The Research of Multistage Interconnection Structure Based on Crossbar

Haiyuan Ni[1]， Wei Li[12]*， Yingjian Yan[1]

[1]Institute of Information Science and Technology, Zhengzhou 450001,China
[2]State Key Lab of ASIC and System, Fudan University, Shanghai 200433,China
*18530021399@163.com

Abstract

To realize the high-speed performance of the processor, we need to research an efficient and flexible interconnection structure. In this paper, we propose a multistage interconnect structure based on Crossbar in the Coarse-Grained Reconfigurable Logic Array (CGRLA). Inner internet implements the connection of Functional operation unit flexibly and the outer internet implements the data transmission of different level of function units. Through the simulation verification, the results show that the structure we put up is better than similar design and there are some characteristics, such as small area, low occupancy rate of resources, high flexibility, high area transfer rate and so on, can effectively reduce the routing time in the algorithm implementation process, and improve the processing performance of the processor.

Keyword: Interconnection structure; Coarse-grained Reconfigurable Logic Array; multistage interconnection network; small area; high flexibility.

1. instruction

With the widely application of the cryptographic algorithm, there are more strict requirements for cryptographic processor for processing speed, power consumption, and the parallel computing power. For cryptographic processor, the ability of reconfigure and the interconnection structure are two key factors for achieving efficient parallel computing, and the efficiency interconnection structure determines the capability of data parallel processing, the ability of reconfigure is reflected in the current high-speed implementation of cryptographic algorithms and allows for a better future of new cryptographic algorithms.

Currently, FPGA is a general purpose cryptographic algorithm processor with high capacity of reconfigure, but the implementation of the algorithm. is not efficiency.

To this end, a high efficiency and flexible coarse-grained reconfigurable logic array processor is proposed, based on the analysis of a large number of symmetric cipher for common characteristics of different cryptographic algorithm. The processor proposed can not only process the algorithm currently existing, can also implement the algorithm that come up in the future. The interconnect structure of this paper has the characteristics of efficient and flexible , and analyses the timing and area of the structure by Design Compiler(DC).

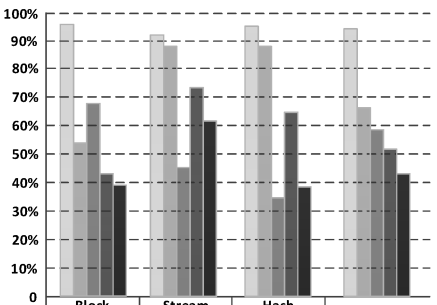
2. Related Work

To design the interconnection network, in this paper, a lot of work is done such as Algorithm Analysis and design the array and so on.

2.1. Algorithm Analysis

In this paper, through the study of cryptographic algorithm, we find that there are a certain commonalities and there are some common structure for symmetric algorithm. Since, to enhance the ability of processor and implement the algorithm more efficiently, the operation are extracted and classified by analyzing existing symmetric cipher and Hash function.

Cryptographic algorithm in this study is mainly aimed at block cipher, stream ciphers and some hash function, wherein including 96 block cipher algorithm, 26 stream ciphers, 26 hash functions. According to the Classification of Cipher unit(CU) in the algorithm, get the results in Figure 1.



	Block Cipher	Stream Cipher	Hash Functions	All
Logic	96.9%	92.3%	96.2%	95.9%
Algorithm	55.2%	88.5%	88.5%	66.9%
S_BOX	68.8%	46.2%	34.6%	58.8%
Nonlinear	42.7%	73.1%	65.4%	52.0%
permutation	39.6%	61.5%	38.5%	43.2%

Figure 1. The ratio of different operations used in cryptographic algorithm

According to the table, the basic computing unit of the array will be divided into the following: logic operation unit (LOU), arithmetic operation unit (AOU),

978-1-4673-9719-3/16/$31.00 ©2016 IEEE

S_BOX, nonlinear operation unit (NOU), and a bit permutation unit (BP).

2.2. Structure of Array

According to the algorithm structure and relationship of the operation, this paper presents an array structure shown in Figure 2.

