Microprocessors and Microsystems 61 (2018) 336–343

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Design of Multi Cipher Processing Architecture for Random Cross Access

Li Li[a,b], Fenghua Li[*,1,c], Kui Geng[c], Guozhen Shi[d]

[a] College of Communication Engineering, Xidian University, Xi'an, China
[b] Department of Electronic and Information Engineering, Beijing Electronic Science and Technology Institute, Beijing, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
[d] Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing, China

ARTICLE INFO

Keywords:
Cross encryption and decryption
Parallel architecture
Multi algorithms
Cryptographic processing chip
Synchronization

ABSTRACT

Aiming at the requirement of random cross business generated by mass data cryptosystems in security field, in this paper, a pipeline data processing architecture which includes four stages (i.e., dispatch, pretreatment, operation and synchronous reorganization) is proposed to accelerate data stream processing. In our work, attribute such as business id and algorithm identification of job package is used to distinguish different business requests. Hierarchical processing based on data identification is used to implement the mapping between job packages and algorithm IP cores. KSM memory access control logic is used to access association job package's intermediate state data. And the synchronization module is used to track the operation state to implement the synchronization between the input and output data. These ensure the correctness of cross access on parallel or serial mode. This architecture realizes the high concurrent processing of multiple algorithms and multiple IP cores on one single chip, and solves the problem of random cross encryption and decryption of multiple cryptographic algorithms, multiple keys, multiple IP cores and multiple data streams in many-to-many communication. The prototype system, developed on the XC7K325t FPGA, demonstrates the correctness of cryptographic processing during multi-threads cross data access. Experiments show the system throughput in our approach is higher than existing schemes.

1. Introduction

With the development of information and e-commerce, the data of business systems has been explosively increased. The amount of data has reached the level of TB and PB, which brings huge challenges to data analysis and data storage. So the parallel design and parallel programming technology of multi-cores and multi-threads are becoming the current mainstream of dealing with high concurrency and high-speed information processing [1]. At the same time as more and more enterprises to deploy SaaS and BYOD, cloud security has also entered a period of rapid growth. Gartner's 2017 report *Market Trends: Global Demand for Cloud – Based Security Is Growing Through* 2020 predicts that the cloud security services market, including e-mail security, web security, identity and access management IAM, and others, will reach 9 billion by 2020. Ciphercloud noted that 63% of the surveyed companies considered data protection as the biggest challenge facing cloud computing applications in 2015 annual report *Key Requirements for Cloud Security*. Take cloud storage as an example, both the owner of the information or the trustee of the information all want to ensure the security of the information during storage and transmission. On the one hand, it involves the encrypted storage and encrypted transmission of information. On the other hand, it also hopes to ensure the legitimacy of information sender and receiver, that is, the confidentiality, integrity and authentication of information. The security of the data is inseparable from the encryption algorithm and the authentication protocol. Different processing stage of the storage information uses different cryptographic algorithm. For example, the public key encryption algorithm is adopted in the authentication stage, and the block cipher algorithm is adopted in the transmission stage. Even under the same cryptographic algorithm, the key of different users is also different. That is, there is diversity of demand in cryptographic application service. In the cloud computing environment, the data storage service has the situation that a large number of users request the service at the same time. That is, the characteristic of service intensive exists in cryptographic application. The cryptogram server, as a device to solve the user's security needs, must ensure the fast and efficient cryptographic service. The diversity of applications and increasing security demand gradually become the focus of current research [2–4].

This paper takes the design of multi-cipher parallel processing

* Corresponding author.
E-mail addresses: laury_li@126.com (L. Li), lfh@iie.ac.cn (F. Li).
[1] Member, IEEE.

https://doi.org/10.1016/j.micpro.2018.05.020
Received 26 January 2017; Received in revised form 7 February 2018; Accepted 19 May 2018
Available online 06 July 2018
0141-9331/

architecture as the main object, discusses how to realize the correct processing of cross-access data under the condition of random cross-cryptographic request of multi-services. This method improves the throughput rate of the system through extensible parallelization design, realizes the rapid and effective response to the diversified cryptographic service request.

This paper is organized as follows: Part II reviews the existing research; part III proposes the communication package structure of cross access and the hierarchical processing mechanism; part IV introduces the hardware architecture of the parallel pipelined cryptographic processing system, and the performance of the system is analyzed in part V.

2. Related research

Till today, the research and application of cryptographic service processing for massive data mainly focus on parallel processing architecture and high-speed parallel processing of algorithm itself. Parallel processing architecture is divided into GPU(graphics processing unit) based general-purpose multi-core CPU architecture and the dedicated multi-core architecture based on cryptographic algorithm IP core. In a general multi-core CPU architecture, parallel programming mode [6] and concurrent [5,8], pipelined processing [7] of multiple GPUs are often used to speed up execution. Each GPU core pipeline processes the same business sequence packages, and does not involve heterogeneous cores.

