Synthesis Report for 'AES_Decrypt'

General Information

Date: Mon Feb 11 18:35:13 2019
Version: 2018.3 (Build 2405991 on Thu Dec 06 23:56:15 MST 2018)
Project: inverse_cipher
Solution: solution1
Product family: zynq
Target device: xc7z020clg400-1

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	8.00	6.896	0.40

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_800	AddRoundKey	0	0	1	1	function
grp_InvMixColumns_fu_882	InvMixColumns	1	1	1	1	function
grp_InvSubBytes_fu_904	InvSubBytes	1	1	1	1	function
call_ret2_InvShiftRows_fu_926	InvShiftRows	0	0	1	1	function

Loop

	Latency			Initiation Interval			
Loop Name	min	max	Iteration Latency	achieved	target	Trip Count	Pipelined
- L_rounds	?	?	19	16	1	?	yes

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT
DSP	-	-	-	-
Expression	-	-	0	868
FIFO	-	-	-	-
Instance	46	-	302	802
Memory	-	-	-	-
Multiplexer	-	-	-	1128
Register	-	-	670	-
Total	46	0	972	2798
Available	280	220	106400	53200

Utilization (%)	16	0	~0	5

Detail

Instance

Instance	Module	BRAM_18K	DSP48E	FF	LUT
AES_Decrypt_CRTLSic_s_axi_U	AES_Decrypt_CRTLSic_s_axi	6	0	298	282
grp_AddRoundKey_fu_800	AddRoundKey	0	0	0	128
grp_InvMixColumns_fu_882	InvMixColumns	32	0	2	388
call_ret2_InvShiftRows_fu_926	InvShiftRows	0	0	0	0
grp_InvSubBytes_fu_904	InvSubBytes	8	0	2	4
Total	5	46	0	302	802

DSP48

N/A

Memory

N/A

FIFO

N/A

Expression

Variable Name	Operation	DSP48E	FF	LUT	Bitwidth P0	Bitwidth P1
j_1_fu_1422_p2	+	0	0	23	16	1
tmp_2_fu_1331_p2	+	0	0	24	17	2
tmp_5_fu_1449_p2	+	0	0	29	22	6
tmp_83_10_fu_1565_p2	+	0	0	29	22	4
tmp_83_11_fu_1575_p2	+	0	0	29	22	4
tmp_83_12_fu_1585_p2	+	0	0	29	22	3
tmp_83_13_fu_1595_p2	+	0	0	29	22	3
tmp_83_14_fu_1685_p2	+	0	0	29	22	2
tmp_83_1_fu_1465_p2	+	0	0	29	22	5
tmp_83_2_fu_1475_p2	+	0	0	29	22	5
tmp_83_3_fu_1485_p2	+	0	0	29	22	5
tmp_83_4_fu_1495_p2	+	0	0	29	22	5
tmp_83_5_fu_1505_p2	+	0	0	29	22	5
tmp_83_6_fu_1515_p2	+	0	0	29	22	5
tmp_83_7_fu_1525_p2	+	0	0	29	22	5
tmp_83_8_fu_1535_p2	+	0	0	29	22	5
tmp_83_9_fu_1545_p2	+	0	0	29	22	4
tmp_83_s_fu_1555_p2	+	0	0	29	22	4
tmp_3_fu_1432_p2	-	0	0	24	17	17
exitcond_fu_1417_p2	icmp	0	0	13	16	16
tmp_7_fu_1460_p2	icmp	0	0	18	17	17
tmp_71_10_fu_1278_p2	or	0	0	20	20	4
tmp_71_11_fu_1288_p2	or	0	0	20	20	4
tmp_71_12_fu_1298_p2	or	0	0	20	20	4
tmp_71_13_fu_1308_p2	or	0	0	20	20	4
tmp_71_14_fu_1318_p2	or	0	0	20	20	4
tmp_71_1_fu_1188_p2	or	0	0	20	20	2
tmp_71_2_fu_1198_p2	or	0	0	20	20	2

tmp_71_3_fu_1208_p2	or	0	0	20	20	3
tmp_71_4_fu_1218_p2	or	0	0	20	20	3
tmp_71_5_fu_1228_p2	or	0	0	20	20	3
tmp_71_6_fu_1238_p2	or	0	0	20	20	3
tmp_71_7_fu_1248_p2	or	0	0	20	20	4
tmp_71_8_fu_1258_p2	or	0	0	20	20	4
tmp_71_9_fu_1268_p2	or	0	0	20	20	4
tmp_71_s_fu_1178_p2	or	0	0	20	20	1
ap_enable_pp0	xor	0	0	2	1	2
Total	37	0	0	868	736	174

