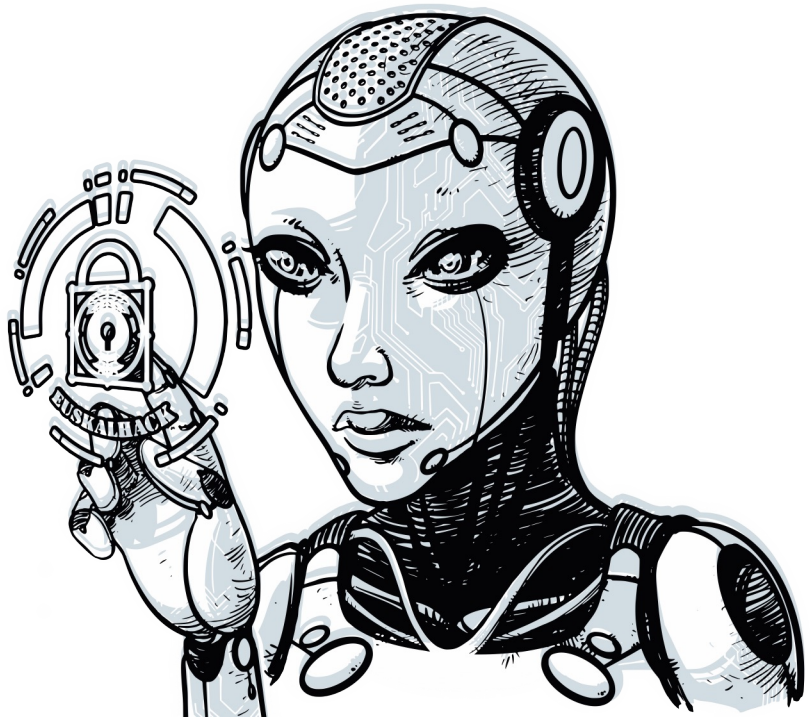


Filtros sin postureo:
Wavelets aplicado a Side Channel

Tània
Matemática
Criptografía
Evaluadora HW

Sara
Ingeniera industrial
Electrónica
Evaluadora HW

Y MUCHAS OTRAS COSAS!

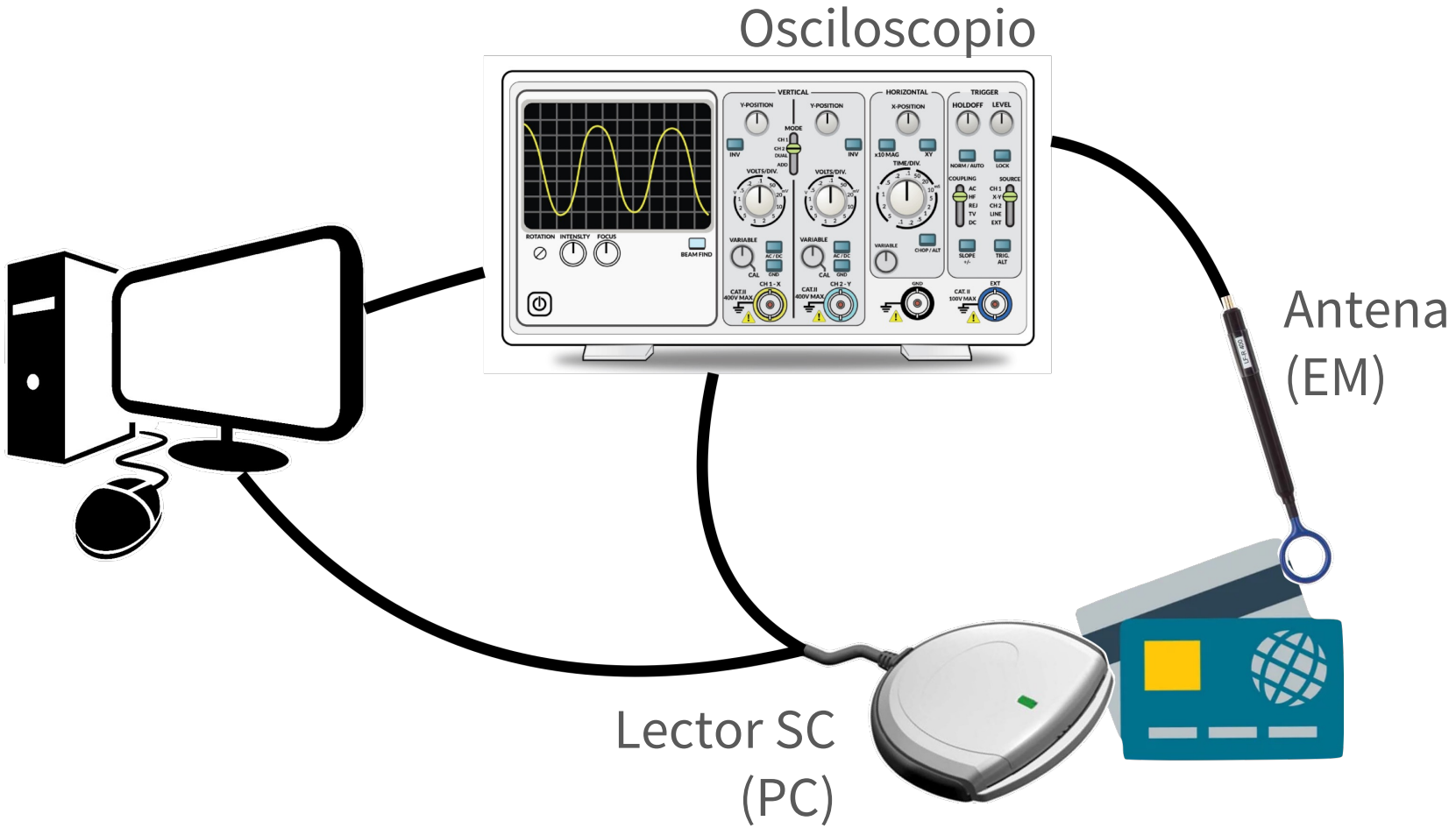
¿A qué nos dedicamos?

Evaluaciones HW
ICs
Smartcards & similar devices

¿De qué os hablaremos?

Side Channel
Wavelets

Set-up de Side Channel



Introducción a la técnica de Side Channel

Ataques basados en la información obtenida gracias a un **canal de comunicación no intencionado** que filtra información de un dispositivo a través de un medio físico.

ATAQUES PASIVOS

Monitorizaremos la SC mientras este procesa información sensible.

