Modern Environmental Science and Engineering (ISSN 2333-2581)
September 2016, Volume 2, No. 9, pp. 625-630
Doi: 10.15341/mese(2333-2581)/09.02.2016/007
Academic Star Publishing Company, 2016
www.academicstar.us

Simulation-Based Power Estimation of Low Power MD5 Design Techniques

Shamsiah Binti Suhaili[1], and Takahiro Watanabe[2]

1. Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

2. Graduate School of Information, Production and Systems, Waseda University, Japan

Abstract: Hash function is important in security system design where transmission of data need to be secured enough to avoid eavesdropping and unauthorized monitoring. Efficient implementation needs to be considered in designing MD5 hash function in terms of high speed, small area and low power design. The objective of this project is to obtain low power MD5 design as well as balancing between maximum frequency and area implementation. Therefore, two low power design techniques have been proposed in order to reduce the power consumption of MD5 hash function such as state encoding and clock gating. In this paper, four different types of MD5 were successfully designed based on Arria II GX Altera Quartus II namely MD5_Binary, MD5_Gray, MD5_Gating and MD5_Gray_Gating. These designs were simulated using ModelSim to evaluate the correctness of the output results. Dynamic power is consumed when signal change their logic state in CMOS transistor. In this paper, dynamic power dissipation of MD5 Gray encoding with clock gating reduce significantly which is 20.72% if compared with MD5 Binary encoding. Furthermore, MD5 Binary encoding with clock gating provides efficient implementation in terms of speed, area and power. From this analysis, simulation-based power estimation generated from the PowerPlay Power Analyzer Altera Quartus II can provide accurate power estimation.

Key words: MD5, simulation-based power, PowerPlay

1. Introduction

Nowadays, implementation of hash function on reconfigurable hardware becomes important aspect because of its fast implementation. Field programmable gate array (FPGA) is one of the solutions for hardware implementation problem. It consists of tenth of thousands building block, known as Configurable Logic Blocks (CLB) which connected with several interconnection programmable [1]. It has input output (I/O) block which provides interface between outside world and internal logic structure. Hardware Description Language (HDL) and schematic design are two methods to describe digital logic design based on FPGA. The main advantage of FPGA is its reconfigurability. Furthermore, it provides low development cost, easy for verification but suffer with high power consumption. Therefore, two techniques on how to reduce power consumption in MD5 hash function design have been proposed such as state encoding and clock gating.

Power consumption of CMOS transistor can be divided into three parts such as dynamic, static (leakage) and short circuit power consumption. Switching power consists of dynamic and short circuits. It occurs when the signals through CMOS transistor and change their logic state. Leakage power happens during circuit is “power-on” because of the sub-threshold currents and reverse biased diodes in a CMOS transistor [2]. Hence, equation 1 shows total power dissipation.

$$P_{total}=P_{dynamic}+P_{short\text{-}circuit}+P_{leakage} \quad (1)$$

In this paper, four different types of MD5 designs were written and synthesized in Verilog code and

Corresponding author: Shamsiah Binti Suhaili, E-mail: sushamsiah@unimas.my.

Altera Quartus II respectively. These results will produce a netlist that represents the mapping of the Verilog code to the Arria II GX. Then, during implementation process, the place-and-route will perform to identify the physical allocation of the MD5 designs. After implementation process was successful, these designs were simulated by using ModelSim to evaluate the results of MD5. The paper was organized as the following. MD5 Algorithm was introduced in section 2. Methodologies of low power MD5 designs were proposed in section 3. Results and discussion was presented in section 4. Finally, conclusion was made in section 5.

2. MD5 Algorithm

Hash function has been widely used in communication security system. One of the famous hash functions was the MD5 message digest which was developed by Ronald Rivest [3]. MD5 Algorithm start with arbitrary message input in order to produce 128-bit message output. The first step was message padding where the message was padded with single 1-bit at the end of the message then it was followed by 0-bit until the length of the message was congruent to 448 modulus 512. Then, the message was appended with 64-bit which was the length of the message. Finally, overall of the input message, M was 512-bit. Four 32-bit register A, B, C, and D are shown in Table 2.0 in little-endian format.

