Synthesis Report for 'AES_Encrypt'

General Information

Date: Mon Feb 11 18:48:33 2019
Version: 2018.3 (Build 2405991 on Thu Dec 06 23:56:15 MST 2018)
Project: cipher
Solution: solution1
Product family: zynq
Target device: xc7z020clg400-1

Performance Estimates

Timing (ns)

Summary

Clock	Target	Estimated	Uncertainty
ap_clk	8.00	5.081	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_1040	AddRoundKey	0	0	1	1	function
grp_MixColumns_fu_1154	MixColumns	1	1	1	1	function
grp_SubBytes_fu_1176	SubBytes	1	1	1	1	function
call_ret3_ShiftRows_fu_1214	ShiftRows	0	0	1	1	function

Loop

	Latency			Initiation Interval			
Loop Name	min	max	Iteration Latency	achieved	target	Trip Count	Pipelined
- L_rounds	?	?	17	16	1	?	yes

Utilization Estimates

Summary

Name	BRAM_18K	DSP48E	FF	LUT
DSP	-	-	-	-
Expression	-	-	0	532
FIFO	-	-	-	-
Instance	30	-	430	802
Memory	-	-	-	-
Multiplexer	-	-	-	1227
Register	-	-	891	-
Total	30	0	1321	2561
Available	280	220	106400	53200

Utilization (%)	10	0	1	4

Detail

Instance

Instance	Module	BRAM_18K	DSP48E	FF	LUT
AES_Encrypt_CRTLSc_s_axi_U	AES_Encrypt_CRTLSc_s_axi	6	0	298	282
grp_AddRoundKey_fu_1040	AddRoundKey	0	0	0	128
grp_MixColumns_fu_1154	MixColumns	16	0	130	388
call_ret3_ShiftRows_fu_1214	ShiftRows	0	0	0	0
grp_SubBytes_fu_1176	SubBytes	8	0	2	4
Total	5	30	0	430	802

DSP48

N/A

Memory

N/A

FIFO

N/A

Expression

Variable Name	Operation	DSP48E	FF	LUT	Bitwidth P0	Bitwidth P1
j_1_fu_1401_p2	+	0	0	23	16	1
tmp_3_fu_1428_p2	+	0	0	28	21	5
tmp_78_10_fu_1767_p2	+	0	0	28	21	5
tmp_78_11_fu_1777_p2	+	0	0	28	21	5
tmp_78_12_fu_1787_p2	+	0	0	28	21	5
tmp_78_13_fu_1603_p2	+	0	0	28	21	5
tmp_78_14_fu_1677_p2	+	0	0	28	21	5
tmp_78_1_fu_1439_p2	+	0	0	28	21	5
tmp_78_2_fu_1593_p2	+	0	0	28	21	5
tmp_78_3_fu_1687_p2	+	0	0	28	21	5
tmp_78_4_fu_1697_p2	+	0	0	28	21	5
tmp_78_5_fu_1707_p2	+	0	0	28	21	5
tmp_78_6_fu_1717_p2	+	0	0	28	21	5
tmp_78_7_fu_1727_p2	+	0	0	28	21	5
tmp_78_8_fu_1737_p2	+	0	0	28	21	5
tmp_78_9_fu_1747_p2	+	0	0	28	21	5
tmp_78_s_fu_1757_p2	+	0	0	28	21	5
tmp_s_fu_1390_p2	+	0	0	24	17	2
ap_condition_271	and	0	0	2	1	1
ap_predicate_op258_call_state21_state33	and	0	0	2	1	1
exitcond_fu_1396_p2	icmp	0	0	13	16	16
tmp_1_fu_1411_p2	icmp	0	0	18	17	17
ap_enable_pp0	xor	0	0	2	1	2
Total	23	0	0	532	405	120

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_889_p4	9	2	16	32
ap_phi_reg_pp0_iter1_state_0_1_40_reg_1031	9	2	8	16
ap_phi_reg_pp0_iter1_state_10_1_30_reg_941	9	2	8	16
ap_phi_reg_pp0_iter1_state_11_1_29_reg_932	9	2	8	16
ap_phi_reg_pp0_iter1_state_12_1_28_reg_923	9	2	8	16
ap_phi_reg_pp0_iter1_state_13_1_27_reg_914	9	2	8	16
ap_phi_reg_pp0_iter1_state_14_1_26_reg_905	9	2	8	16
ap_phi_reg_pp0_iter1_state_15_1_25_reg_896	9	2	8	16
ap_phi_reg_pp0_iter1_state_1_1_39_reg_1022	9	2	8	16
ap_phi_reg_pp0_iter1_state_2_1_38_reg_1013	9	2	8	16
ap_phi_reg_pp0_iter1_state_3_1_37_reg_1004	9	2	8	16
ap_phi_reg_pp0_iter1_state_4_1_36_reg_995	9	2	8	16
ap_phi_reg_pp0_iter1_state_5_1_35_reg_986	9	2	8	16
ap_phi_reg_pp0_iter1_state_6_1_34_reg_977	9	2	8	16
ap_phi_reg_pp0_iter1_state_7_1_33_reg_968	9	2	8	16
ap_phi_reg_pp0_iter1_state_8_1_32_reg_959	9	2	8	16
ap_phi_reg_pp0_iter1_state_9_1_31_reg_950	9	2	8	16
ciphertext_address0	85	17	4	68
ciphertext_d0	85	17	8	136
expandedKey_address0	149	33	8	264
grp_AddRoundKey_fu_1040_p_read19	15	3	8	24
grp_AddRoundKey_fu_1040_p_read20	15	3	8	24
grp_AddRoundKey_fu_1040_p_read21	15	3	8	24
grp_AddRoundKey_fu_1040_p_read22	15	3	8	24
grp_AddRoundKey_fu_1040_p_read23	15	3	8	24
grp_AddRoundKey_fu_1040_p_read24	15	3	8	24
grp_AddRoundKey_fu_1040_p_read25	15	3	8	24
grp_AddRoundKey_fu_1040_p_read26	15	3	8	24
grp_AddRoundKey_fu_1040_p_read27	15	3	8	24
grp_AddRoundKey_fu_1040_p_read28	15	3	8	24
grp_AddRoundKey_fu_1040_p_read29	15	3	8	24
grp_AddRoundKey_fu_1040_p_read30	15	3	8	24
grp_AddRoundKey_fu_1040_p_read31	15	3	8	24
grp_AddRoundKey_fu_1040_state_0_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_10_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_11_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_1213_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_13_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_14_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_15_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_1_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_2_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_3_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_4_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_5_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_6_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_7_read	15	3	8	24
grp_AddRoundKey_fu_1040_state_8_read	15	3	8	24

