The Research and Design of Reconfigurable Cipher Processing Architecture Targeted at Block Cipher

Zi-Bin DAI Xiao-Hui YANG Qiao Ren Xue-Rong Yu

(Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004, China)

Email: yxh7887@yahoo.com.cn

Abstract: The design of a cipher processing system adopts reconfigurable computing technology, which can support multiple cryptographic algorithms in the cipher application. Therefore, it can achieve crypto algorithms processing with efficiency and flexibility, and it also solves the hidden trouble in the cipher processing system. This paper has analyzed processing structure characteristics of popular block cipher algorithms, and proposed a reconfigurable cipher processing architecture (RCPA) combining the design method of reconfigurable processing architecture. And a prototype has been implemented successfully based on RCPA. The prototype is realized using Altera's FPGA. Synthesis, placement and routing of RCPA have accomplished under 0.18μm CMOS technology. The results prove that RCPA can achieve relatively high performance in block cipher algorithms processing.

Keywords: Reconfigurable, Block cipher, RCPA

1. Introduction

With the development of the information technology and network communication, the increasing security demands should be satisfied in the applications such as the data storage and network communication. There are two possible approaches to the data encryption traditionally[1,2,3]. One approach is general purpose processor, while the performance it can achieve is poor. The second option is the ASICs, while its flexibility is hard to satisfy different security demands and crypto algorithms update demands. Therefore, it's difficult for ASIC and general purpose microprocessor to achieve reasonable tradeoff of speed and flexibility.

Reconfigurable Computing is a novel computing system which can combine the reconfigurable hardware processing unit and the software programmable processor. Reconfigurable Computing can satisfy different computing demands, through configuring reconfigurable processing unit. Therefore, it can achieve the demands of performance and flexibility at the same time. Reconfigurable computing technology can be used in cipher processing system, thereby can support multiple cryptographic algorithms in the cipher application. Therefore, it can achieve crypto algorithms processing with efficiency and flexibility, and it also solves the hidden trouble in the cipher processing system. The reconfigurable cipher processing system will be widely used in military and commerce fields.

2. Previous Work on Reconfigurable Architecture

Currently, many research groups and companies worldwide are working on application-specific hardware implemented in reconfigurable architecture to match different application demands. Major reconfigurable architecture will be briefly mentioned in this section. Those which were cited frequently are MorphoSys[4], PipeRench[5], OneChip[6], GARP[7], Chimera[8], REMARC[9] and OneChip98[10].

Generalized reconfigurable architectures consist of an interconnected network of configurable logic and storage elements where the granularity of the architecture is dependent upon the target application. Architectures are typically distinguished based on the control of processing resources—SIMD, MIMD, VLIW, systolic, microcoded, etc. The Garp, MorphoSys, and PipeRench platforms are examples of reconfigurable architectures suited to accelerating some block cipher algorithms. However, the above reconfigurable architectures are mainly targeted at multimedia processing and wireless communication application fields. None of these reconfigurable architectures are the specialized structures for block cipher processing which can supported most of the popular block cryptographic algorithms flexibly and efficiently.

3. The Reconfigurable Cipher Processing Architecture-RCPA

3.1 Critical Technology of RCPA Design

When designing the Reconfigurable Cipher Processing Architecture for block cipher processing, the operation and processing structure characteristics of block cipher algorithms should be analyzed, which including the characteristics of operation and the constitutions of basic operation unit in block cipher algorithms. Moreover, the critical design technology of reconfigurable architecture should be discussed, which includes reconfigurable granularity, interconnection architecture, computation type and reconfiguration mode.