512-bit messages were divided into 16 blocks. The process of the message executed from input message M[0] until M[15]. In this algorithm, there are four different non-linear functions in the step function such as *F, G, H* and *I*. The messages processed in 64 rounds where 16 steps number for each non-linear function.

Table 1 Buffer initialization.

Register	Little-endian Format
A	32'h67452301
B	32'hefcdab89
C	32'h98badcfe
D	32'h10325476

There were 16 32-bit Message input, $M_i[j]$, 64 constant value, *K* and 64 shift value, *S* in order to obtain the hash code of MD5. The following Eq. (2) shows the operations of MD5. Func(B,C,D) represents non-linear function *F, G, H* and *I* as shown in Table 2. Symbol <<S denotes shift value of the function. *i* and *j* represent round value and input message respectively.

$$A = B + ((A + Func(B,C,D) + Mi[j] + K[i]) << S)$$
$$A = D,\ B = A,\ C = B,\ D = C \quad (2)$$

From Table 2, symbol ∧, ∨, ¬ and ⊕ denote logical AND, OR, NOT and XOR operation respectively. Finally, the output of MD5 designs were obtained by adding the initial input with the last 64 round of non-linear function *I*.

3. Proposed Design

There are many researchers involved in designing MD5 design with different objectives and goals [5-8]. In this paper, the proposed designs focus on low power design implementation. One of the techniques to reduce dynamic power is switching activity. In this paper, two techniques of switching activity of low power designs are introduced in order to reduce the power consumption of MD5 such as state encoding and clock gating using Verilog code. For state encoding, MD5 designs were divided into two different designs namely MD5_Binary and MD5_Gray which represent FSM for Binary encoding and Gray encoding. Table 3 shows simple example encoding transition for seven states for both Binary and Gray encoding. From this table, maximum transition per clock cycle for Gray encoding is one while for Binary encoding is three. This is because the Gray encoding only changes 1-bit per state during transition. By using this technique to Finite State Machine (FSM) design, the usage of power consumption can be reduced.

Table 2 Non-linear function of MD5.

Func(B,C,D)	
F(B,C,D)	(B ∧ C) ∨ (¬B ∧ D)
G(B,C,D)	(B ∧ D) ∨ (C ∧ ¬D)
H(B,C,D)	(B ⊕ C ⊕ D)
I(B,C,D)	(C ⊕ (B ∨ ¬D)

Table 3 State encoding.

State	Gray	Binary
S0	000	000
S1	001	001
S2	011	010
S3	010	011
S4	110	100
S5	111	101
S6	101	110
S7	100	111
Maximum transition per clock cycle	1	3

The second technique to reduce power consumption is clock gating. By gating the clock, the power consumption can also be reduced because the designs only execute the operation when there is available input which is already ANDed together with the clock input. Fig. 1 illustrates the example of clock gating. In order to analyse the effect of clock gating to MD5 designs, both Binary encoding and Gray encoding MD5 designs were designed using clock gating namely MD5 Binary gating and MD5 Gray gating.

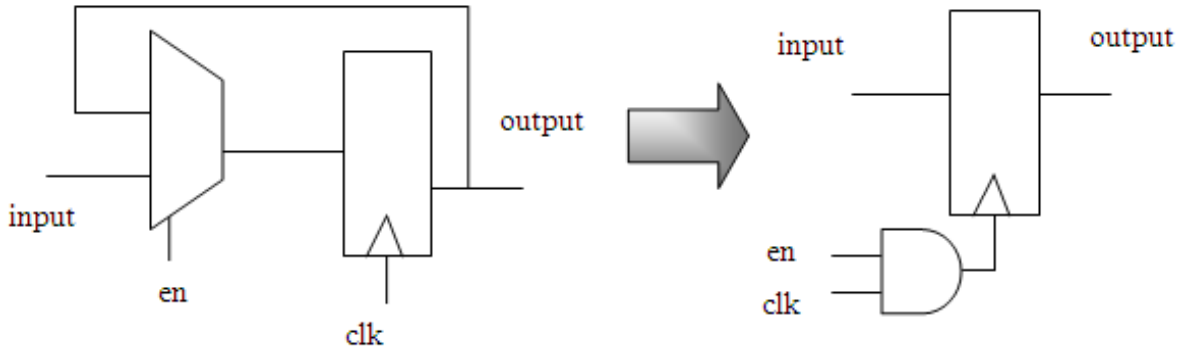

Fig. 1 Clock gating.

