

Encrypter and Decrypter AES

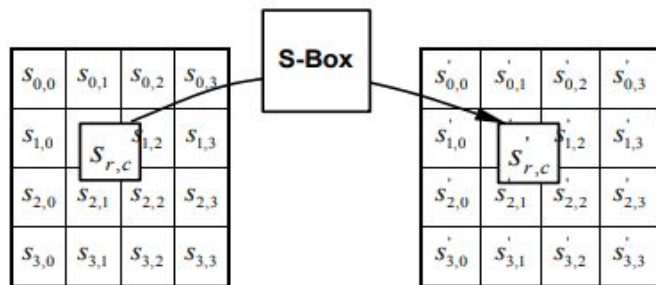
Autor: Ing. Maffrand, Carlos
GitHub: https://github.com/cmaffrand/CESE_CPL/AES

CESE 2022

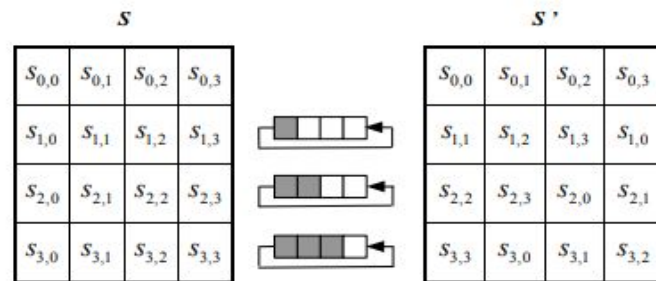
AES (Advanced Encryption Standard)

- Basado en el algoritmo de Rijndael, que es una familia de cifradores de bloques desarrollada por los criptógrafos Belgas Rijmen and Daemen.
- El Rijndael ganó la competencia realizada por el National Institute of Standards and Technology's (NIST) para seleccionar el Advanced Encryption Standard (AES) con el objetivo de reemplazar al Data Encryption Standard (DES).
- Implementa la forma de cifrado en bloques, es decir una palabra de un ancho determinado, generará un texto cifrado del mismo ancho de palabra. Esto implica que las operaciones dentro del algoritmo se realizan dentro del campo de Galois. Por lo que como la palabra de entrada es siempre de 128 bits el campo utilizado es el 2^8 .
- El algoritmo está basado en el uso de una clave (key) simétrica.
- Basado en los conceptos de encriptado de difusión, confusión e iteración.
 - **Difusión:** si se cambia un bit en el texto sin cifrar, deberían cambiarse la mayor cantidad posible de bits en el texto cifrado. Para conseguir este efecto se realizan las permutaciones.
 - **Confusión:** la relación entre el texto cifrado y el original sea lo más compleja posible. Para este caso las sustituciones cumplen con dicho objetivo.
 - **Iteración asimétrica:** repetir los procesos de difusión y confusión varias veces pero que la repetición no sea siempre uniforme.