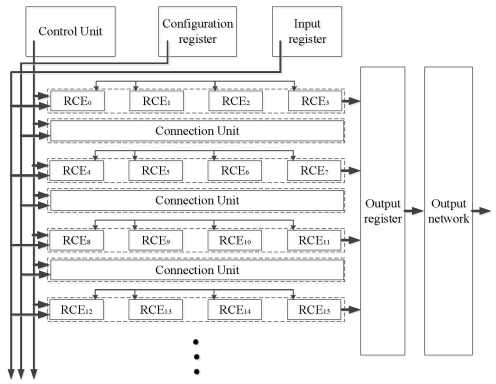


Figure 2. The structure of CGRLA

Figure 2 shows that each level has four Reconfigurable Cipher Unit (RCE) and each RCE contains five CU connected by inner interconnect network. Different levels are connected by outer interconnect network. To implement greater bit-wide operation, a fast cascading line is set to implement different RCE in each level. Meantime, each level has an output interface achieving data output fast, so as to implement algorithm more flexible and can implement cryptographic algorithms by stream processing and enhance the throughput.

When algorithm is implemented, the data is injected to RCE first from input buffer, Then the data is divided into different CUs in the RCE by inter interconnect network. The CU can not only compute themselves, can also compute by each other through the inner network, so as to decrease the operation time. When one level RCE can not map the algorithm, a large number of RCE are needed, data transmission in different level RCE is complemented by outer network. The outer network is set aimed at improving the capability of parallel computing. In this paper, what we do is to propose a multistage interconnection network as following described.

3. Structure of interconnection

Interconnection network is inseparable for Coarse-grained reconfigurable logic array and the design of interconnection network decides the degree of parallel of data flow. Currently, the Crossbar, Benes network are two ways that used most. In this paper, according to the analysis of the structure of algorithm and the characteristics of algorithm, proposing a multistage interconnection structure based on Crossbar, so as to enhance the efficiency of realization.

3.1. Inner network

Inner network is used to connect the different CU and realize the data transmission between different CUs. The inner network is shown in Figure 3.

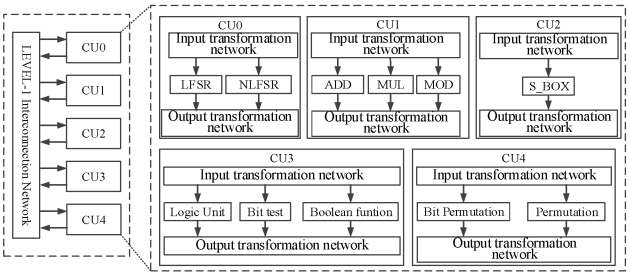


Figure 3. The structure of Inner Network

According to the study of the structure and the operation characteristics of the algorithm, the bit width in different algorithm is different. According to statistics, the bit width in most algorithm is 32 bit. Since the bit width of the CU is 32 bit and each RCE has fifteen input ports, there are nine from out and six from CU as feedback data. So as to improve the efficiency of data transmission and the structure is shown in Figure4.

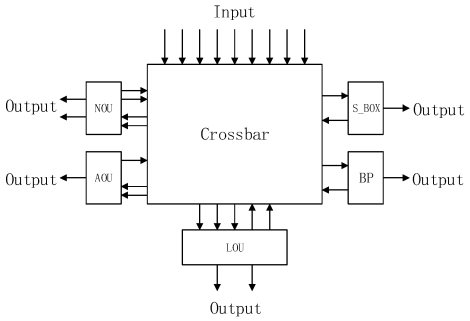


Figure 4. The connection of Inner Network

Figure 4 is the connection relationship of different CU in an RCE, wherein input data transmit the data through the input transmission network to each CU,

As we can see that the input transmission network is constructed by crossbar, and the number of Crossbar is nine to choose which data to where.

Data from input is divided into different CU, in first operation, the data is from out, and then the result can transmit in itself and also transmit in different RCE. To implement greater bit width operation, a fast cascading line is set to cascade the different CU in identical level of RCE.

3.2. Outer network

A complete realization of algorithm require multistage RCE to participate in operation. To implement the flexibility of data transmission between the RCE of different levels. In this paper, an outer

interconnection network is proposed based on Crossbar to realize data transmission between different levels' RCE and enhance the degree of parallel in implementation of algorithm. The outer interconnection is shown in Figure6.