4. Results and Discussion

MD5 designs were successfully designed using Verilog code. The MD5 designs have been synthesized and implemented based on Arria II GX Altera Quartus II. The results of MD5 designs were based on frequency, area and power consumption. The MD5 designs were simulated using ModelSim to evaluate the output of the designs in terms of both functional and timing simulation. There are four different types of MD5 designs; MD5, MD5_Gray, MD5_Gating and MD5_Gray_Gating. MD5 represents MD5 design with Binary encoding, MD5_Gray denotes MD5 design with Gray encoding, MD5_Gating means MD5 Binary encoding with clock gating and finally MD5_Gray_Gating refers to MD5 Gray encoding with clock gating. The power analysis has been done using PowerPlay Power Analyzer in order to verify the effect of switching activity such as state encoding and clock gating to the MD5 designs.

Table 4 shows the result of simulation-based power estimation of four different types of MD5 designs. From this table, power dissipation is divided into three different components such as dynamic thermal power dissipation, static power dissipation and I/O thermal power dissipation. As mentioned earlier, dynamic power is caused by signal toggling and static power due to leakage currents while I/O Power considers the I/O pin and it takes into account every possible parameter describing the off-chip board trace at each I/O pin [8]. Altera Quartus II PowerPlay Power Analyzer is a power analysis tool that can provide the most accurate power analysis which uses actual design placement and routing and logic configuration. In other words, it can provide accurate power estimation of power consumption. PowerPlay power analyzer usually provides ±10% accuracy when used with accurate design information [8]. These power predictions by PowerPlay power analyzer tools are accurate if compared with actual silicon.

The results show the total thermal power dissipation of MD5_Binary is the highest power consumption if compared with others which is 363.70 mW. This is because of dynamic thermal power dissipation of MD5 Binary encoding is high if compared with other designs. The results for static and I/O power dissipation are almost the same. Figs. 2-5 show the total thermal power dissipation result of MD5_Binary, MD5_Gray, MD5_Binary_Gating and MD5_Gray_Gating.

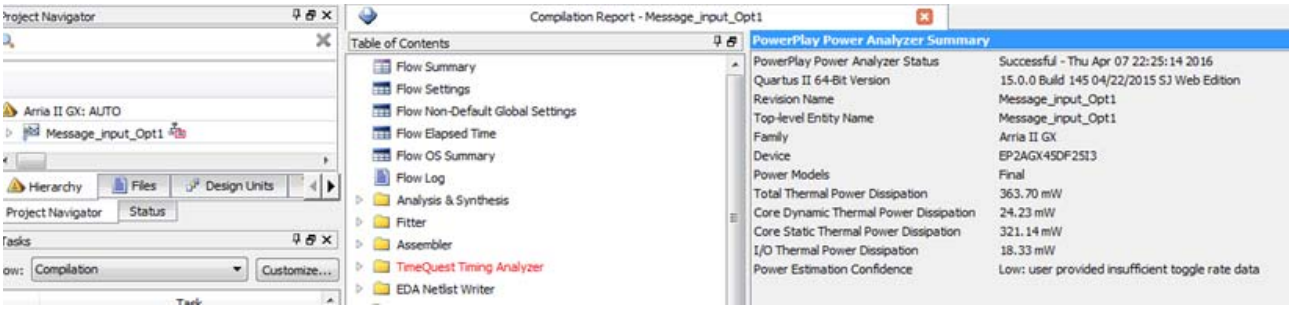

Fig. 2 Total thermal power dissipation of MD5_Binary.

