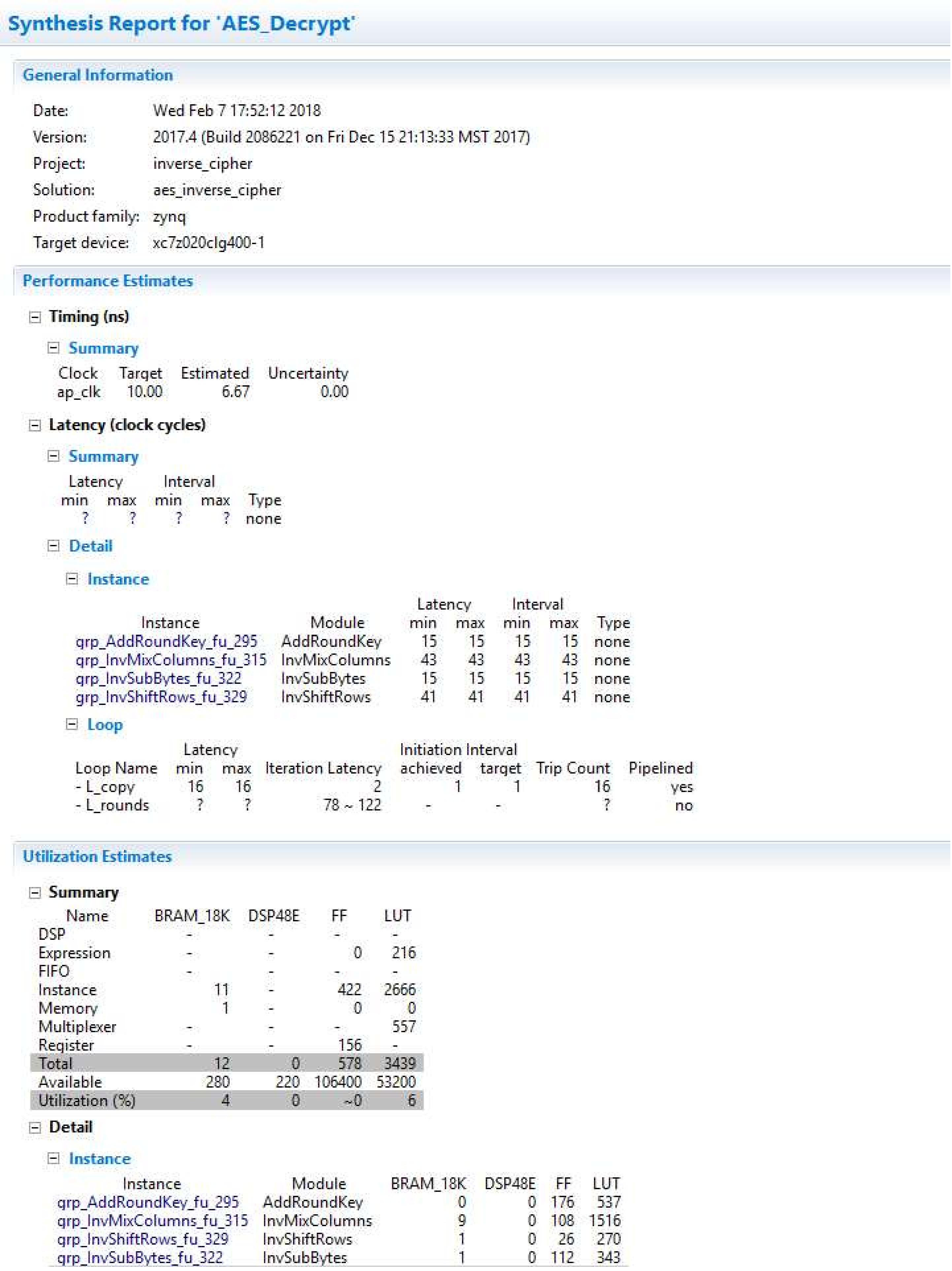


Synthesis Report for 'AES_Decrypt'

