به نام خداوند بخشنده و مهربان

گزارش فاز سوم پروژه fpga

وجیهه ترحمی

فاطمه سادات هاشمی گلپایگانی

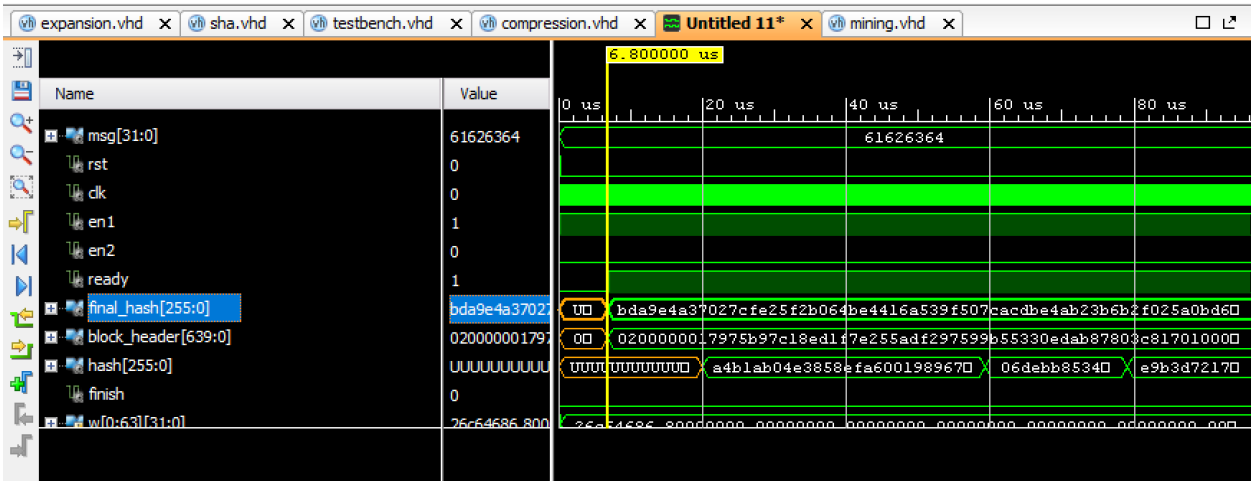
برای پیاده سازی این فاز کار های مربوط به الگوریتم sha همگی در یک ماژول پیاده سازی شد. برای عملکرد دقیق تر برای این ماژول یک ورودی enable در نظر گرفته شد. در ماژول sha یک ماژول expansion موجود می باشد که فعالساز ان همان enable ماژول sha است. زمانی که این ماژول خروجی اماده کند سیگنال finish را یک کرده و باعث فعال شدن ماژول compression یک می شود. پس از پایان کار ماژول compression اول خروجی finish ان ۱ می شود. حال اگر طول پیام طوری باشد که نیاز به کار ماژول compression دوم باشد ان ماژول فعال می شود وگرنه خروجی finish ماژول sha ۱ می شود بدین معنا که خروجی معتبر است. اینکه ایا نیاز به کار ماژول compression دوم هست یا نه توسط سیگنالی به نام two_block که توسط expansion با توجه به طول پیام ورودی مقدار دهی می شود.

برای بخش mining ماژول دیگری ساخته شد که در ان از sha استفاده می شود. بدین صورت که ورودی به یک ماژول sha داده می شود و خروجی ان به sha دیگری داده می شود. ماژول دوم در صورتی که کار ماژول اول تمام شود و خروجی finish ان ۱ شود فعال می شود.

با تغییر خروجی finish ماژول دوم (یعنی زمانی که ماژول دوم نیز کارش تمام شد) در پراسس بررسی می شود که ایا مقدار hash از مقدار target کمتر شده یا نه. اگر کمتر شده بود که سیگنال finish ماژول ماینینگ ۱ می شود به این معنی که کار این ماؤول تمام شده و خروجی معتبر است. اما اگر کمتر نشده بود مقدار nonce یک واحد افزایش می باید و ماژول های sha ریست می شوند تا برای ورودی جدید مقدار هش را حساب کنند. Process مربوطه حساس مقدار ready1 که همان خروجی finish ماژول sha دوم می باشد است.

برای تست این مدار ابتدا با یک ماژول sha مقدار هش اولیه را حساب می کنیم و به کمک ان block_header را مقدار دهی می کنیم. سپس این مقدار را به ماژول mining ورودی می دهیم و حاصل را بررسی می کنیم.

تصویر شبیه سازی:



مشاهده می شود که هنگامی که مقدار block_header محاسبه شده سیگنال ready که در اصل فعالساز ماژول mining می باشد ۱ شده است و از ان جا کار ماژول ماینینگ شروع شده است. مقدار hash مدام تغییر می کند تا زمانی که کمتر از target شود.

گزارش زمان اجرای الگوریتم:

ماژول sha برای اجرا با کلاک 50ns نیاز به 6.8 us دارد. (در ماژول compression به جای استفاده از حلقه فور با هر کلاک یکبار محاسبات مربوطه انجام می شود. از ان جایی که این محاسبات باید ۶۴ بار انجام شود نیاز به ۶۴ سیکل کلاک داریم. همین طور ماژول expansion در بیش از ۱ کلاک کار خود را انجام می دهد.). از طرفی ماژول mining برای تولید هر هش نیاز به 20us دارد و ان قدر هش تولید می کند (حلقه while) تا مقدار هش از مقدار تارگت کمتر شود.