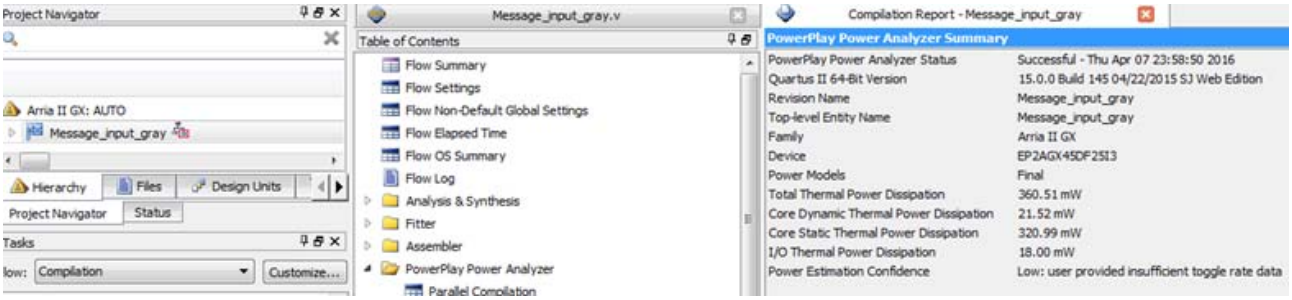

Fig. 3 Total thermal power dissipation of MD5_Gray.

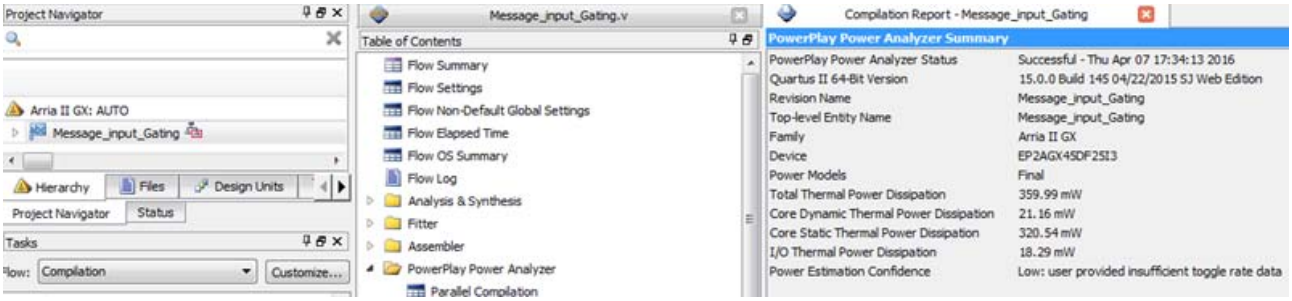

Fig. 4 Total thermal power dissipation of MD5_Gray_Gating.

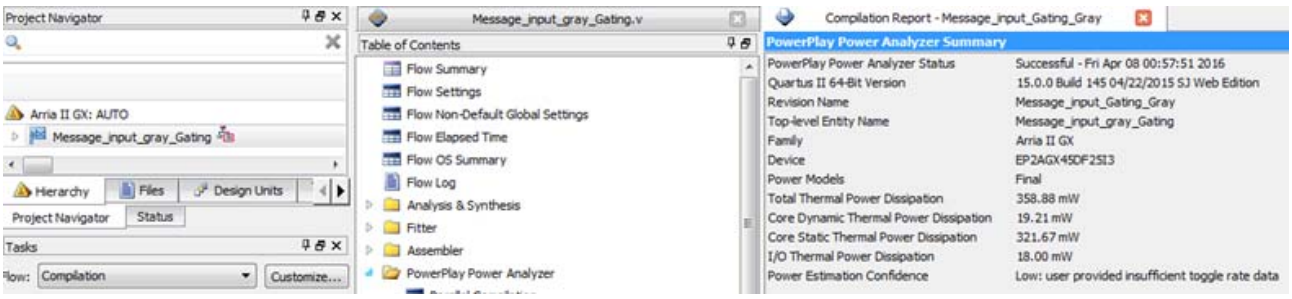

Fig.5 Total thermal power dissipation of MD5_Gray_Gating.

