一种可重构体系结构用于高速实现 DES、3DES和 AES

高娜娜, 李占才, 王 沁
(北京科技大学信息工程学院, 北京 100083)

摘 要: 可重构密码芯片提高了密码芯片的安全性和灵活性, 具有良好的应用前景. 然而目前的可重构密码芯片吞吐率均大大低于专用芯片, 因此, 如何提高处理速度是可重构密码芯片设计的关键问题. 本文分析了常用对称密码算法 DES、3DES和 AES的可重构性, 利用流水线、并行处理和可重构技术, 提出了一种可重构体系结构. 基于该体系结构实现的 DES、3DES和 AES吞吐率在 110MHz工作频率下分别可达到 7Gbps、2.3Gbps和 1.4Gbps 与其他同类设计相比, 本文设计在处理速度上有较大优势, 可以很好地应用到可重构密码芯片设计中.

关键词: 可重构体系结构; DES算法; AES算法
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2006) 08-1386-05

A Reconfigurable Architecture for High-Speed Implementations of DES, 3DES and AES

GAO Na-na, LI Zhan-cai, WANG Qin
(Information Technology School, University of Science & Technology Beijing, Beijing 100083, China)

Abstract A reconfigurable cipher chip which can improve the security and flexibility, has good potential to become a vital component in the future security system. However, the throughput of most reconfigurable cipher chips is pretty lower than that of specific purpose chips. How to improve the throughput becomes more and more important. In this paper, based on the analysis about the reconfiguration of the DES, 3DES and AES, we propose a reconfigurable architecture, which combines reconfiguration technology with pipeline, parallel structure. We also implement DES, 3DES, AES algorithms based on the reconfiguration architecture. The simulations show that the throughput is 7Gbps for DES, 2.3Gbps for 3DES and 1.4Gbps for AES under a 110MHz clock. Moreover, the comparison with other current designs shows that the solution proposed in this paper achieves better performance than other solutions, and thus is suitable to the design of reconfigurable cipher chips.

Key words reconfigurable architecture; data encryption standard; advanced encryption standard

1 引言

目前, 大多数密码芯片是实现一种固定密码算法的专用芯片, 难以满足不同密码用户多层次的安全性能需要和密码算法升级换代的需求, 从而带来安全隐患. 因此, 近年来许多研究机构都致力于可重构密码芯片的研究[1~3]. 可重构密码芯片是利用可重用的硬件资源, 根据不同的应用需求灵活地改变自身硬件结构, 为不同的密码算法提供与之相匹配的内部结构和外部特性, 从而大大提高了密码芯片的灵活性、安全性和扩展性, 具有良好的应用前景.

信息技术的飞速发展, 对密码算法的处理速度要求越来越高, 尤其是分组密码算法, 它们在安全体制中主要应用于数据的加/解密, 因此低吞吐率的分组密码算法往往会成为安全通信的瓶颈. 与单一密码算法芯片相比, 可重构密码芯片虽然增强了安全性和灵活性, 但是处理速度却大大降低了. 例如, SNL (Sandia National Laboratories)的 DES算法 ASIC 实现[4], 吞吐率可达到 9.28Gbps; Henry Kuo的 AES算法 ASIC 实现[5]对 128位分组加/解密吞吐率可达到 1.6Gbps 而文献[2]中可重构安全模块 Cryptonite的 DES和 AES吞吐率仅为 0.73Gbps 因此, 提高处理

收稿日期: 2005-03-25; 修回日期: 2006-04-15

速度是可重构密码芯片设计的关键问题.

本文提出了一种用于实现常用分组密码算法 DES、3DES和 AES的高吞吐率可重构体系结构, 它既有 ASIC的高处理速度, 又具有一定的"柔性", 增强了算法的安全性和灵活性.