Filtros sin postureo:
Wavelets aplicado a Side Channel

Esquema de un ataque de Side Channel

Single Power Analysis

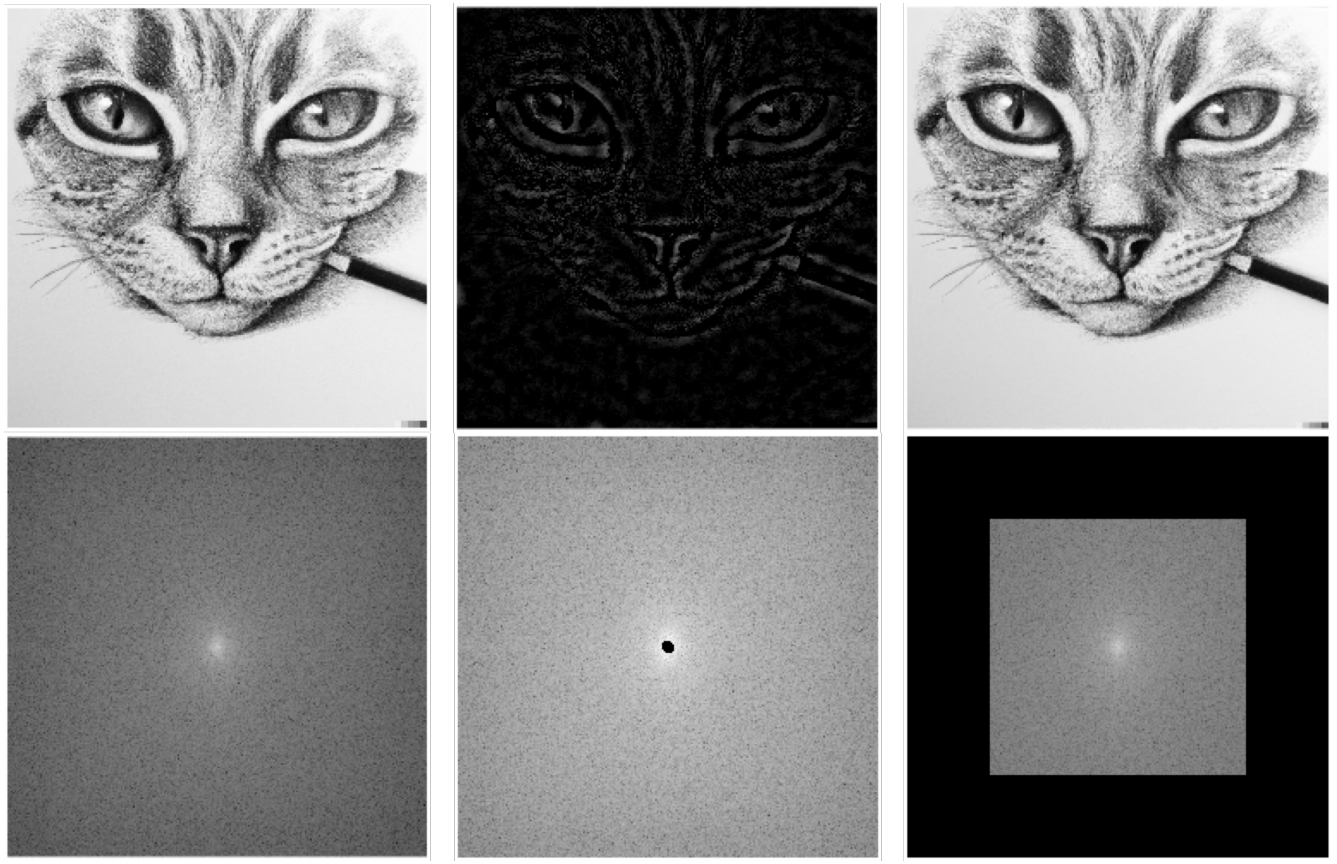
Adquirir trazas PC/EM

Técnicas post-procesado

Ataque!

Conseguir secretos

Breve introducción a los wavelets



Filtros sin postureo:
Wavelets aplicado a Side Channel

Time domain
Solo tiempo

Fourier Transform (CFT)
Funciones continuas | Solo frecuencias

$$CFT_f(\omega) = \int_{-\infty}^{+\infty} f(t)e^{-i\omega t}dt$$

Discrete Fourier Transform (DFT)
Solo frecuencias

$$DFT_f(\omega) = \sum_{t=0}^{T-1} f(t)e^{-2i\pi\omega\frac{t}{T}}\,dt$$

Short Time Fourier Transform (STFT)
Frecuencias en ventanas de tiempo fijas

$$DSTFT_f(\omega,\tau) = \sum_{t=0}^{T-1} f(t)g(t-\tau)e^{-2i\pi\omega\frac{t}{T}}\,dt$$

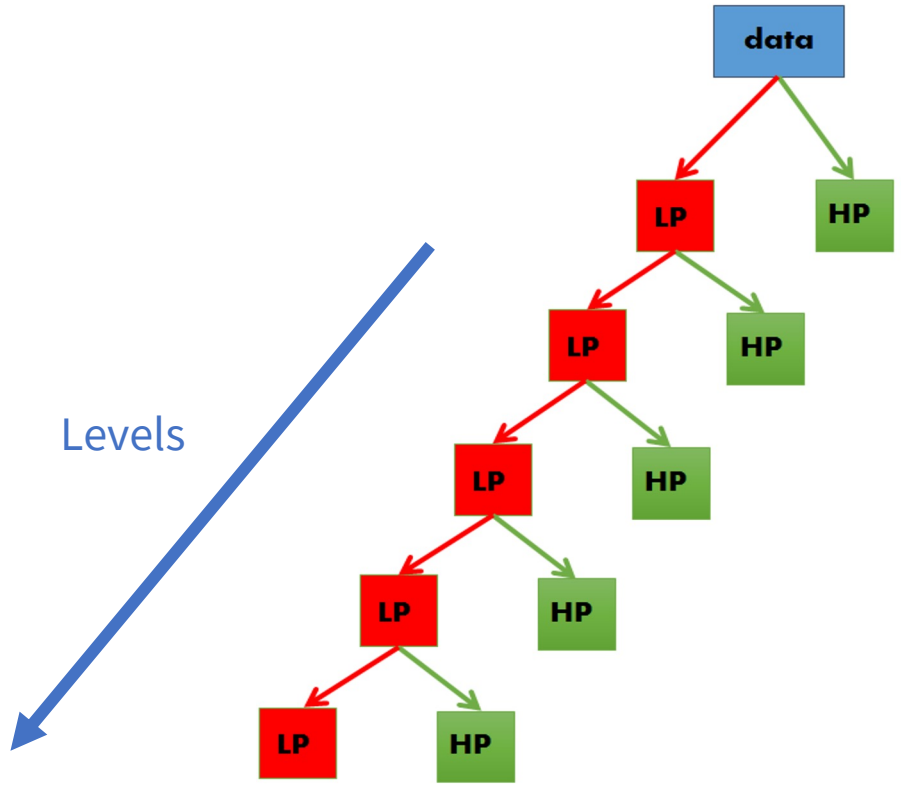
Wavelet Transform (CWT)
Funciones continuas

