High performance and area efficiency design of global register file for coarse-grained reconfigurable cryptographic processor

Ge Wei, Yang Jinjiang, and Yang Jun[a)]

National ASIC System Engineering Research Center, Southeast University,
Nanjing, China, 210096
a) *dragon@seu.edu.cn*

Abstract: The global register files (GRF) seriously affect performance and area of coarse-grained reconfigurable cryptographic processor (CGRCP). By studying the direct factors affecting the performance of GRF and the characteristics of block cipher algorithms implemented on CGRCP, a distributed whole interconnected global register files (DWI-GRF) was proposed. Compared with other GRF architecture with 14 mainstream block cipher algorithms as the experimental benchmarks, the average performance improved up to 17.24%~230.67% and average area efficiency improved from 36.37%~95.59% respectively.

Keywords: global register files, coarse-grained reconfigurable cryptographic processor, high performance, area efficiency

Classification: Integrated circuits

References

[1] G. Sayilar and D. Chiou: 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (2014) 155 (DOI: 10.1109/ICCAD.2014.7001346).

[2] Y. Ming, *et al.*: 2012 IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS) (2012) 834.

[3] D. Zi-bin, *et al.*: 7th International Conference on ASICON'07 (2007) 814.

[4] J. Yang, *et al.*: 2015 International Conference on Automation, Mechanical Control and Computational Engineering (2015) 1402.

[5] B. Wang and L. Liu: 2015 IEEE International Symposium on Circuits and Systems (ISCAS) (2015) 1182 (DOI: 10.1109/ISCAS.2015.7168850).

[6] B. Mei, *et al.*: in *Fine- and Coarse-Grain Reconfigurable Computing* (Springer, 2008) 255.

[7] A. Garcia, *et al.*: Application-Specific Systems, Architectures and Processors (2008) 245 (DOI: 10.1109/ASAP.2008.4580186).

[8] Y. Wang, *et al.*: IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **1** (2013) 99.

[9] H. Parizi, *et al.*: in *Euro-Par 2002 Parallel Processing* (Springer, 2002) 844.

DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

[10] Z. Kwok and S. J. E. Wilton: FCCM: 13th Annual Ieee Symposium on Field-Programmable Custom Computing Machines, Proc. (2005) 35 (DOI: 10.1109/FCCM.2005.58).

1 Introduction

Subject to the limited computing resources in a coarse-grained reconfigurable cryptographic processor (CGRCP), an algorithm mapping on the reconfigurable array required to divide into several configuration parts [1, 2, 3]. It needs to not only deal with a large number of temporary data between reconfigurable configurations switching, but also satisfy the different operations between rounds of block cipher [4, 5]. Global register files (GRF) are good choice to satisfy the high-speed data exchange requirements and achieve arbitrary computing pipeline when different block ciphers mapping on the reconfigurable array. However, neither the data throughput nor size limited of GRF, it will seriously influence the computing efficiency of the CGRCP. Therefore, area efficiency GRF design becomes one of the key researches of CGRCP.

Cryptoraptor [1] introduces a concentrate multi-port design to realize the GRF, which improves data bandwidth and access efficiency. However, this design causes extraordinary area overhead. ADRES [6, 7] adopts a tightly-coupled and parameterized GRF as an external data buffer, which meets the data communication requirement between the Very Long Instruction Word (VLIW) mode and Coarse-grained Reconfigurable Array (CGRA) mode. Although fetch queue re-ranking method is used to relieve the bottleneck of data bandwidth, it still restricts the performance of reconfigurable array seriously [8]. MorphoSys [9] takes a double frame buffer to ensure the data transfer and computation could be overlapped. But, single-port design makes it not suitable for high throughput implementation of block cipher. Current researches of GRF [10] in CGRCP mainly focus on either improving the computing performance or achieving more algorithms. How to satisfy different futures of block cipher and match the performance and area efficiency requirement at the same time become the key researches of GRF.