Table 1 Occurrences of block ciphers basic operations

Basic operations	Occurrences
logic operation	97.56%
S box substitution	73.17%
shift or rotation	85.36%
modular addition/subtraction	48.78%
bit-permutation	24.39%
modular multiplication	17.07%
multiplication in Galois field	17.07%

From the analysis of block cipher processing, we can find that block ciphers have regular operation width and are suited to parallel processing in one block and pipeline processing in multiple blocks. Furthermore, we conclude that the most block ciphers have the common basic operations in hardware, and the basic operations that should be included: logic operation, shift or rotation operation, bit-permutation operation, S box substitution, modular multiplication, multiplication in a Galois

1-4244-1132-7/07/$25.00 © 2007 IEEE

field and modular addition or subtraction. The result of the block ciphers basic operations occurrences analysis is shown in table 1[11]. Therefore, we concluded that the reconfigurable cipher processing architecture for block cipher should possess the characteristics of coarse-grained, mixed interconnection, VLIW/EPIC computation and static and dynamic reconfiguration mode.

3.2 RCPA Architecture

Based on the analysis of processing structure characteristics of block cipher algorithms, this paper has proposed a reconfigurable cipher processing architecture (RCPA) combining the design method of reconfigurable processing architecture, which is shown as figure 1. RCPA is composed of Reconfigurable Cipher processing Unit (RCU), Inter-Connection Module (ICM), Memory Access Module (MAM) and Configuration and Control Module (CCM). RCPA is a reconfigurable cipher processing architecture with coarse-grained, mixed interconnection, VLIW/EPIC computation and static and dynamic reconfiguration mode.

RCPA can be provided with variable parallelism and configurable pipelined architecture, and the cipher processing unit can be organized in the planar array. Thus, RCPA has been realized pipelined processing with alterable parallelism which the depth can be configured. The static and dynamic reconfiguration mode is mixed in RCPA, and multiple contexts are supported. As a result, RCPA is adapted to two processing modes with parallel processing in one block and pipeline processing in multiple blocks which matches the cipher processing architecture. In addition, defining different RCPA parameters' values can attain different size and usability of reconfigurable cipher processing architecture.

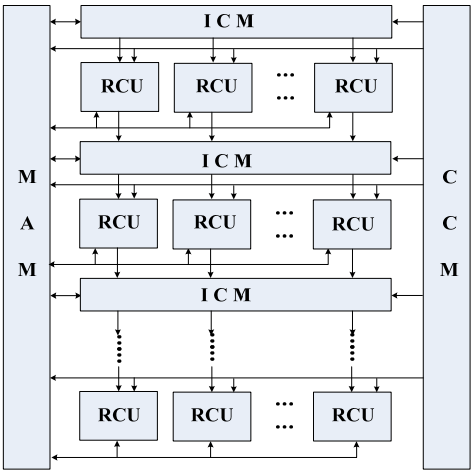

Figure1 RCPA Architecture and Interconnection

The CMM is designed to control and configure the whole operation of RCPA, which main function is to control the configurations in internal modules and the data transfer between internal modules and I/O peripherals as well. The ICM is used to accomplish the data exchange between different stages RCU and the interconnection between MAM and RCU. The MAM provides storage for keys in the crypto algorithms, constants and temporary value in the processing of algorithms. The RCU takes charge to process the operation data and the data width is set as 32-bit which can meet the requirements of a large number of algorithms. As the most critical part of RCPA, RCU will execute all kinds of configuration instructions under the control of CCM.

The RCU is composed of the RCE(Reconfigurable Cipher processing Element) array. Through analysis, we find out that the RCE includes the following basic elements: logic operation, shift or rotation operation, bit-permutation operation, S box substitution, modular multiplication, multiplication in Galois field and modular addition or subtraction. These RCE can be reconfigured according to the configuration instructions, and achieve the function that different crypto algorithms needed flexibly. Besides, the RCE array can be organized by parallel connection, serial connection and a mixed mode.