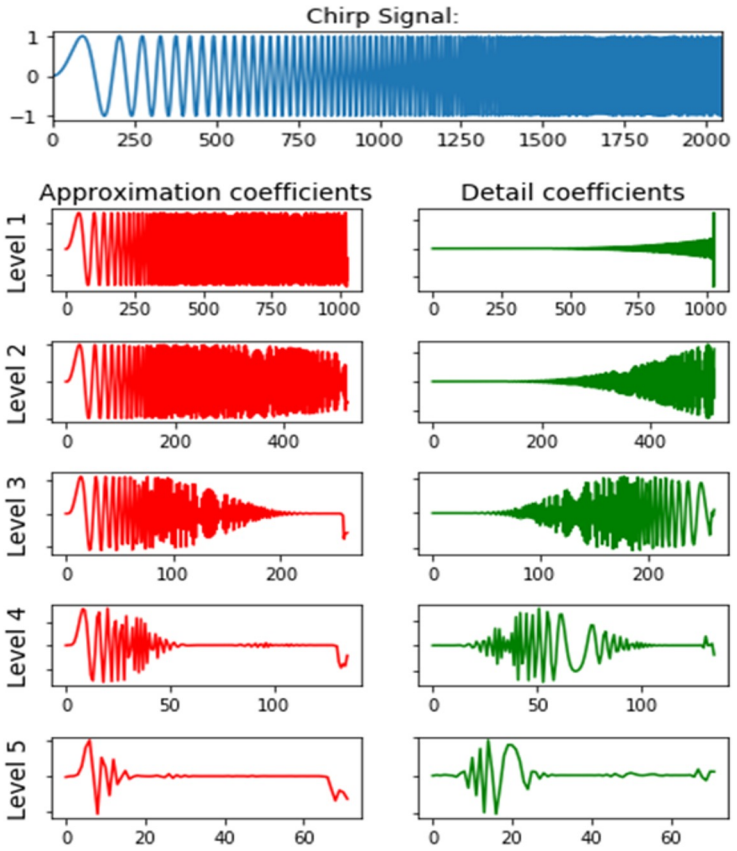
$$CFT_f(\tau,s) = \frac{1}{\sqrt{s}}\int_{-\infty}^{+\infty} f(t)\Psi^*\left(\frac{t-\tau}{s}\right)dt$$

Discrete Wavelet Transform (DWT)
Las ventanas de tiempo se adaptan para capturar variaciones rápidas o lentas en las señales

$$f_{Approx} = \left[0, \frac{f_s}{2^{p+1}}\right], f_{Det} = \left[\frac{f_s}{2^{p+1}}, \frac{f_s}{2^p}\right]$$

Filtros sin postureo:
Wavelets aplicado a Side Channel



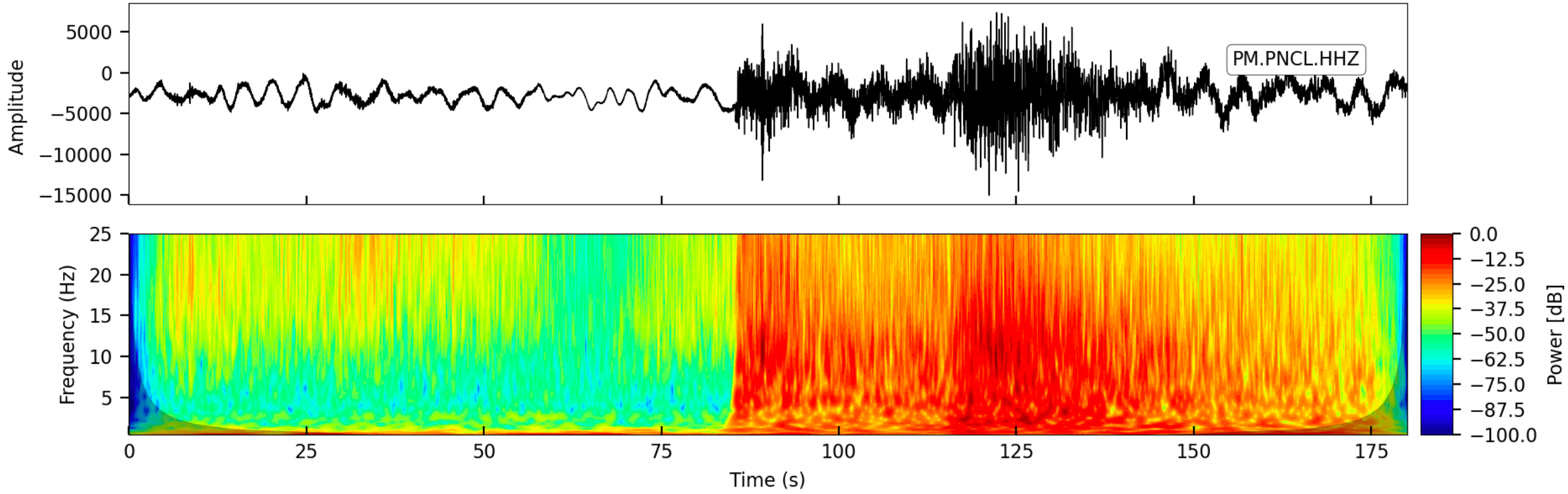


Discrete Wavelet Transform (DWT)

Las ventanas de tiempo se adaptan para capturar variaciones rápidas o lentas en las señales

$$f_{Approx} = \left[0, \frac{f_s}{2^{p+1}}\right], f_{Det} = \left[\frac{f_s}{2^{p+1}}, \frac{f_s}{2^p}\right]$$

