DOI 10.31489/2020No1/151-156

UDC: 621.38.049.77

DESIGN AND RESEARCH OF THE BEHAVIORAL MODEL FOR THE MODULAR REDUCTION DEVICE

Aitkhozhayeva Y.Zh.[1], Tynymbayev S. [2], Adilbekkyzy S. [3], Skabylov A.[4*], Ibraimov M.[4]

[1] K.I. Satbayev Kazakh National Research Technical University, Almaty, Kazakhstan
[2]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
[3]L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
[4]Al-Farabi Kazakh National University, Almaty, Kazakhstan, skabylov212@gmail.com

A behavioral model of the modular reduction device with optimal hardware costs was designed in CAD Quartus Prime Lite Edition. An algorithm of operation is implemented in the Verilog HDL language. A method is used where, at each step of the calculation, the value of either tripled, doubled, or single value of the module is subtracted from the most significant bits shifted to the left by two. Functional and timing modeling of the behavioral model algorithm using examples was carried out and the correctness of the algorithm was confirmed. The device circuit at the register transfer level (RTL) for the low-budget FPGA Cyclone VE 5CEBA4F23C7 from Altera is obtained. A timing analysis was performed using a time analyzer to determine the maximum clock frequency for the principal and behavioral models in various working conditions.

Keywords: asymmetric crypto-algorithms, hardware encryption, modular reduction, behavioral model, design.

Introduction

New information and communication technologies, which are the technological drivers of the Fourth Industrial Revolution, bring with them not only new opportunities, but also new challenges of ensuring information security. The relevance of these problems is evident against the backdrop of a global trend towards an increase in the number of cyber-attacks, leading to significant financial, material and human losses. Systems based on new technologies, such as Blockchain, Cloud Computing, Internet of Things (IOT), Cyber-Physical Systems (CPS), are systems with an unlimited number of network interaction participants. High-speed symmetric encryption, requiring the transfer of an individual secret key to each participant, is not applicable to protect information in such systems. Besides, the use of asymmetric encryption, in which public keys are distributed to participants of network interaction, is associated with the issue of low speed of asymmetric cryptographic algorithms. Complex and cumbersome procedures for modular exponentiation very large integers during encryption and decryption in asymmetric cryptographic algorithms are time consuming. The transition from software to hardware implementation of asymmetric encryption can improve the characteristics of encryption in terms of performance. However, the hardware implementation does not improve the performance of asymmetric cryptographic algorithms so much as to approach the speed of symmetric cryptographic algorithms.

The international research community pays great attention to solving the problem of improving the performance of asymmetric cryptosystems. The emphasis is on the hardware implementation of asymmetric cryptographic algorithms. The most complex basic operation of modular exponentiation large numbers with asymmetric encryption is the modular reduction. Moreover, in many research papers, acceleration of asymmetric encryption is proposed by accelerating the operation of modular reduction of integers by developing new and adapting (modifying) existing algorithms and circuit solutions of modular reduction devices [1-12].

1. Purpose and objectives

There are an increase in speed is achieved by increasing the hardware costs, which are directly proportional to the capacity of the given numbers in most solutions. Therefore, their use in reducing multi-bit numbers is justified if there are no requirements for optimizing hardware costs. It should be borne in mind that increasing hardware costs leads to increased power consumption and lower reliability. The actual issue is the accelerated determination of the remainder modulo an arbitrary number (modular reduction) with optimization of hardware costs and low cost.

The functional block diagram of a device for modular reduction of binary integers with optimization of hardware costs and low cost is developed and presented by the authors in [13]. The purpose of this work is to design and study the behavioral model of this modular reduction device, to determine its advantages and disadvantages compared to the principal model. In previous studies, the design of the circuit diagrams of the device blocks and the principal model of the entire device as a whole was performed [14, 15]. For the design and debugging of the principal model CAD Quartus Prime Lite Edition Version 16.0 (Altera) was used. The implementation of the device is focused on the low-budget board DE0-CV with an integrated circuit FPGA of the Cyclone VE base family, manufactured by Altera (the parent organization of Intel) - 5CEBA4F23C7.

The objectives of this study are to develop a behavioral in Verilog HDL language, to study it and to perform a comparative analysis of the principal model and behavioral model of a device using a textual description of circuits of a device for quickly reducing binary integers modulo from the point of view of hardware and time costs when implementing a device on a low-budget FPGA family Cyclone VE base – 5CEBA4F23C7. Cyclone series low-cost boards are designed for use in a variety of applications where low power consumption and low cost are key parameters. Therefore, the Cyclone family is the optimal solution for mass, cost-critical applications.

