第38卷 第21期 计 算 机 工 程 2012年11月
Vol.38 No.21 Computer Engineering November 2012

• 工程应用技术与实现 • 文章编号：1000—3428(2012)21—0245—04 文献标识码：A 中图分类号：TP393

面向无线局域网安全领域的片上网络多核架构

王 帅，韩 军，李 阳，曾晓洋

(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： 在计算机系统和通信网络中，安全协议和密码算法用于保护敏感信息，但如何快速计算上述协议和算法成为难题。为此，提出一种面向无线局域网安全领域的片上网络多核架构。该片上网络架构包括4个类MIPS的精简指令集处理器和12个面向安全领域的专用指令集处理器(ASIP)。每个ASIP中含有一个改进的并行查找表用来加速高级加密标准算法。该架构凭借任务并行能够获得较高的计数器模式密码块链消息完整码协议吞吐率。在SMIC 0.13 μm标准CMOS工艺下，实现该架构需要约308万等效门。实验结果表明，该系统的最大工作频率为84 MHz，能获得787 Mb/s的吞吐率。

关键词： 无线局域网；片上网络；高级加密标准；并行查找表；专用指令集处理器

NoC Multicore Architecture for WLAN Security Domain

WANG Shuai, HAN Jun, LI Yang, ZENG Xiao-yang

(State Key Laboratory of ASIC & System, Fudan University, Shanghai 201203, China)

【Abstract】 Security protocols and cryptography algorithms(ciphers) are widely used to protect the sensitive digital information in computer systems and communication networks. How to process these computation-intensive protocols and algorithms has become a crucial issue. This paper presents a Network on Chip(NoC) architecture for Wireless Local Area Network(WLAN) security domain. Four MIPS-like RISC processors and twelve security-oriented ASIPs fabricate the proposed 4×4 mesh NoC architecture. In each ASIP, the Parallel Look-Up Table (PLUT) method is implemented to accelerate Advanced Encryption Standard(AES) encryption. Moreover, task parallelism in Counter CBC-MAC Protocol(CCMP) is exploited, thus high throughput is obtained. The proposed architecture is synthesized under SMIC 0.13 μm CMOS technology and costs 3083 k-gates. Experimental results show that the system achieves a throughput of 787 Mb/s at 84 MHz.

【Key words】 Wireless Local Area Network(WLAN); Network on Chip(NoC); Advanced Encryption Standard(AES); Parallel Look-Up Table (PLUT); Application Specific Instruction-set Processor(ASIP)

DOI: 10.3969/j.issn.1000-3428.2012.21.065

1 概述

随着无线技术的高速发展，在无线系统中的信息很容易被监听，这使得通信安全问题越发成为关注的焦点。为此，人们制定了多种安全协议对无线通信提供安全保证。在无线局域网中，IEEE 802.11i[1]标准中建议采用计数器模式密码块链消息完整码协议(Counter CBC-MAC Protocol, CCMP)。传统做法是采用通用处理器来处理诸如CCMP这些加密协议中的复杂运算，但随着越来越多的数据需要经过高强度的安全加密处理，通用处理器有限的处理能力就成为运算瓶颈。

本文提出一种基于片上网络(Network on Chip, NoC)的异质多核架构。通过任务的并行处理，该架构能够快速进行CCMP中的相关加密运算。该架构采用4×4的mesh拓扑结构，包含有4个精简指令集处理器(Reduced Instruction Set Computer, RISC)和12个面向安全领域的专用指令集处理器(Application Specific Instruction-set Processor, ASIP)。其中，RISC处理器作为主控器承担着运行操作系统，封装以及解封数据包，为12个ASIP调配加密任务等职能。每个ASIP内部都有一个并行查找表可以快速实现AES加密。

2 AES算法及CCMP协议

2.1 高级加密标准

高级加密标准是一种对称分组密码，美国国家标准与技术研究院推荐将AES用于块数据的加密，现已被很多安全协议所采用，其具体算法在FIPS PUB-197[2]中被明确规定。CCMP协议中所用到的AES的密钥宽度是128位，它是CCMP的核心运算。

