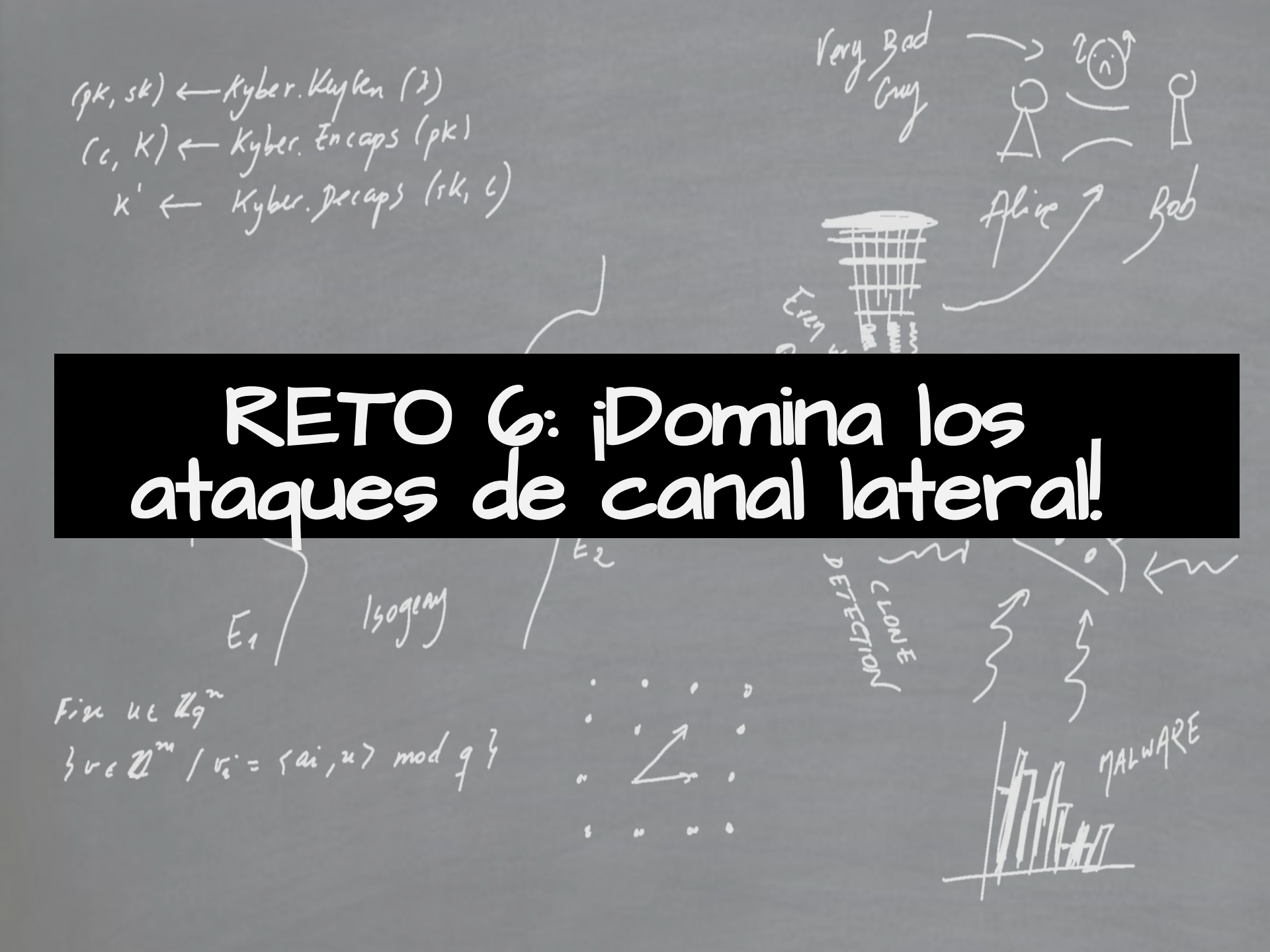
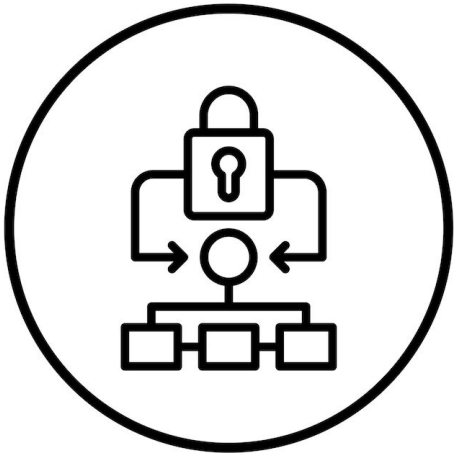
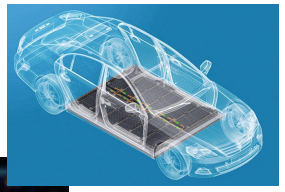


