Ciberseguridad en Sistemas Físicos

Análisis de canal lateral

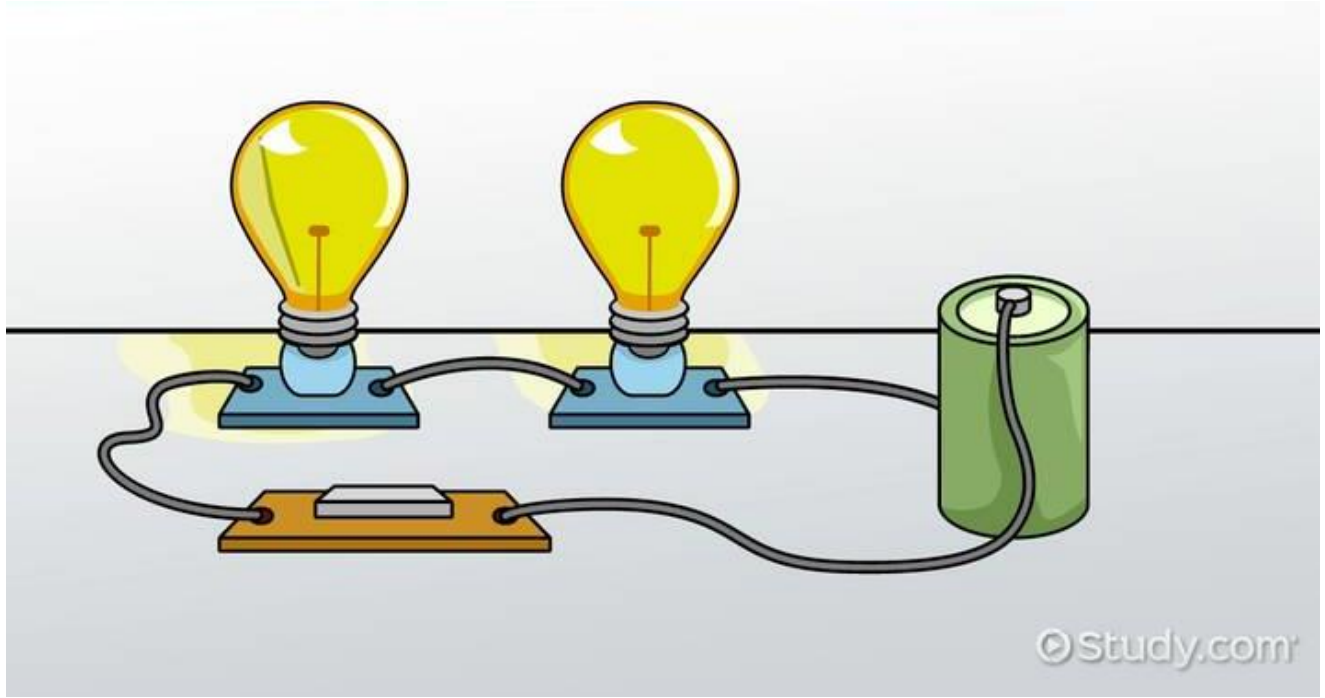
Servio Paguada, Ph.D

Agenda

1. Lo básico
2. Canal lateral.
3. Implementación de algoritmos criptográficos.
4. Ataques de canal lateral usando redes neuronales.
5. Protecciones contra ataques de canal lateral.
6. Video demostración (Lennert Wouters - KU Leuven).

0.

Lo Básico.



ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Definiciones.

Algoritmo criptográfico: Algoritmo que, dado un texto original, es capaz de generar otro texto con la codificación suficiente, que nadie puede determinar el texto original solo con leerlo.

Texto plano: El texto original antes de ser cifrado.

Texto encriptado: El texto resultado del algoritmo criptográfico.