2 可重构性分析

任何一个密码算法都是由一系列的基本操作按照一定的顺序连接而成, 并且不同密码算法往往具有相同和相似的操作, 因此可以将这些操作设计为可重构处理单元(Reconfigurable Processing Unit, RPU), 为不同的密码算法所共用. 为了适应不同的应用需求, RPU 内部有可控节点, 可控节点可以是一个功能单元, 如选通器(MUX)等, 也可以是一些控制信号. 通过对可控节点的控制, 改变 RPU 的内部结构以及和其他部件的连接关系, 从而匹配不同的密码算法.

DES(3DES)[6]和 AES算法[7]的基本运算如表 1所示, 由表 1可看出 DES(3DES)和 AES相似性运算有循环移位、异或运算和 S盒变换. 由于循环移位的位数固定, 为了提高处理速度, 可以不用移位寄存器而采用直接连线的方式实现, 因此, 循环移位不设计为 RPU. 异或运算虽然是所有分组密码算法都用到的操作, 但将其设计为 RPU 需要增加相应的 MUX, 实现不同输入的异或运算. 由 TSMC 0.25标准单元库[8]知, MUX的规模和时延都大于异或单元, 因此若将异或单元设计为 RPU, 则其时延是固定异或单元的两倍以上, 大大降低了处理速度. 所以, 为了高速实现密码算法, 异或运算不设计为 RPU.

表 1 DES、3DES和 AES的基本运算

算法	DES(3DES)	AES(分组为 128位)
基本运算	28位循环移位	32位循环移位
	6* 4S盒变换	8* 8S盒变换
	32位异或运算	128位和 32位异或运算
	32* 48扩展置换	列混合
	64* 64初始(逆)置换	
	32* 32P盒置换	
	56* 48密钥压缩置换	

S盒的规模占算法规模的 30%以上, 是密码算法的唯一非线性部件, 它的密码强度决定了整个密码算法的安全强度. 目前, S盒的实现均是采用固定运算部件实现, 一旦实现, S盒变换就不可更改, 因而导致安全隐患. 将 S盒设计为 RPU, 通过对 S盒的更新换代可以提高算法的安全性. 例如 DES算法的安全性已经受到威胁, 1998年 EFF宣布用一台专用"DES破译机"破译了 DES, 然而直到目前 DES仍广泛应用于商业领域, 因此有必要采用抗攻击性强的 S盒来增强 DES的安全性, 文献[9]通过演化设计得到一批比 DES原 S盒性能更为优异的 S盒组, 所以若将 S盒设计 RPU, 可通过配置文献[9]中新的 S盒, 提高 DES算法的安全性.

AES解密运算中的 S盒是加密运算 S盒的逆变换, 若既要实现加密运算又能完成解密运算, 则需要两套不同的 S盒, 将 S盒设计为 RPU, 可以通过配置使它既能用于加密又能用于解密. 因此, S盒作为 RPU 不仅可以实现 DES(3DES)和 AES算法 S盒的重构, 还可以实现 AES加密 S盒和解密 S盒的重构, 这对分组算法可重构的实现和安全性的提高具有重要影响.

3 可重构体系结构

可重构体系结构的设计目标是根据不同的应用需求, 灵活、快速的改变自身的结构, 以便为每个特定的应用需求提供与之相匹配的体系结构. 其难点在于如何提高处理速度, 因为灵活性的提高往往以降低处理速度为代价. 因此, 如何在增强灵活性和安全性的同时, 保障高吞吐率已经成为可重构密码芯片设计中至关重要的问题. 本文的设计思想是将流水线、并行处理技术和可重构技术相结合, 达到提高可重构密码芯片处理速度的目的.

3.1 系统结构

可重构系统结构如图 1所示. 其中, RPU 阵列由多个 RPU 构成, 是系统结构的核心单元, 完成可重构计算; ALU 完成其他非可重构计算, 不同的算法对应于不同的 ALU 单元; 控制单元产生控制信号, 控制可控节点确定数据传输路径, 即 RPU 之间以及 RPU 和 ALU 之间的连接关系, 以实现不同的密码算法; 外部接入单元完成数据的输入输出, RPU 配置输入等.

