

Arbiter PUF implementation on FPGA

Prof. Christiancarmine Esposito

Salvatore Ruocco
Mat. 0512115080



ARBITER CHE?

Contenuti



Crittografia e sicurezza

Leggere chiavi private su un dispositivo



PUF

Una soluzione al problema



FPGA

Dove ho implementato e testato la PUF



Conclusione


Analisi dei risultati ottenuti



1

Crittografia e sicurezza

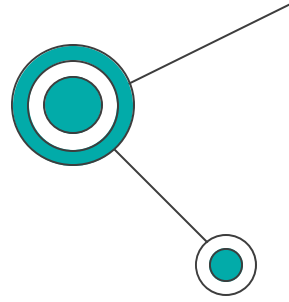
Leggere chiavi private salvate su un
dispositivo





Che cos'è la **crittografia**?

E' una tecnica usata per rendere le informazioni illeggibili a chi non ha il permesso di leggerle.





Che cos'è la **crittografia**?

E' una tecnica usata per rendere le informazioni illeggibili a chi non ha il permesso di leggerle.

**Caro Babbo
Natale**



Che cos'è la **crittografia**?

E' una tecnica usata per rendere le informazioni illeggibili a chi non ha il permesso di leggerle.

**Caro Babbo
Natale**



Algoritmo di crittografia



Che cos'è la **crittografia**?



E' una tecnica usata per rendere le informazioni illeggibili a chi non ha il permesso di leggerle.

**Caro Babbo
Natale**

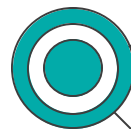


Algoritmo di crittografia

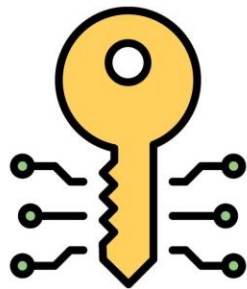
**gchdsjvkbshdbc
rhejvbehrejvbhj**



Che cos'è una **chiave crittografica**?

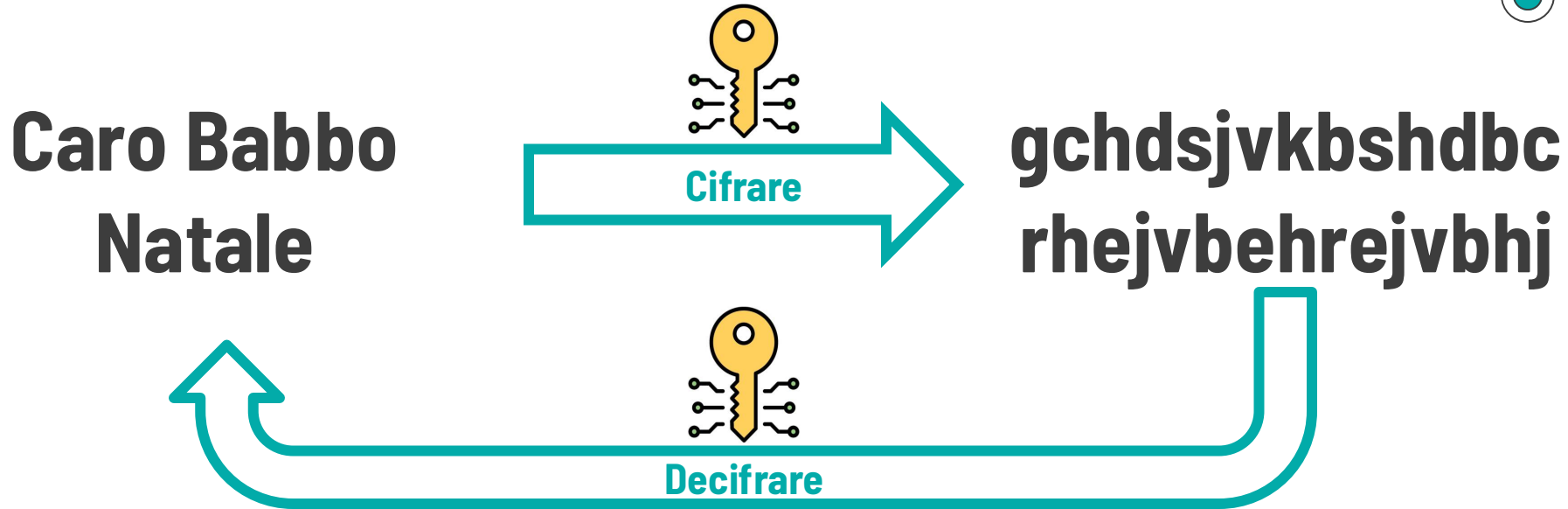


● Che cos'è una **chiave crittografica**?