2. Designing a behavioral model of the high-speed device for modular reduction

The structure of the considered device of fast reduction of numbers modulo consists of a controlling block, a block of shift register, a block of former of the multipliers of the module *P*, and a block of former of the partial remainders r_i (Figure-1). In this device, to accelerate the calculation of the remainder twice when dividing the $2n$-bit number *A* by the *n*-bit module *P*, we used the method where, at each step of the calculation, the value*P* of either tripled *(3P)*, or doubled *(2P)*, or a single *(P)* value of the module *P* is subtracted from the high-order bits of the previous remainder ($4r_{i-1}$) shifted by two bits to the left.

The controlling block receives the signals *Reset*, *Start*, clock pulses *(CP)*, $K = n/2$ (*n* - the capacity of the module *P*, n/2 - determines the number of clock pulses required to perform the operation of reduction modulo). In the block of former of the multipliers of the module *P* the binary representation and ones' complement (for further subtraction operations) of the doubled and tripled module (*2P* and *3P*) are pre-calculated. The Block of shift register is used initially to store the reducible number *A*, then the partial remainders, and to shift them to the left by two bits with the subsequent supply of the most significant bits $(4r_{i-1})$ to the partial remainder shaper.

An analysis of the performance of the principal and behavioral models of the module for fast reduction of numbers was performed using the Quartus Prime Time Quest Timing Analyzer. The time relationships that must be respected for the proper operation of the project were determined, and the signal transit time was compared with the time required for the stable operation of the project (Figure-1 and Figure-2). Comprehensive static timing analysis includes analysis of all signal paths. The Time Quest Timing Analyzer shows data required times, data arrival times, and clock arrival times. With its help, you can check the circuit performance and detect possible timing violations.

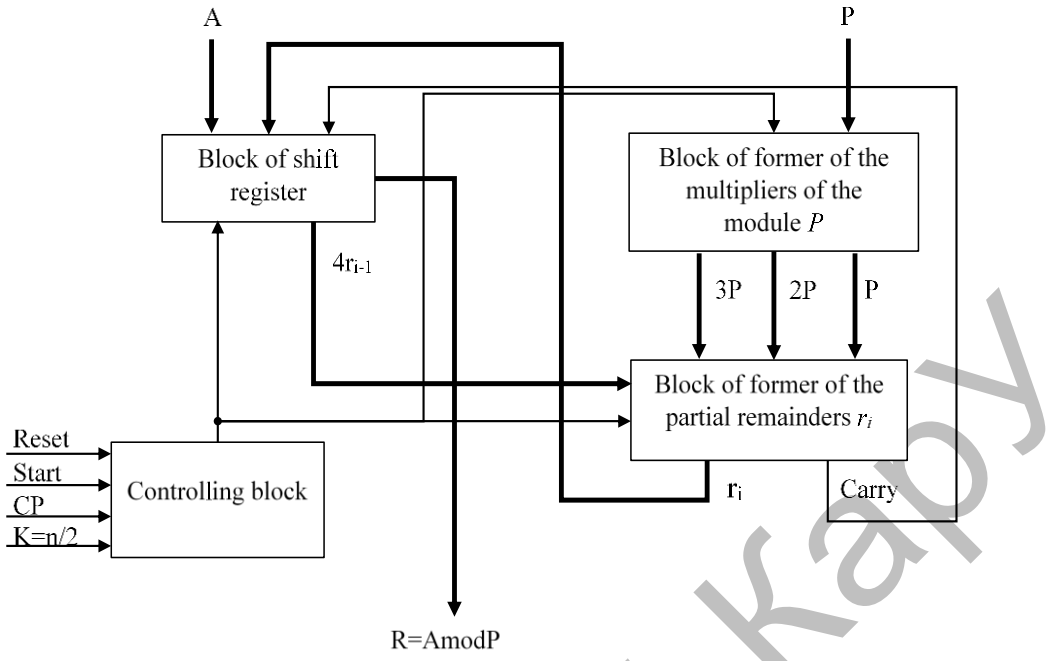

Fig.1. Structural diagram of a device for fast reduction of numbers modulo [14].