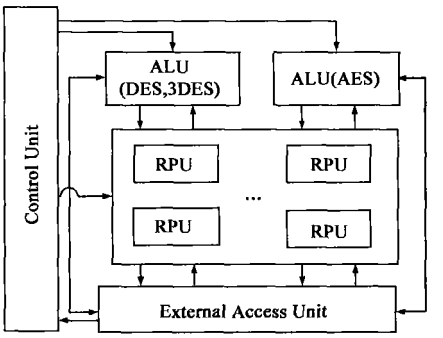

图 1 可重构系统结构图

由此可见, 影响可重构体系结构处理速度主要因素包括: ①RPU 的设计; ②数据传输路径.

RPU 为不同的密码算法所公用, 而不同的算法要求 RPU 实现的功能往往是不同的. 如表 1中 DES和 AES都要进行 S盒变换, 但 DES算法 S盒是实现 48* 32查表, 而 AES算法 S盒则实现 8* 8查表. 所以, RPU 内部电路结构必须是可变的. RPU 结构的复杂度直接影响它的时延, 从而影响到整个系统的处理速度. 因此, 关键问题之一是找到复杂度低、可重构性强的 RPU 解决方案.

数据传输路径是指逻辑模块之间的连接关系, 它直接相关于不同算法的具体实现. 数据传输路径时延决定了密

码算法完成一个分组加/解密所需的时间,从而决定了密码算法的处理速度.因此,关键问题之二是在体系结构层次找到可以缩短路径时延的解决方案.

3.2 RPU设计

第2节分析了DES、3DES和AES的可重构性,确定S盒可以设计为RPU,即可重构S盒(RC-S: Reconfigurable S-box).RC-S的设计是可重构体系结构设计的一个难点,它既要实现DES或3DES的48*32查表,又要实现AES的8*8查表.图2是本文提出的RC-S内部结构,其中2选1的MUX和4选1的MUX(只用于AES算法)为可控节点.8个并行的RAM用于S盒查表,每个RAM有6位地址线,输出为4位,占用32字节空间.RC-S的输入为DES(3DES)和AES地址线、WEN信号、REN信号和CTRL信号.CTRL用于可控节点的控制,WEN和REN用于控制RAM的读写,使RC-S实现不同算法的S盒功能.RC-S的输出为DES(3DES)和AES的S盒查表结果.

实现DES或3DES时,RC-S地址为48位,输出32位,每个RAM有不同的地址线;实现AES时,RC-S地址为8位,每个RAM的地址相同为地址中的低六位,8个RAM的输出分为4组,RAM0和RAM1的输出为一组,RAM2和RAM3,RAM4和RAM5,RAM6和RAM7分别组合,其中RAM0、RAM2、RAM4和RAM6输出分别为每组的高位,由AES地址的高两位选通其中一组作为输出,因此实现AES时RC-S的输出为8位.

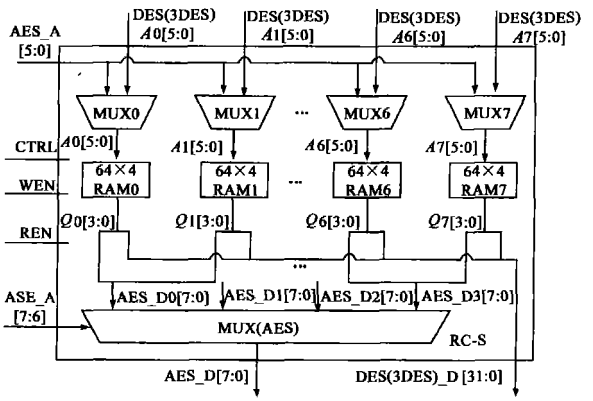

图2 RC-S结构图

可见,与固定S盒相比,实现DES或3DES时,RC-S仅增加了一级MUX时延;实现AES时,RC-S增加了两级MUX时延.因此RC-S结构简单、时延较短,有利于处理速度的提高.