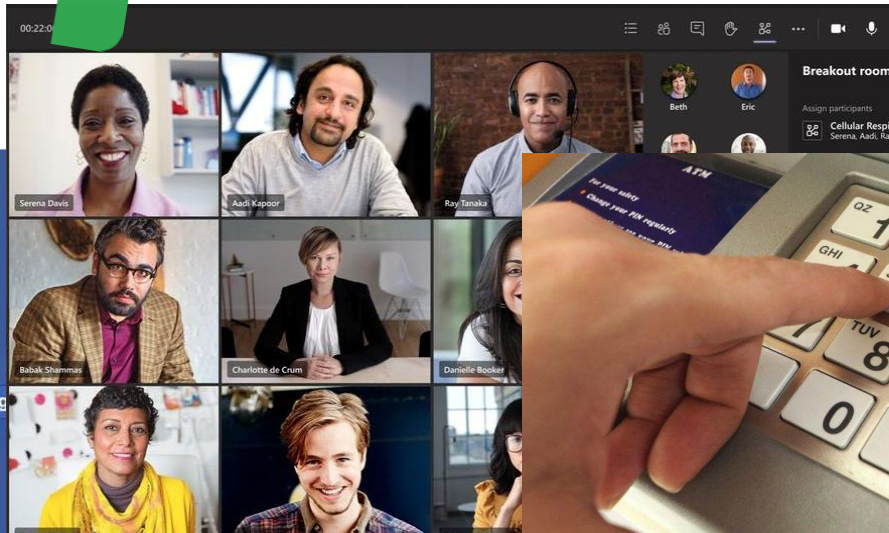
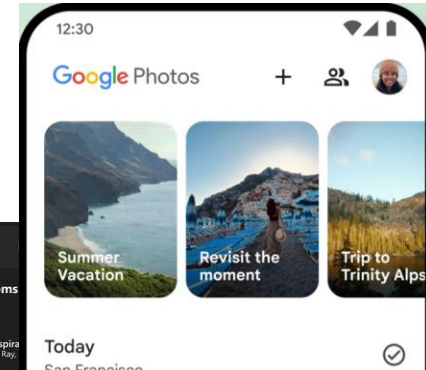


È una sorta di PASSWORD

Che cos'è una **chiave crittografica**?

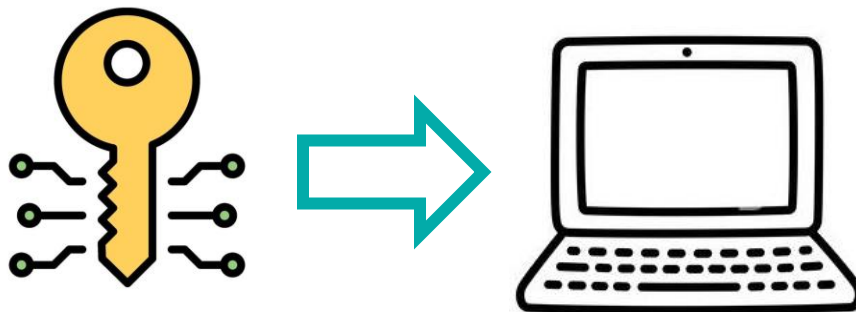
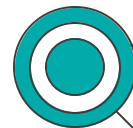


A cosa serve?



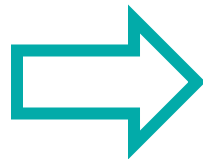
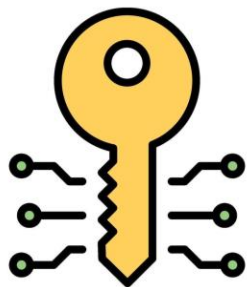
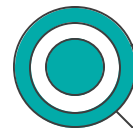


Hackerare una chiave crittografica





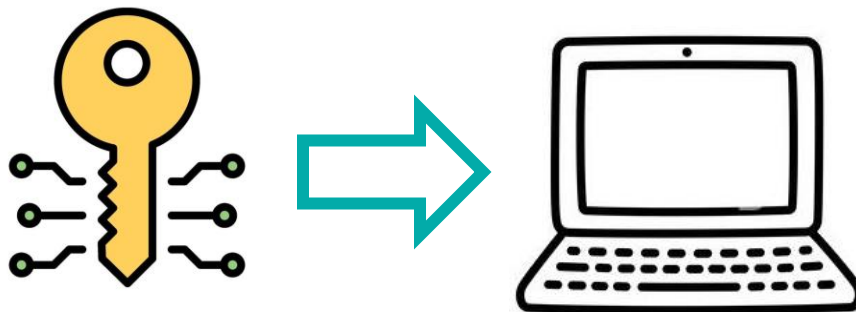
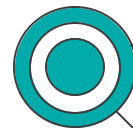
Hackerare una chiave crittografica



**Memoria
vulnerabile!!**



Hackerare una chiave crittografica



**Difficile
correggere**

**Memoria
vulnerabile!!**

Hackerare una chiave crittografica



SPECTRE

2018
90%
PROCESSORI



2

PUF

Una soluzione al problema





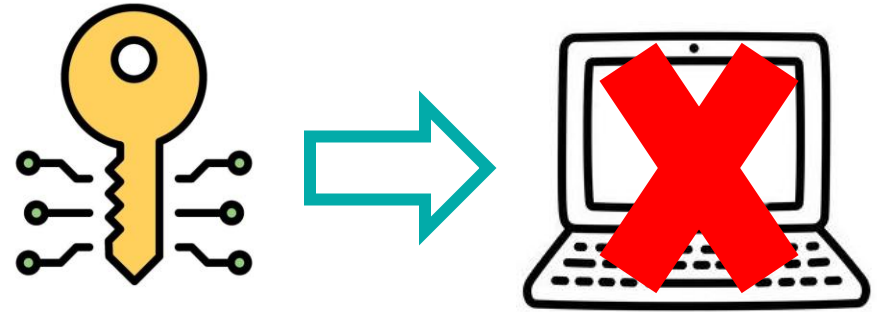
Che cos'è una PUF?



