

# UN ATAQUE PARA GOBERNARLOS A TODOS: ATAQUE DE COLISIÓN DE TIEMPO VS 42 AES ASIC CORES

BRANDON MEZA - 3CV11

Este ataque funciona incrementando la intensidad a fallos hasta que una característica pueda ser observada



## FAULT SENSITIVITY ANALYSIS

### CORRELATION COLLISION ATTACK

AES S-box

3ns 10ns

49 XX

4a OF

Para medir el tiempo del circuito combinacional objetivo:

- El adversario puede acceder y controlar la señal de reloj
- Se sabe en que ciclo de reloj el objetivo procesa la información deseada
- Puede controlar el dispositivo objetivo de modo que el valor  $i$  de la entrada sea procesado múltiples veces
- Esta equipado con los instrumentos adecuados

AES S-box

5ns 10ns

ff XX

12.6ns 2f

12.4ns OF

### COMO MEDIR EL TIMING

### COLLISION TIMING ATTACK

AES S-box

5ns 10ns

ff XX

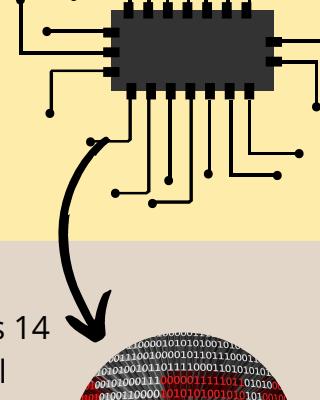
12.6ns 2f

12.4ns OF

El algoritmo del ataque anterior es el siguiente:

```
Algorithm 1. Correlation Timing Attack  
(at the last round of an AES encryption)  
Input:  ${}_1T^o : \{\Delta t^{o=0}, \dots, \Delta t^{o=255}\}$ ;  $o = S(i) \oplus k_1$   
Input:  ${}_2T^o : \{\Delta t^{o=0}, \dots, \Delta t^{o=255}\}$ ;  $o = S(i) \oplus k_2$   
1: for  $\Delta \in \{0, 1, \dots, 255\}$  do  
2:    $C^\Delta = \text{Correlation}({}_1T^o, {}_2T^{o+\Delta})$   
3: end for  
4: return  $\arg \max C^\Delta$ 
```

### ALGORITMO DE COLLISION TIMING ATTACK



El ataque de colisión usa eficientemente los datos dependiendo de las características de timing de circuitos combinacionales para revelar secretos, este ataque no requiere ningún conocimiento sobre las características del circuito combinacional objetivo

Este ataque rompió todos las 14 implementaciones AES del SASEBO LS12 y LS13 en todas las tecnologías que lo contienen actualmente

AES S-box

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

000000000000