128位的AES算法要进行10轮运算。在其中每一轮，128位的明文被划为一个4×4的字节阵列，要进行4种操作，具体说来包括字节替换、行移位、列混淆和轮密钥加。这些运算的详细过程可以参考文献[2]。需要指出的是，在

基金项目： 国家自然科学基金资助项目(60776028)；教育部科学技术研究基金资助重点项目(109055)

作者简介： 王 帅(1986－)，男，硕士研究生，主研方向：多核SoC系统设计；韩 军，助理研究员；李 阳，硕士研究生；曾晓洋，教授、博士生导师

收稿日期： 2012-02-13 **修回日期：** 2012-03-11 **E-mail：** junhan@fudan.edu.cn

AES 的 10 轮运算中，前 9 轮每一轮都需要执行这 4 种运算，而最后一轮不需要列混合运算。

AES 算法可以用查找表的方式来实现。文献[3]采用了一种并行查找表的方式。如图 1 所示，该方法可以通过简单的查表方式来实现字节替换、行移位和列混淆的复杂运算过程，因此可以极大地提高 AES 的加密速度。

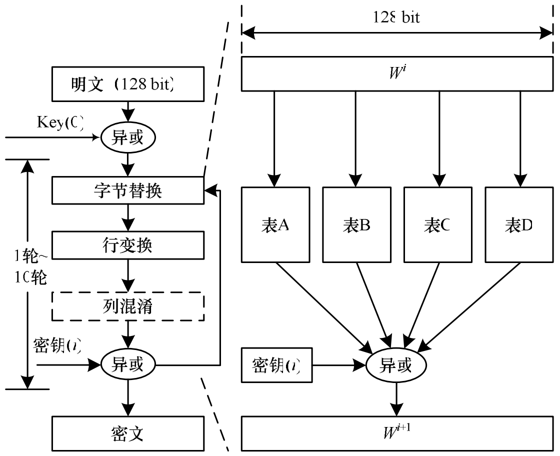

图 1 AES 算法及其并行查找表实现方式

2.2 CCMP 协议

CCMP 协议是建立在 AES 基础之上，以计数器(CTR)方式对数据进行加密，以密码分组链(CBC-MAC)方式计算消息的认证码(Message Integrity Check, MIC)。

图 2 展示 CCMP 的加密过程。具体说来可以分为 3 步。首先，从 MAC 协议数据单元(MAC Protocol Data Unit, MPDU)中提取出 CCMP 头、MAC 帧头等信息，并对明文进行封装打包。之后，对封装好的信息进行 2 种模式的 AES 运算：(1)在 CBC-MAC 模式下通过 AES 加密计算出 MIC 值以保证数据的有效性及完整性。(2)待加密的数据及 MIC 值经过 CTR 模式的 AES 加密保证其机密性。在解密时，用相同的密钥把密文还原成明文，并计算所还原明文的 MIC 值，其值与解密所得到的 MIC 值对比，若相同，则接收该帧；若不同，则表明该帧在数据传递过程中出现问题，拒绝该帧并作后续处理。