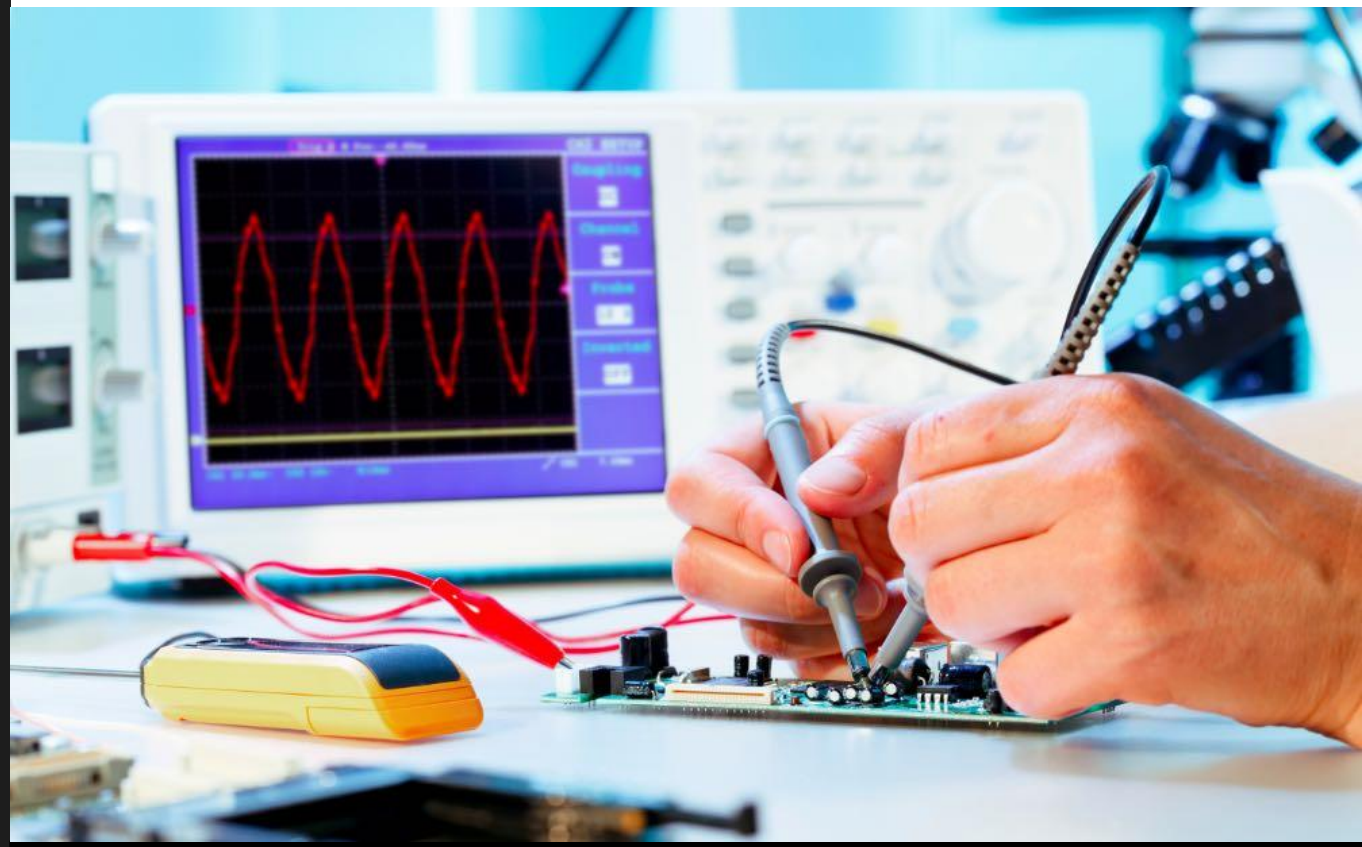
Dispositivo copia: una copia del hardware o bien del elemento de ese hardware del cual tenemos pleno control.

Red neuronal: Algoritmo inferido, cuyo propósito es realizar una tarea especifica.

Problema de clasificación: La agrupación de observaciones que permite identificarlas de forma única.

1.

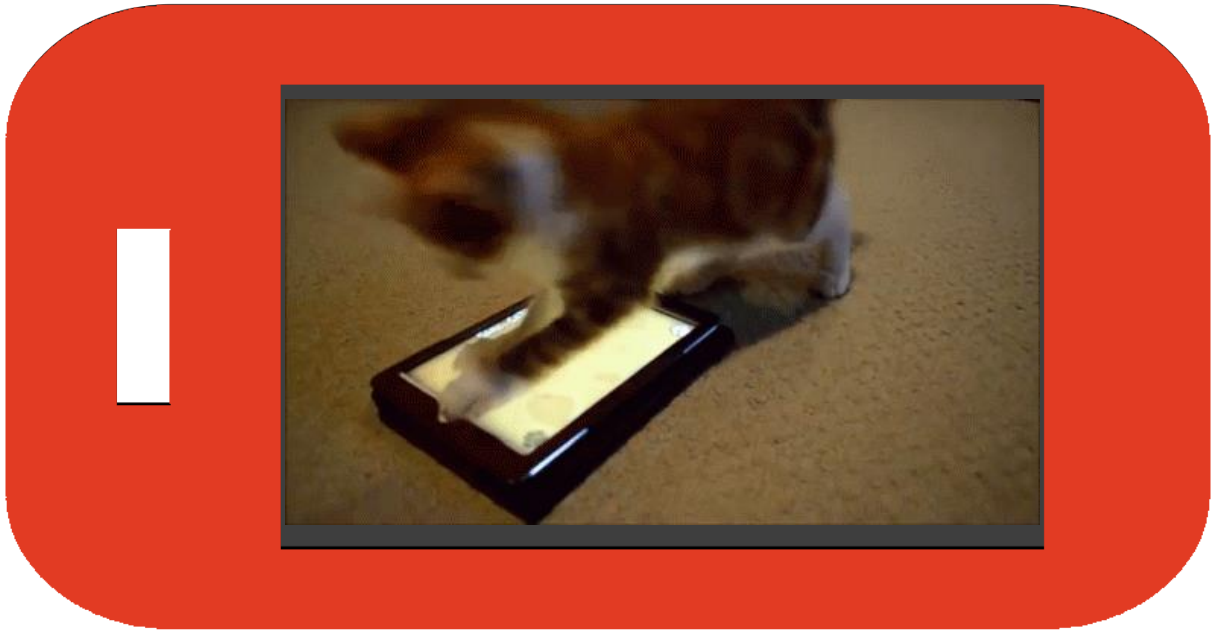
Canal Lateral.