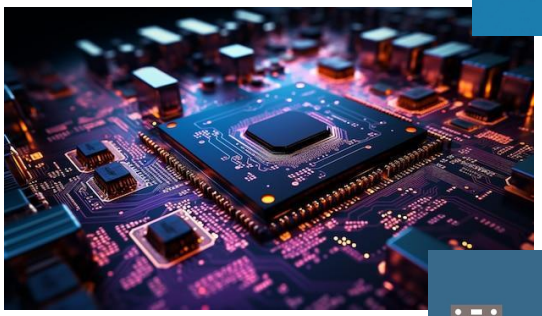
RETO 6: ¡Domina los ataques de canal lateral!

Implementaciones de criptografía



Algoritmo/primitiva criptográfica

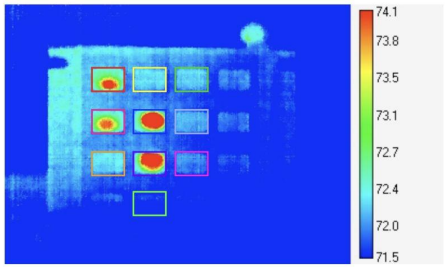




Sistemas embebidos

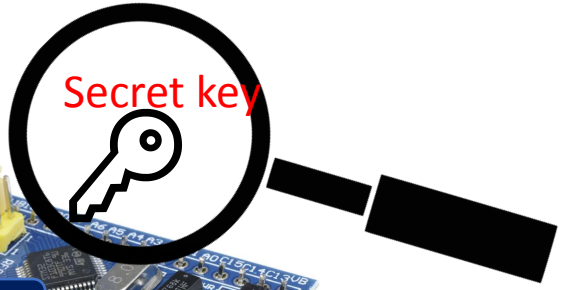
Ataques de canal lateral (Side-Channel Analisis, SCA)

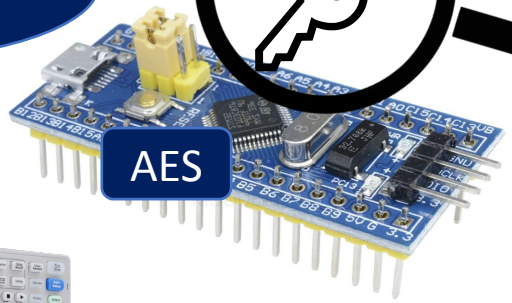
Información “lateral”: características no funcionales