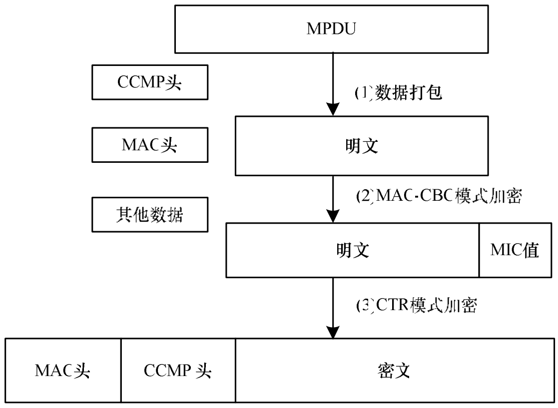

图 2 CCMP 的加密流程

2.2.1 CBC-MAC 模式

图 3 展示了 AES 的密码分组链消息认证码(Cipher Block Chaining Message Authentication Code, CBC-MAC)模式的流程。首先通过构造的 CCMP 头与原始的 MAC 帧头来产生起始的待加密数据(MIC_IV, MIC_HDR1, MIC_HDR2)。对这部分数据与明文以 16 Byte 为单位进行数据分组，并且按照顺序依次对每一组进行加密和异或处理。对明文的最后数据进行分组时，不足 16 Byte 则补零。这样可以最终得到 16 Byte 加密数据，选择其中的 8 个字节作为 MIC 值。

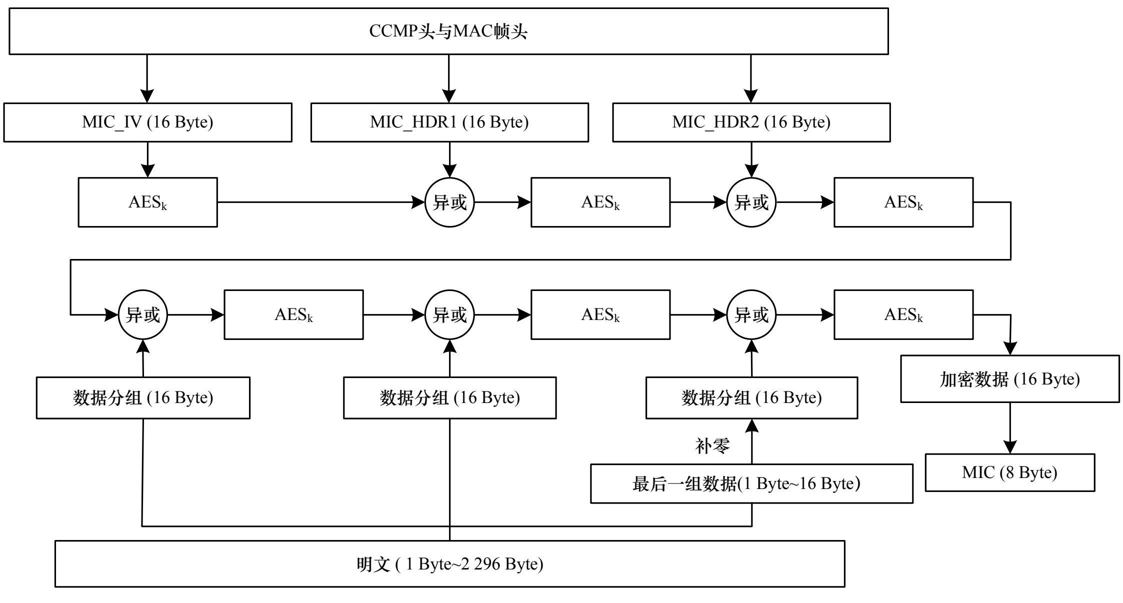

图 3 CBC-MAC 模式的 AES 加密

2.2.2 CTR 模式

在 CTR(计数器)模式下，明文与在 CBC-MAC 模式下得到的 MIC 值一起进行加密。同样的，数据以 16 Byte 为单位进行分组，每组都会异或上一个 AES 加密的结果，如图 4 所示。其中，明文的最后部分以及 MIC 值由于不足 16 Byte，因此异或操作时会从 AES 加密的结果中截取出相应字节数。对于每一次的 AES 加密，其加密的内容(CTR(x))为不同的计数值，其值与分组序号有关。