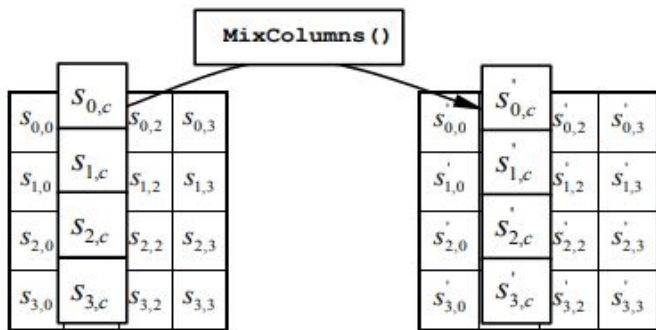
AES Building blocks



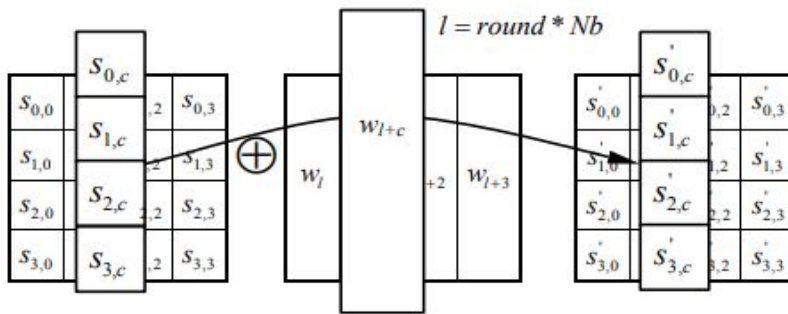
Bytes Substitution



Shiftrows

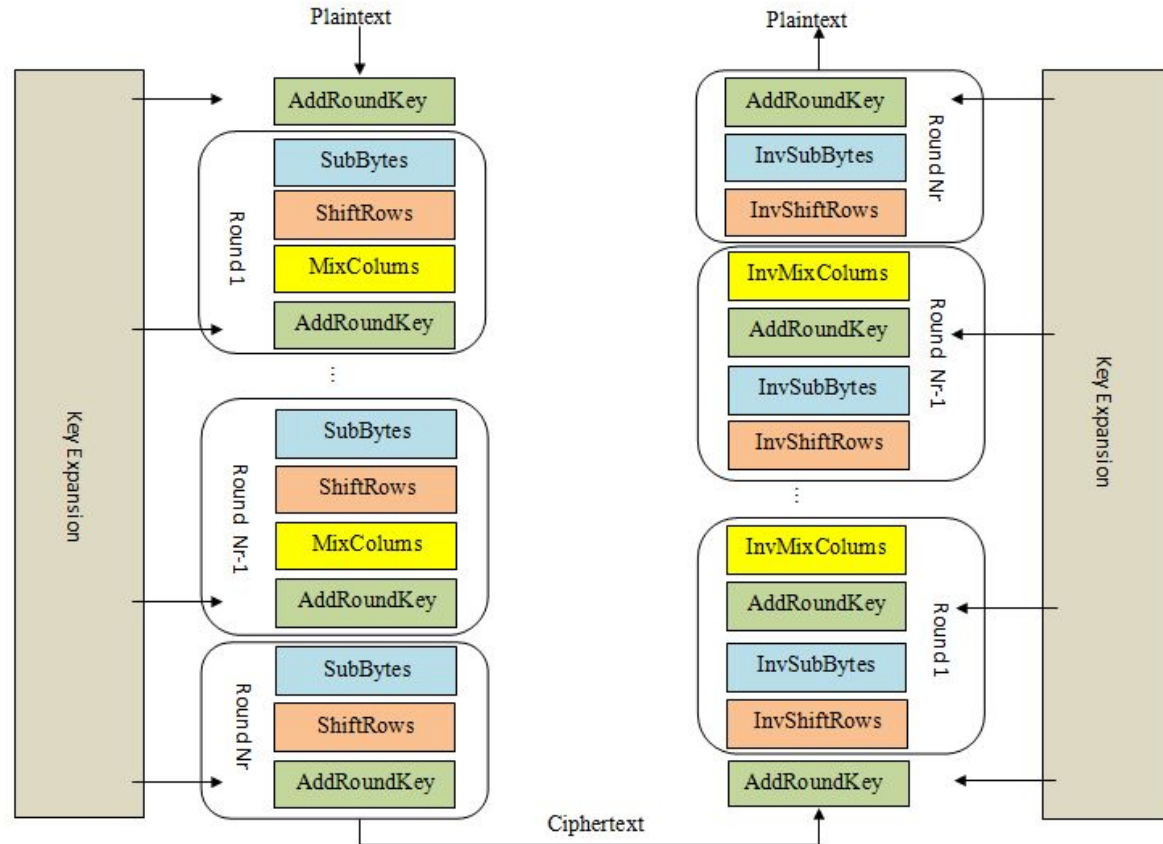


Mix Columns

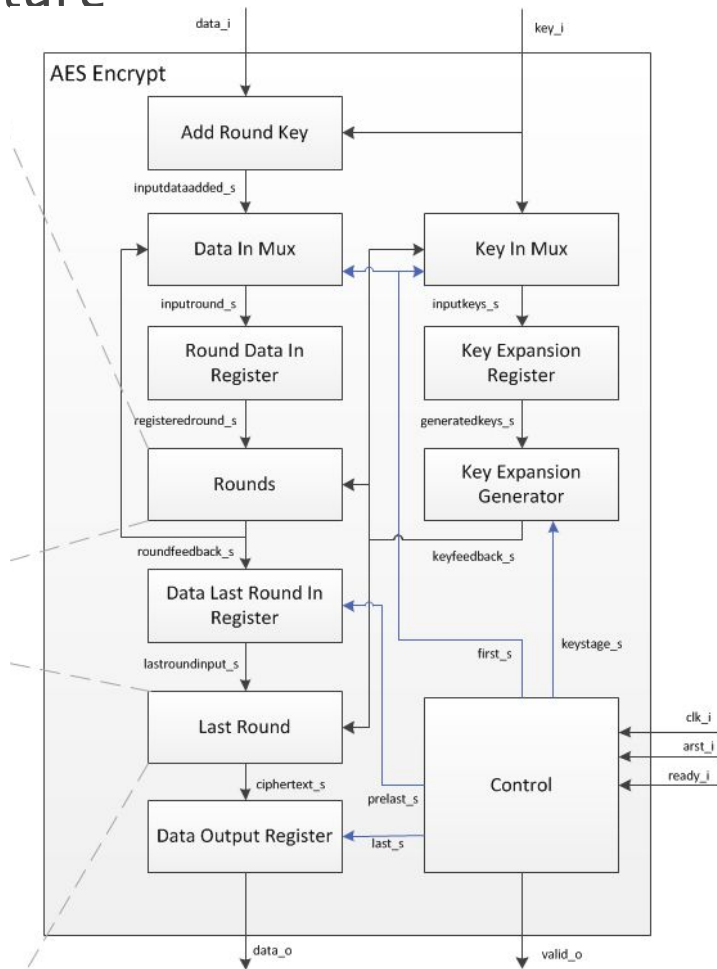
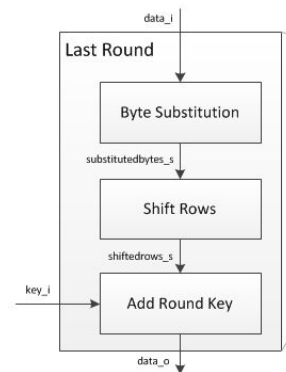
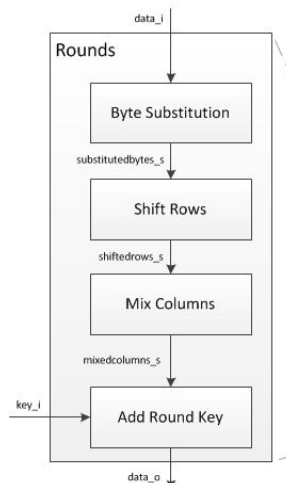