2 Analyses and design of global register file

2.1 Performance analysis of GRF parameter

In order to fully analyze the key factors that influencing the computing performance, it is necessary to consider variety constraints including the feature of both block cipher algorithm and hardware architecture. We collate 105 kinds of related block cipher algorithm in existing references, and comprehensive statistical analysis characteristics of algorithm. Round number less than or equal to 32 accounts for 84.06% of total algorithms. The percentages of block size are 64-bit and 128-bit, which accouted for 40.80% and 39.20% respectively. Thus, the study should focused on the round number less than or equal 32 and block size less than or equal 128-bit respectively.

The key factors are not only associated with the characteristics of the algorithm itself, but also correlated with parameters of hardware architecture as Table I

DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

Table I. Constraints of effecting on computing performance

Parameters	Abbreviation	Description
Round Count	RC	number of block cipher rounds
Reconfigurable Cell Line	RCL	number of reconfigurable cell line
Global Register Count	GRC	number of GRF maximum row
Global Register Width	GRW	data width of each GRF row
Stall time	Tstall	time of data initialization and configuration switch

shown. Here, RC is decided by the characteristics of block cipher itself. Each reconfigurable cell line is assumed to finish one round function within an iteration interval (II). Where, the Interval of the adjacent two loop body start called II. When the size of GRF could not handle the temporary data, the computing have to divided into several times to deal with these data. The Tstall is related to the access pattern of system storage. Following analysis the performance under the influence of architecture and algorithm features.

Fig. 1 shows the performance differences of these algorithms that RC equal 32 under the conditions of different GRC. In order to simplify the assessment, we assumed that execution time of each round function, II and Tstall are all one cycle. Key performance indicators of block cipher algorithms can be abbreviated as BPC. Block per cycle (BPC), which determined by Block/Cycle, is the performance characterization of the parallel computing ability.

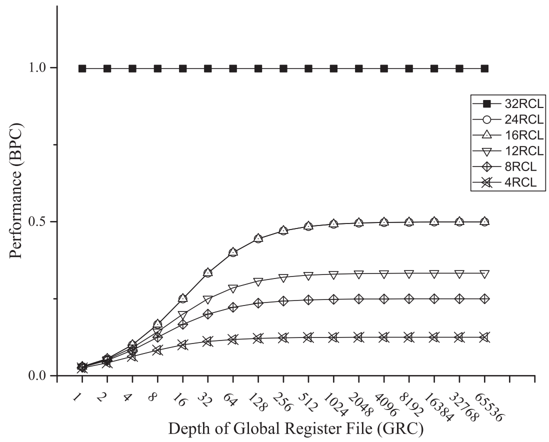

Fig. 1. Performance of algorithm with 32 round function under different RCL.

According to the line graph, the algorithm has the highest performance (1BPC) when RCL equal to GRC. This is because the reconfigurable array handle all the computing pipeline without temporary data. When RCL less than GRC, the computing performance continue to improve with GRC increasing, and eventually the performance tends to a stable value.

Further analysis, at the expense of Tstall equaling one cycle, the performance is only related to the number of configuration set. When the RCL changes from 32 to

© IEICE 2016
DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

4, the number of configuration set also increase gradually from 1 to 8. However, the computing performance is in inverse relationship with the number of configuration set. Both the RCL equaling 16 and 24 obtain the same performance. It is owing to the fact that in both cases only two sets of configuration to complete the calculation. In addition to GRC, GRW as resource-dependent restriction of reconfigurable array directly affect the cycle number of iteration interval (II), also has a great impact on the computing performance of reconfigurable cryptographic processor.

Fig. 2 shown the difference in performance of these algorithms that block size equal 128-bit with the GRW growing. In order to simplify the evaluation, we assumed that both round function and Tstall occupied one cycle. Meanwhile, all the capacity of GRF, memory access parallel and latency meet the maximum demand of block cipher algorithms.