Filtros sin postureo:
Wavelets aplicado a Side Channel



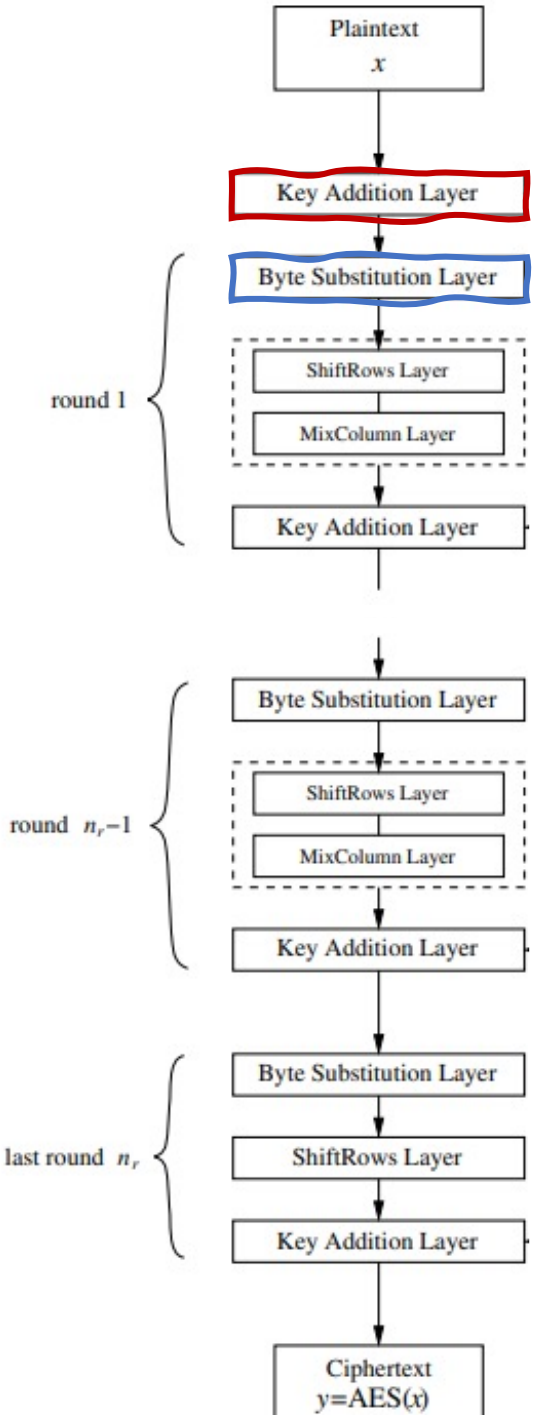
Nuestro ataque

Objetivo

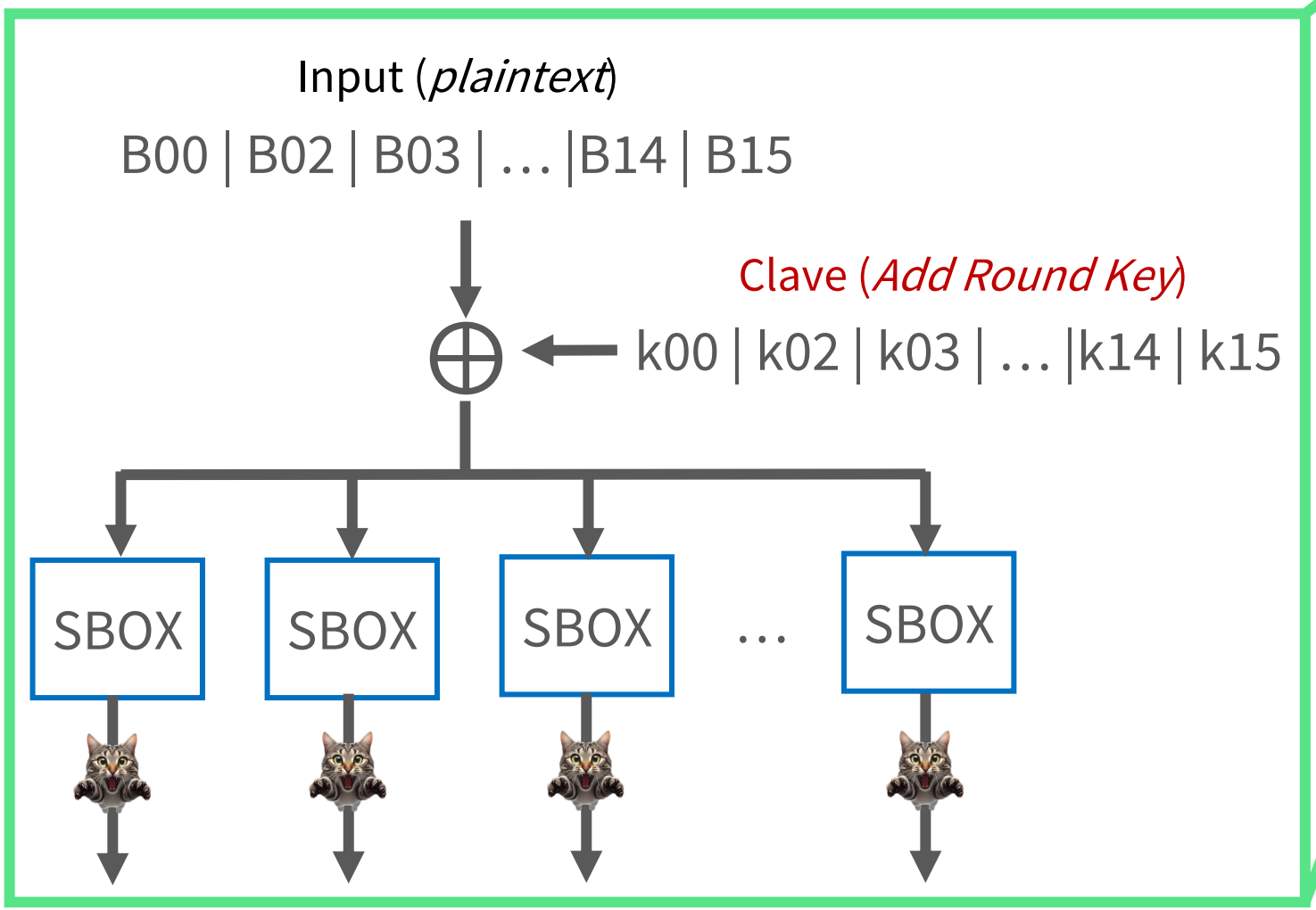
Conseguir la clave secreta de un AES durante la encriptación de datos

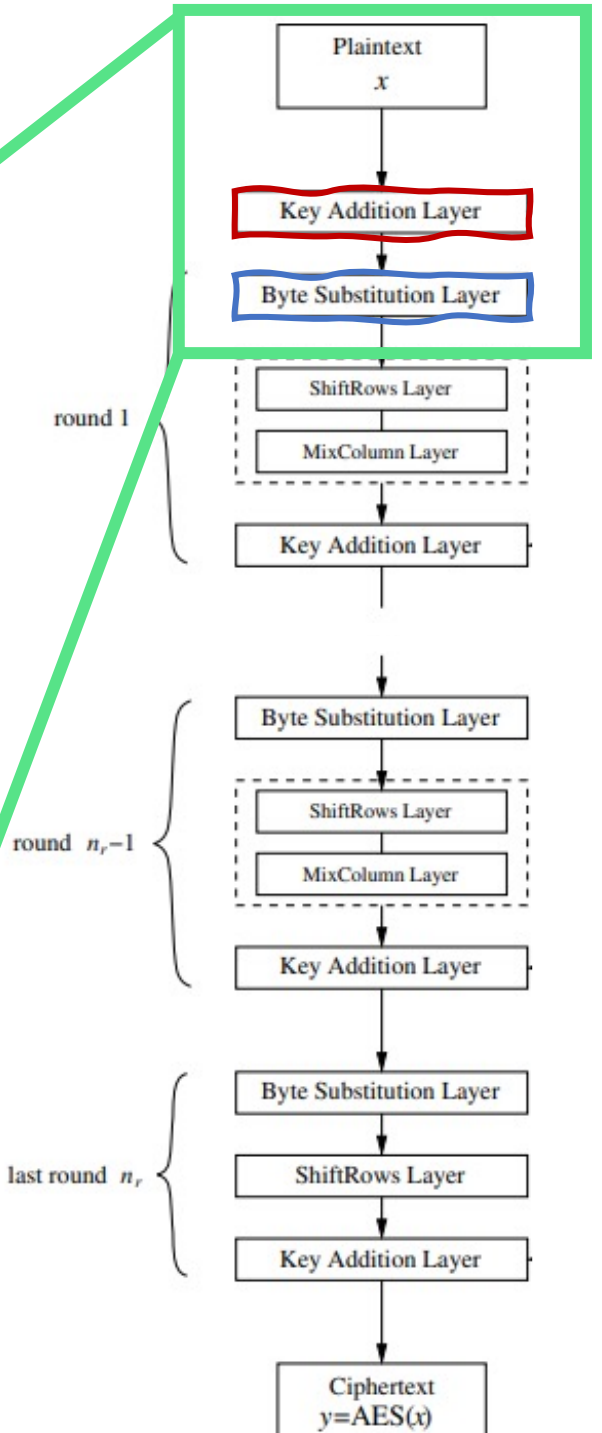
¿Cómo?