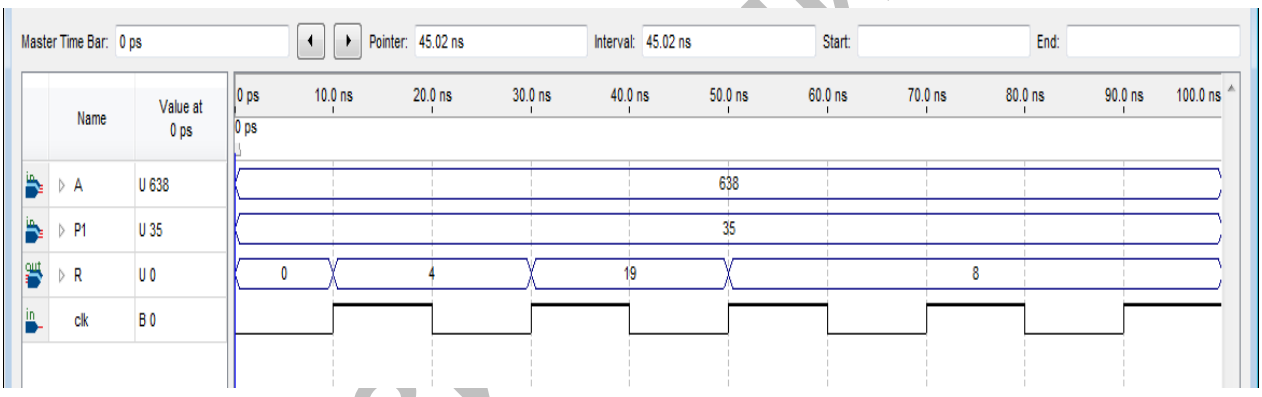

Fig.2. Timing diagrams with the value of the reducible number A = 638 and the module P1 = 35.

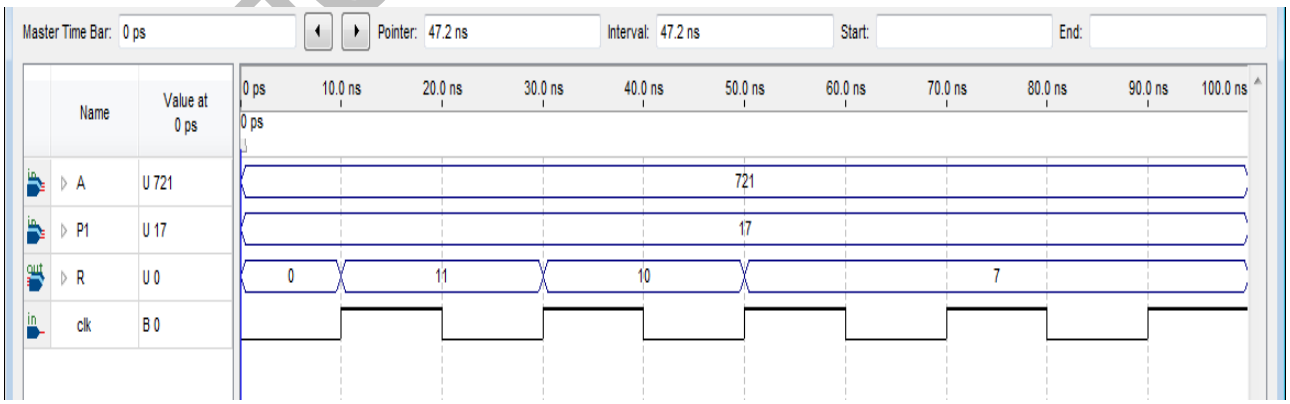

Fig.3. Timing diagrams, with the value of the reducible number A = 721 and the module P1 = 17.

3. Results and Discussions

The analysis of delays (Time Analysis) in the logic circuit is performed to determine the conditions under which the circuit operates reliably. These conditions include the maximum clock frequency (F_{MAX}) at which the circuit will produce the correct result. Time reports were created for all critical paths in the project. Multilateral analysis made it possible to verify the design (the principal and behavioral models) under various operating conditions, changing the voltage, speed, and temperature when performing a static timing analysis of the design (Fig. 4).

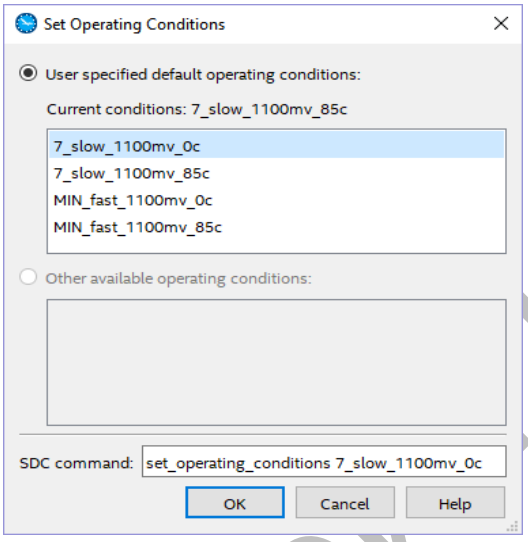

Fig.4. Selection of an operating condition for multilateral analysis.