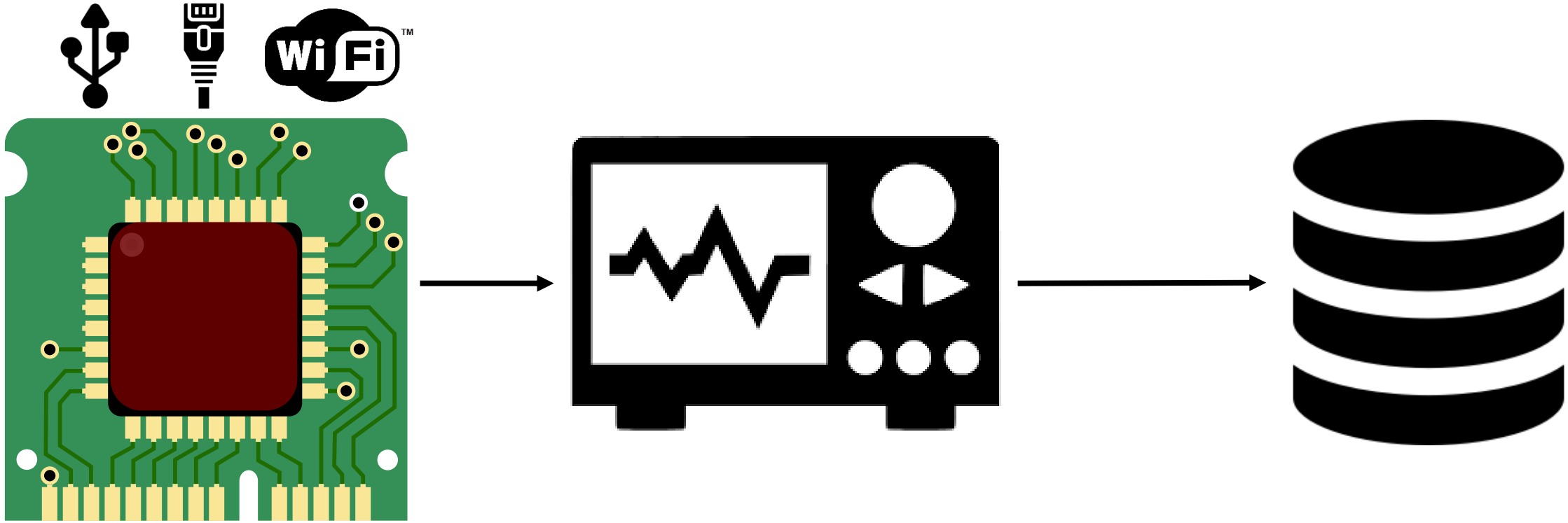
Cortesía de: Rambus

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

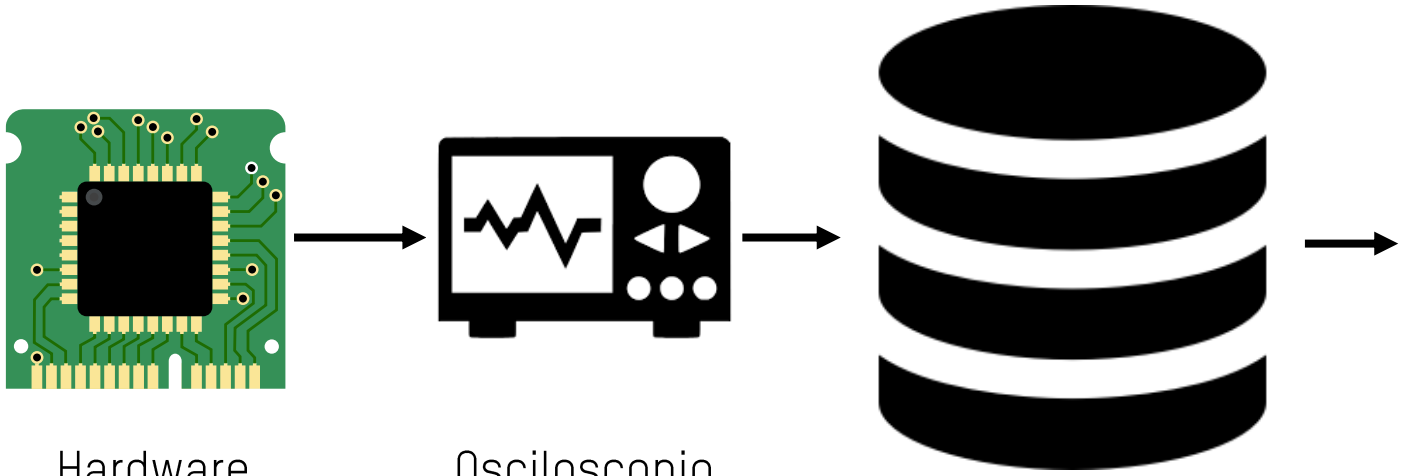
¿Canal lateral?.



Canal lateral de los dispositivos hardware.



Canal lateral de los dispositivos hardware.