3.3 流水线和并行处理

为了解决数据传输路径问题,本文采用流水线和并行两种体系结构.为此,需要考虑以下几个问题:

(1)规模的约束,如何在规模和性能上找到一个平衡点;(2)RPU个数的确定,采用多少个RPU才能以最少的硬件资源满足不同密码算法高吞吐率的需求;(3)RPU间的连接关系,不同的算法有不同的流水线和并行结构,如何改变RPU的连接关系以匹配不同密码算法.

分组密码算法的多圈循环加密结构非常适合建立流水线,但这并不意味着可以不计成本对所有算法建立流水线.由于DES圈变换规模较小,对DES和3DES的高速硬件实现大多采用流水线方式,文献[10]给出了不同流水线深度的DES吞吐率和性价比,当DES的16轮循环全部展开为16级流水线时称为满流水(full pipeline),这时的吞吐率最大、性价比最高.而AES圈变换有很好的并行性,S盒变换、列变换和异或运算均可并行的作用在状态的字节或列上.由于AES圈变换规模较大,一般不建立流水线.因此,本文对DES(3DES)的实现采用16级流水方式,对AES则采用并行结构.

DES采用16级流水需要16个S盒,AES加/解密128bits分组时,并行结构也需要16个S盒.因此,可定义RPU阵列为16级结构RPU0~RPUF,每一级包含1个RC-S RPU.连接关系如图3所示.实现DES或3DES算法时,A节点闭合,B节点断开形成线性连接,构成16级流水线结构.实现AES算法时,A节点断开,B节点闭合,各级RPU同时并行工作,彼此之间不存在相关性.

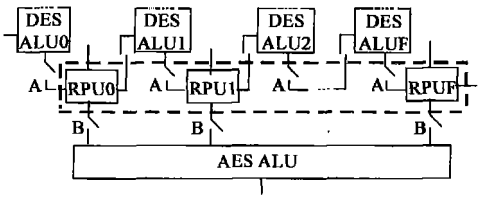

图3 RPU连接关系图

4 算法实现

4.1 DES和3DES的实现

DES和3DES的实现如图4所示,工作在ECB(Electronic Codebook Book)模式.每轮运算内部采用组合逻辑实现,包含扩展置换、异或运算、RC-S查表和P盒置换.实现DES时,每个时钟周期输入一个分组,在第一个时钟周期,第1个分组经过初始置换后存入寄存器REG1中,在下一个时钟周期,REG1的结果经过第一轮处理存入REG2

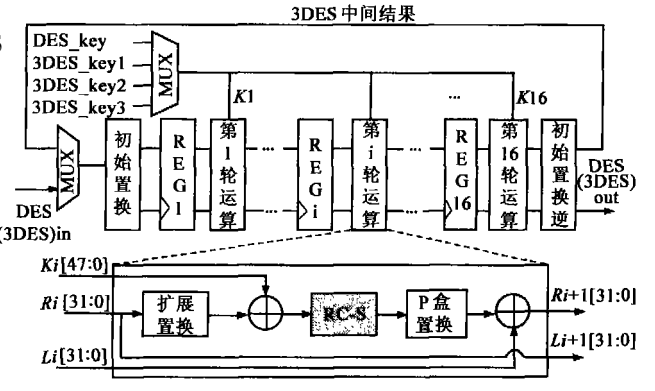

图4 DES和3DES实现图

中, 同时第 2个分组可以经过初始置换存入 REG 1 依此类推, 从第 1个分组进行加 /解密起, 经过 16个时钟周期流水线排空后, 每个时钟周期能完成一个分组的加 /解密.