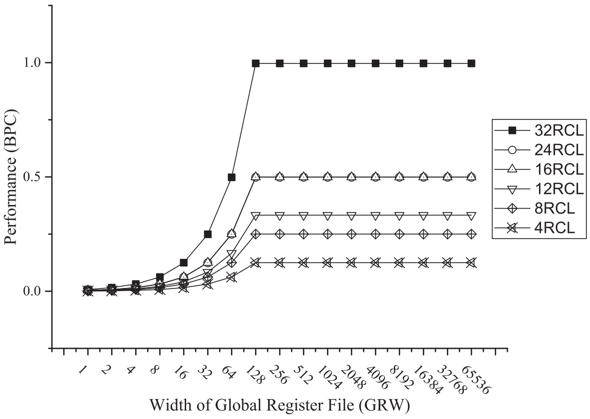

Fig. 2. Performance of algorithm with 128-bit block size under different RCL.

As can be seen from Fig. 2, the GRC set as 32, the RCL variety from 4 to 32. For different RCL, the computing performance improves continuously with the GRW increasing, and eventually reaches stabilized value. The highest computing performance of block cipher implemented with different RCL is inversely proportional to the number of configuration contents, which achieve maximum computing performance of (1/RC/RCL) BPC. With the GRW increasing continuous, the computing performance change exponentially. Especially, when the GRW more than or equal block size, the computing performance does not change.

2.2 The area efficient design of GRF architecture

As above analyzed, the GRF design parameter achieve the highest performance per area when GRC choosing 128, and GRW choosing 128-bit. Furthermore, the design and implementation of GRF should not only consider the influence on computing performance, but also meet the different requirement of block cipher algorithms. The block cipher futures that the data between different round is independent and data in round has read-after-write (RAW) dependence. Base on the characteristics of data independent between round function, the GRF can adopt multiple bank structure to replace a single physical structure. Fig. 3 shown

DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

the area trend of register body and decode logic with different register number and access port.

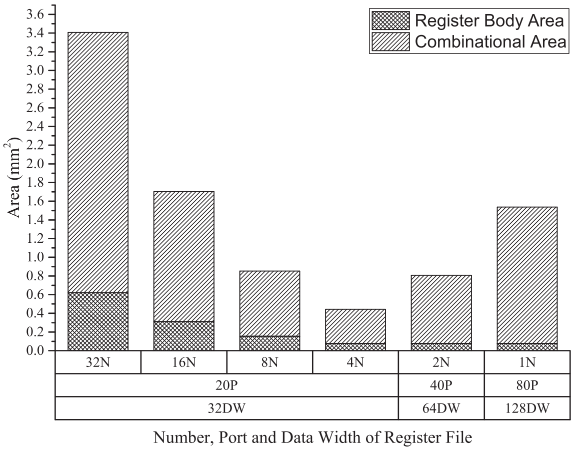

Fig. 3. Area trend of register body and combinational under different number, port and data with of register file.

As shown in the column chart, the GRF design parameter meet the constraint of the minimum register capacity with the register number deminishing. And the access port meet the parallel access requirement. In order to meet the parallel read/write requirement, the multiple of the register number and register data satisfy the data bandwidth of each round function. Consider the composition of the GRF, the decoding logic area is becoming the key factor. The decoding logic area is related to the register number and register data width, which is decreasing with the register number increasing and register data width decreasing. So this paper select the optimal solution set of design parameters as follow Table II.

Table II. The design parameters of GWID-GRF

Number	Number
Register address width	7
Register data width	32
Register number	4
Read port	20
Write port	2

As shown in Fig. 4, The GRF contains four 7x32 bit register body. Each register body shared by every four reconfigurable cells. Meanwhile, the GRF are design independent read port for every two rows of reconfigurable array, and one write port for every twenty rows. Multiple write ports operate the GRF by arbitration. Take advantage of concurrent access ability of proposed GRF can meet the arbitary pipeline requirement of reconfigurable array, and satisfy access requirements of different block cipher algorithm.