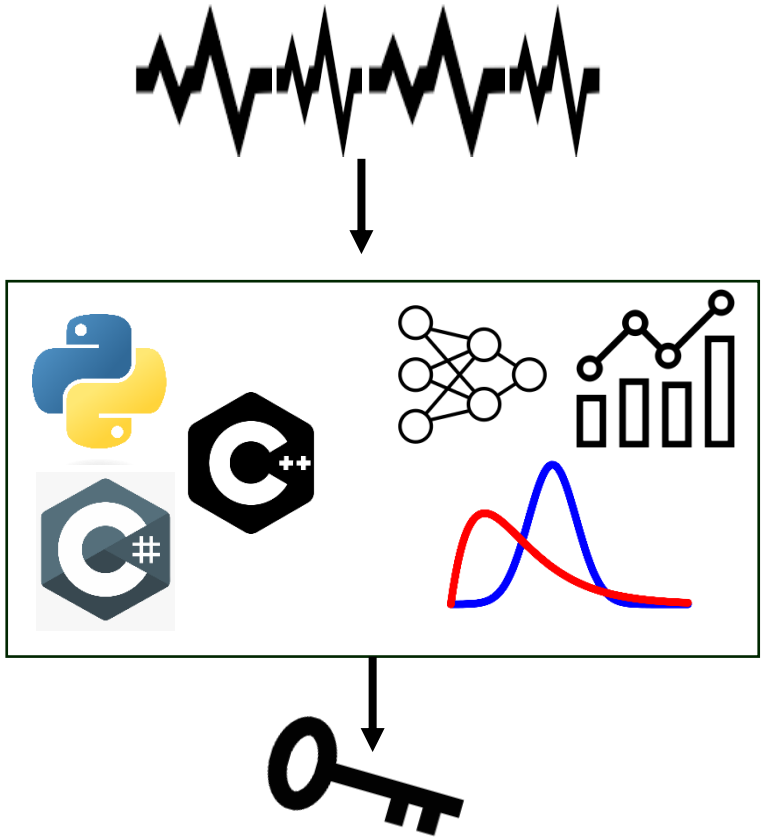


Hardware

Osciloscopio

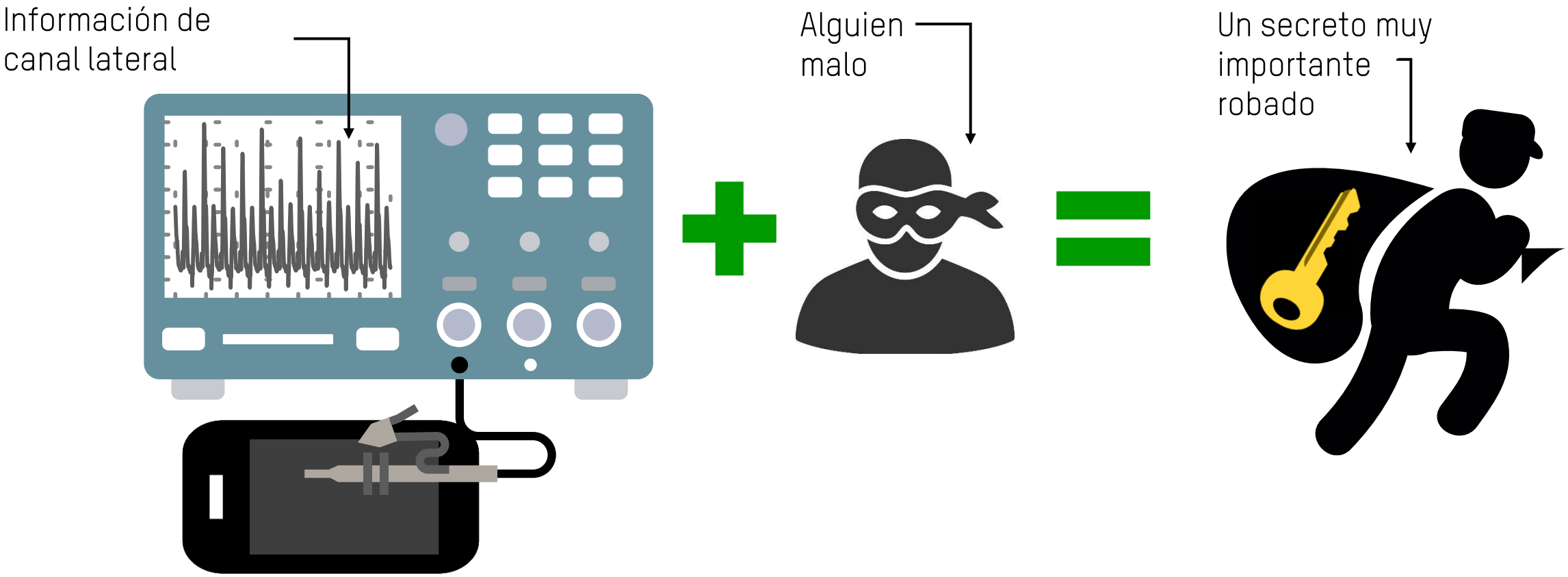
Información de canal lateral

Análisis de canal lateral



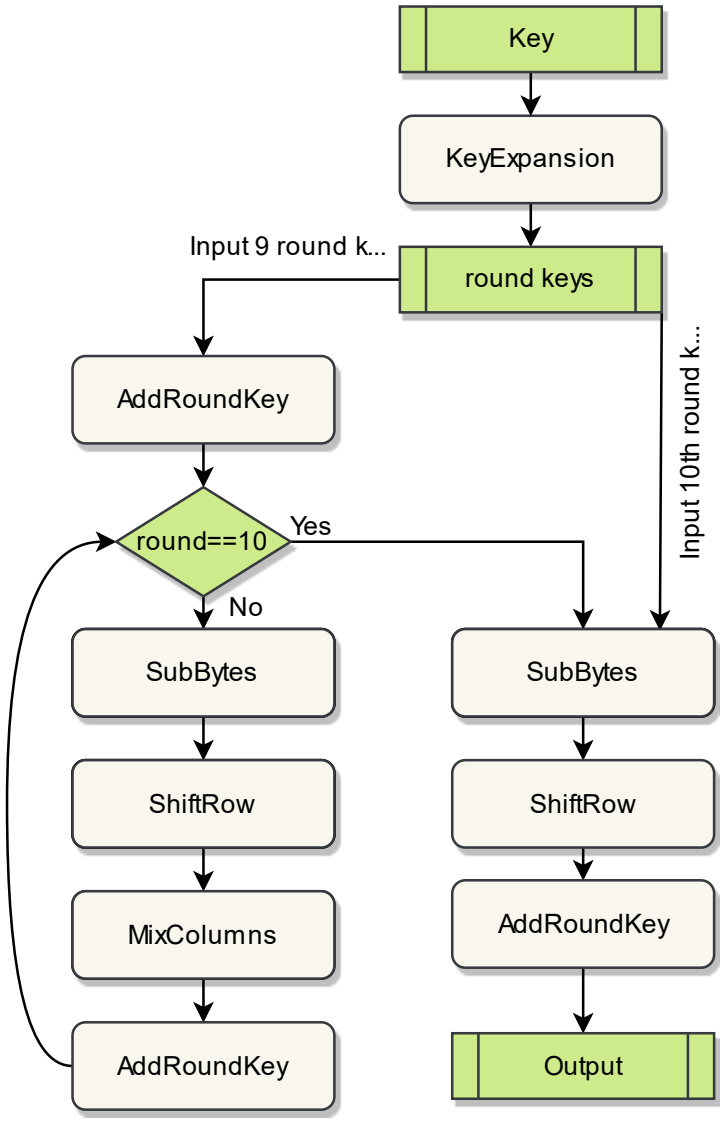
Secretos

Canal lateral de los dispositivos hardware.

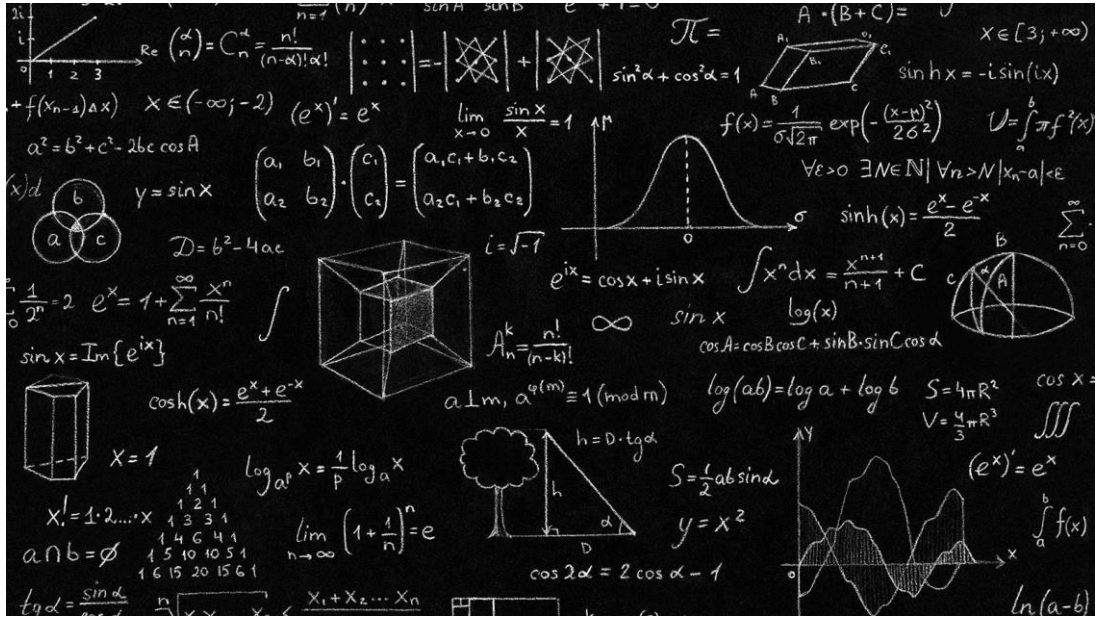


2.

Implementación de algoritmos criptográficos.



Orígenes de un algoritmo criptográfico.

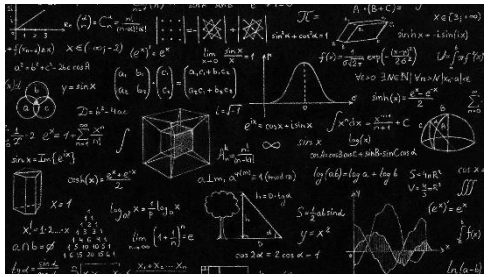