3DES的实现是 DES模块的三次串行调用, 考虑到规模的约束, 采用重复调用方式, 通过在原有 DES的硬件资源上增加控制节点实现 DES模块的 3次复用. 如图 4所示, 实现 3DES时, 开始每个时钟输入一个分组, 到第 17个时钟时, 不再输入新的分组, 而是将前面处理的结果输入, 即进行第 2次 DES模块运算. 经过 16个时钟后, 将第 2次 DES运算的结果输入, 进行第 3次 DES运算, 再经过 16个时钟后第一个分组的运算结果输出, 同时输入新的分组, 因此 3DES连续处理 16个分组共需 48个时钟周期, 平均 3个时钟周期处理一个分组, 吞吐率是 DES的 1/3.

DES、3DES算法的每一轮迭代都需要一个子密钥, 采用流水线结构实现 DES或 3DES时, 需要提前生成子密钥, 随流水进程发送给各级流水. 本文在子密钥生成设计时, 参考了文献[5]的高速密钥生成方法如下: DES算法的每一轮子密钥皆通过对初始密钥的置换和移位实现, 而且置换和移位位数是固定的, 可以通过完整的分析推导出每个子密钥对应于初始密钥的数值. 所以, 硬件实现时, 可仅通过硬件布线来实现, 这样一旦得到密钥即可生成 16个子密钥.

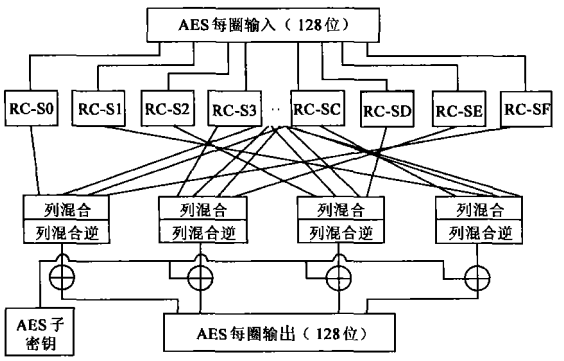

图 5　AES圈变换实现图

4.2　AES的实现

本文对 AES的实现是基于密钥为 128bites的实现. AES分组首先进行初始密钥加运算, 采用 4个异或单元实现; 然后进行 10次圈变换, 最后一次圈变换没有列混合运算. AES的每圈变换如图 5所示, 由 16个 RC-S、4个列混合模块、4个列混合逆运算模块、4个异或单元. 其中, 行移位不用循环移位寄存器实现, 而是直接采用硬件布线方式, 这也是提高处理速度的有效方法. AES实现时, 一个时钟周期完成一圈变换, 因此处理一个分组需要 10个时钟周期.

AES的解密和加密运算过程相同, 只是解密时需要对 RC-S重新配置实现解密 S盒, 且采用列混合逆运算代替列混合运算.

4.3　实现结果

本文用 Verilog HDL硬件描述语言建立了仿真模型, 编写测试激励进行行为级仿真验证. 仿真工具为 Cadence的 Verilog-XL™ 仿真器, 待仿真正确后, 基于 TSMC 0.25标准单元库用 Cadence的 Ambit™ 进行了综合优化, 结果和性能参数如表 2所示. 与单一算法芯片及其他可重构密码算法设计比较如表 3所示.

表 2　实现结果表

算法	功能	密钥扩展	流水线设计	最差路径时延 (ns)	系统时钟(MHz)	吞吐率 (Gbps)	规模 (门数)
DES	加 /解密	片内	16	7.85	110	7	19万
3DES	加 /解密	片内	16			2.3	
AES	加 /解密	片内	无			1.4	