3.3 RCPA Performance Analysis

The proposed RCPA is suited to the characteristic of the block cipher processing structure, so it matches well in most of the block cipher processing. Its high performance is mainly derived from the parallel processing and pipeline structure design. From the above analysis, we can find that one-step operation in one block is divided into several smaller sub-blocks in most cases, and the processing width is mainly 32-bit. In RCPA, the numbers of sub-blocks which can be parallel and pipeline processed are variable according to different algorithms and the division and scheduling in processing. Based on above-mentioned characteristics, RCPA can be reconfigured to diverse pipeline structures with different depth and width. While analyzing its performance, we should define several RCPA parameters. In RCPA, the number of RCU in each row is defined as R(usually is the integer times of 4), the rows of RCU is denoted as C_r, the number of ICM is set as C_i. The pipeline width is defined as P, the depth is set as H and the number of pipeline is denoted as L. To assume the block length is N, then we can conclude the following equations:

The maximal depth: $H = (C_r + C_i) \times (\frac{R}{N} \times 32)$

The maximal lines: $L = \frac{R}{N} \times 32$

The maximal width: $P = \frac{N}{32}$

Figure 2 shows RCPA can be the reconfigured diverse pipeline stages with different width and depth according to different block length, and the parameter R=4 in figure 2

Now we assume that the number of blocks which will be processed is M and the length of each block is N-bit. The algorithm which will be executed includes r rounds and each round consists of parallel k operation steps. Therefore, we can conclude the performance of three architectures which supporting block cipher processing as the following:

1. In the 32-bit general purpose processor(GPP), the ideal minimal processing cycles are: $CP_1 = M \times \frac{N}{32} \times k \times r$

2. In the RCPA model, supposing the operation is performed by the maximal pipeline depth h and the numbers of RCU can satisfy the k-step sub-block parallelism, then: $h = (C_r + C_i) \times (\frac{R}{N} \times 32)$ the ideal minimal processing circles are:

$$CP_2 = m + r \times k \times \left\lceil \frac{M}{h} \right\rceil - 1 \quad m = \begin{cases} M \bmod h & M \neq hn \quad n = 1,2,3\cdots \\ h & M = hn \quad n = 1,2,3\cdots \end{cases}$$

3. In full pipeline ASIC, the depth of the pipeline can be reached r and all parallel operations can be realized, then the ideal processing circles are: $CP_3 = M + r - 1$

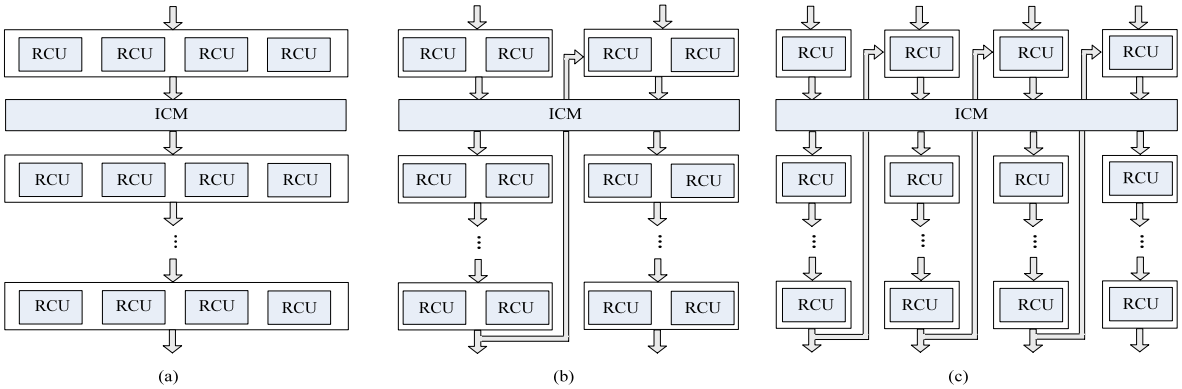

Figure 2 Reconfigurable Stages in RCPA

From the above analysis, the performance has biggish differences along with the increase of the block number M. In the RCPA, it can achieve higher performance than the GPP, and attain better flexibility and security than ASIC implementation. For instance, to define N=128，k=4，r=10，R=4，C_r =4，C_i =4，and we can calculate the value of CP_1、CP_2 和 CP_3 with the increase of M in figure 3. From the performance evaluation of the three different architectures, the performance in RCPA is about 30 times on average than that of GPP, when the value M is between 50 and 300. And its performance is one fifth of the performance of ASIC.