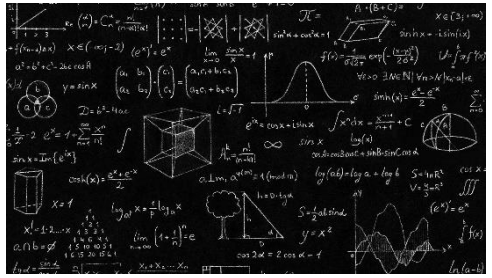
Fundamento matemático

DES
AES
PRESENT
Kyber (PQC)
Saber (PQC)

Ataques de criptoanálisis en algoritmos criptográficos.

Análisis Criptoanalítico





Fundamento matemático

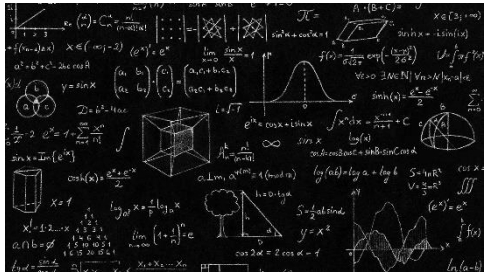
DES
AES
PRESENT
Kyber (PQC)
Saber (PQC)

Garantía de robustez a nivel analítico-matemático

Integridad

Ataques algebraicos

Implementación del algoritmo.