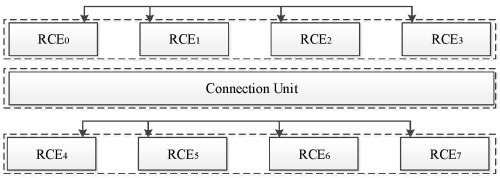


Figure 6. The structure of Outer Network

The Transmission is shown in Figure 7.

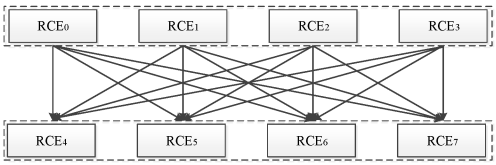


Figure 7. The transmission of Different RCE

As seen in Figure 7, the outer interconnection network is mainly to achieve full interconnection between superior RCE and subordinate RCE and realize flexible data transmission. In outer interconnection network, superior RCE can get the data to any RCE in the next level. This network can not only enhance the degree of parallel, but also can improve the usage rate of Cipher Unit. To realize a jump in data transmission, a jump structure is designed in outer interconnection network, the structure is shown in Figure 8.

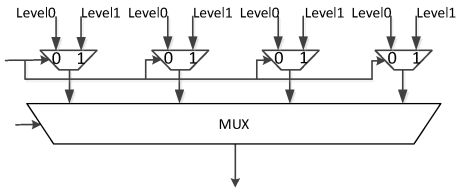


Figure 8. Jump structure

The jump structure proposed in this paper is based on outer interconnection network and increase a MUX in the input port to choose where the data from, the level0 represents the data from two previous level, Level1 represents the data from last level and they are controlled to choose data where from by 1bit. By this way, it can realize the data jumping to improve the degree of parallel.

4. system verification

As the design of interconnection network complete, in order to verify the accuracy and flexibility of the structure, it need to be verified. But the independent verification can not guarantee the correctness and completeness, therefore, the verification platform of the interconnection structure is based on the whole array structure to complete the verification of array structure and interconnection network. Procession is shown in Figure9.

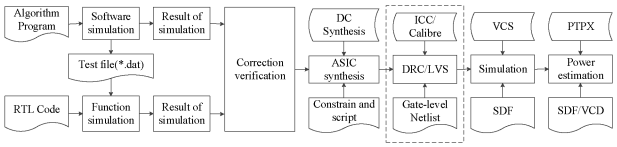


Figure 9. Procession of System Verification

In this paper, DC the logic synthesis tool is used to synthesize for RTL code. The verification of interconnection network is by estimating area and path delay. The performance test of this work is by mapping algorithm to test. The performance we get is shown in Table 1.

Table 1. Performance of implementation of ASIC

		Optimal delay	Single area (um²)	Whole area (um²)	Gate (ten thousand)
Array System		2.3ns	—	8644058.1	450.21
Inner Network	Input Network	0.87ns	1624.3	181787.2	9.47
	Output Network		9524.6		
Outer Network		0.52ns	1563.4	46178.6	2.24
The Occupation of Network in the whole system		—	—	2.6%	2.6%

Compared with similar design, the result is shown in Figure 10.

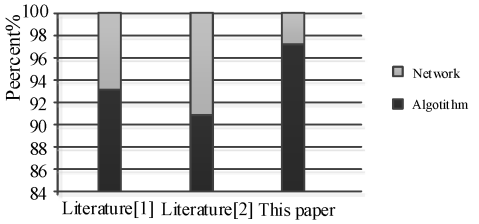


Figure 10. Comparison of source in different structure

As seen from the Figure, the interconnection structure proposed in this paper is small proportion of the overall structure. To illustrate the interconnection structure with efficient flexibility and with great degree of parallel, different algorithms are mapped, and use network data transfer rate description of its data processing capabilities, which is defined as:

$$Net\ Transmission\ Rate = \frac{M \times n}{t}(bit/s) \quad (1)$$

Wherein M represents a network width of output ports, n represents the number of ports, t represents the maximum transmission delay of the network. The unit is also often referred to as Gbps or Mbps. The highest data transfer rate of interconnection network proposed this paper can be up to 66.7 Gbps, and mapping different algorithm get the result as shown in Figure 11.