General Information

Date:	Wed Feb 7 17:52:12 2018
Version:	2017.4 (Build 2086221 on Fri Dec 15 21:13:33 MST 2017)
Project:	inverse_cipher
Solution:	aes_inverse_cipher
Product family:	zynq
Target device:	xc7z020clg400-1

Performance Estimates

⊟ Timing (ns)

⊟ Summary

Clock	Target	Estimated	Uncertainty
ap_clk	10.00	6.67	0.00

⊟ Latency (clock cycles)

⊟ Summary

Latency		Interval		
min	max	min	max	Type
?	?	?	?	none

⊟ Detail

⊟ Instance

		Latency		Interval		
Instance	Module	min	max	min	max	Type
grp_AddRoundKey_fu_295	AddRoundKey	15	15	15	15	none
grp_InvMixColumns_fu_315	InvMixColumns	43	43	43	43	none
grp_InvSubBytes_fu_322	InvSubBytes	15	15	15	15	none
grp_InvShiftRows_fu_329	InvShiftRows	41	41	41	41	none

⊟ Loop

	Latency			Initiation Interval			
Loop Name	min	max	Iteration Latency	achieved	target	Trip Count	Pipelined
- L_copy	16	16	2	1	1	16	yes
- L_rounds	?	?	78 ~ 122	-	-	?	no