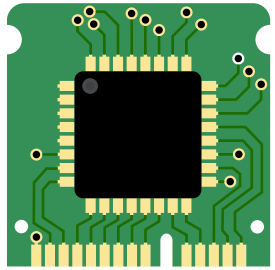


Fundamento matemático

DES
AES
PRESENT
Kyber (PQC)
Saber (PQC)

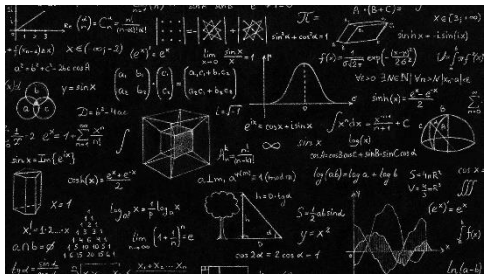
Internet

Programas
ó
Software



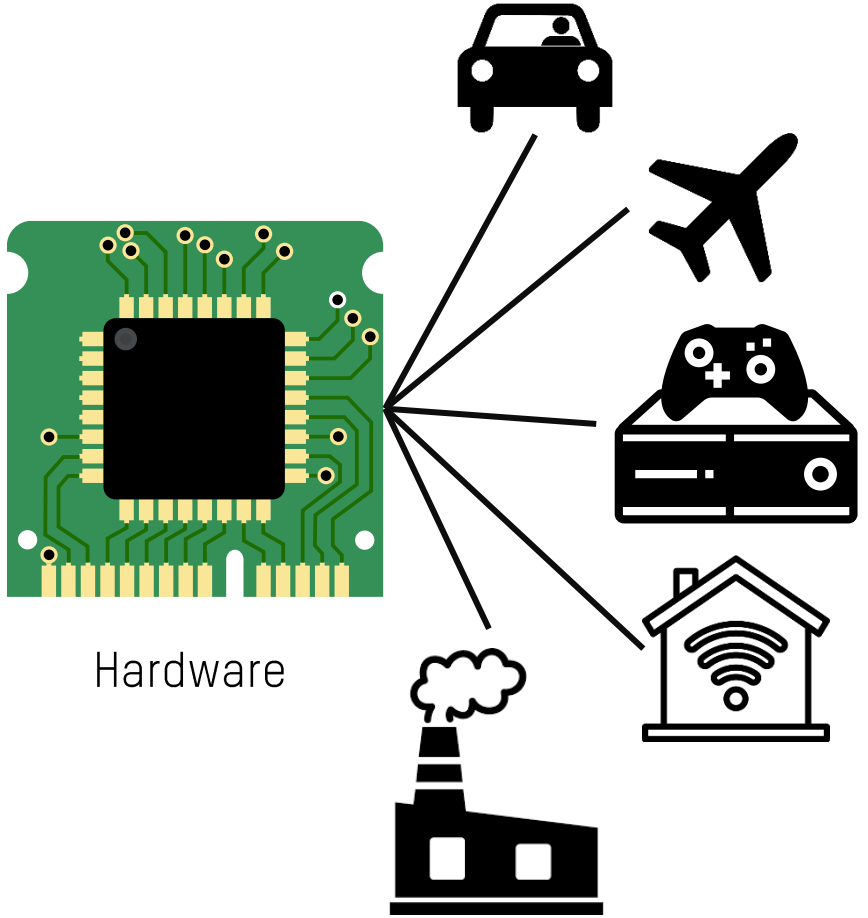
Hardware

Implementación del algoritmo en hardware.



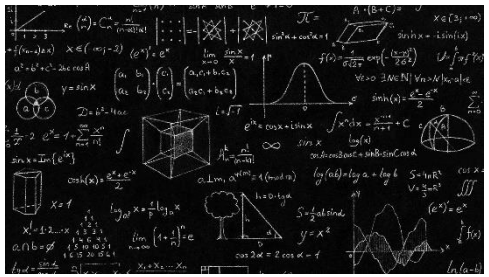
Fundamento matemático

DES
AES
PRESENT
Kyber (PQC)
Saber (PQC)



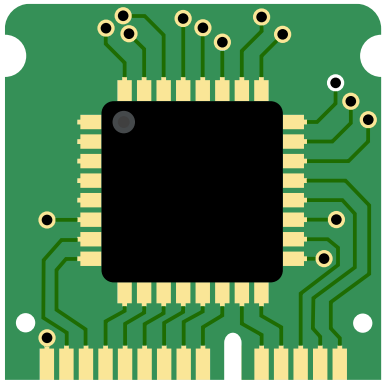
Hardware

Implementación del algoritmo en hardware.



Fundamento matemático

DES
AES
PRESENT
Kyber (PQC)
Saber (PQC)