Physical Unclonable Function

Che cos'è una **PUF**?

Physical
Unclonable
Function



Ottenere **chiavi crittografiche**
quando ne abbiamo bisogno,
senza salvarle su un dispositivo.

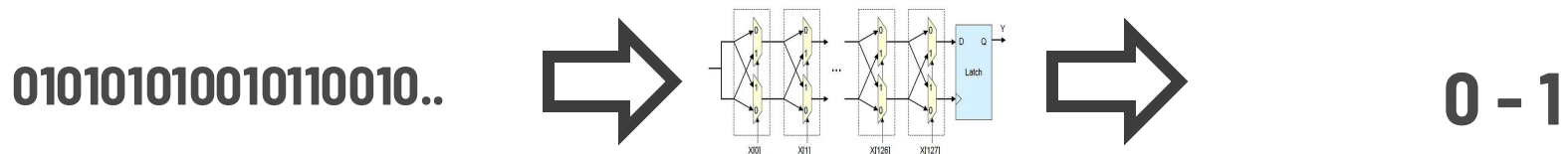
Che cos'è una **PUF**?

Physical
Unclonable
Function

Sfruttano imperfezioni fisiche
presenti sui chip per generare
randomicità.



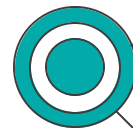
Come funziona una PUF?





Proprietà fondamentali di una PUF

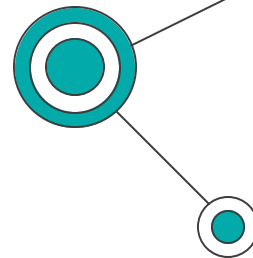
Senza le quali una PUF non può essere definita tale