grp_AddRoundKey_fu_1040_state_9_read	15	3	8	24
j_reg_885	9	2	16	32
plaintext_address0	85	17	4	68
Total	1227	259	418	1604

Register

Name	FF	LUT	Bits	Const Bits
Nr_read_reg_2032	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_phi_reg_pp0_iter0_state_0_1_40_reg_1031	8	0	8	0
ap_phi_reg_pp0_iter0_state_10_1_30_reg_941	8	0	8	0
ap_phi_reg_pp0_iter0_state_11_1_29_reg_932	8	0	8	0
ap_phi_reg_pp0_iter0_state_12_1_28_reg_923	8	0	8	0
ap_phi_reg_pp0_iter0_state_13_1_27_reg_914	8	0	8	0
ap_phi_reg_pp0_iter0_state_14_1_26_reg_905	8	0	8	0
ap_phi_reg_pp0_iter0_state_15_1_25_reg_896	8	0	8	0
ap_phi_reg_pp0_iter0_state_1_1_39_reg_1022	8	0	8	0
ap_phi_reg_pp0_iter0_state_2_1_38_reg_1013	8	0	8	0
ap_phi_reg_pp0_iter0_state_3_1_37_reg_1004	8	0	8	0
ap_phi_reg_pp0_iter0_state_4_1_36_reg_995	8	0	8	0
ap_phi_reg_pp0_iter0_state_5_1_35_reg_986	8	0	8	0
ap_phi_reg_pp0_iter0_state_6_1_34_reg_977	8	0	8	0
ap_phi_reg_pp0_iter0_state_7_1_33_reg_968	8	0	8	0
ap_phi_reg_pp0_iter0_state_8_1_32_reg_959	8	0	8	0
ap_phi_reg_pp0_iter0_state_9_1_31_reg_950	8	0	8	0
ap_phi_reg_pp0_iter1_state_0_1_40_reg_1031	8	0	8	0
ap_phi_reg_pp0_iter1_state_10_1_30_reg_941	8	0	8	0
ap_phi_reg_pp0_iter1_state_11_1_29_reg_932	8	0	8	0

Interface

Summary

RTL Ports	Dir	Bits	Protocol	Source Object	C Type
s_axi_CRTLSc_AWVALID	in	1	s_axi	CRTLSc	array
s_axi_CRTLSc_AWREADY	out	1	s_axi	CRTLSc	array
s_axi_CRTLSc_AWADDR	in	10	s_axi	CRTLSc	array
s_axi_CRTLSc_WVALID	in	1	s_axi	CRTLSc	array
s_axi_CRTLSc_WREADY	out	1	s_axi	CRTLSc	array
s_axi_CRTLSc_WDATA	in	32	s_axi	CRTLSc	array
s_axi_CRTLSc_WSTRB	in	4	s_axi	CRTLSc	array
s_axi_CRTLSc_ARVALID	in	1	s_axi	CRTLSc	array
s_axi_CRTLSc_ARREADY	out	1	s_axi	CRTLSc	array
s_axi_CRTLSc_ARADDR	in	10	s_axi	CRTLSc	array
s_axi_CRTLSc_RVALID	out	1	s_axi	CRTLSc	array
s_axi_CRTLSc_RREADY	in	1	s_axi	CRTLSc	array
s_axi_CRTLSc_RDATA	out	32	s_axi	CRTLSc	array
s_axi_CRTLSc_RRESP	out	2	s_axi	CRTLSc	array
s_axi_CRTLSc_BVALID	out	1	s_axi	CRTLSc	array

s_axi_CRTLSc_BREADY	in	1	s_axi	CRTLSc	array
s_axi_CRTLSc_BRESP	out	2	s_axi	CRTLSc	array
ap_clk	in	1	ap_ctrl_hs	AES_Encrypt	return value
ap_rst_n	in	1	ap_ctrl_hs	AES_Encrypt	return value
interrupt	out	1	ap_ctrl_hs	AES_Encrypt	return value

Export the report(.html) using the Export Wizard

Open Analysis Perspective Analysis Perspective