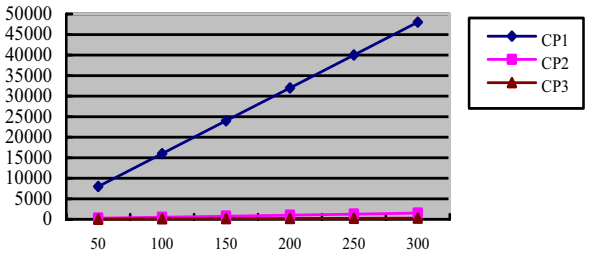

Figure 3 Performance Analysis of GPP, RCPA and AISC

4. Implementation of Prototype Based On RCPA

4.1 Implementation of Prototype

Based on the design and analysis of the RCPA, We have implemented a prototype with its parameters defined as R=4，C_r =4，C_i =4. The prototype adopts VLIW/EPIC computation type and static and dynamic reconfiguration mode which can reach higher practical ILP. Combining its owned architecture this prototype designs the Application Special Instruction Set by reference to EPIC instruction set design in Intel Itanium processor. This instruction set has five types including static configuration, short, long, very long and control instructions. The instruction length is 192-bit, and the instruction RAM address is set as 11-bit. The MAM is realized by adopting register files which are divided into general purpose register files and key register files, the storage capacity is 5120-bit overall. The GPR(general purpose register) is to store initial key, temporary value and constants, the final results are also stored in it. The key register files are designed to store sub-keys and constants. It splits into four banks and each one is 32×32-bit, so it has four read ports and four write ports. There is a fixed read port and a write port for each bank correspondently.

4.2 Results of Prototype

The prototype has been accomplished RTL description using Verilog language. And the design process continues with the synthesis using QuartusII 6.0 from Altera Corporation. The prototype has been verified successfully based on Altera's Stratix II EP2S180F1020I4. Furthermore, the RCPA has been synthesized under 0.18μm CMOS technology using Synopsys' Design Compiler to evaluate performance more accurately. Synthesis, place and route of the prototype based on RCPA have accomplished. The performance results of the prototype based on FPGA and 0.18μm CMOS technology have been shown in table 2 and 3.

Table 2 The prototype's performance based on FPGA

Device	Maximum Frequency	Resource		
		ALUT	Memory (bits)	DSP
EP2S180F1020I4	47.74 MHz	32863	458752	32

Table 3 The prototype's performance based on ASIC

Area (μm^2)	Equivalent Gates (Thousand)	Critical Path Delay	Maximum Frequency
14899092	1489. 9	5.55ns	180MHz

4.3 Prototype Performance Comparison

The prototype's throughput has been computed base on the 180 MHz clock frequency according to the equation: Throughput = (Message block size /number of clock cycles) * clock frequency. The performance of prototype has been increased 3.1 times on average compared with other specialized reconfigurable architectures [3,11], moreover it can support more block cipher algorithms than these architectures. When compared with high-performance general purpose processor (Pentium4 2.1GHz) [12,13,14], the performance of the prototype is much higher than that of this. Figure 4 details the prototype performance comparison with software and other architectures implementations in the several popular algorithms.

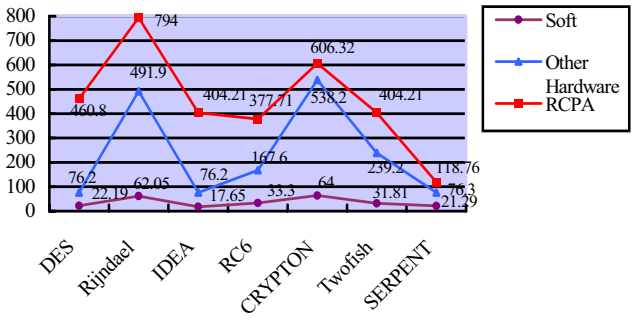

Figure 4 Performance Comparison with implementations of Soft and Other Architectures