Proprietà fondamentali di una PUF

Senza le quali una PUF non può essere definita tale



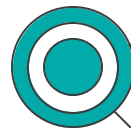
1

Unicità



Proprietà fondamentali di una PUF

Senza le quali una PUF non può essere definita tale



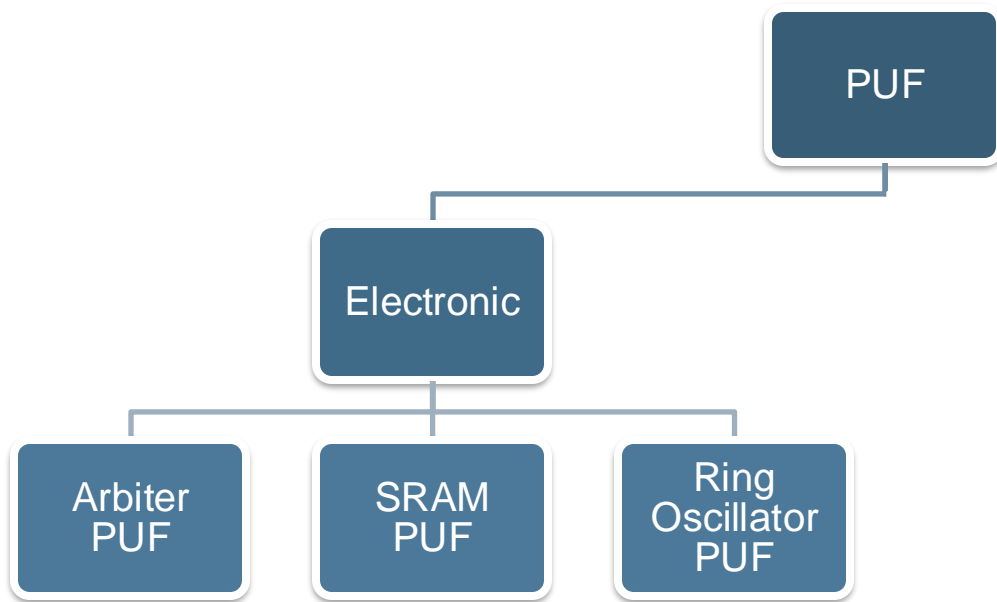
1

Unicità

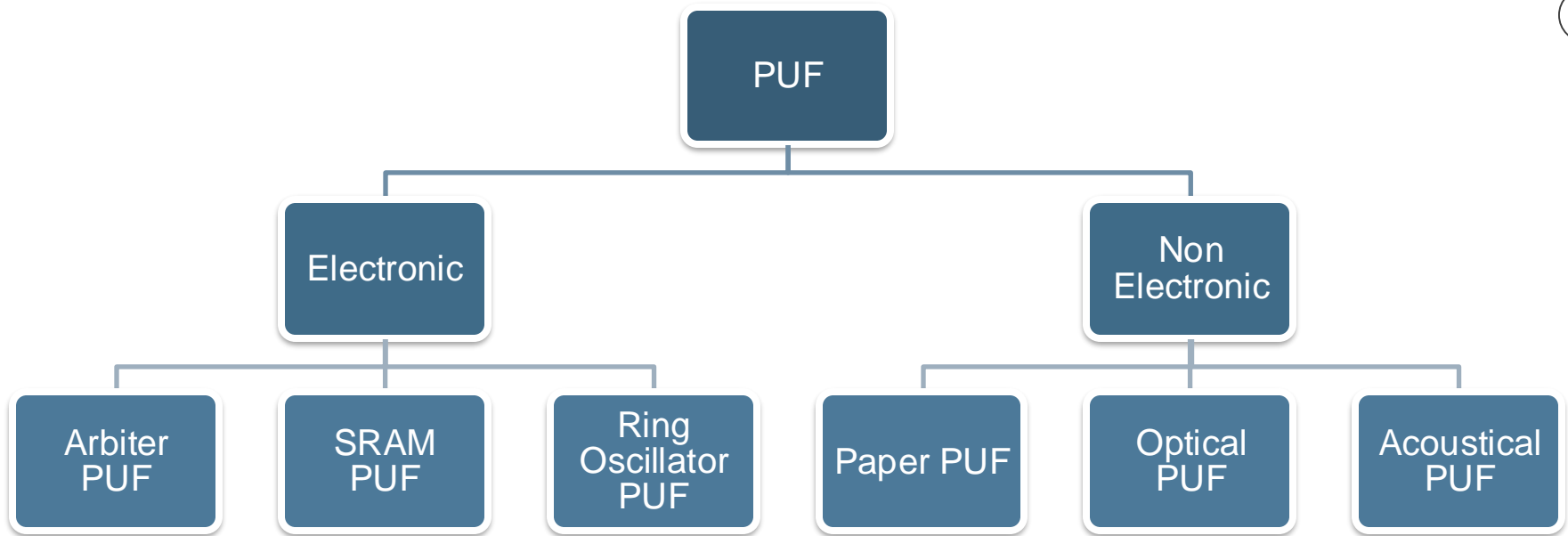