Add Round Key

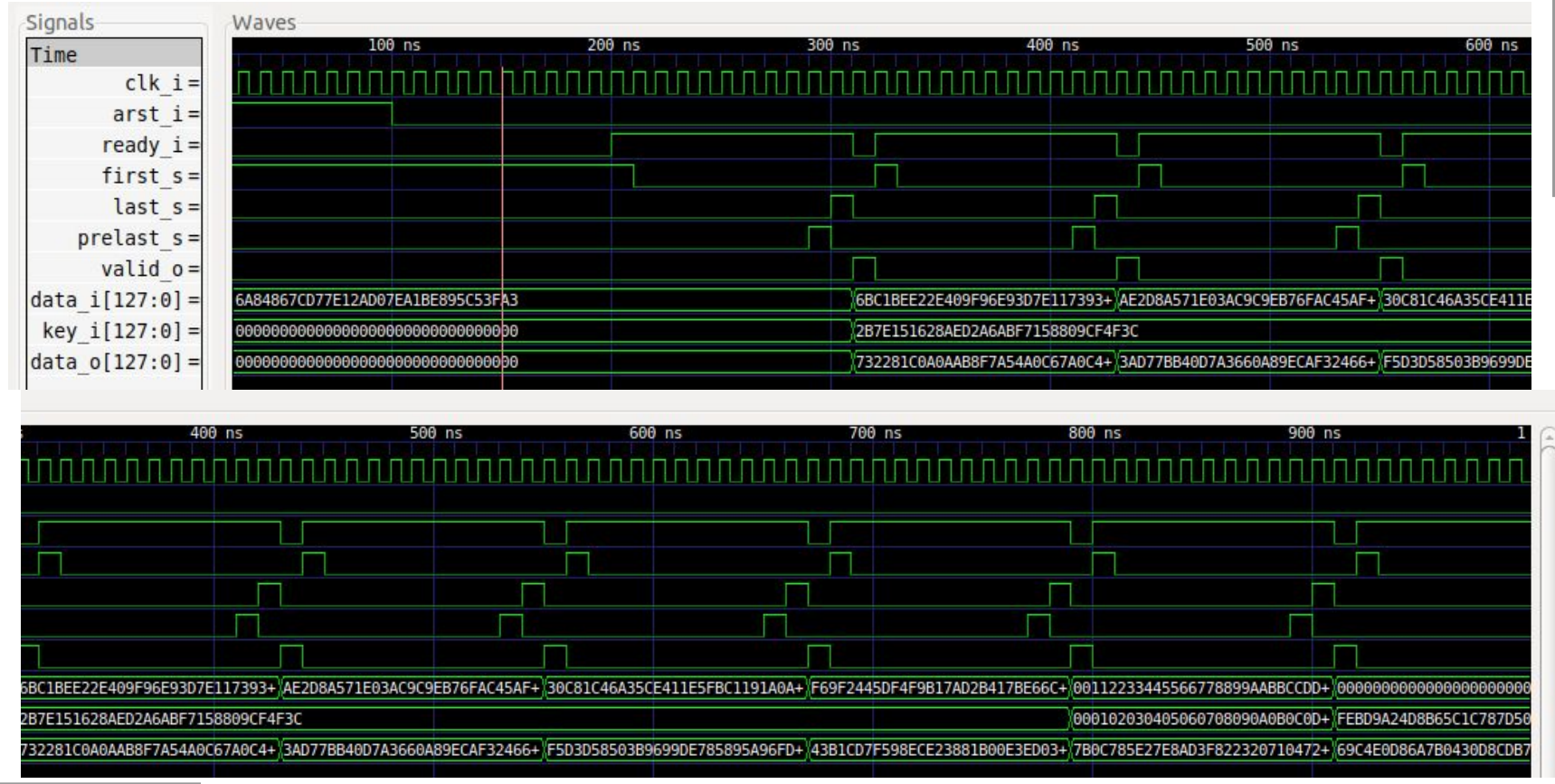
AES Encryption and Decryption



AES Encryption IP Architecture

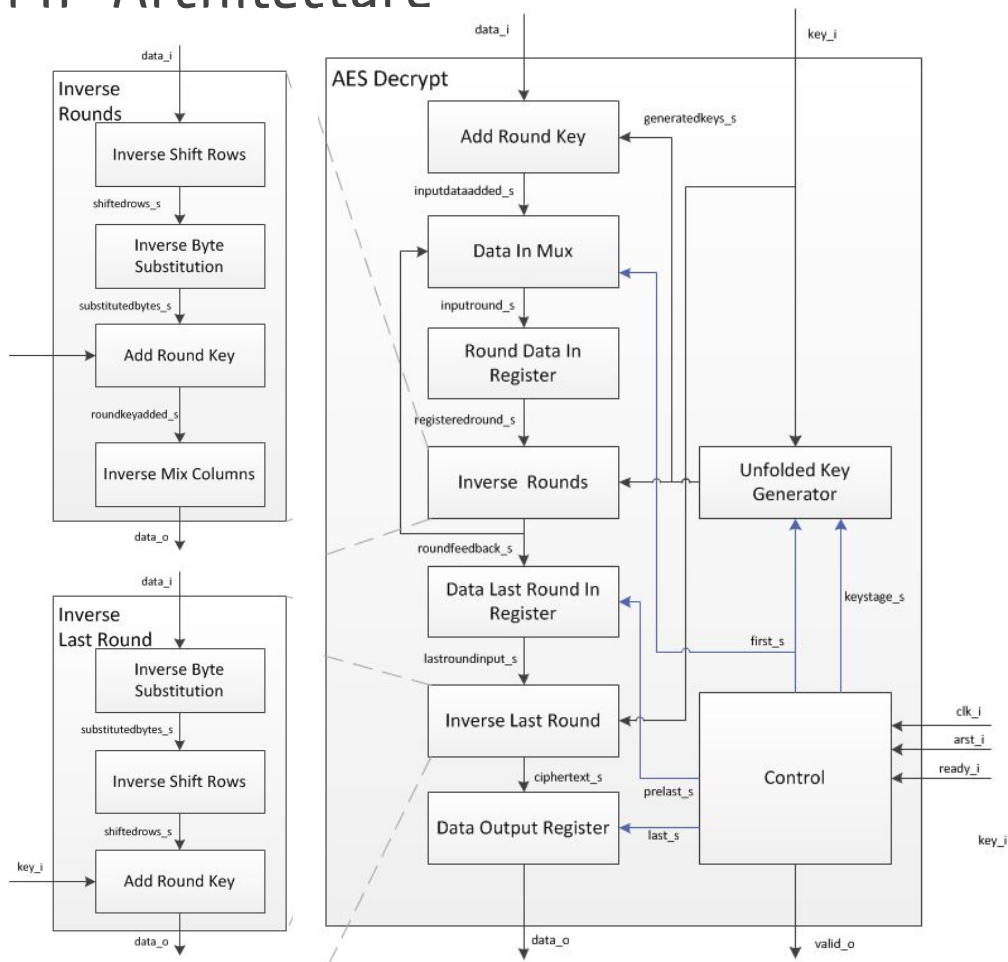


AES Encryption IP Testbench

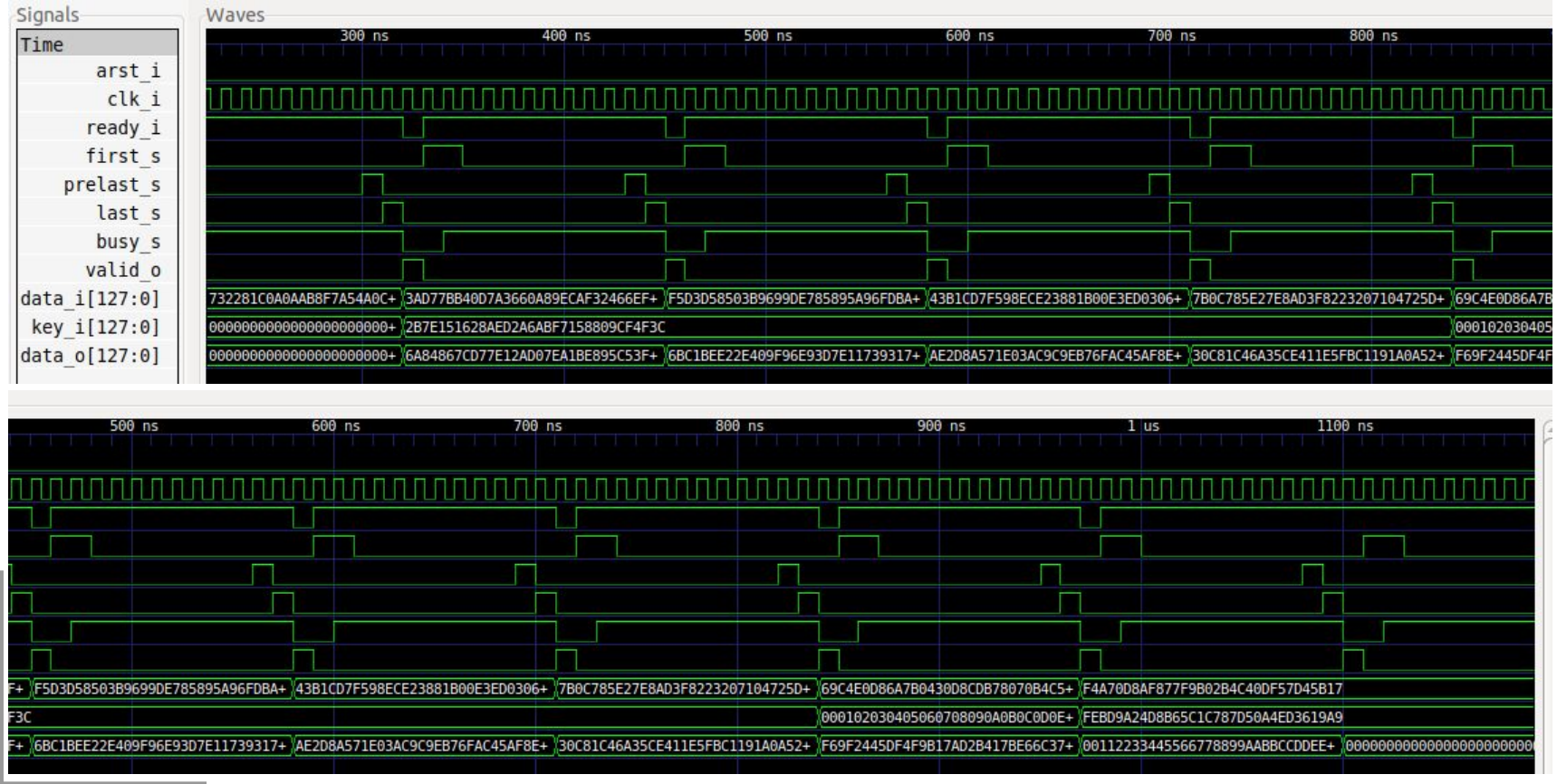


Test Vectors: [NIST.FIPS.197](#) and [AES_Core128](#)