© IEICE 2016
DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

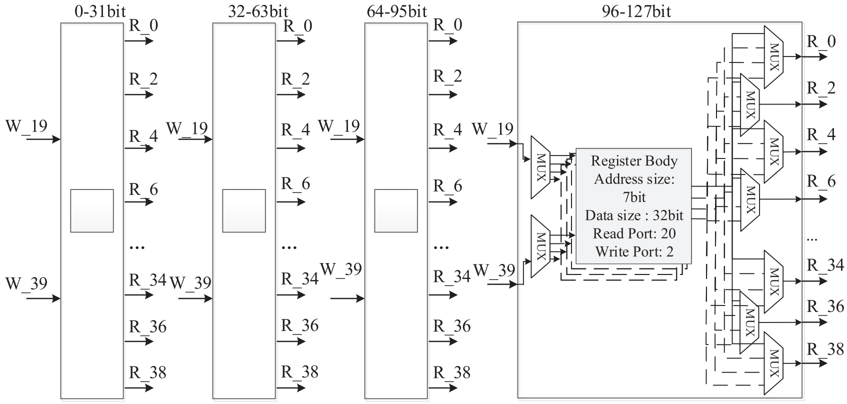

Fig. 4. The design detail of GWID-GRF.

3 Simulation results and comparison

The Cryptoraptor achieved the maximum algorithms, which was the highest performance reconfigurable cryptographic processor. In order to carry out effective experimental analysis for the optimization design of GRF, a base architecture like Cryptoraptor was designed. The base architecture adopted the same array size, operating behavior and other aspects, only changing the design parameters of GRF architecture.

Table III shows the parameters of different GRF architectures. In Cryptoraptor design, the GRF contains only one register body, which has 80 read ports, 2 write ports. And register body has 256 entry 32-bit registers (8x32), total 8 Kbit capacity. The ADRES design adopt reordering queue mechanism of register file to reduce memory access conflicts and hardware overhead, but need to resolve the access arbitration and multi-port competition. In the reference design, four single-port registers and each data width was 32-bit, total 16 Kbit capacity. This paper implemented the distributed GRF using four register bodies, each register body has 128 entry 32 bit registers (7x32), total 16 Kbit capacity. And each register body contains 20 read ports, 2 write ports.

All the comparison GRF architecture are implementation in TSMC 40 nm process CMOS technology, and synthesized by Design Compiler tool to get the area information. Finally, mapping the target block cipher algorithm on the reconfigurable processor to obtain computing performance.

Fig. 5 show the comparative results of different GRF architecture. Block per cycle per area (BPCPA) is an area efficient indicators of performance per unit area, which is defined by BPC/Area. The area relies on different design constraints and process implementation.

Compare with Cryptoraptor, the capacity of proposed GRF capacity increased one time, but area resources was reduced by 39.74%. This is due to the Cryptoraptor GRF design adopts 8-bit width decoder, which takes up double decoding logic resources than 7-bit width decoder theoretically. By proposing four register bodies and each with 7-bit decoder, the proposed design of GRF greatly reducing the decoder logic area up to 46.92%. Compare with ADRES, the area resources was increased by 141.88% under the same capacity. This is because the access

© IEICE 2016
DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

Table III. The parameter comparison of different GRF design

Design	register number	register address width (bit)	register size (Kbit)	read port number	write port number
Cryptoraptor	1	8	8	80	2
ADRES	4	7	16	1	1
Proposed	4	7	16	20	2