Hardware

Ataques sobre la implementación

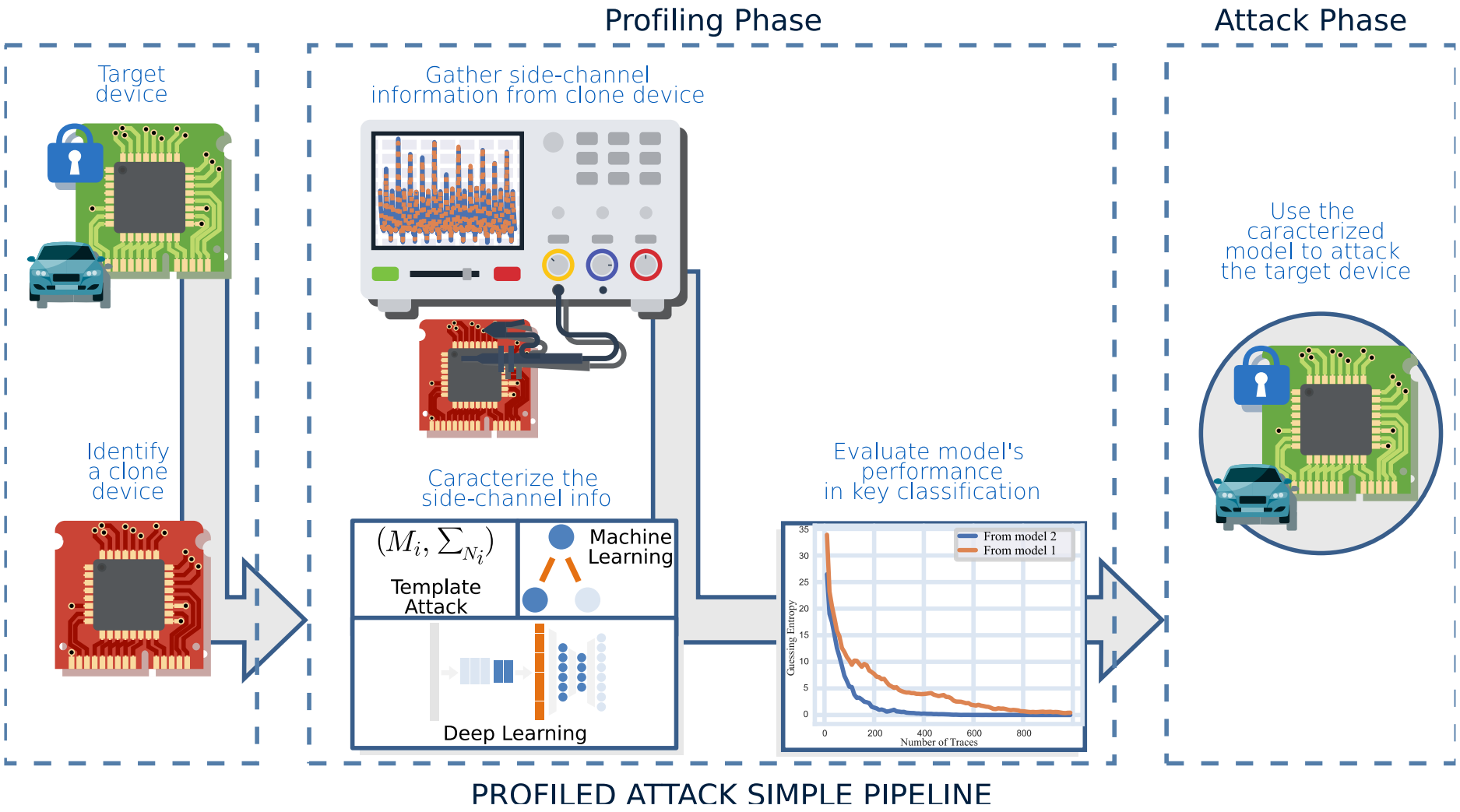
Ataques canal lateral

3.

Ataques de canal lateral.

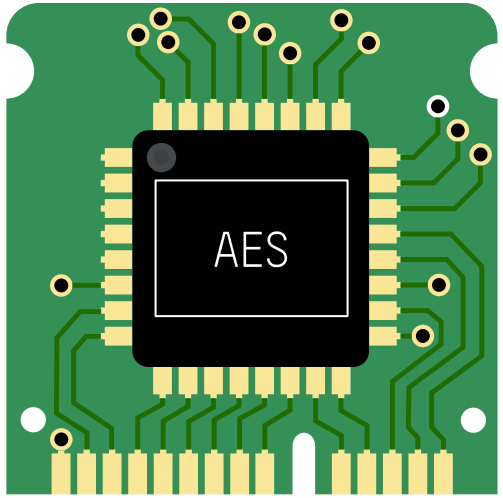
ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Ataques de canal lateral usando redes neuronales.

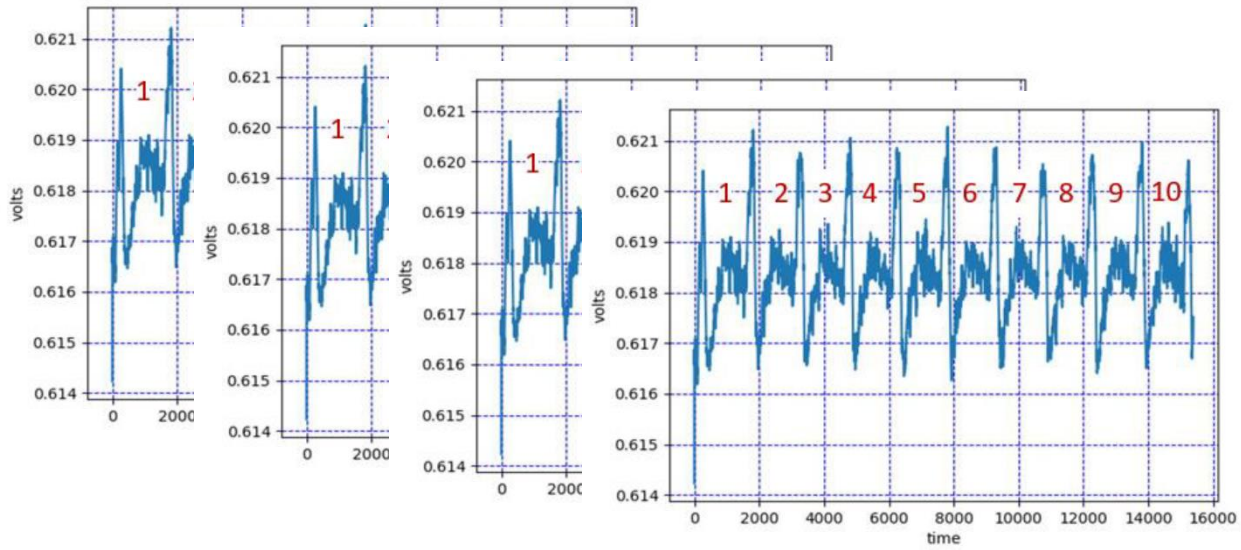


Recolección de información de canal lateral.