The maximum delay in the circuit corresponds to the critical path, which determines the longest period and, accordingly, the maximum frequency of the device (F_{MAX}). Fig. 5 represent fragment of the analysis result for determining the maximum clock frequency of the principal model under various operating conditions.

Slow 1100mV 85C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	27.43 MHz	27.43 MHz	Start	
2	30.8 MHz	30.8 MHz	Reset	
3	33.25 MHz	33.25 MHz	Clk	

Slow 1100mV 0C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	27.6 MHz	27.6 MHz	Start	
2	30.83 MHz	30.83 MHz	Reset	
3	32.91 MHz	32.91 MHz	Clk	

Fast 1100mV 85C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	52.21 MHz	52.21 MHz	Start	
2	63.0 MHz	63.0 MHz	Clk	
3	66.54 MHz	66.54 MHz	Reset	

Fast 1100mV 0C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	56.54 MHz	56.54 MHz	Start	
2	68.77 MHz	68.77 MHz	Clk	
3	72.53 MHz	72.53 MHz	Reset	

Fig.5. Determination of the maximum clock frequency under various operating conditions of the device for fast reduction of numbers modulo for the principal model.

Slow 1100mV 85C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	117.3 MHz	117.3 MHz	clk	

Slow 1100mV 0C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	115.18 MHz	115.18 MHz	clk	

Fast 1100mV 85C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	248.57 MHz	248.57 MHz	clk	

Fast 1100mV 0C Model

	Fmax	Restricted Fmax	Clock Name	Note
1	267.52 MHz	267.52 MHz	clk	

Fig.6. Determination of the maximum clock frequency under various operating conditions of the device for fast reduction of numbers modulo for the behavior model.

Figure 6 represent fragment of the analysis result for determining the maximum clock frequency of the behavioral model under various operating conditions. The compiler report contains detailed information about the results of project processing and its components. Of the summary reports that contain complete information about the hardware costs of compiled projects, the main characteristics obtained are presented in table 1.

Table 1. Resources used FPGA.

Resource Name	Principal model	Behavioral model	Total FPGA Resources
Adaptive Logic Module (ALM)	72	74	18480
Registers	22	65	73920
I/O Pins	48	29	224
Logic Array Block (LAB)	12	11	1848

Table 1 shows how many total resources (ALM, Registers, I/O Pins, LAB) are available in Altera FPGA - 5CEBA4F23C7 and how many resources are required to implement a *12-bit* binary number reduction using a *6-bit* binary module. The table does not show data for the Combinational Adaptive Look-Up Table (ALUT), since ALUTs are logical constructs from ALM hardware and are not an independent FPGA resource.

Information on ALUT in the compiler report: for the principle model - *116*, for the behavioral model - *122*. The compiler report also contains information on the average fan-out coefficient for the output: for the principle model - *2.55*, for the behavioral model - *2.56.*Analysis of timing characteristics shows that the behavioral model is faster than the principal model, regardless of the operating conditions of the device. The threshold maximum frequency during operation of the device in the worst conditions (voltage *1100 mV* and temperature *85*) for both the principal model and the behavioral model is almost two times lower than the threshold maximum clock frequency of the device under normal conditions. Moreover under normal operating conditions, the maximum clock frequency for the principal model is F_{MAX} *= 68.77 MHz*, for the behavioral model F_{MAX} *= 267.52MHz*, which is higher than the clock frequency of existing special RSA processors (from *5 MHz* to *30 MHz*), which are implemented on very-large-scale integration (VLSI) devices [16].

An analysis of the resources used and available shows that to implement the proposed high-speed modular reduction device for $n = 6$, both in principle model and in behavior model, no more than *0.6%* of the available resources of the low-budget FPGA Cyclone VE 5CEBA4F23C7 were used. A comparative analysis shows that the hardware of high-speed modular reduction device in the graphical description of the schematic diagram (principle model) will be *10.5%* less, since the device developer himself chooses the necessary resources at the design stage. While using textual methods for describing circuits, CAD independently distributes resources according to a given logic, which leads to non-optimal resource consumption.

Conclusion

The development of a modular reduction device using a behavioral model makes it possible to obtain a faster device compared to using a principle model, but with high hardware costs. The obtained results confirm the possibility of using the low-budget FPGA Cyclone VE 5CEBA4F23C7 to implement a high-speed modulator for binary numbers with high bit grid *(n <= 1000*).

The FPGAs of the Cyclone VE family also include multipliers, DSP blocks, and internal RAM. The results obtained with the implementation of the modular reduction device in Cyclone VE 5CEBA4F23C7, on the use of hardware resources and the maximum clock frequency provide grounds for a real discussion and solution of issues of implementing a crypto processor on one

.