Multiplexer

Name	LUT	Input Size	Bits	Total Bits
ap_NS_fsm	217	50	1	50
ap_enable_reg_pp0_iter1	9	2	1	2
ap_phi_mux_j_phi_fu_793_p4	9	2	16	32
ciphertext_address0	85	17	4	68
expandedKey_address0	149	33	8	264
grp_AddRoundKey_fu_800_state_0_read	15	3	8	24
grp_AddRoundKey_fu_800_state_10_read	15	3	8	24
grp_AddRoundKey_fu_800_state_11_read	15	3	8	24
grp_AddRoundKey_fu_800_state_1213_read	15	3	8	24
grp_AddRoundKey_fu_800_state_13_read	15	3	8	24
grp_AddRoundKey_fu_800_state_14_read	15	3	8	24
grp_AddRoundKey_fu_800_state_15_read	15	3	8	24
grp_AddRoundKey_fu_800_state_1_read	15	3	8	24
grp_AddRoundKey_fu_800_state_2_read	15	3	8	24
grp_AddRoundKey_fu_800_state_3_read	15	3	8	24
grp_AddRoundKey_fu_800_state_4_read	15	3	8	24
grp_AddRoundKey_fu_800_state_5_read	15	3	8	24
grp_AddRoundKey_fu_800_state_6_read	15	3	8	24
grp_AddRoundKey_fu_800_state_7_read	15	3	8	24
grp_AddRoundKey_fu_800_state_8_read	15	3	8	24
grp_AddRoundKey_fu_800_state_9_read	15	3	8	24
j_reg_789	9	2	16	32
plaintext_address0	85	17	4	68
plaintext_d0	85	17	8	136
state_0_6_fu_160	15	3	8	24
state_10_6_fu_200	15	3	8	24
state_11_6_fu_204	15	3	8	24
state_12_6_fu_208	15	3	8	24
state_13_6_fu_212	15	3	8	24
state_14_6_fu_216	15	3	8	24
state_15_6_fu_220	15	3	8	24
state_1_6_fu_164	15	3	8	24
state_2_6_fu_168	15	3	8	24
state_3_6_fu_172	15	3	8	24
state_4_6_fu_176	15	3	8	24
state_5_6_fu_180	15	3	8	24

state_6_6_fu_184	15	3	8	24
state_7_6_fu_188	15	3	8	24
state_8_6_fu_192	15	3	8	24
state_9_6_fu_196	15	3	8	24
Total	1128	236	314	1420

Register

Name	FF	LUT	Bits	Const Bits
Nr_read_reg_2111	16	0	16	0
ap_CS_fsm	49	0	49	0
ap_enable_reg_pp0_iter0	1	0	1	0
ap_enable_reg_pp0_iter1	1	0	1	0
ap_rst_n_inv	1	0	1	0
ap_rst_reg_1	1	0	1	0
ap_rst_reg_2	1	0	1	0
exitcond_reg_2381	1	0	1	0
grp_InvMixColumns_fu_882_ap_start_reg	1	0	1	0
grp_InvSubBytes_fu_904_ap_start_reg	1	0	1	0
j_1_reg_2385	16	0	16	0
j_reg_789	16	0	16	0
reg_1090	8	0	8	0
reg_1095	8	0	8	0
reg_1100	8	0	8	0
reg_1105	8	0	8	0
reg_1110	8	0	8	0
reg_1115	8	0	8	0
reg_1120	8	0	8	0
reg_1125	8	0	8	0
reg_1130	8	0	8	0
reg_1135	8	0	8	0
reg_1140	8	0	8	0
reg_1145	8	0	8	0
reg_1150	8	0	8	0
reg_1155	8	0	8	0
reg_1160	8	0	8	0
state_0_4_reg_2493	8	0	8	0
state_0_6_fu_160	8	0	8	0
state_0_reg_2146	8	0	8	0
state_10_4_reg_2553	8	0	8	0
state_10_6_fu_200	8	0	8	0
state_10_reg_2296	8	0	8	0
state_11_4_reg_2559	8	0	8	0
state_11_6_fu_204	8	0	8	0
state_11_reg_2311	8	0	8	0
state_12_4_reg_2565	8	0	8	0
state_12_6_fu_208	8	0	8	0
state_12_reg_2326	8	0	8	0
state_13_4_reg_2571	8	0	8	0