AES Decryption IP Architecture

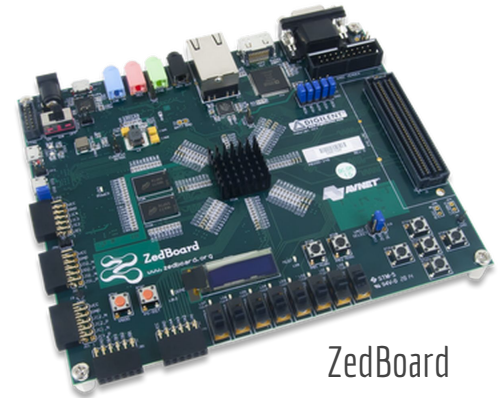
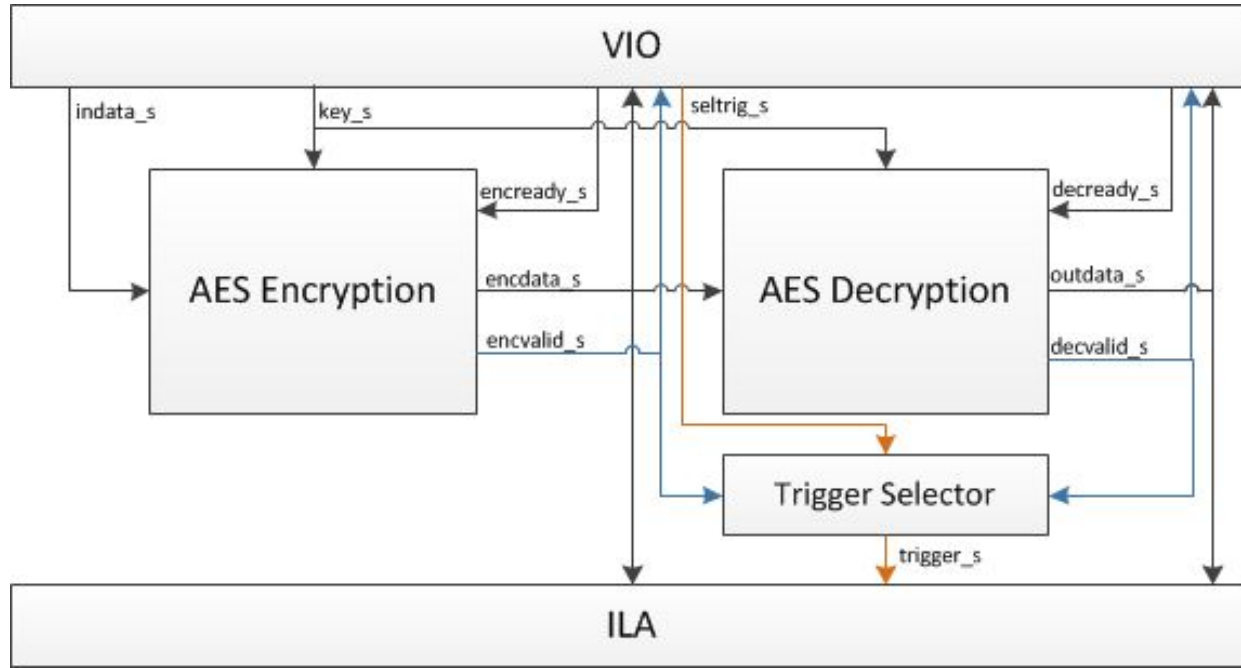