2

Imprevedibilità

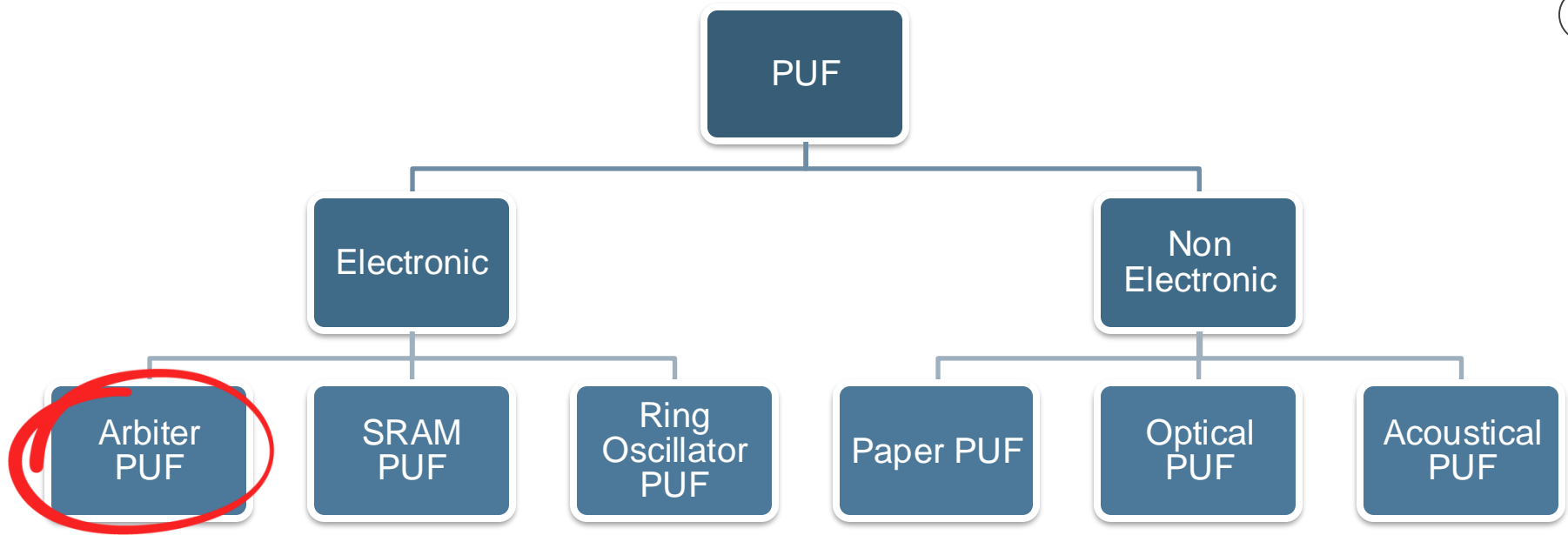
Diversi **tipi** di PUF



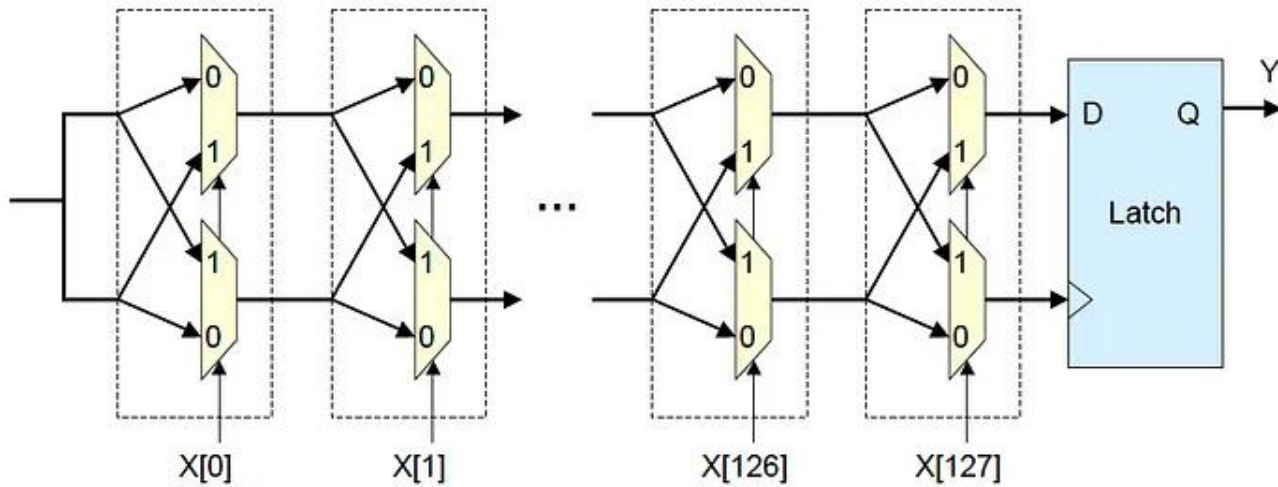
Diversi tipi di PUF



Diversi tipi di PUF

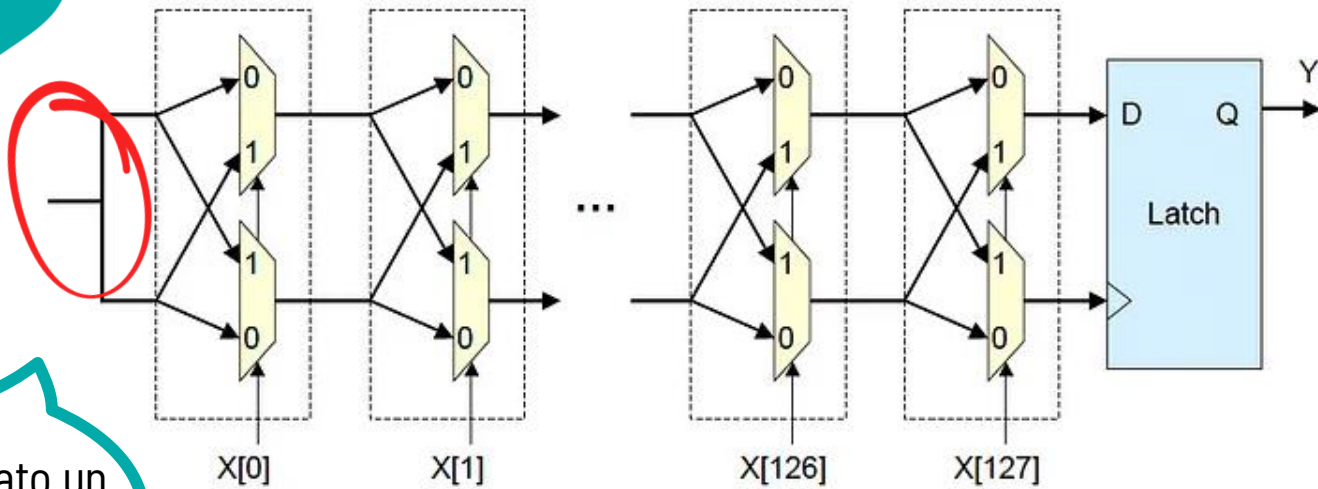


Arbiter PUF



Arbiter PUF

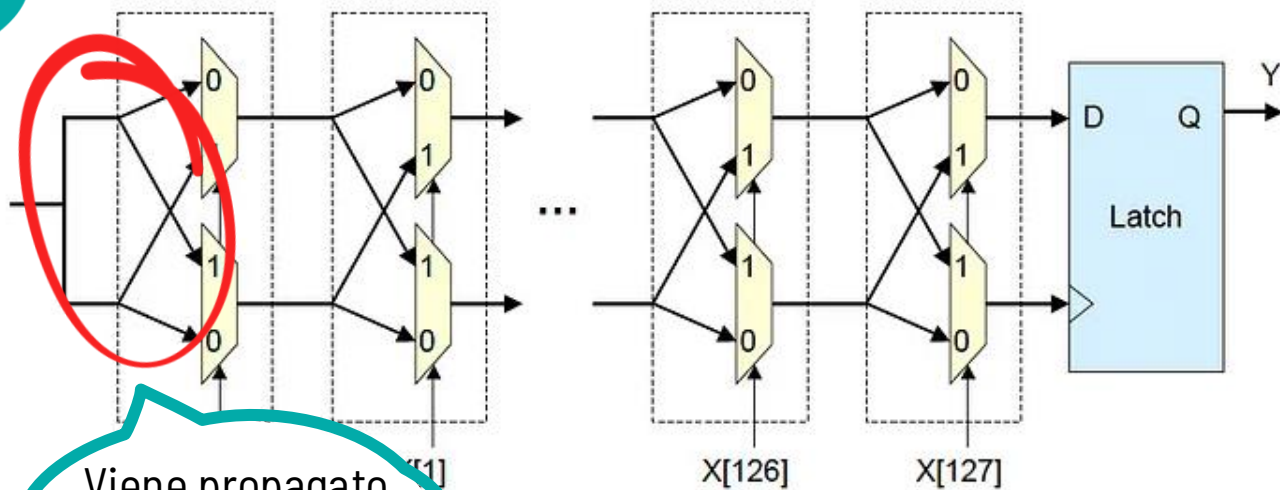
1



Viene inviato un