Utilization Estimates

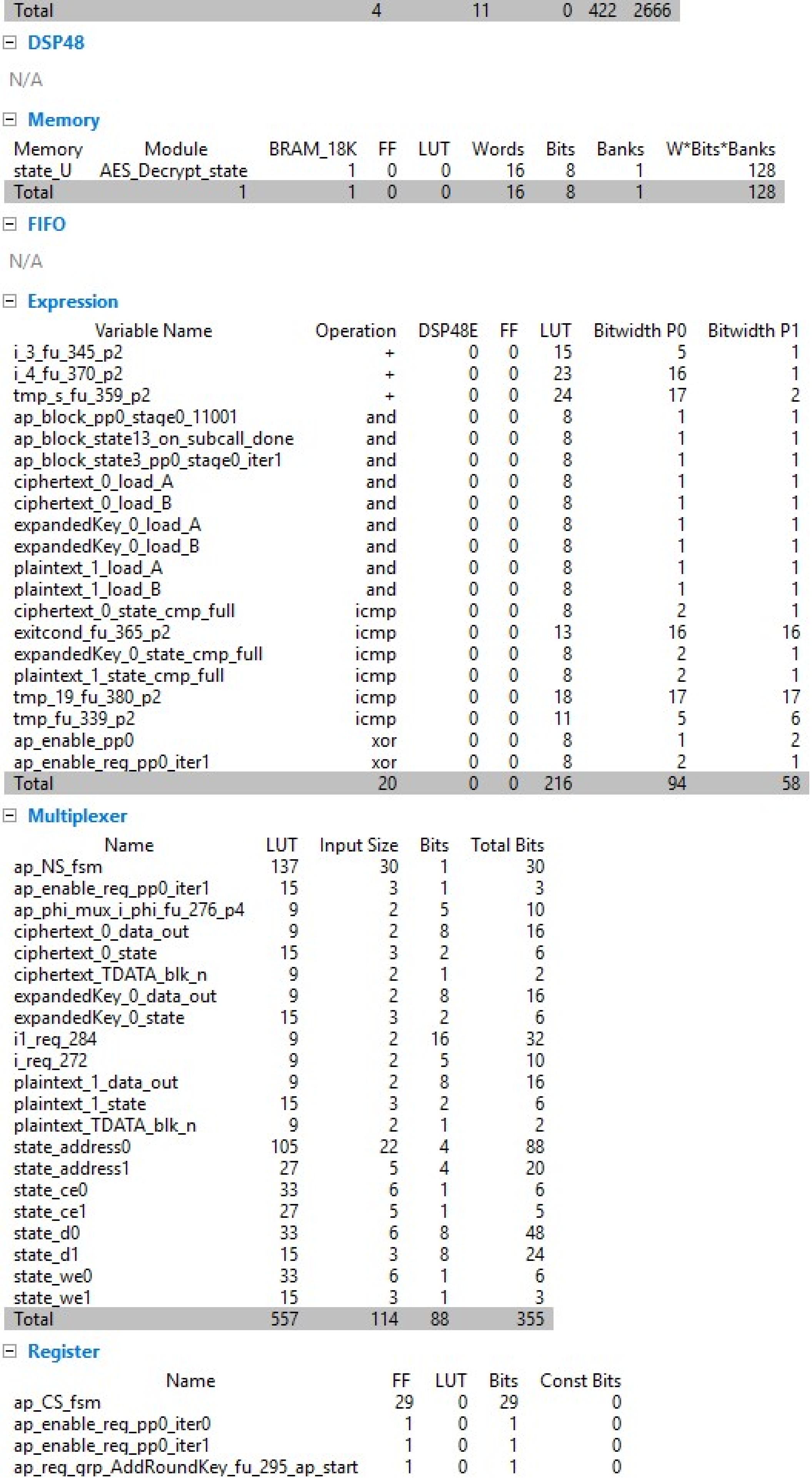
⊟ Summary

Name	BRAM_18K	DSP48E	FF	LUT
DSP	-	-	-	-
Expression	-	-	0	216
FIFO	-	-	-	-
Instance	11	-	422	2666
Memory	1	-	0	0
Multiplexer	-	-	-	557
Register	-	-	156	-
Total	12	0	578	3439
Available	280	220	106400	53200
Utilization (%)	4	0	~0	6

⊟ Detail

⊟ Instance

Instance	Module	BRAM_18K	DSP48E	FF	LUT
grp_AddRoundKey_fu_295	AddRoundKey	0	0	176	537
grp_InvMixColumns_fu_315	InvMixColumns	9	0	108	1516
grp_InvShiftRows_fu_329	InvShiftRows	1	0	26	270
grp_InvSubBytes_fu_322	InvSubBytes	1	0	112	343



Total	4	11	0	422	2666

⊟ DSP48

N/A

⊟ Memory

Memory	Module	BRAM_18K	FF	LUT	Words	Bits	Banks	W*Bits*Banks
state_U	AES_Decrypt_state	1	0	0	16	8	1	128
Total	1	1	0	0	16	8	1	128