AES Decryption IP Testbench



Test Vectors: [NIST.FIPS.197](#) and [AES_Core128](#)

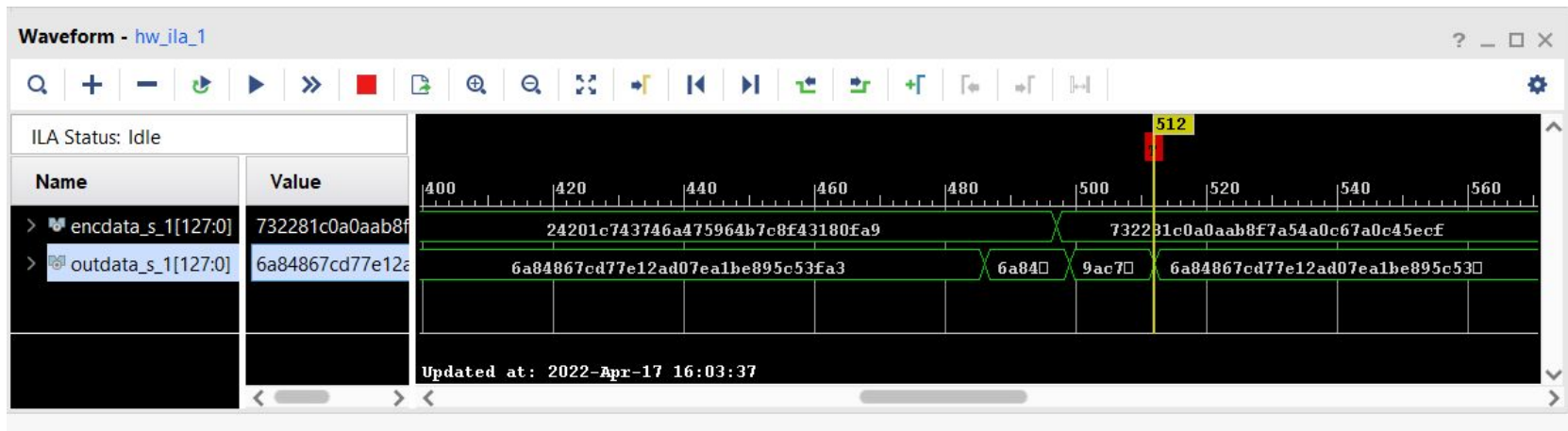
AES Encryption/Decryption HW Implementation