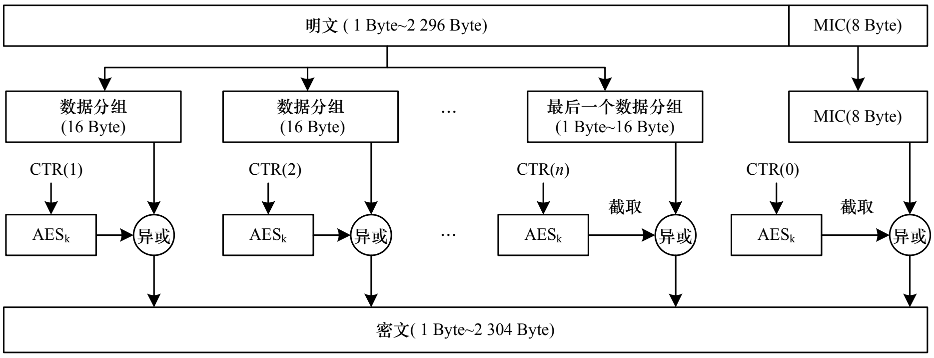

图 4　CTR 模式的 AES 加密

3　面向 CCMP 的异质多核架构及任务分配

3.1　ASIP 架构

如前所述，AES 加密是 CCMP 的核心运算。为了加速 CCMP，本文设计了加速 AES 加密的 ASIP。如图 5 所示，该 ASIP 是一个拥有 5 级流水线结构的精简指令集处理器。特别地，在执行级引入改进的并行查找表来加速 AES 运算。

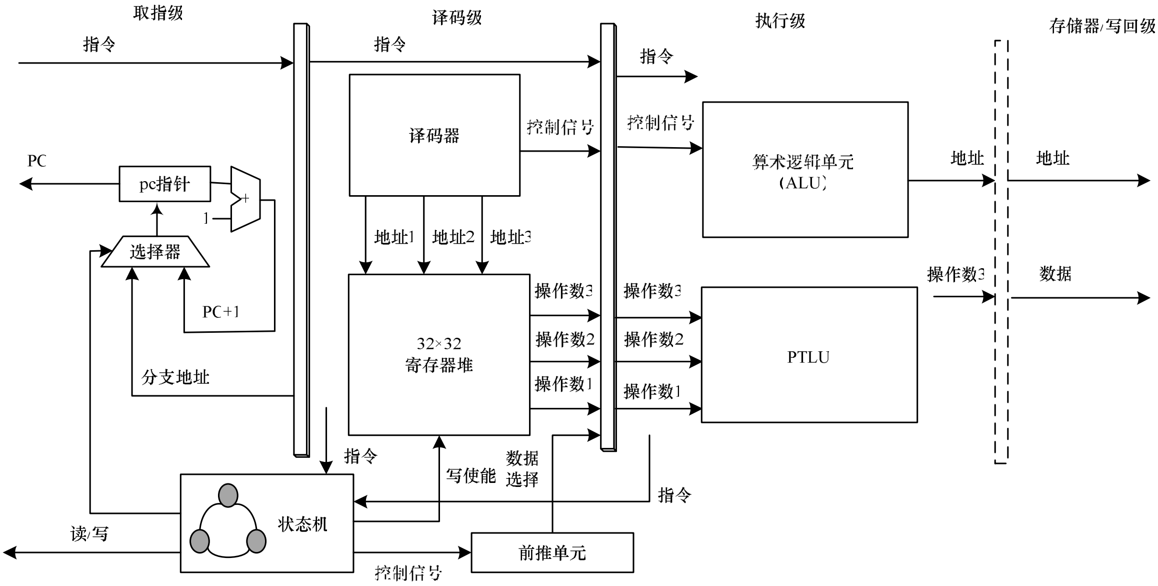

图 5　ASIP 架构

在硬件中引入 PTLU 的同时，在软件中本文也扩展了相应的专用指令，如表 1 所示。其中 r1、r2 表示处理器中的 2 个全局寄存器，p1 是一个特殊寄存器。

表 1　扩展的 AES 专用指令

指令代码	执行周期	执行操作
ld_ptlu p1 r1 r2	1	p1←Ram[r1+r2]
mf_ptlu r2 p1	1	r2 ← p1
mt_ptlu p1 r2	1	p1 ← r2
ptaes p1	1	AES1 至 9 轮的结果存入 p1
ptaes_last p1	1	最后一轮的结果存入 p1