Correlation Power Analysis (CPA) en la salida del primer *bytes substitution*



Filtros sin postureo: Wavelets aplicado a Side Channel





Esquema de un ataque de Side Channel

Single Electro Magnetic Analysis

Adquirir trazas EM

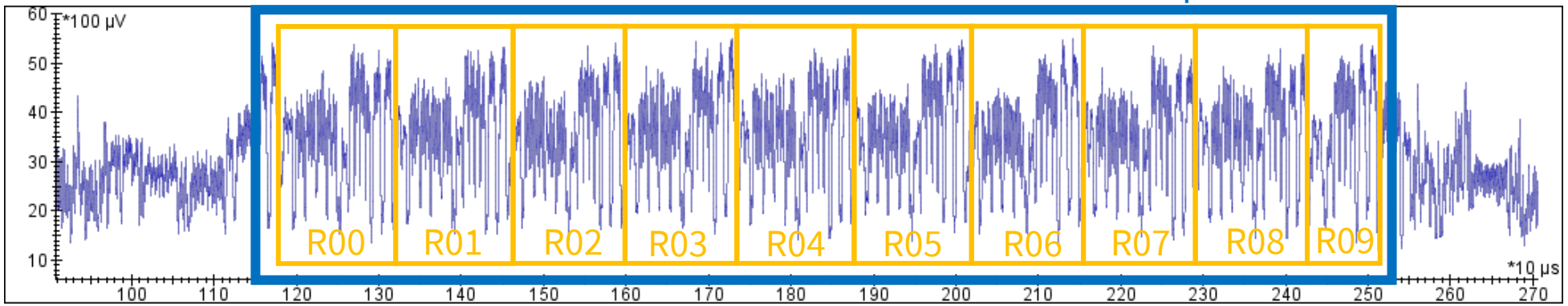
Técnicas post-procesado

Ataque!

Conseguir secretos

Single Electro Magnetic Analysis (SEMA)

Encriptación AES



¿Què estamos viendo?