Because of the programmable and configurable characteristics of FPGA, FPGA is the main platform to improve the performance of cryptographic algorithms in professional multi-core architecture. The special multi-core architecture based on cryptographic algorithm IP core has advantages of fast computation speed and good confidentiality. It adds several crypto IPs in one system, these IP cores are used to operate fast key expansion and maximum data superimposed flow processing to improve the system throughput and to speed up data processing [13–16]. In [9], a heterogeneous multi-core SOC architecture was proposed to deal with different security protocols, which integrates a general MIPS processor GP, a special packet processor PP, and four security processors SPs. So that the processing of various cryptographic algorithms is realized, but the data throughput is low. In [29], an implementation method for a parameterized AES encryption coprocessor was proposed. It implemented AES algorithm in a full pipeline mode on the general 32bits 5 level pipelined MIPS processor. The effect of round number to delay, storage space and area was studied. Literature [10] proposed a configurable Multi-Core Crypto-Processor (MCCP), which supported a variety of AES cipher mode. It assigned tasks to a plurality of algorithm cores by task schedule module. On the basis of studying the processing characteristics of elliptic curve cryptography and the parallel scheduling algorithms on Finite Field, paper [17] presented a parallel processor architecture model for elliptic curve cryptography based on instruction level and data level parallelism. It ensured the flexibility of the elliptic curve cryptography algorithm, as well as high performance. Paper [18] designed a hybrid encryption system using symmetric and public key system. But the model is relatively fixed, and its flexibility is poor. All of these above documents do not take into account the cross cipher request between different services. In view of cross encryption and decryption of business data, paper [11] proposed a multi-thread cipher chip architecture. Compared with the typical cipher processor architecture, special volatile memory was added in it, but it was not implemented and verified. Literature [12] proposed a parallelization scheme for multi-core parallel execution of Gentry fully homomorphic encryption, which involved the processing of cross services. This method solved the problem of context related business in parallel processing by establishing data dependence graph, but this method required high parallelism programming and lacked scalability of the system.

The parallel high-speed processing of algorithm is mainly focused on two aspects: algorithm's parallelism mining and pipelined implementation. Amdahl law points out that the speed of single task processing is limited by the serial execution of the task itself, and can not increase with the increase of the number of nodes. So for single task, the processing speedup ratio of a single task can be improved only by decreasing the serial execution part of the algorithm. Most papers parallelized part structure of algorithm [20] and combined with algorithm pipeline to improve algorithm performance. For example, paper [19] parallelized GHASH in sub-key expansion. Asymmetric cryptographic algorithm performance largely depends on the modular exponentiation. Papers [21–25] improved the computing speed of the elliptic curve cryptography by parallel processing of scalar multiplication architecture. Papers [26,27] discussed the scalable VLSI architecture for inverse operations of Montgomery modules, in order to improve the computational speed of algorithm cores and reduce resource occupancy.

As mentioned above, in the existing research, the high-speed parallel processing of the algorithm itself is mostly concentrated on the optimization design of the algorithm core. It is accelerated by the parallel and pipeline implementation of part of the algorithm structure. In addition, although the design of parallel processing architecture realizes the encryption and decryption of data with different keys and encryption and decryption of different data with a single key, it does not involve the cross encryption of multi-algorithms, multi-keys, multi-data streams. This paper focuses on the design of processing architecture. According to the characteristics of high concurrent data, this paper proposes a hierarchical processing mechanism based on data identification. Through the construction of job packages with specific identification, this method realizes the parallel operation between multiple algorithm modules, completes the data processing of cross business flow, and improves the efficiency of cryptographic services.

3. High concurrent data processing model

In cloud computing, information security service has massive, continuous, multi-links, multi-processing requirement characteristics. In this paper, the process of mass data cryptographic service is divided into five stages: parallelization, distribution, parallel computing, feedback and package reorganization. High concurrency cross data processing model is shown in Fig. 1, where cryptographic module is managed by cluster. For example, P_{i-j} indicates the j-th execution module of algorithm i. Parallelization stage realizes isomorphic processing of different business from different links, to facilitate the later parallel computing of package. Distribution stage sends the package of different demand to the corresponding algorithm operation module; parallel computing stage operates data processing according to its needs; feedback stage loops processed packages back to the respective application server; package reorganization stage reassembles processed packages of the same business to one result on application servers.

3.1. Communication data package

In order to guarantee the correct processing of crypto algorithm

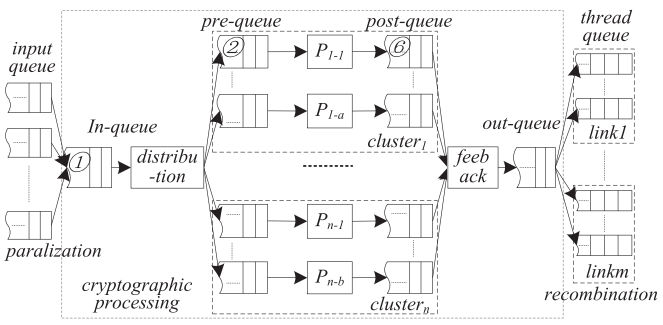

Fig. 1. High concurrent data processing module.