3.2　异质多核架构

本文所设计的异质多核架构采用 4×4 的 mesh 拓扑结构[4]，如图 6 所示。采用传统的 x-y 路由算法来传递数据包。4 个具有 MIPS 架构的精简指令集处理器作为主控单元来处理系统的一般性事务。在处理 CCMP 协议时，它们负责从共享存储器中读取 MPDU 并将它们打包后分发给各个 ASIP，之后将加密后的 MDPU 存回共享存储器。

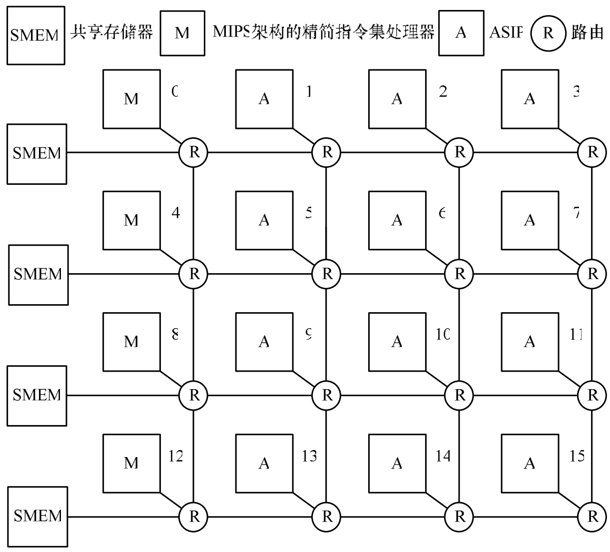

图 6　4×4 mesh 拓扑的异质多核架构

3.3　CCMP 任务分配

在 2.2 节讲述了 CCMP 的加密流程。观察到由于 MIC 值的计算是一个串行的过程，因此这个过程不能通过任务

的并行来进行加速。相反地，由于 CTR 运算中各个分组中的 AES 加密彼此间没有任何的相关性，因此对于一个 MDPU 可以将 CTR 运算与 MIC 值的计算用 2 个 ASIP 来加速，如图 7 所示。对于第 1 个 MDPU 帧，它的 MIC 值运算由 ASIP1 来完成，而 CTR 运算由 ASIP2 来完成。注意到 ASIP1 与 ASIP2 任务的起始时间并不相同，这是由于数据在 NoC 网络上的传输延时所引起的。为了减少传输延时所带来的性能损耗，MIC 值的 CTR 计算并不是传给 ASIP2 来进行的，而是立刻在 ASIP1 上完成。

可以看到，对于每个 MDPU 帧来说，MIC 值的计算由于数据的相关性无法并行展开，因此其是最为耗时的部分。但是如图 7 所示，本文所提供的拥有 12 个 ASIP 的 NoC 架构可以以 2 个 ASIP 为一组同时加密 6 个 MDPU 帧，因此能够极大地提高 CCMP 的加密速度。