⊟ FIFO

N/A

⊟ Expression

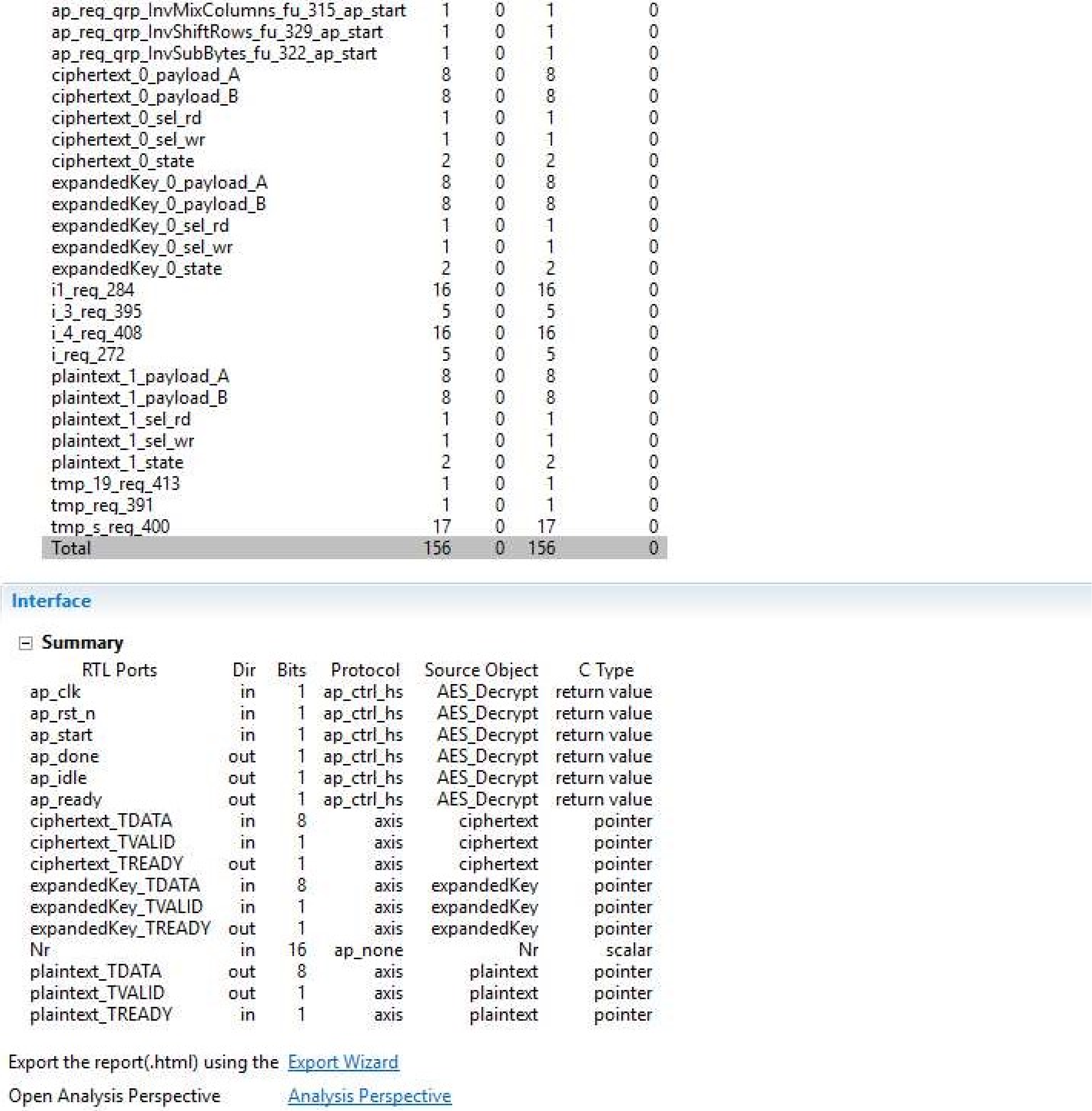
Variable Name	Operation	DSP48E	FF	LUT	Bitwidth P0	Bitwidth P1
i_3_fu_345_p2	+	0	0	15	5	1
i_4_fu_370_p2	+	0	0	23	16	1
tmp_s_fu_359_p2	+	0	0	24	17	2
ap_block_pp0_stage0_11001	and	0	0	8	1	1
ap_block_state13_on_subcall_done	and	0	0	8	1	1
ap_block_state3_pp0_stage0_iter1	and	0	0	8	1	1
ciphertext_0_load_A	and	0	0	8	1	1
ciphertext_0_load_B	and	0	0	8	1	1
expandedKey_0_load_A	and	0	0	8	1	1
expandedKey_0_load_B	and	0	0	8	1	1
plaintext_1_load_A	and	0	0	8	1	1
plaintext_1_load_B	and	0	0	8	1	1
ciphertext_0_state_cmp_full	icmp	0	0	8	2	1
exitcond_fu_365_p2	icmp	0	0	13	16	16
expandedKey_0_state_cmp_full	icmp	0	0	8	2	1
plaintext_1_state_cmp_full	icmp	0	0	8	2	1
tmp_19_fu_380_p2	icmp	0	0	18	17	17
tmp_fu_339_p2	icmp	0	0	11	5	6
ap_enable_pp0	xor	0	0	8	1	2
ap_enable_reg_pp0_iter1	xor	0	0	8	2	1
Total	20	0	0	216	94	58

