Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 107 (2017) 395 – 400

Procedia Computer Science

International Congress of Information and Communication Technology (ICICT 2017)

A Flexible Data Scheduling Scheme for Block Cipher Processor

Gongli Li [a,b*], Jinhui Xu [a], Zibin Dai [a], Shoucheng Wang [a], Yufei Zhu [a]

[a]*Institute of Information Science and Technology, Zhengzhou, 450001, China*
[b]*College of Computer & Information Engineering, Henan Normal University, Xinxiang, 453002, China*
** Corresponding author：ligl522@163.com Tel.: +1-593-737-1786*

Abstract

In order to improve the performance of block cipher, clustered processor structure is put forward. How to schedule data in multiple clusters will influence the processor performance directly. Based on the analyzing characteristics of block cipher data flow, we propose a data scheduling scheme according to block width and operation mode. The final algorithm mapping and experiment results show that the data scheduling scheme not only meets the data distribution demand of different algorithms, but also reduces the number of instructions that the algorithms need, thus it can enhance the throughput of most algorithms.

Keywords: block cipher; data scheduling; mode of operation; algorithm mapping

1. Introduction

Data encryption, as one of the effective means of information security, has become the research focus with the increasingly serious information security problem. Data encryption can be represented in the abstract model as shown in figure 1.(a). The data is loaded to on-chip memory by the controller first, and then the data is processed by the crypto unit. At present, most researchers focus on the crypto unit and develop new crypto processor architecture to improve the performance of cryptographic processor, such as multi-core[1], array[2] and clusters[3]. However, when the general processor architecture is applied to design cryptographic processor, it tends to produce some new problems, one of which is the data scheduling, because the cipher data flow has its own characteristics and it is different from traditional application data flow. In order to analyze the characteristics of the block cipher data flow, 52 international typical block cipher algorithms are selected as sample and it includes DES, AES, ISO/IEC block cipher standard[4] (Camellia, MISTY1, CAST-128, TDEA and SEED), European NESSIE plan[5], Japan CRYPYTEC plan[6], industry standard such as IDEA, SM4, CLEFIA, FOX, Skipjack, etc. The sample algorithms have been used extensively, and

Peer-review under responsibility of the scientific committee of the 7th International Congress of Information and Communication Technology
doi:10.1016/j.procs.2017.03.124

they can represent the attribution of the current block cipher. According to the analysis of sample algorithms, we reach the following conclusions:

(1) The block width of different algorithms is not identical, for example, the block width of DES, AES and ABC is 64-bit, 128-bit, and 256-bit respectively. The block width of algorithms in sample is concluded in Table 1.

Table 1. The statistics of block width.

Block width	Amount of algorithms	Typical algorithms
64-bit	24	DES, IDEA, MISTY1, KASUMI, Skipjack
128-bit	25	AES, ARIA, Camellia, MARS, SEED, SMS4
256-bit	3	ABC, SHACAL2, Iraqi

(2) Every algorithm has several different operation modes[7], (shown in Table 2.) the data demands of different operation modes are also different. For example, in CBC mode, as blocks can't be processed in parallel, and only one block can be operated once a time, but in ECB mode, multiple blocks can be processed in parallel, it is obvious that data demands in different operation modes are also different, so it requires to scheduling data flexibly according to the operation mode. The following discussion takes CBC and ECB mode as representative of parallel and serial operation mode.

Table 2. Analysis of operation mode.

Operation mode	Parallel	Operation mode	Parallel	Operation mode	Parallel
CBC	N	IACBC	N	CBC-MAC	N
ECB	Y	IAPM	Y	CMAC	N
CFB	N	OCB	Y	XOR-MAC	Y
OFB	N	CCM	Y	PMAC	Y
CTR	Y	GCM	Y		

(3) The most of block cipher algorithms exist multiple-level parallelism[8, 9]. This is because that the block width of algorithm is large, and one block is processed by multiple function units in parallel. At the same time, in order to improve the throughput, multiple blocks also can be processed in parallel. It means that the parallelism not only exists in block, but also exists among multiple blocks.

So the purpose of this article is to design a flexible and efficient data scheduling scheme basing on the above characteristics of block cipher, and provide flexible and efficient data services for encryption or decryption.

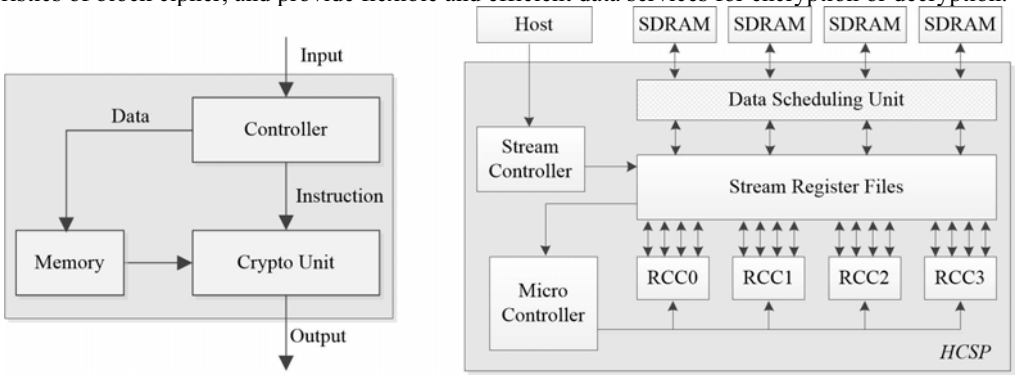

Fig. 1. (a) abstract model of cryptographic processor; (b) architecture of HCSP.

2. Analysis of data scheduling

Data scheduling is a part of the entire cryptographic processor, and it provides service for data encryption operation. In order to illustrate data scheduling problem, we first introduce the component of HCSP (High-efficacy