1. Slice Logic

Site Type	Used	Fixed	Available	Util%
Slice LUTs*	1	0	303600	<0.01
LUT as Logic	1	0	303600	<0.01
LUT as Memory	0	0	130800	0.00
Slice Registers	1	0	607200	<0.01
Register as Flip Flop	1	0	607200	<0.01
Register as Latch	0	0	607200	0.00
F7 Muxes	0	0	151800	0.00
F8 Muxes	0	0	75900	0.00

Copyright 1986-2015 Xilinx, Inc. All Rights Reserved.

|Tool Version : Vivado v.2015.4 (win64) Build 1412921 Wed Nov 18 09:43:45 MST 2015
|Date : Fri Jul 13 23:11:44 2018
|Host : Fatemeh running 64-bit major release (build 9200)
|Command : report_utilization -file mining_utilization_synth.rpt -pb mining_utilization_synth.pb
|Design : mining
|Device : 7vx485tffg1157-1
|Design State : Synthesized

Utilization Design Information

Table of Contents

.۱Slice Logic
۱,۱Summary of Registers by Type
.۲Memory

۳.DSP

۴.IO and GT Specific

۵.Clocking

۶.Specific Feature

۷.Primitives

۸.Black Boxes

۹.Instantiated Netlists

۱.Slice Logic

Site Type	Used	Fixed	Available	Util%
Slice LUTs*	1	0	303600	<0.01
LUT as Logic	1	0	303600	<0.01
LUT as Memory	0	0	130800	0.00
Slice Registers	1	0	607200	<0.01
Register as Flip Flop	1	0	607200	<0.01
Register as Latch	0	0	607200	0.00
F7 Muxes	0	0	151800	0.00
F8 Muxes	0	0	75900	0.00

*Warning! The Final LUT count, after physical optimizations and full implementation, is typically lower. Run opt_design after synthesis, if not already completed, for a more realistic count.

۱,۱.Summary of Registers by Type

Total	Clock Enable	Synchronous	Asynchronous
-	-	_	0
-	_	0	Set
-	_	0	Reset
_	0	Set	-
_	0	Reset	-
0	Yes	-	-

٠	Yes	-	Set
٠	Yes	-	Reset
٠	Yes	Set	-
١	Yes	Reset	-

+----------+----------+----------+-------+

.٢Memory

+-------+----------+-------+------+----------+
|Site Type | Used | Fixed | Available | Util| ٪
+-------+----------+-------+------+----------+
Block RAM Tile	0	0	1030	0.00
RAMB36/FIFO*	0	0	1030	0.00
RAMB18	0	0	2060	0.00
+-------+----------+-------+------+----------+

※Note: Each Block RAM Tile only has one FIFO logic available and therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a RAMB18E1

.٣DSP

+-------+----------+-------+------+----------+
|Site Type | Used | Fixed | Available | Util| ٪
+-------+----------+-------+------+----------+
|DSPs | 0 | 0 | 2800 | 0.00|
+-------+----------+-------+------+----------+

.٤IO and GT Specific

+-------+----------+-------+------+----------+
|Site Type | Used | Fixed | Available | Util| ٪
+-------+----------+-------+------+----------+
|Bonded IOB | 259 | 0 | 600 | 43.17|

Bonded IPADs	0	0	62	0.00
Bonded OPADs	0	0	40	0.00
PHY_CONTROL	0	0	14	0.00
PHASER_REF	0	0	14	0.00
OUT_FIFO	0	0	56	0.00
IN_FIFO	0	0	56	0.00
IDELAYCTRL	0	0	14	0.00
IBUFGDS	0	0	576	0.00
GTXE2_COMMON	0	0	5	0.00
GTXE2_CHANNEL	0	0	20	0.00
PHASER_OUT/PHASER_OUT_PHY	0	0	56	0.00
PHASER_IN/PHASER_IN_PHY	0	0	56	0.00
IDELAYE2/IDELAYE2_FINEDELAY	0	0	700	0.00
ODELAYE2/ODELAYE2_FINEDELAY	0	0	700	0.00
IBUFDS_GTE2	0	0	28	0.00
ILOGIC	0	0	600	0.00
OLOGIC	0	0	600	0.00

5. Clocking

Site Type	Used	Fixed	Available	Util%
BUFGCTRL	1	0	32	3.13
BUFIO	0	0	56	0.00
MMCME2_ADV	0	0	14	0.00
PLLE2_ADV	0	0	14	0.00
BUFMRCE	0	0	28	0.00
BUFHCE	0	0	168	0.00
BUFR	0	0	56	0.00

6. Specific Feature

Site Type	Used	Fixed	Available	Util%

BSCANE2	0	0	4	0.00
CAPTUREE2	0	0	1	0.00
DNA_PORT	0	0	1	0.00
EFUSE_USR	0	0	1	0.00
FRAME_ECCE2	0	0	1	0.00
ICAPE2	0	0	2	0.00
PCIE_2_1	0	0	4	0.00
STARTUPE2	0	0	1	0.00
XADC	0	0	1	0.00

.YPrimitives

_____

Ref Name	Used	Functional Category
OBUF	257	IO
IBUF	2	IO
LUT2	1	LUT
LUT1	1	LUT
FDRE	1	Flop & Latch
BUFG	1	Clock