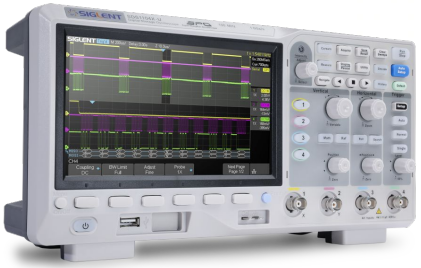


https://www.kaspersky.com/blog/thermal-imaging-attacks/46041/

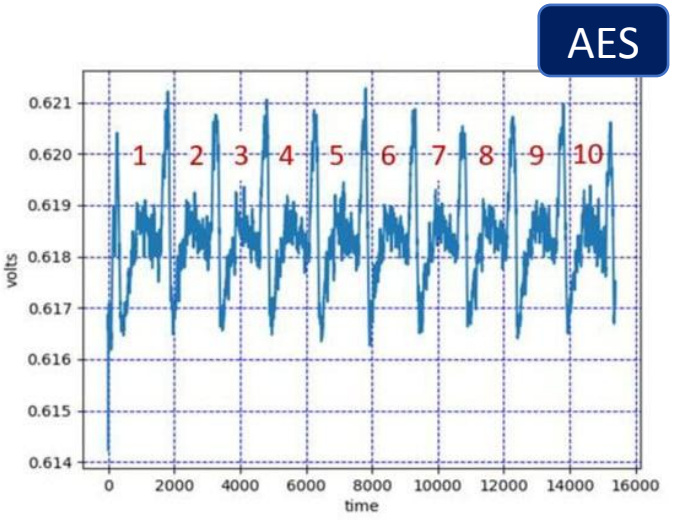
Power SCA







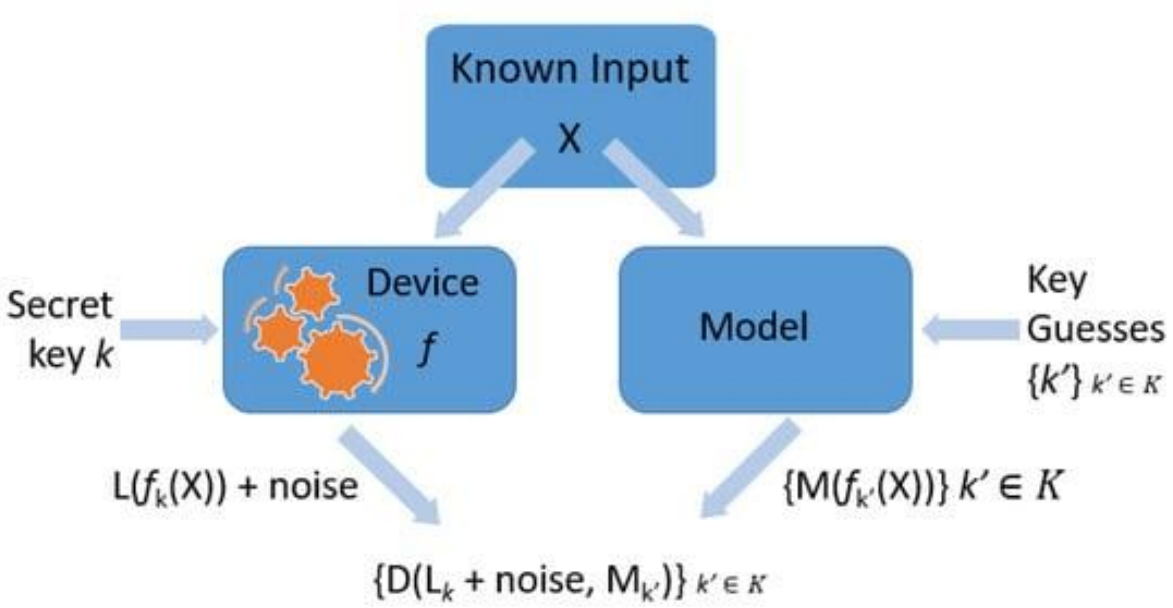
Análisis de la información



Randolph, M.; Diehl, W. Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. *Cryptography* **2020**, *4*, 15. https://doi.org/10.3390/cryptography4020015

Ataques de canal lateral (Side-Channel Analisis, SCA)

Información “lateral”: características no funcionales



Estadística

Machine learning

Modelos de fugas

Randolph, M.; Diehl, W. Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. *Cryptography* **2020**, *4*, 15. https://doi.org/10.3390/cryptography4020015

EL RETO

Recuperar la clave secreta de un AES-128 a partir de sus trazas de consumo

-> Menor número de trazas posible

Punto de partida:

- Set de **trazas** de consumo de un **AES-128** en SW. Texto plano y clave
  - Sin protección. Nivel 1
  - Con protección. Nivel 2
- Set de **trazas** del reto (sin información de clave)

ChipWhisperer-Lite

Microcontrolador ARM Coretx M4

Resultados:

- **Código fuente** utilizado
- **Documento justificativo** del ataque: ¿por qué funciona? ¿cómo? ¿Cuántas trazas?

Si quieres participar:

- Escribe a marta.portela@uc3m.es antes del 17/2/2025
  - Acceso a trazas