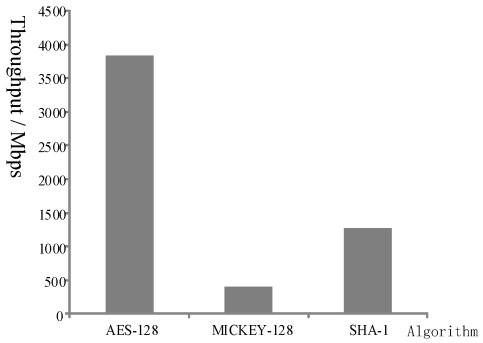


Figure 11. The throughput of different algorithm

In order to prove the merits of the interconnection network, this paper introduces the concept of network area efficiency, and compared with other structure, the result is shown in Figure 12. The Network Area Efficiency is that the ability of the interconnection network unit area can achieve network transmission rate, which is calculated as:

$$Transmission\ Area\ Proportion = \frac{P}{area} \quad (2)$$

Where P is the network transmission speed and the network data throughput will be used to describe it; area is network area. In order to avoid bias caused by different technologies, where the area is equivalent the number of gates as the calculation data.

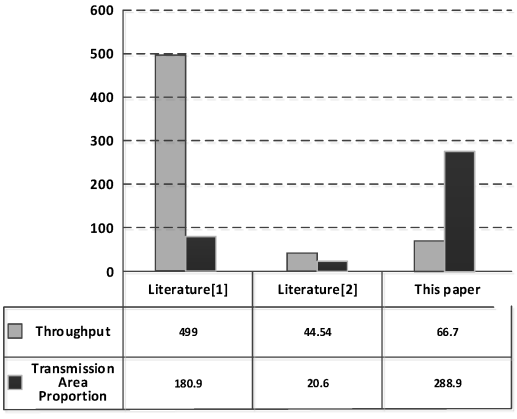


Figure 12. Comparison of Transmission area proportion in similar design

Through the statistical data can be seen that the data throughput of interconnection network is not better than [1], but the network area in literature [1] is larger. From the Figure we can see that the area rate is obvious better than literature [1] and [2]. So, the interconnection network proposed this paper has advantages in data transfer rate per unit area.

5. Conclusion

In this paper, a multistage interconnection network is proposed based on Crossbar. The inner network realizes the connection of different CU, the outer network realize the data transmission between different level function units. The structure has the advantages of small occupation of area, high flexibility and high efficiency of area data transmission and so on. It can improve the degree of parallel of algorithm and enhance the efficiency of implementation. It is a good way to implement the interconnection network for Coarse-Grained Reconfigurable Logic Array.

6. Reference

[1] Phi-Hung Pham, Phuong Mau, Jungmoon Kim, and Chulwoo Kim, An On-Chip Network Fabric Supporting Coarse-Grained Processor Array [C]. IEEE transactions on very large scale integation (VLSI) systems, vol. 21, no. 1, p178-182, Jan.2013.

[2] D. N. Truong, W. H. Cheng, T. Mohsenin, Y. Zhiyi, A. T. Jacobson, G. Landge, M. J. Meeuwsen, C. Watnik, A. T. Tran, X. Zhibin, E. W. Work, J. W. Webb, P. V. Mejia, and B. M. Baas, A 167-Processor computational platform in 65 nm CMOS [C]. IEEE J. Solid-State Circuits, vol. 44, no. 4, p. 1130–1144, Apr. 2009.

[3] Junhui wang. Research of Topology and Routing Algorithm for 3D Network-on-Chip [D]. Xian ： Xidian University. 2013.

[4] M. Plat, J. Teich, ad N. When, Dynamically Reconfigurable Systems: Architectures, Design Methods and Applications[C]. New York：Springer, 2010.

[5] Mefalingam R K, Joseph I P, Gautham P, et al. Reconfigurable Cryptographic Processor for multiple Crypto-algorithm[C], 2011 IEEE. IEEE, p.204-210, 2011.

[6] GUO Yan-song， LIU Lei-bo， A Block-Cipher Oriented Coarse-Grained Reconfigurable Array and AES Algorithm Mapping[J], Microelectronics & Computer，32(9):p.1-5，2015.

[7] Yang Xiaohui, Dai Zibin, Zhang Yongfu. Research and Design of Reconfigurable Computing Targeted at Block Cipher Processing[J]. Journal of Computing Research and Development: p.962-967, 2009.