segnale
elettronico

2

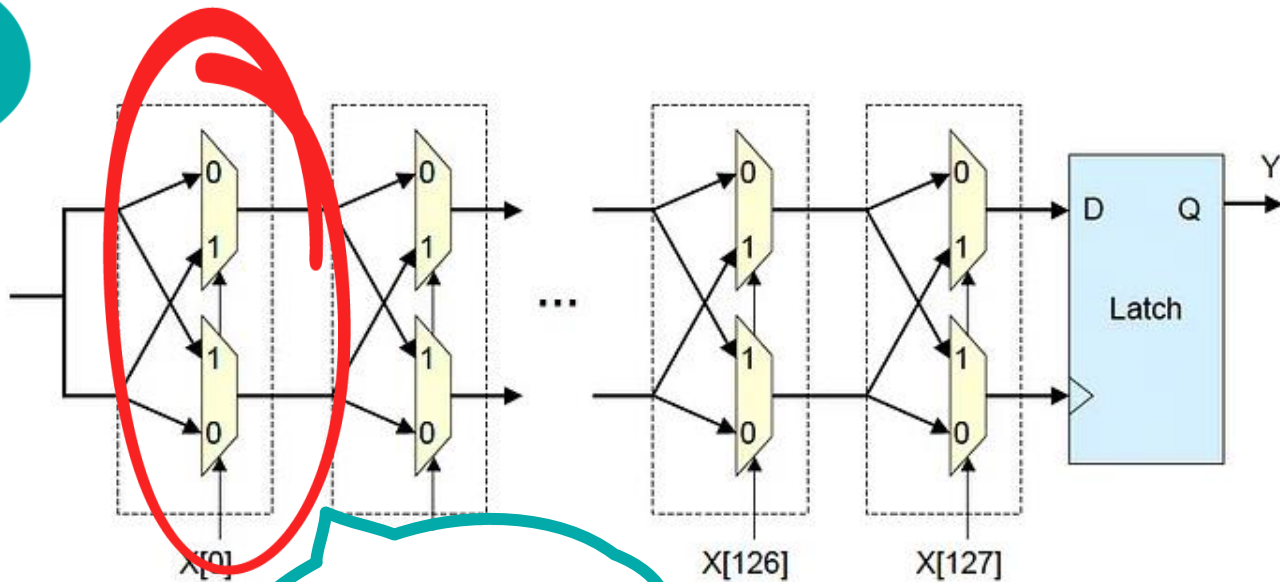
Arbiter PUF



Viene propagato
su 2 percorsi
paralleli

3

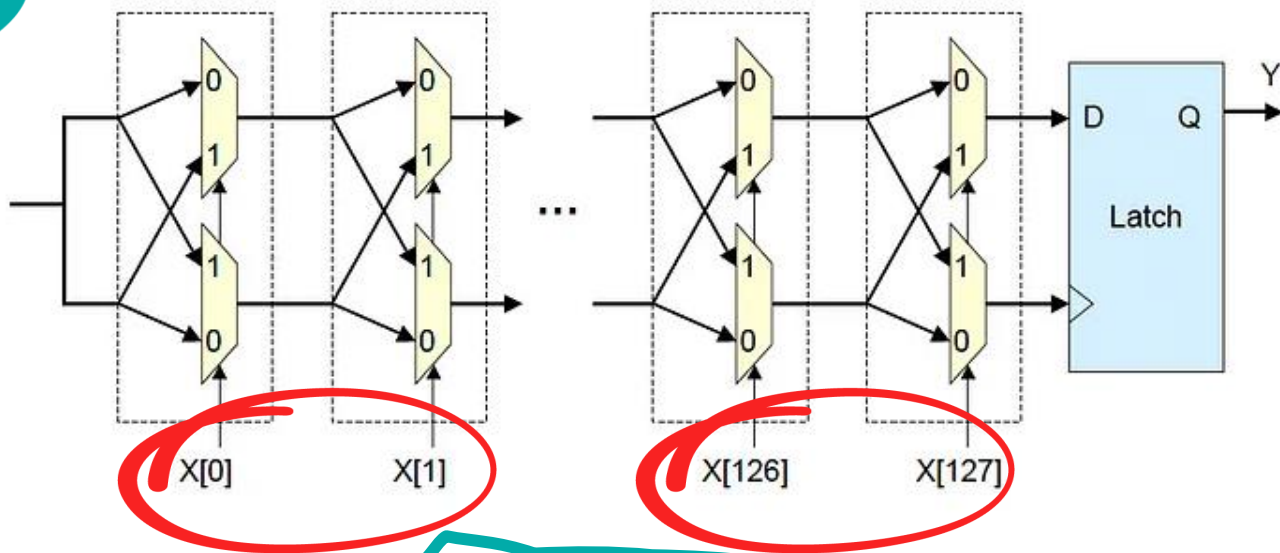
Arbiter PUF



Lungo il percorso
ci sono dei blocchi
di multiplexer

4

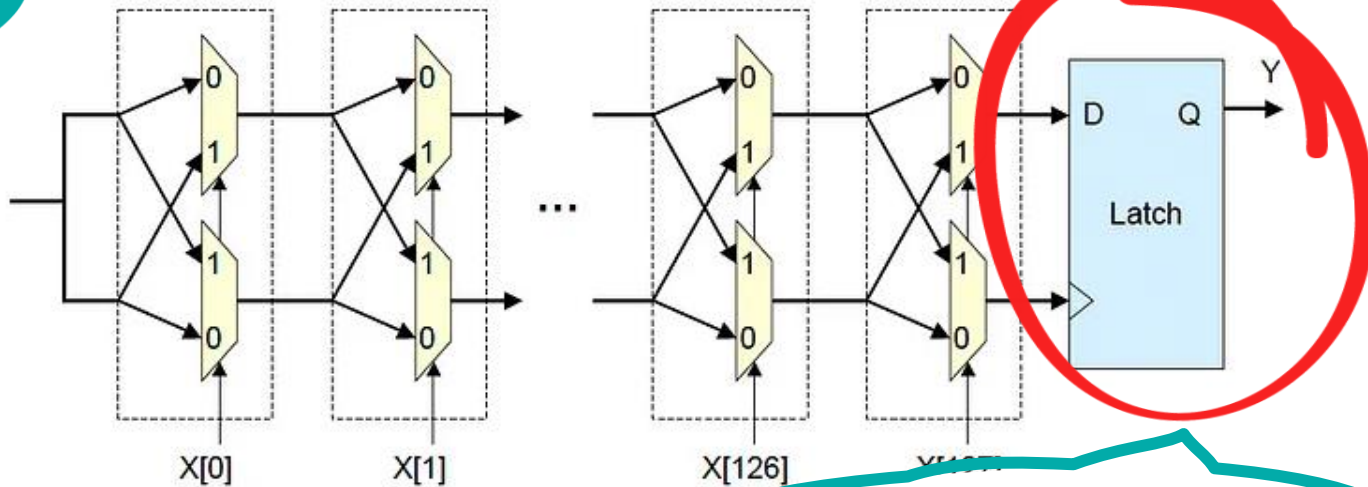
Arbiter PUF