⊟ Multiplexer

Name	LUT	Input Size	Bits	Total Bits
ap_NS_fsm	137	30	1	30
ap_enable_reg_pp0_iter1	15	3	1	3
ap_phi_mux_i_phi_fu_276_p4	9	2	5	10
ciphertext_0_data_out	9	2	8	16
ciphertext_0_state	15	3	2	6
ciphertext_TDATA_blk_n	9	2	1	2
expandedKey_0_data_out	9	2	8	16
expandedKey_0_state	15	3	2	6
i1_reg_284	9	2	16	32
i_reg_272	9	2	5	10
plaintext_1_data_out	9	2	8	16
plaintext_1_state	15	3	2	6
plaintext_TDATA_blk_n	9	2	1	2
state_address0	105	22	4	88
state_address1	27	5	4	20
state_ce0	33	6	1	6
state_ce1	27	5	1	5
state_d0	33	6	8	48
state_d1	15	3	8	24
state_we0	33	6	1	6
state_we1	15	3	1	3
Total	557	114	88	355

⊟ Register

Name	FF	LUT	Bits	Const Bits
ap_CS_fsm	29	0	29	0
ap_enable_reg_pp0_iter0	1	0	1	0
ap_enable_reg_pp0_iter1	1	0	1	0
ap_reg_grp_AddRoundKey_fu_295_ap_start	1	0	1	0



ap_reg_grp_InvMixColumns_fu_315_ap_start	1	0	1	0
ap_reg_grp_InvShiftRows_fu_329_ap_start	1	0	1	0
ap_reg_grp_InvSubBytes_fu_322_ap_start	1	0	1	0
ciphertext_0_payload_A	8	0	8	0
ciphertext_0_payload_B	8	0	8	0
ciphertext_0_sel_rd	1	0	1	0
ciphertext_0_sel_wr	1	0	1	0
ciphertext_0_state	2	0	2	0
expandedKey_0_payload_A	8	0	8	0
expandedKey_0_payload_B	8	0	8	0
expandedKey_0_sel_rd	1	0	1	0
expandedKey_0_sel_wr	1	0	1	0
expandedKey_0_state	2	0	2	0
i1_reg_284	16	0	16	0
i_3_reg_395	5	0	5	0
i_4_reg_408	16	0	16	0
i_reg_272	5	0	5	0
plaintext_1_payload_A	8	0	8	0
plaintext_1_payload_B	8	0	8	0
plaintext_1_sel_rd	1	0	1	0
plaintext_1_sel_wr	1	0	1	0
plaintext_1_state	2	0	2	0
tmp_19_reg_413	1	0	1	0
tmp_reg_391	1	0	1	0
tmp_s_reg_400	17	0	17	0
Total	156	0	156	0

Interface

⊟ Summary

RTL Ports	Dir	Bits	Protocol	Source Object	C Type
ap_clk	in	1	ap_ctrl_hs	AES_Decrypt	return value
ap_rst_n	in	1	ap_ctrl_hs	AES_Decrypt	return value
ap_start	in	1	ap_ctrl_hs	AES_Decrypt	return value
ap_done	out	1	ap_ctrl_hs	AES_Decrypt	return value
ap_idle	out	1	ap_ctrl_hs	AES_Decrypt	return value
ap_ready	out	1	ap_ctrl_hs	AES_Decrypt	return value
ciphertext_TDATA	in	8	axis	ciphertext	pointer
ciphertext_TVALID	in	1	axis	ciphertext	pointer
ciphertext_TREADY	out	1	axis	ciphertext	pointer
expandedKey_TDATA	in	8	axis	expandedKey	pointer
expandedKey_TVALID	in	1	axis	expandedKey	pointer
expandedKey_TREADY	out	1	axis	expandedKey	pointer
Nr	in	16	ap_none	Nr	scalar
plaintext_TDATA	out	8	axis	plaintext	pointer
plaintext_TVALID	out	1	axis	plaintext	pointer
plaintext_TREADY	in	1	axis	plaintext	pointer

Export the report(.html) using the Export Wizard

Open Analysis Perspective Analysis Perspective