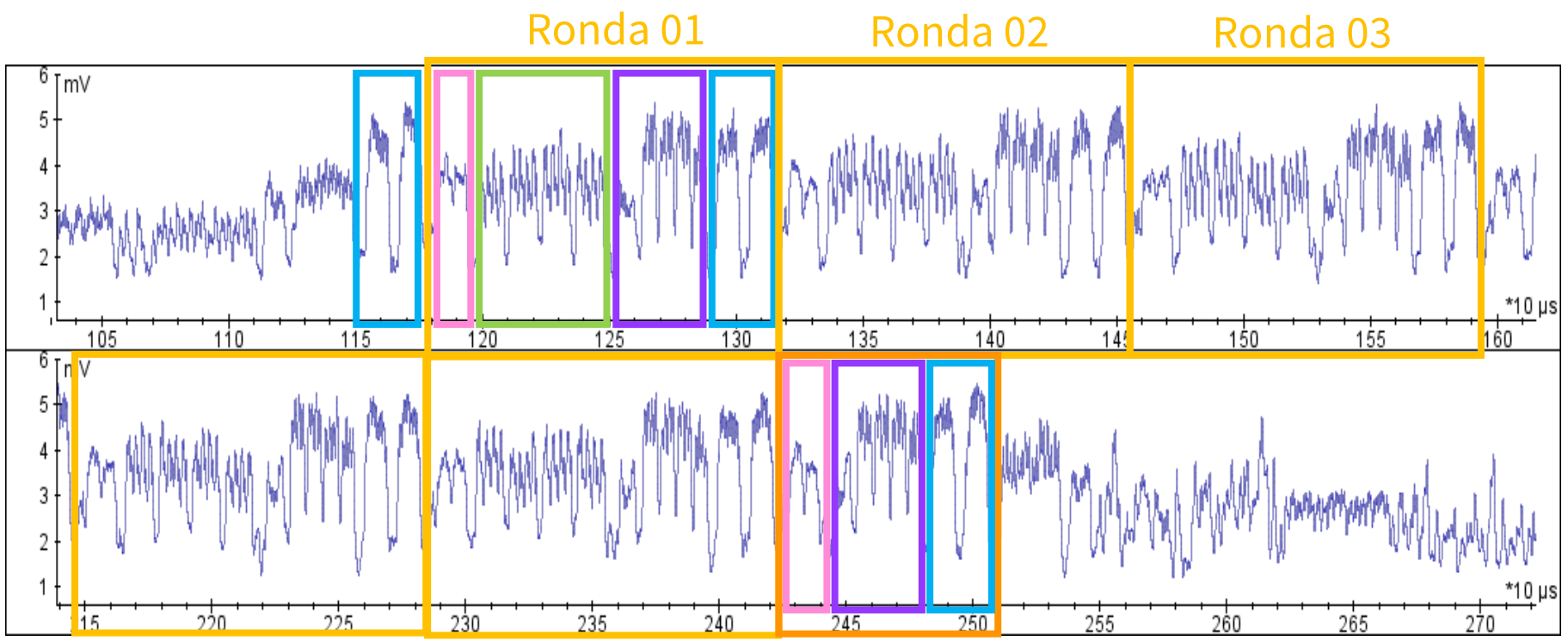
AES programado en software

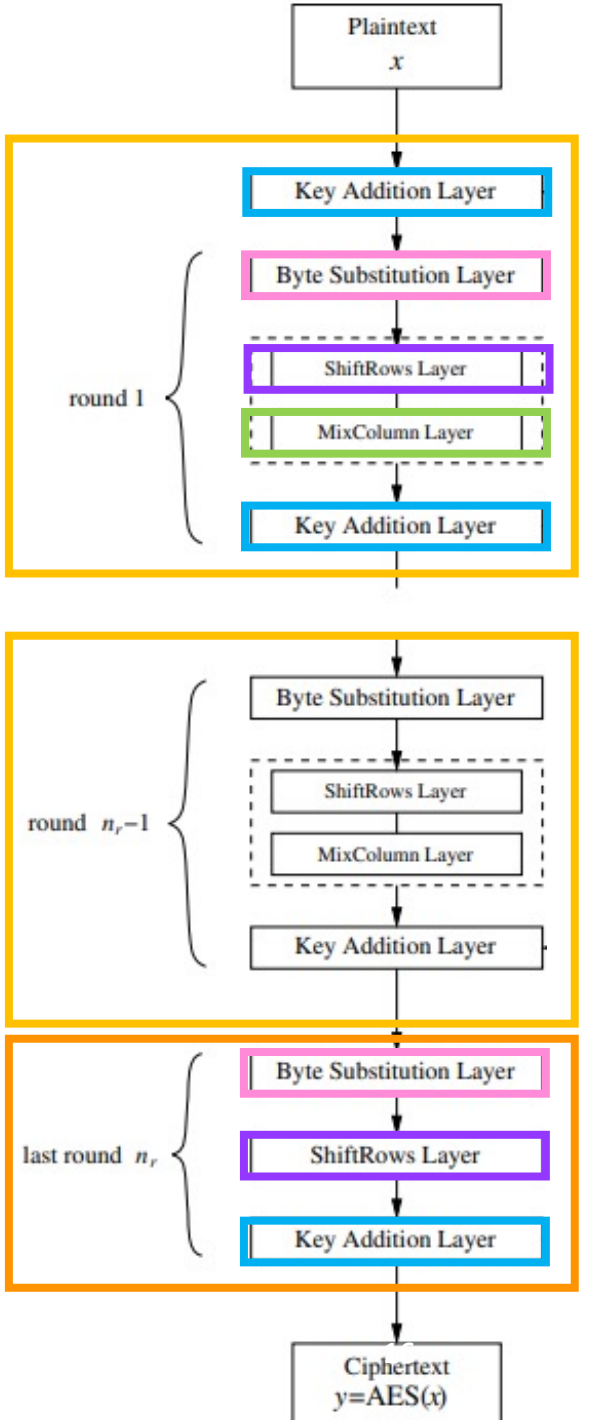
Producto ATmega163

V = 5V

f_{int} = 1 MHz

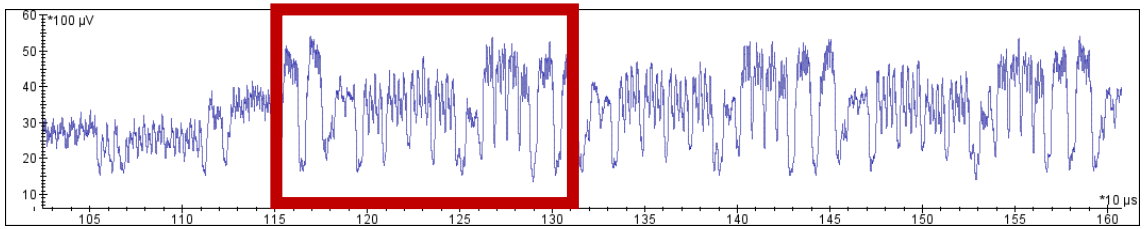
Filtros sin postureo: Wavelets aplicado a Side Channel





Adquisición trazas de EM

Adquisición de 20.000 trazas
Frecuencia de adquisición 25 M Samples/s
Región de adqusición:



¿Por qué 25 M Samples/s?

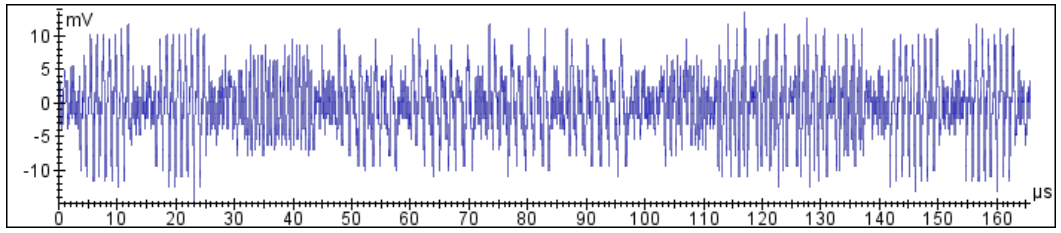
f_{int} = 1 MHz
Calidad Nyquist = 2*1 M Samples/s = **2 M Samples/s**

Primer harmónico = 2 MHz
Segundo harmónico = 3 MHz
Tercer harmónico = 4 MHz
Calidad Side Channel = 2*4 M Samples/s = **8 M Samples/s**