ZedBoard

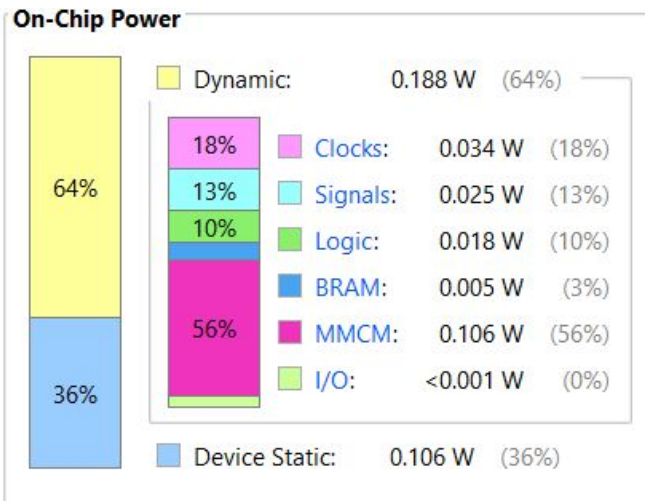
AES on HW Reports

- Timing:
 - Post Synthesis: Tiempo total de camino combinacional crítico 26.729 ns (37.41 MHz).
 - Post Implementation: Tiempo total de camino combinacional crítico 29.631 ns (33.75 MHz).
 - El lazo crítico observado es el que va desde el VIO para la generación de las keys mediante un circuito unfolded de expansión de key. En las pruebas con ILA alimentando el circuito con 100 MHz se logra detectar fallos o valores anómalos a la salida del circuito de decrypt.



AES on HW Reports

- Timing:
 - Post Synthesis: Tiempo total de camino combinacional crítico 6.527 ns (153.21 MHz).
 - Post Implementation: Tiempo total de camino combinacional crítico 9.129 ns (109.54 MHz).
 - Se observa que la implementación en el kit de desarrollo con ILA desaparecen las oscilaciones a la salida del decrypter.
- Power:




AES on HW Reports

Name	Slice LUTs (53200)	Slice Registers (106400)	F7 Muxes (26600)	F8 Muxes (13300)	Block RAM Tile (140)	Bonded IOB (200)	BUFGCTRL (32)	MMCME2_ADV (4)
encdecvio	9033	6820	1603	757	7.5	1	2	1
> clk_wiz_inst (clk_wiz_0)	0	0	0	0	0	0	2	1
dbg_hub (dbg_hub_CV)	0	0	0	0	0	0	0	0
> dec_inst (aesdecrypt)	4855	1872	1152	576	0	0	0	0
> enc_inst (aesencrypt)	2000	560	320	160	0	0	0	0
> ila_inst (ila_0)	1192	2249	3	0	7.5	0	0	0
> vio_inst (vio_1)	985	2139	128	21	0	0	0	0

Post Synthesis Utilization Report

Name	Slice LUTs (53200)	Block RAM Tile (140)	Bonded IOB (200)	BUFGCTRL (32)	MMCME2_ADV (4)	BSCANE2 (4)	Slice Registers (106400)	F7 Muxes (26600)	F8 Muxes (13300)	Slice (13300)	LUT as Logic (53200)	LUT as Memory (17400)
encdecvio	9369	7.5	1	3	1	1	7513	1603	757	3272	9020	349
> clk_wiz_inst (clk_wiz_0)	0	0	0	2	1	0		0	0	0	0	0
> dbg_hub (dbg_hub)	484	0	0	1	0	1		0	0	259	460	24
> dec_inst (aesdecrypt)	4855	0	0	0	0	0		1152	576	1406	4855	0
> enc_inst (aesencrypt)	2000	0	0	0	0	0		320	160	585	2000	0
> ila_inst (ila_0)	1045	7.5	0	0	0	0		3	0	592	720	325
> vio_inst (vio_1)	984	0	0	0	0	0		128	21	600	984	0

Post Implementation Utilization Report



¿Preguntas? ¿Dudas?
¿Sugerencias? ¿Críticas?



¡Muchas Gracias a todos por la atención!