I bit di selezione dei multiplexer, ovvero la challenge della PUF

5

Arbiter PUF



Alla fine, c'è un arbitro che stabilisce
il segnale arrivato per primo



3

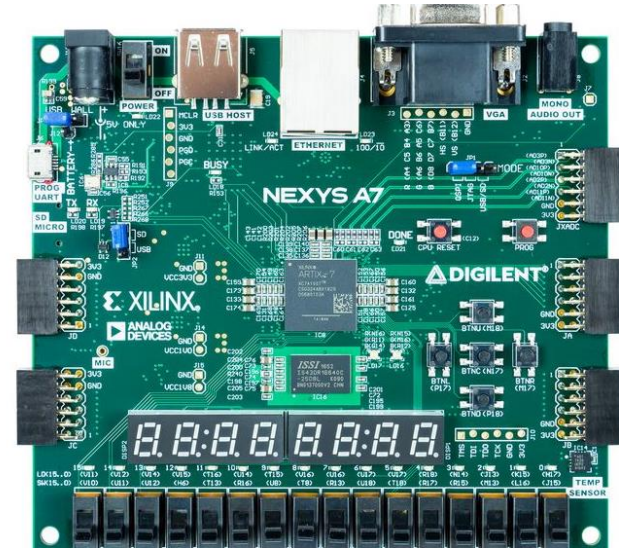
FPGA

Dove ho implementato e testato la
PUF



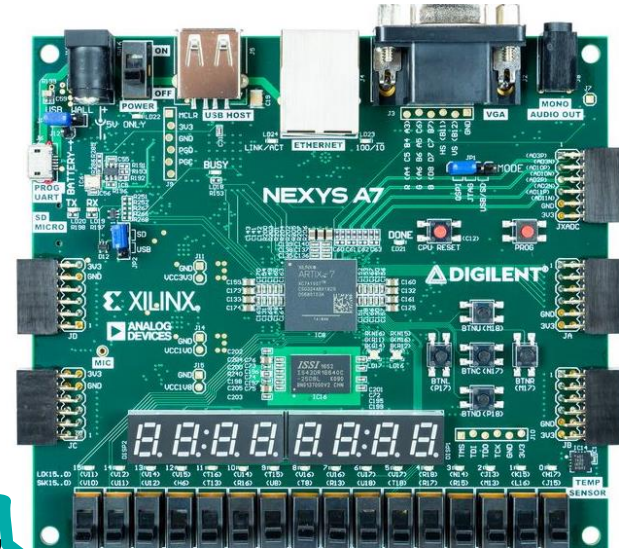
Field Programmable Gate Array

Che cos'è un **FPGA**?