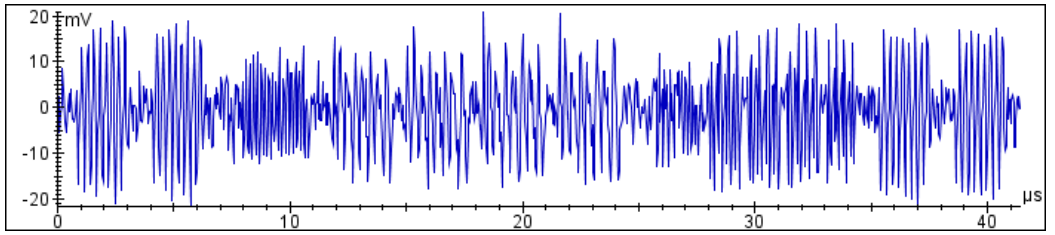
+ extra de calidad = 25 M Samples/s

Técnicas de post-procesado

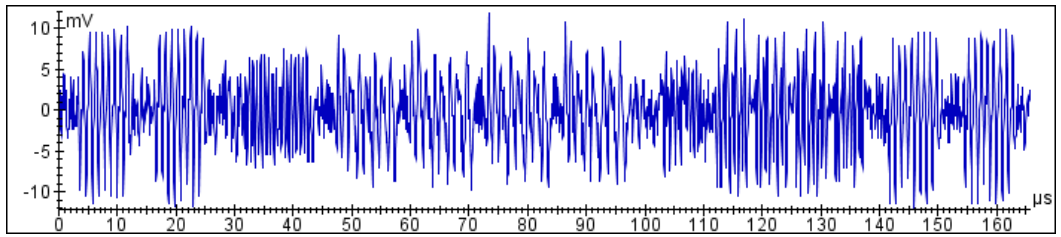
Raw



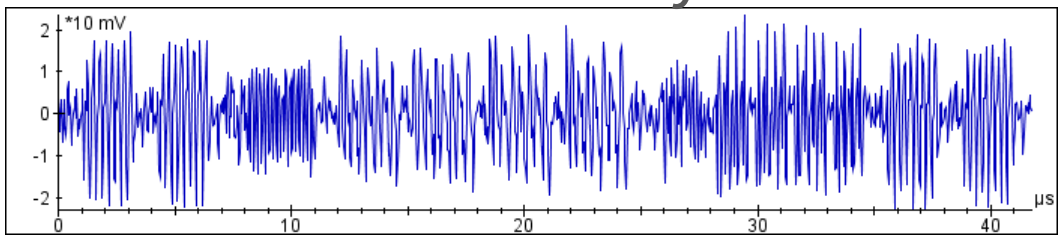
Haar Level 2



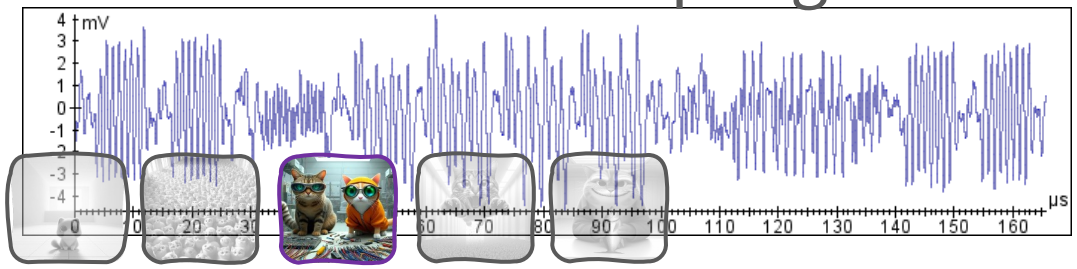
Low Pass



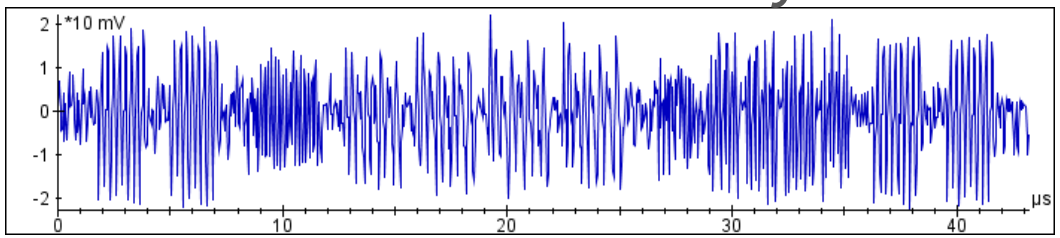
Sym7 Level 2



Resampling 12MHz

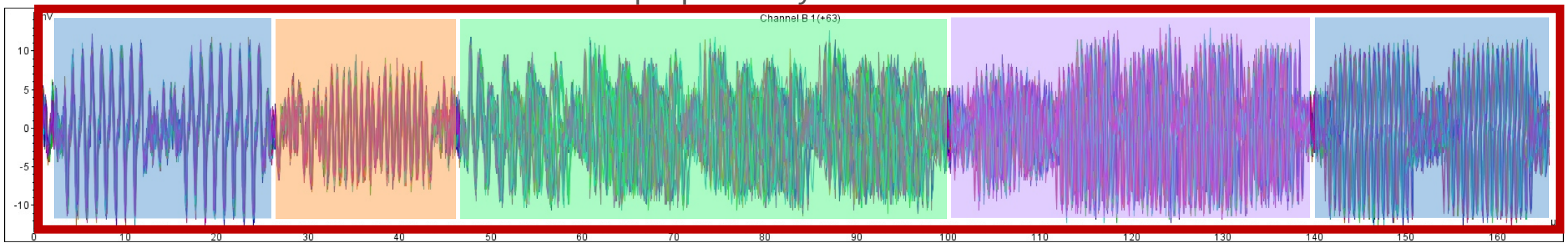


Dmey Level 2

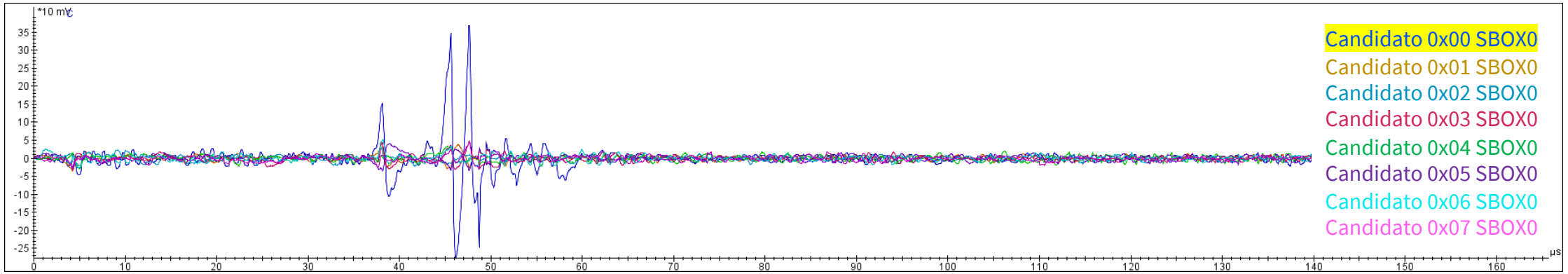


Ataque!

64 trazas de EM superpuestas y alineadas al inicio de la ronda OO



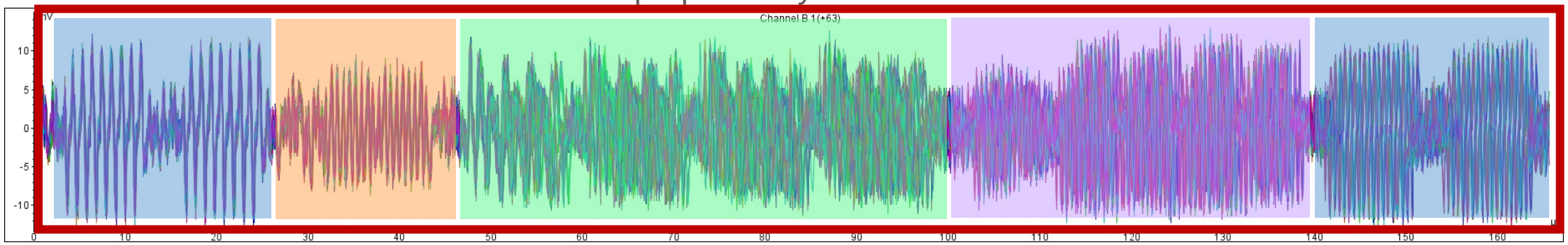
Resultados del CPA SBOX0-out candidatos 00-07