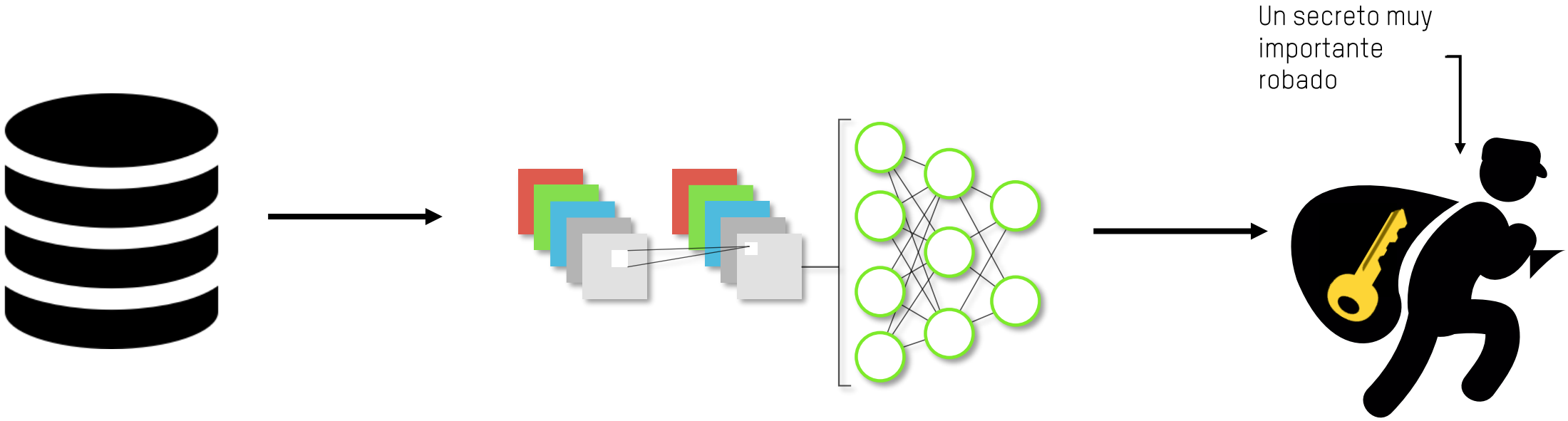
Mi clave secreta



Mi clave secreta ENCRIPTADA



Usar una red neuronal para extraer la clave.

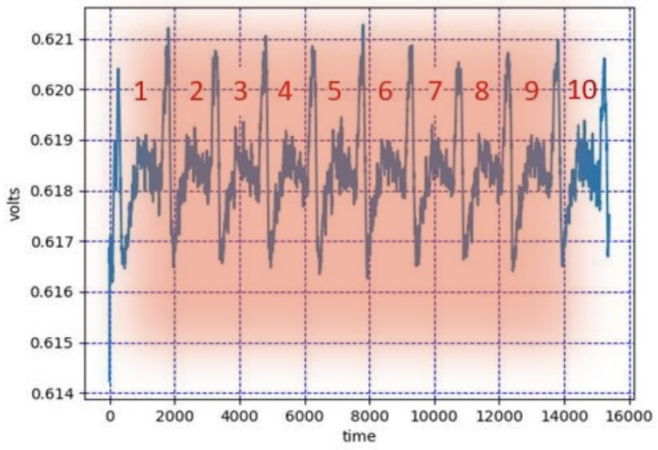


4.

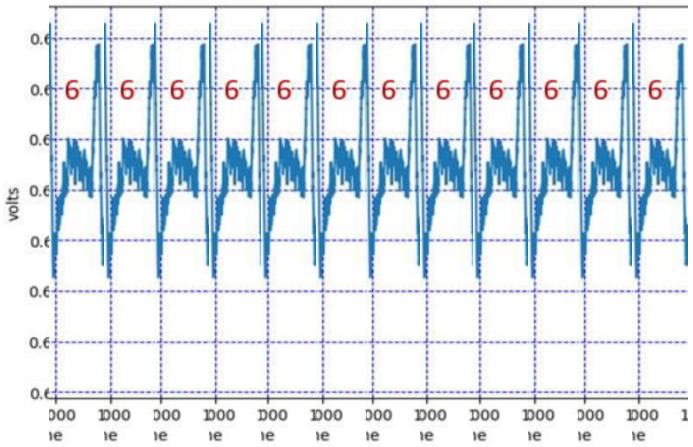
Protecciones contra ataques de canal lateral.

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Algunas protecciones.



Masking
(Enmascaramiento)



Shuffling faking
operations

5.

Video Time!

Paper:
My other car is your car: compromising the Tesla Model X keyless entry system. **Lennert Wouters*, Benedikt Gierlichs*, Bart Preneel***
*imec-COSIC