5. Conclusion

This paper has focused on the field of block cipher processing application, and proposed a reconfigurable cipher processing architecture (RCPA) combining the design method of reconfigurable processing architecture. A prototype based on RCPA has been implemented successfully based on Altera's FPGA. The experiment results indicate that on the prototype based on RCPA, the performance of many block ciphers is 10~20 times that on high-performance general purpose processor and 1.1~5.1 times higher than that on other specialized reconfigurable architecture. The results prove that RCPA can guarantee high flexibility for most of block cipher algorithms and can achieve relatively high performance.

Acknowledgements

The authors would like to acknowledge and appreciate the immeasurable help and support provided by the schoolmates and teachers in 301 lab.

References

[1] J. Dray. NIST Performance Analysis of the Final Round Java™ AES Candidates. In The Third Advanced Encryption Standard Candidate Conference, pages 149–160,New York, New York, USA, April 13–14 2000.

[2] K. Aoki and H. Lipmaa. Fast Implementations of AESCandidates. In The Third Advanced Encryption Standard Candidate Conference, pages 106–122, New York, New York, USA, April 13–14 2000.

[3] Adam J. Elbirt. Reconfigurable Computing For Symmetric-Key Algorithms[D]. Massachusetts: Electrical and Computer Engineering Department University of Massachusetts Lowell, 2002:

[4] H. Singh, M. Lee, G. Lu, F. J. Kurdahi, N. Bagherzadeh, and E. M. C. Filho. MorphoSys: An Integrated Reconfigurable System for Data-Parallel and Computation-Intensive Applications. IEEE Transactions on Computers, 49(5):465–481, May 2000.

[5] R. Reed Taylor and Seth Copen Goldstein A High-Performance Flexible Architecture for Cryptography. The Proceedings of the 2000 IEEE International Conference on Computer Design: VLSI in Computers & Processors.

[6] R.D. Witting and P. Chow. OneChip: An FPGA Processor with Reconfigurable Logic. In Worshop FPGAs and Custom Computing Machines (FCCM '96), pages 126–135, 1996.

[7] J.R. Hauser and J. Wawrzynek. Garp: A MIPS Processor with a Reconfigurable Coprocessor. In Workshop FPGAs and Custom Computing Machines (FCCM '97), pages 12–21, 1997.

[8] S. Hauck, T.Fry, M.Hosler, and J.Kao. The Chimera Reconfigurable Functional Unit. In Workshop FPGAs and Custom Computing Machines (FCCM '97), pages 87–96, 1997.

[9] C.R. Rupp, M. Landguth, T. Garverick, E. Gomersall, and H. Holt. The NAPA Adaptive Processing Architecture. In Workshop FPGAs and Custom Computing Machines (FCCM '98), pages 28–37, 1998.

[10] J.A. Jacob and P. Cow. Memory Interfacing and Instruction Specifiacation for Reconfigurable Processors. In Seventh International Symposium on Field-Programmable Gate Array (FPGA '99), pages 145–154, 1999.

[11] AJ Elbirt. Instruction-Level Distributed Processing for Symmetric-Key Cryptography[A]. In: Proceedings of the Seventeenth International Parallel and Distributed Processing Symposium-IPDPS[C]. April 2003.

[12] A. Menezes，P. van Oorschot，S. Vanstone. Handbook of Applied Cryptograph[M]. CRC Press,

[13] Crypto++ 5.1 Benchmarks[EB]. http://www.eskimo.com/~weidai/benchmarks.html.

[14] Cylink Corporation. SAFER+ Cylink Corporation's Submission for the Advanced Encryption Standard[R]. Ventura, CA: Standard First Advanced Encryption Standard Candidate Conference, August 1998:

[15] Chae Hoon Lim. Specification and Analysis of CRYPTON Version 1.0[R]. Cryptography&Network Security Center, Future Systems, Inc., 1999: