1-8 core

GPU



100-1k processing units

FPGA

Mix vari

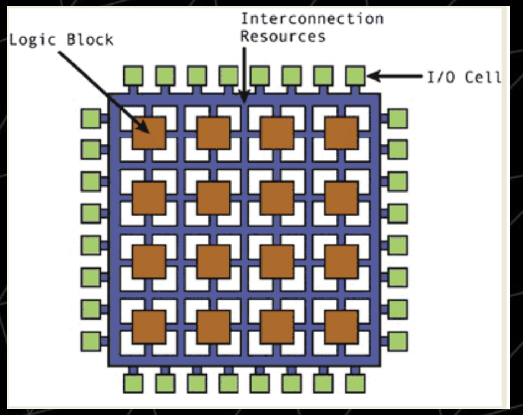
- CPU con acceleratori HW
- CPU on GPU
- FPGA con CPU «soft»
- FPGA con CPU «hard»

...

Telsy

FPGA: diverse tecnologie per diversi contesti applicativi

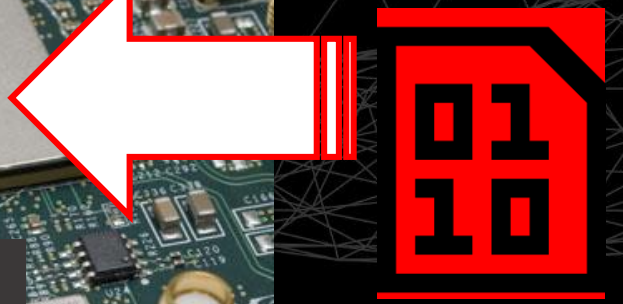
La configurazione del dispositivo è effettuata scaricando un file di configurazione (bitfile) in una memoria contenuta nel dispositivo, che imposta i singoli Logic Block e determina le connessioni tra essi



- FLASH: configurazione permanente
- RAM: configurazione volatile
- Riconfigurazione parziale
- FPGA in piattaforme *cloud*

Lo sviluppo utilizza linguaggi specifici

E richiede competenze «hardware» …



«configurare» e non «programmare» …

Telsy

FPGA: la sicurezza

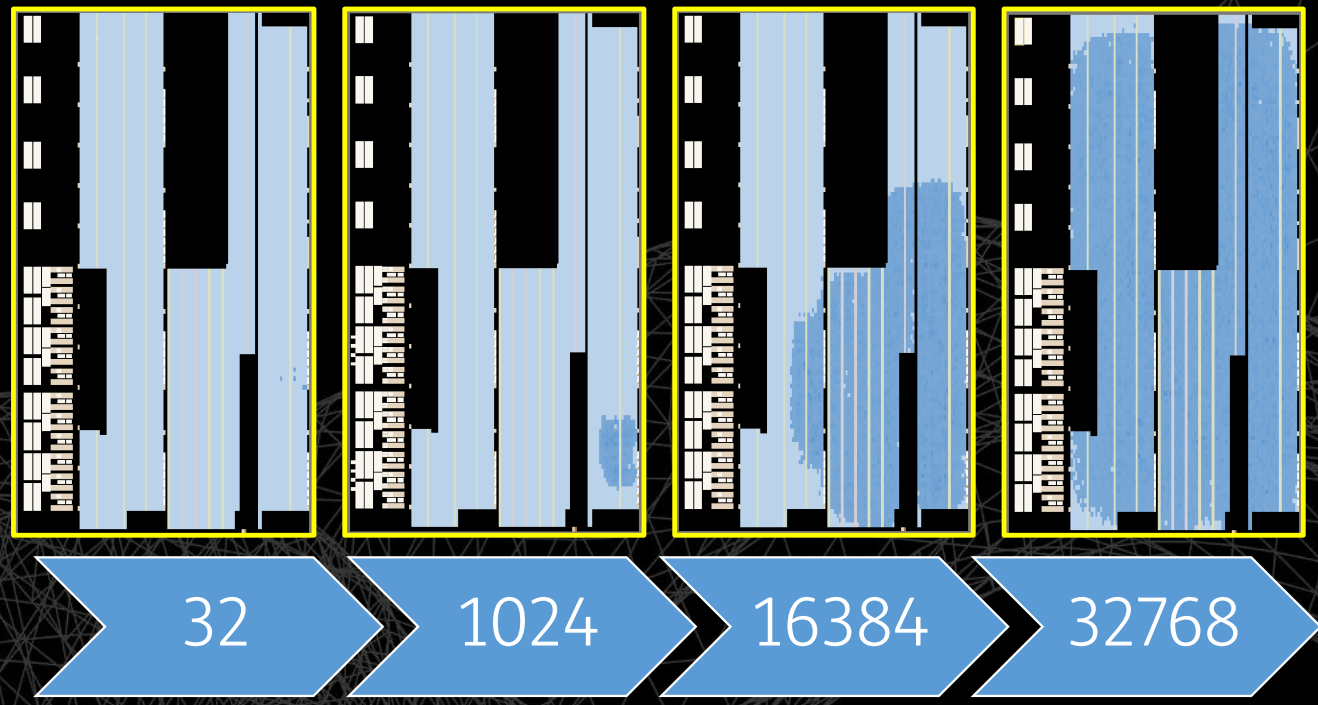
- Reverse *engineering* più difficile a partire dal contenuto del bitfile
- Possibilità di utilizzare *bitfile* cifrati con chiave volatile tenuta nel dispositivo

- Sensori di *antitampering* integrati e memoria chiave volatile alimentata con batteria tampone
- Possibilità di « offuscare » il circuito implementato e determinarne un *mapping* complesso per irrobustire le difese ad attacchi di tipo *side channel*

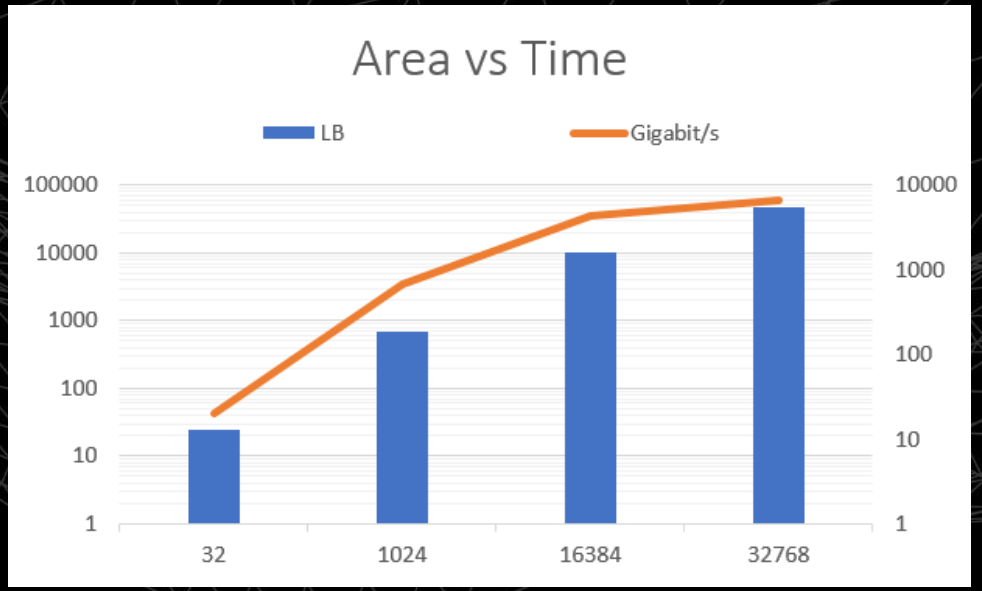
Telsy

La versatilità: esempio XOR tra vettori

- Area vs Time
- Possibilità di esplorare tutti gli spazi di implementazione (*pipelining*)



XOR tra due vettori di <k> bit



Telsy

In conclusione

- I dispositivi programmabili di nuova generazione offrono grandi prestazioni e margini di compromesso per adattarsi ai diversi contesti (consumi di energia/potenza)
- Piattaforme come le FPGA sono sempre più accessibili sia come costi di approvvigionamento che come *effort* di sviluppo, ma richiedono ancora competenze specifiche
- In Telsy poter ragionare sugli aspetti implementativi fin dalle prime fasi del progetto è un grande valore aggiunto che diminuisce le iterazioni di processo

Grazie per l’attenzione

Telsy