多核密码处理器中的片上网络互连结构研究

杜怡然[1]，李 伟[1,2]，戴紫彬[1]
(1 解放军信息工程大学，河南 郑州 450000；
(2 复旦大学 专用集成电路与系统国家重点实验室，上海 201203)

摘 要：为有效解决目前单核密码处理器性能无法满足高速密码运算处理需求的问题，研究了片上网络结构的基本特点，设计并实现了基于共享存储式的簇状片上网络多核密码处理器架构，分析密码运算特征并完成密码算法的多核适配.与单核密码处理器性能相比，本架构有较强的并行性及可扩展性，能够更好地完成大位宽、细粒度密码算法的支持.高效的核间数据交互机制大大提升了片上网络多核密码处理器密码处理性能，能够实现最大426 Gb/s的网络数据吞吐量，与通用多核处理器实现密码算法相比，性能提升约5.7%～37.5%.

关键词：共享存储；片上网络；算法适配
中图分类号：TN4 **文献标识码**：A **文章编号**：1000－7180(2016)01－0010－05

Research and Implementation of Network-on-Chip Interlinkage Structure for Multi-core Cipher Processor

DU Yi-ran[1], LI Wei[1,2], DAI Zi-bin[1]
(1 PLA Information Engineering University, Zhengzhou 450000, China;
2 State Key Laboratory of Special Integrated Circuit and System, Fudan University, Shanghai 201203, China)

Abstract: In order to solve the problem that a single-core cipher processor cannot satisfy the high speed cryptographic operations' demand, this paper focused on the network-on-chip architecture and proposed a new architecture based on shared memory for multi-core cipher processor. In the proposed architecture, this paper analyzed the characteristic of cryptographic operations and achieved a DES algorithm mapping. Comparing with the single-core cipher processor, the proposed architecture gets a better parallelism and expansibility, to provide a giant bandwidth and fine grit cryptographic algorithm support. An efficient data interaction mechanism is able to improve the performance of multi-core cipher processor, and achieved a maximum throughput for 426 Gb/s. The performance of the proposed architecture improved about 5.7% ～ 37.5% when compared with the general purpose multi-core processor in achieving cryptographic algorithms.

Key words: shared memory; network-on-chip; algorithm mapping

作者简介：

杜怡然 男，(1991-)，硕士研究生.研究方向为安全专用芯片设计.E-mail:420197028@qq.com

李 伟 男，(1983-)，博士研究生，讲师.研究方向为专用集成电路设计.

戴紫彬 男，(1966-)，博士，教授.研究方向为专用集成电路设计、芯片可重构设计.