FPGA board of the Cyclone VE family. The device can be used both in crypto-processors and in digital computing devices to accelerate the division operation. Low cost Cyclone family FPGAs allow them to be used in mass solutions where it is necessary to provide low power consumption and low cost.

Acknowledgements

The presented results were obtained during research in the framework of the state order for the implementation of the scientific program for the budget program of the Republic of Kazakhstan "Development of science", the subprogram "Program-targeted financing of subjects of scientific and/or scientific and technical activity" of the scientific and technical program: BR053236757 "Development of software and hardware and software for cryptographic protection of information during its transmission and storage in info-communication systems and general purpose networks"

REFERENCES

1 Hars L., Joye M., Quisquater J. Long Modular Multiplication for Cryptographic Applications. Cryptographic Hardware and Embedded Systems. *CHES 2004, Lecture Notes in Computer Science*, 2004, Issue 3156, pp. 45 – 61.

2 Petrenko V.I., Sidorchuk A.V., Kuz'minov J.V. *Device for generating remainder with arbitrary modulus:* pat. 2368942 C2 Russian Federation. No. 2007124282/09; Publ. 27.09.2009, Bull. No. 27, 9 p.

3 Pankratova I.A. *Number-theoretical methods of cryptography*. Tomsk, Tomsk State University, 2009, 120 p.

4 Zakharov V.M., Stolov E.L., Shalagin S/V. *Apparatus for generating remainder for given modulo:* pat 2421781 C1 Russian Federation.No. 2009138613/08; Publ. 20.06.2011, Bull. No. 17, 9 p.

5 Kopytov V.V., Petrenko V.I., Sidorchuk A.V. *Device for generating remainder from arbitrary modulus of numbe.* Pat. 2445730 C2 Russian Federation. No.2010106685/08; Publ. 20.03.2012, Bull. No.8, 8p.

6 Skryabin I., Sahin Y.H. *Support operations for encryption algorithms with public key and their implementation in the microprocessor Elbrus*. 2013. Available at: www.myshared.ru/ slide/213088

7 Eran Pisek, Plano, T.X., Th.M. Henige, Dallas, T.X. *Method and apparatus for efficient modulo multiplication*: pat. No. 8417756 B2 United States. No.12/216,896; Publ. 09.04.2013, 12 p.

8 Aitkhozhayeva Y. Zh., Tynymbayev S.T. Aspects of hardware reduction modulo in asymmetric cryptography. *Bulletin of National Academy of Sciences of the Kazakhstan*. 2014, No. 5(375), pp. 88 – 93.

9 Markus Bockes, Munich (DE); Jurgen Pulkus, Munich (DE) *Method for arbitrary-precision division or modular reduction*: pat. 9042543 B2 United States. No. 13/885, 878; Publ. 26.05.2015, 12p.

10 Yu H., Bai G., Hao J., Wang C. Yap Efficient Modular Reduction Algorithm Without Correction Phase. *Frontiers in Algorithmics. Lecture Notes in Computer Science*, 2015, Vol. 9130, pp. 304 – 313.

11 Tynymbayev S.T., Aitkhozhayeva Y.Zh. The remainder generator by an arbitrary modulus of the number: pat. 30983 The Republic of Kazakhstan. No. 014/1450.1; Published 15.03.2016, 5 p.

12 Kovtun M., Kovtun V. *Review and classification of algorithms for dividing and modulating large integers for cryptographic applications*. 2017. Available at: http://docplayer.ru/30671408-Obzor-i-klassifikaciya-algoritmov-deleniya

13 Tynymbayev S.T., Aitkhozhayeva Y.Zh, Adilbekkyzy S. High speed device for modular reduction. *Bulletin of National Academy of Sciences of the Republic of Kazakhstan*. 2018, No. 6 (376), pp. 147 – 152.

14 Adilbekkyzy S. Aitkhozhayeva Y.Zh., Tynymbayev S.T. Modeling of the partial reminder former of the modular reduction device. *Eurasian Union of Scientists*. 2019, Vol. 6 (63), pp. 47 – 51.

15 Tynymbayev S.T., Aitkhozhayeva Y.Zh, Adilbekkyzy S., et al. Development and modeling of schematic diagram for the modular reduction device. *Problems of Informatics*, 2019, No. 4, pp.42 – 52.

16 Kramarov S.O., Mityasova O.Yu., Sokolov S.V., Tishchenko E.N., Shevchuk P.S. *Cryptographic information security.* Moscow: RIOR Publishing Center, 2018, 322 p.

Article accepted for publication 25.05.2020