Furthermore, dynamic power dissipation reduces to 21.52 mW for MD5 Gray encoding. Similar with MD5 Binary encoding with clock gating the amount of dynamic power reduces to 21.74 mW. From Table 4,

the power consumption of MD5 Gray encoding with clock gating reduce significantly to 19.21 mW. Hence, by using both techniques such as state encoding and clock gating, low power MD5 design can be obtained. Our design can reduce dynamic power dissipation, but it is about 1/15 of the static power. Therefore, static power dissipation can be reduced by using another low power techniques.

Table 5 shows the results for maximum frequency and area implementation of MD5 designs. From this table, MD5 Binary encoding give the highest maximum frequency, 154.62 MHz with small area implementation which is 1623 and 650 ALUT and total register respectively. However, based on power analysis of MD5 Binary encoding, this design consumes high dynamic power dissipation. Therefore, in order to obtain efficient MD5 design implementation in terms of power, frequency and area, MD5 Binary encoding with clock gating is the most suitable where the total register is small, 649 and the maximum frequency reduce a little bit if compared with MD5 Binary encoding which is 141.62 MHz but it provides low dynamic power dissipation which in only 21.74 mW. Figs. 6-9 shows the simulation result by using ModelSim Altera of MD5_Binary, MD5_Gray, MD5_Binary_Gating and MD5_Gray_Gating.

Table 4 Simulation-based power estimation of four different types of MD5 designs.

Design	MD5_Binary	MD5_Gray	MD5_Binary_gating	MD5_Gray_gating
Total Thermal power dissipation	363.70 mW	360.51 mW	399.99 mW	358.88 mW
Core Dynamic Thermal Power Dissipation	24.23 mW	21.52 mW	21.16 mW	19.21 mW
Core Static Thermal Power Dissipation	321.14mW	320.99 mW	320.54 mW	321.67 mW
I/O Thermal Power Dissipation	18.33 mW	18.00 mW	18.29 mW	18.00 mW

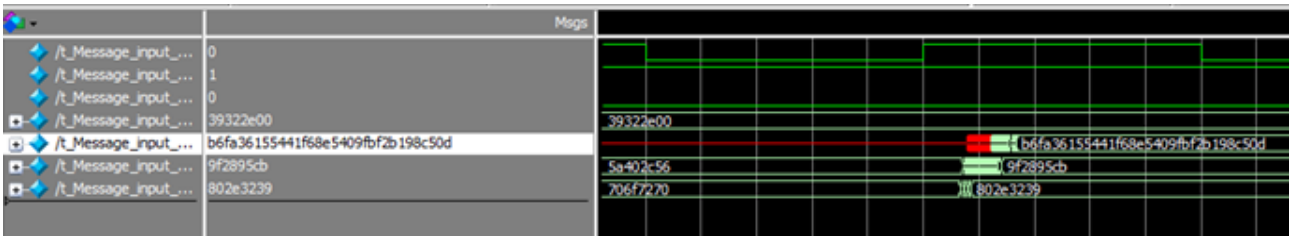

Fig. 6 Simulation result of MD5 binary.

Fig. 7 Simulation Result of MD5 Gray.

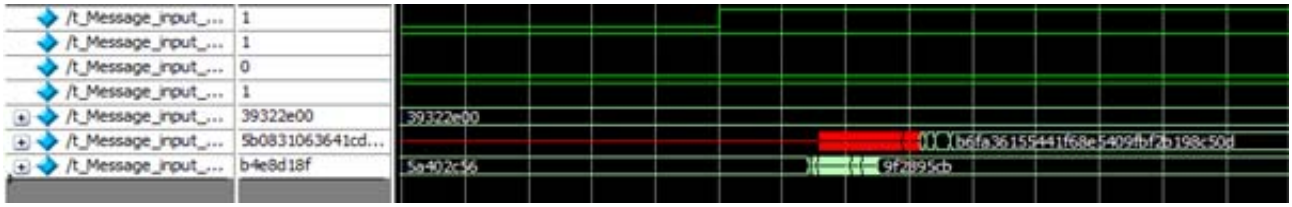

Fig. 8 Simulation Result of MD5 Binary Gating

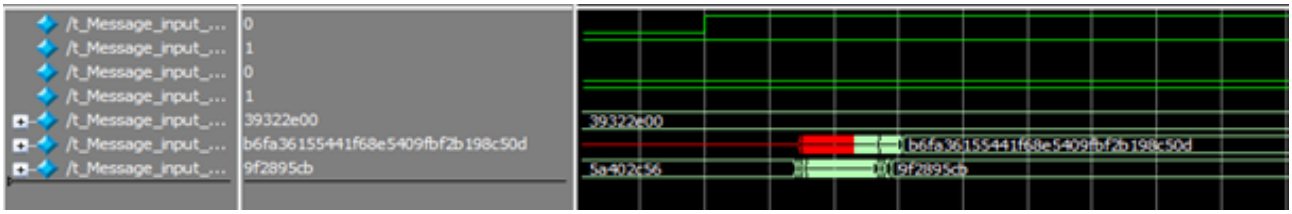

Fig. 9 Simulation Result of MD5 Gray Gating.

Table 5 Maximum Frequency and Area Implementation.

Design	MD5_Binary	MD5_Gray	MD5_Binary_gating	MD5_Gray_gating
Constraint (sdc)	7	10	7.5	10.5
FMax 100C Model	147.36 MHz	128.57 MHz	135.83 MHz	130.74 MHz
FMax -40C Model	154.61 MHz	134.16 MHz	141.62 MHz	137.7 MHz
ALUT	1623	1818	1647	1793
Total Register	650	974	649	973

5. Conclusions

In conclusion, four different types of MD5 designs were successfully designed by using Verilog such as MD5_Binary, MD5_Gray, MD5_gating, and MD5_Gray_gating. Based on PowerPlay Power Analyzer, implementation with Gray encoding and clock gating can reduce the power consumption. It provides accurate simulation-based power estimation. From this analysis, dynamic power dissipation of MD5 Gray encoding with clock gating reduces about 20.72% if compared with MD5_Binary. Moreover, MD5 binary encoding can be classified as an efficient implementation of MD5 design which can provide balance in terms speed, area and power.

Acknowledgments

This work was supported by Universiti Malaysia Sarawak (UNIMAS)

References

[1] F. R. Henriquez, N. A. Saqib, A. D. Perez and C. K. Koc, *Cryptogtraphic Algorithm on Reconfigurable Hardware*, Springer series on Signal and Communication, 2006, pp. 35-62.

[2] P. R. Panda, B. V. N. Silpa, A. Shrivastava and K. Gummidipudi, *Basic Low Power Digital Design, Power-efficient System Design*, Chapter 2, Springer Science Business Media, LLC, 2010.

[3] R. L. Rivest, *The MD5 Message-Digest Algorithm, RFC 1321*, MIT Laboratory for Computer Science and RSA Data Security Inc., April 1992.

[4] Y. Wang, Q. Zhao, L. Jiang and Y. Shao, Ultra high throughput implementation for MD5 hash algorithm on FPGA, high performance computing and applications, *Lecture Notes in Computer Science 5938*, 2010, pp. 433-441.

[5] K. Jarvinen, M. Tommiska and J. Skytta, Hardware implementation analysis of the MD5 hash algorithm, in: *Proceedings of the 38th Hawaii International Conference on System Sciences*, 2005.

[6] J. M. Diez, S. Bojanix, L. J. Stanimirovic, C. Carreras and O. Nieto-Taladriz, *Hash Algorithms for Cryptographic Protocols: FPGA Implementations, 10th Telecommunications Forum TELFOR'2002*, Belgrade, Yugoslavia, Nov. 26-28, 2002.

[7] J. Deepakumara, H. M. Heys and R. Venkatesan, FPGA implementation of MD5 hash algorithm, in: *Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE 2001*, Toronto, Canada, 2001, Vol. 2, pp. 919-924.

[8] FPGA Power Management and Modeling Techniques, White Paper, (December 2010), Altera Corporation, 101 Innovation Drive San Jose, CA 95134, available online at: https://www.altera.com/en_US/pdfs/literature/wp/wp-01044.pdf.