Che cos'è un **FPGA**?

Field
Programmable
Gate
Array



Nexys A7
di Xilinx

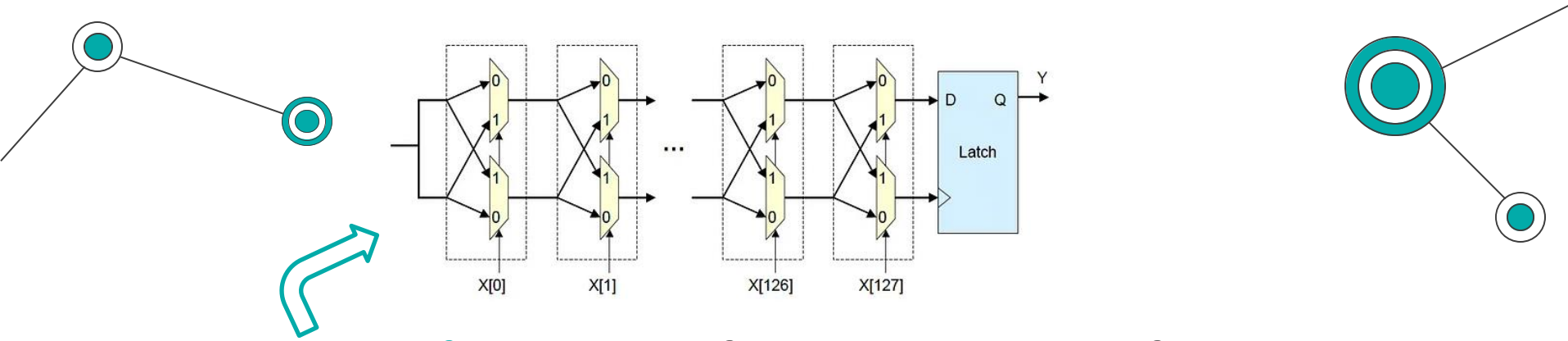
Che cos'è un **FPGA**?

Utile per
disegnare
processori

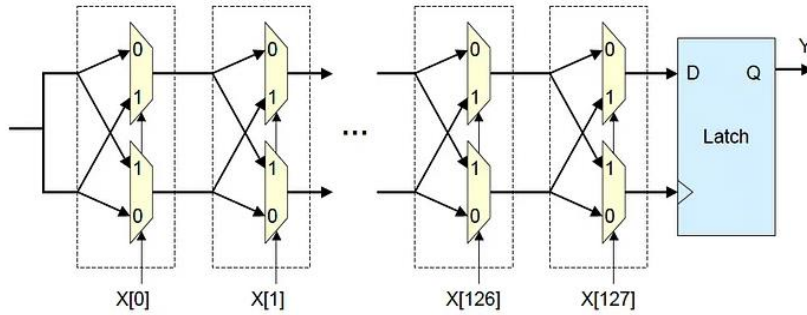




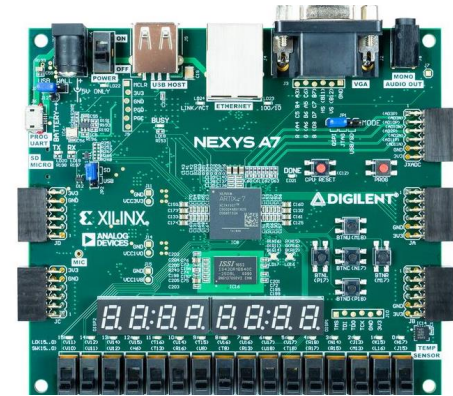
Arbiter PUF implementation on FPGA



Arbiter PUF implementation on FPGA



Arbiter PUF implementation on FPGA



4

Conclusione

Analisi dei risultati ottenuti



● Metriche utilizzate per valutare la PUF



● Metriche utilizzate per valutare la PUF

1

Uniformità

**Calcolare la proporzione di 0 e 1 in più response.
Idealmente dovrebbe essere vicina al 50%**

Metrische utilizzate per valutare la PUF

1

Uniformità

Calcolare la proporzione di 0 e 1 in più response.
Idealmente dovrebbe essere vicina al 50%

Esempio

001110

Numero di 0: 3

Numero di 1: 3



Uniformità = 50%

Metrische utilizzate per valutare la PUF

1

Uniformità

Calcolare la proporzione di 0 e 1 in più response.
Idealmente dovrebbe essere vicina al 50%

Esempio

001110

Numero di 0: 3

Numero di 1: 3



Uniformità = 50%

47%



◎ **Metriche** utilizzate per valutare la PUF

2

Stabilità

**Dare in input alla PUF la stessa challenge e verificare che produca la stessa response.
La percentuale deve essere il più vicino possibile al 100%**

97,99%

● **Metriche** utilizzate per valutare la PUF

3

Randomicità

Dare in input challenge simili ma diverse per assicurarci che le responses non si assomiglino.

Esempio

01010011

0101001**0**

11010011

0**0**010011

99,01%

Grazie!

Salvatore Ruocco