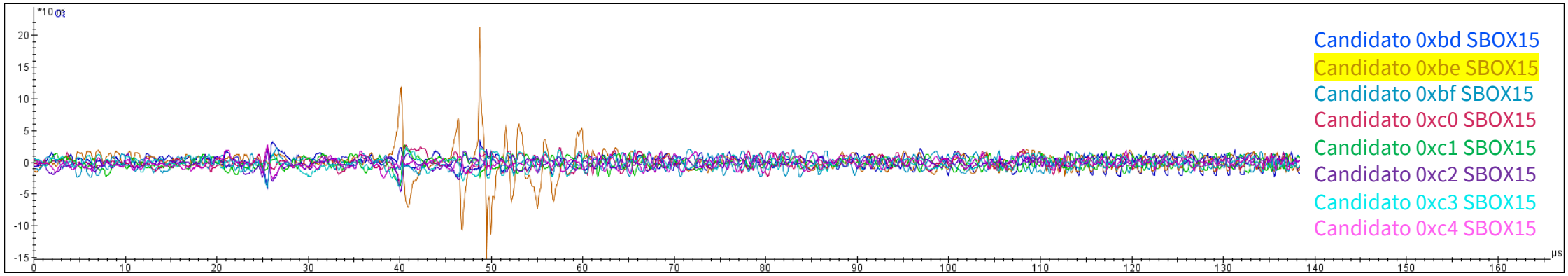
Low Pass

Ataque!

64 trazas de EM superpuestas y alineadas al inicio de la ronda OO



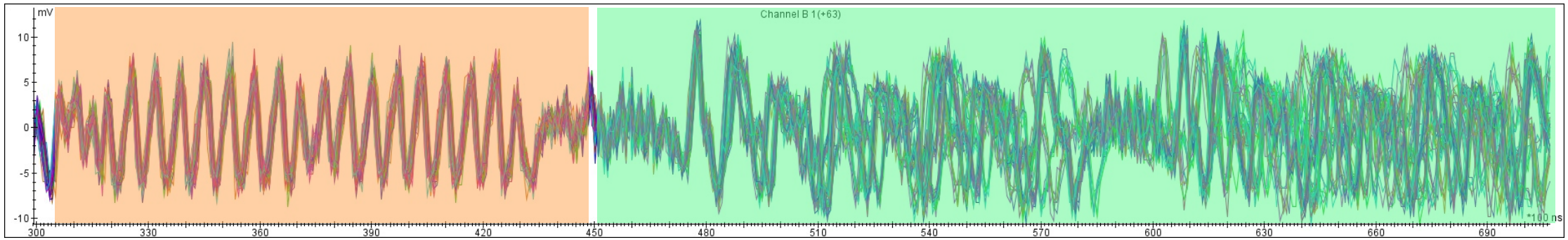
Resultados del CPA SBOX15-out candidatos 0xBD-C4



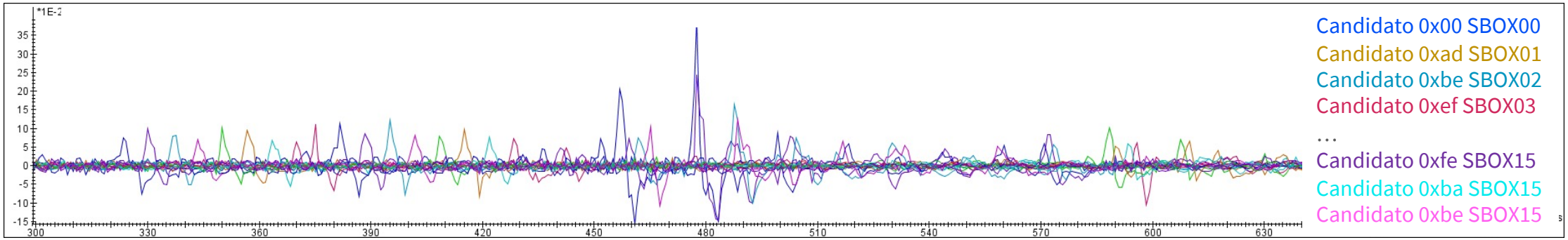
Low Pass

Ataque!

64 trazas de EM superpuestas y alineadas al inicio de la ronda OO ampliación SBOXes



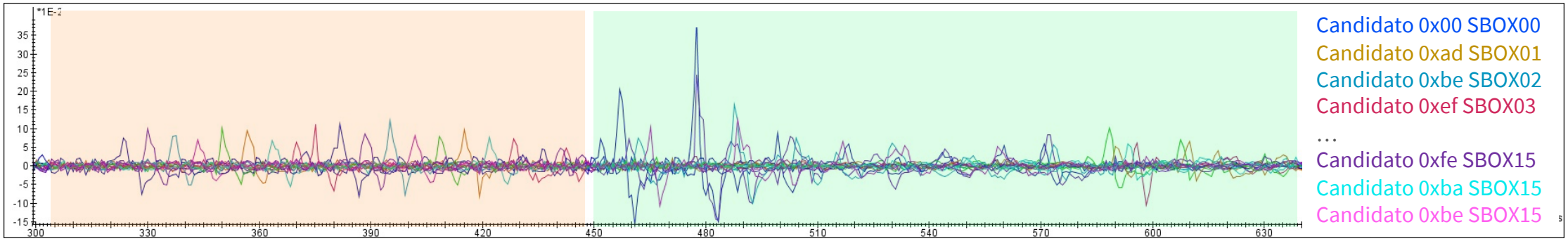
Resultados del CPA SBOXes-out 00-15



CLAVE SECRETA: 00 AD BE EF CA FE BA BE 00 AD BE EF CA FE BA BE

Resultado conseguido

Resultados del CPA SBOXes-out 00-15



CLAVE SECRETA: 00 AD BE EF CA FE BA BE 00 AD BE EF CA FE BA BE

Conclusiones CPA:

- Picos de correlación en *SubBytes* y *Shift Rows*
- Los bytes no aparecen de forma secuencial

Wavelets en tiempo de ejecución

	Tiempo ejecución [s]	
Raw	1616	🐛
Resampling	868	🐰
Low Pass	1620	🐛
Wavelets (dmey2)	608	🐰🐰
Wavelets (sym2)	568	🐰🐰

Wavelets en resultados

	Diferencia absoluta entre 1º y 2º candidatos	
Raw	20%	
Resampling	22%	
Low Pass	27%	
Wavelets (dmey2)	25%	
Wavelets (sym2)	25%	

Conclusiones

	Mejora rapidez	Mejora resultados
Raw vs wavelets	✅	✅
Resampling vs wavelets	=	✅
Low Pass vs wavelets	✅	❌

ESKERRIK ASKO!

Agradecimientos

A nuestras compañeras
de Applus+ Laboratories <3

@taniadiazcancer @sara.ribes.amoros