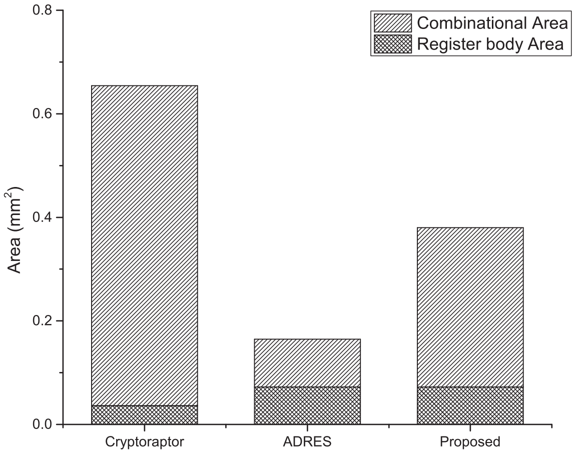

Fig. 5. The area distribution of different GRF design.

arbitration in single-port register file cost less combinational area. However, this design greatly limited the ability of data parallelism access.

Table IV shows the performance comparison and area efficiency of mainstream block cipher under different GRF design. Experiments using 14 kinds of mainstream block algorithms including AES, Blowfish and so on. From the table the algorithm performance improved from 0.35 to 0.41, an average increase of 17.24%. Since only a set of configuration, AES algorithm can get the maximum theoretical performance, suffering a small amount of impact by prologue and epilogue processing. For other algorithms, whose RC bigger than the RCL, need one more set of configurations. Benefitting from the larger capacity of GRF design parameters, the performance improved by reducing the configuration switch times. Even if the capacity increasing, the proposed GRF realize higher area efficiency compared to Cryptoraptor by adopting the distributed GRF architecture. Under the same application conditions of block cipher algorithms and reconfigurable arrays, the paper achieved the area efficiency improve from 0.54 to 1.07, an average increase of 95.59%.

Compared with ADRES design, the algorithm performance improved from 0.12BPC to 0.41BPC, an average of 230.67%. This is utilization the proposed multiport register to provide a higher degree of parallelism data access, which greatly reduced access times suffered by the register data width mismatch with cryptographic algorithms. From the area efficiency results, benefit from the advantages of the area, ADRES has the similar area efficiency under 64-bit block size, but greatly reduced under the 128-bit cipher set. Compared with ADRES design, area efficiency improved from 0.78 up to 1.07, an average increase of 36.37%.

DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016

Table IV. The performance and area efficiency comparison of different GRF design

Algorithm	Algorithm parameters		BPC (Block/Cycle)			BPCPA ((Block/Cycles)/mm^2)		
	Round	Block Size	[1]	[6]	Proposed	[1]	[6]	Proposed
AES	10	128	1	0.24	1	1.57	1.51	2.60
Blowfish	16	64	0.33	0.16	0.4	0.52	1.01	1.04
Camellia	18	128	0.28	0.07	0.36	0.44	0.44	0.94
CAST128	16	64	0.28	0.13	0.36	0.44	0.82	0.94
DES	16	64	0.33	0.16	0.4	0.52	1.01	1.04
GOST	32	64	0.2	0.08	0.25	0.31	0.50	0.65
KASUMI	6	64	0.3	0.14	0.38	0.47	0.88	0.99
RC5	12	64	0.33	0.16	0.4	0.52	1.01	1.04
SEED	16	128	0.14	0.03	0.18	0.22	0.19	0.47
Twofish	16	128	0.28	0.07	0.36	0.44	0.44	0.94
Average	NA	NA	0.35	0.12	0.41	0.54	0.78	1.07

4 Conclusion

By analyzing the effect of GRF on performance and area for different cryptographic algorithms, this paper explores the design parameters of GRF under the architecture constraints. The performance and area influence of GRF parameters was considering. Finally, the optimal parameters of GRF are concluding from the exploration under the mainstream block algorithms set.

This paper proposed a DWI-GRF, which improved the target set of block cipher algorithm at an average of 17.24%~230.67%. Under the limited reconfigurable computing resource, the GRF reduce the area overhead up to 39.74% and achieve 36.37%~95.59% increasing on area efficiency.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant 61404028).

DOI: 10.1587/elex.13.20160545
Received May 31, 2016
Accepted June 29, 2016
Publicized July 15, 2016
Copyedited August 10, 2016