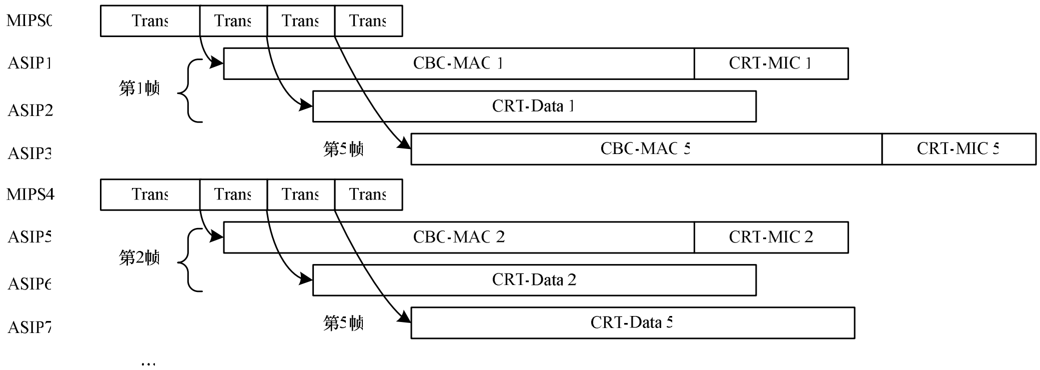

图 7 CCMP 的任务划分

4 实验结果

本文设计并实现该面向 CCMP 的异质多核 NoC 架构，采用 SMIC 0.13 μm 的标准 CMOS 工艺，对 RTL 代码进行综合。综合结果表明该系统最大工作频率为 84 MHz，面积为 308 万等效门。表 2 列举了该系统中各主要模块的面积，单位是万等效门。其中，MIPS 指代图 5 中 MIPS 架构的精简指令集处理器。从表中看到，对于整个系统来说，存储器消耗了大量的面积资源。表 3 比较了本文异质多核方案与其他设计方案。相比较与文献[5-6]的处理器设计方案，本文所提出的架构能够获得更高的吞吐率，达到 787 Mb/s，同时能够获得很高的效率值(吞吐率/频率)。虽然文献[7]的专用集成电路(ASIC)设计方案能够获得较高的吞吐率，但是 ASIC 的灵活性远不如本文所采用的多核方案。

表 2 本文方案各主要模块的面积 万等效门

模块	面积	模块	面积
MIPS 存储器	12.7	ASIP 核	2.7
MIPS 核	3.4	路由	2.1
ASIP 存储器	9.2	多核系统	308.3

表 3 本文异质多核方案与其他设计方案实验结果对比

方案	设计工艺	平台	面积	系统频率/MHz	吞吐率/($Mb\cdot s^{-1}$)	效率值/($Mb\cdot s^{-1}\cdot MHz^{-1}$)
本文方案	0.13 μm CMOS	异质多核处理器	308 万等效门	84	787	9.370
文献[5]方案	0.13 μm CMOS	处理器	6 万等效门	250	275	1.100
文献[6]方案	FPGA Stratix	处理器	7 383 个单元(slice)	50	562	11.240
文献[7]方案	FPGA Virtex4	ASIC	2 1862 个单元(slice)	193	17 518	90.767

5 结束语

本文提出一种面向无线局域网安全领域的片上网络多核设计方案。实验结果表明，该方案能够获得较高的吞吐率，可以胜任 IEEE 802.11i 及 IEEE 802.11n 等标准。同时由于具有可编程的特性，因此本文方案还可以进一步兼容 SMS4, SHA-1 等安全算法。

参考文献

[1] LAN/MAN Standards Committee. IEEE Std: 802.11i-2004 Part11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications[S]. 2004.

[2] National Institute of Standards and Technology. FIPS: 197-2001 Advanced Encryption Standard(AES)[S]. 2001.

[3] Fiskiran A M, Lee R B. Fast Parallel Table Lookups to Accelerate Symmetric-key Cryptography[C]//Proc. of International Conference on Information Technology: Coding and Computing. Las Vegas, USA: [s. n.], 2005: 526-531.

[4] 欧阳一鸣, 董少周, 梁华国. 基于 2D Mesh 的 NoC 路由算法设计与仿真[J]. 计算机工程, 2009, 35(22): 227-229.

[5] Smyth N, McLoone M, McCanny J. WLAN Security Processor[J]. IEEE Trans. on Circuits and Systems, 2006, 53(7): 1506-1520.

[6] Bae D, Kim G, Kim J. Design and Implementation of Efficient Cipher Engine for IEEE 802.11I Compatible with IEEE 802.11n and IEEE 802.11e, Lecture Notes in Computer Science[C]//Proc. of IEEE CIS'05. [S. 1.]: IEEE Press, 2005: 439-444.

[7] Hoseini S A, Khodabandeloo B, Mamaghani M J. High Throughput Low Power CCMP Architecture for Very High Speed Wireless LANs[C]//Proc. of the 15th CSI International Symposium on Computer Architecture and Digital Systems. [S. 1.]: IEEE Press, 2010: 59-65.

编辑 索书志