state_13_6_fu_212	8	0	8	0
state_13_reg_2341	8	0	8	0
state_14_4_reg_2577	8	0	8	0
state_14_6_fu_216	8	0	8	0
state_14_reg_2356	8	0	8	0
state_15_4_reg_2583	8	0	8	0
state_15_6_fu_220	8	0	8	0
state_1_4_reg_2499	8	0	8	0
state_1_6_fu_164	8	0	8	0
state_1_reg_2161	8	0	8	0
state_2_4_reg_2505	8	0	8	0
state_2_6_fu_168	8	0	8	0
state_2_reg_2176	8	0	8	0
state_3_4_reg_2511	8	0	8	0
state_3_6_fu_172	8	0	8	0
state_3_reg_2191	8	0	8	0
state_4_4_reg_2517	8	0	8	0
state_4_6_fu_176	8	0	8	0
state_4_reg_2206	8	0	8	0
state_5_4_reg_2523	8	0	8	0
state_5_6_fu_180	8	0	8	0
state_5_reg_2221	8	0	8	0
state_6_4_reg_2529	8	0	8	0
state_6_6_fu_184	8	0	8	0
state_6_reg_2236	8	0	8	0
state_7_4_reg_2535	8	0	8	0
state_7_6_fu_188	8	0	8	0
state_7_reg_2251	8	0	8	0
state_8_4_reg_2541	8	0	8	0
state_8_6_fu_192	8	0	8	0
state_8_reg_2266	8	0	8	0
state_9_4_reg_2547	8	0	8	0
state_9_6_fu_196	8	0	8	0
state_9_reg_2281	8	0	8	0
tmp_2_reg_2376	17	0	17	0
tmp_4_cast_reg_2390	18	0	22	4
tmp_7_reg_2414	1	0	1	0
tmp_7_reg_2414_pp0_iter1_reg	1	0	1	0
tmp_cast1_reg_2371	16	0	17	1
tmp_s_reg_2122	16	0	20	4
Total	670	0	679	9

Interface

Summary

RTL Ports	Dir	Bits	Protocol	Source Object	C Type
s_axi_CRTLSic_AWVALID	in	1	s_axi	CRTLSic	array
s_axi_CRTLSic_AWREADY	out	1	s_axi	CRTLSic	array
s_axi_CRTLSic_AWADDR	in	10	s_axi	CRTLSic	array

s_axi_CRTLSic_WVALID	in	1	s_axi	CRTLSic	array
s_axi_CRTLSic_WREADY	out	1	s_axi	CRTLSic	array
s_axi_CRTLSic_WDATA	in	32	s_axi	CRTLSic	array
s_axi_CRTLSic_WSTRB	in	4	s_axi	CRTLSic	array
s_axi_CRTLSic_ARVALID	in	1	s_axi	CRTLSic	array
s_axi_CRTLSic_ARREADY	out	1	s_axi	CRTLSic	array
s_axi_CRTLSic_ARADDR	in	10	s_axi	CRTLSic	array
s_axi_CRTLSic_RVALID	out	1	s_axi	CRTLSic	array
s_axi_CRTLSic_RREADY	in	1	s_axi	CRTLSic	array
s_axi_CRTLSic_RDATA	out	32	s_axi	CRTLSic	array
s_axi_CRTLSic_RRESP	out	2	s_axi	CRTLSic	array
s_axi_CRTLSic_BVALID	out	1	s_axi	CRTLSic	array
s_axi_CRTLSic_BREADY	in	1	s_axi	CRTLSic	array
s_axi_CRTLSic_BRESP	out	2	s_axi	CRTLSic	array
ap_clk	in	1	ap_ctrl_hs	AES_Decrypt	return value
ap_rst_n	in	1	ap_ctrl_hs	AES_Decrypt	return value
interrupt	out	1	ap_ctrl_hs	AES_Decrypt	return value

Export the report(.html) using the Export Wizard

Open Analysis Perspective Analysis Perspective