表 3　与其他实现比较表

	出处	设计	流水线设计	吞吐率 (Gbps)		
				DES	3DES	AES
单一算法芯片	SNL[4]	ASIC (0.18)	16	9.28	–	–
	Schaffer [11]	FPGA	48	–	7	–
	Henry Kuo [5]	ASIC (0.18)	无	–	–	1.6
可重构设计	Cryptonite[2]	–	–	0.73	0.24	0.73
	Otello[3]	–	–	1.6	0.53	1.48
	本文	ASIC (0.25)	DES、3DES(16) AES(无)	7	2.3	1.4

由表 2和表 3可知, 处理速度上, 本文的实现接近单一算法密码芯片, 比其他可重构的设计有较大优势; 规模上, 文献[5]仅实现了 AES算法, 规模为 17.3万门, 而本文可重构实现了三种算法, 规模为 19万门, 比文献[5]仅增加了 2万门.

5　结论

针对目前可重构密码芯片处理速度偏低的问题, 本文将流水线、并行处理和可重构技术有效地结合起来, 提出了一种可重构体系结构, 高速实现了 DES、3DES和 AES.

从仿真结果可以看到, 该实现的处理速度明显快于报道的其他同类设计, 接近单一算法专用密码芯片, 能够满足高速加 /解密的需求. 并且, 由于该体系结构具有一定的"柔性", 能适合不同密码用户多层次需求, 增强了密码芯片的灵活性和安全性, 尤其是 RC-S的设计方便了 S盒的更新换代, 增强了 S盒的安全性, 从而进一步增强了密码算法的安全性.

由于密码技术的特殊性, 密码产品, 特别是硬件产品是进出口限制产品, 本文研究的高速可重构体系结构, 对生产具有自主知识产权的高速可重构密码芯片具有重要意义, 在国内信息安全领域可以得到广泛应用.

参考文献:

[1] R Reed Taylor. A high-performance flexible architecture for cryptography[A]. Seth Copen Goldstein. Proceeding of the

Workshop on Cryptographic Hardware and Embedded Systems[C]. London: Springer-Verlag Press, 1999. 231-245.

[2] Rainer Beuchy. A programmable crypto processor architecture for high-bandwidth applications[D]. Germany: Technische Universität München, 2002.

[3] T W Arnold, L P Van Doorn. The IBM PCIXCC: A new cryptographic coprocessor for the IBM eServer[J]. IBM Journal of Research and Development, 2004, 48(3): 475-487.

[4] D C Wilcox. A DES ASIC suitable for network encryption at 10Gbps and beyond[A]. L G Pierson, P J Robertson. Proceeding of the Workshop on Cryptographic Hardware and Embedded Systems[C]. London: Springer-Verlag Press, 1999. 37-48.

[5] Henry Kuo. A 2.29Gbits/sec, 56mW non-pipelined Rijndael AES encryption IC in 1.8V, 0.18um CMOS technology [A]. Ingrid Verbauwhede, Patrick Schaumont. IEEE Custom Integrated Circuits Conference[C]. Piscataway: IEEE Press, 2002. 147-150.

[6] FIPS PUB 46-3, Data Encryption Standard (DES)[S].

[7] FIPS PUB 197, Advanced Encryption Standard (AES)[S].

[8] Artisan Components. TSMC 0.25μm Process 2.5-Volt SAGE™ Standard Cell Library Data book[Z]. Sunnyvale: Artisan Components, Inc, 1999.

[9] 张焕国,冯秀涛,覃中平,等. 演化密码与DES的演化研究[J]. 计算机学报, 2003, 26(12): 1678-1684.
ZHANG Huan-Guo, FENG Xiu-Tao, QIN Zhong-Ping etc. Research on evolutionary cryptosystems and evolutionary DES[J]. Chinese Journal of Computers, 2003, 26(12): 1678-1684. (in Chinese)

[10] Maire McLoone. A high performance FPGA implementation of DES[A]. John V McCanny. IEEE Conference on Signal Processing Systems[C]. Washington: IEEE Computer Society Press, 2000. 374-383.

[11] Toby Schaffer, Alan Glaser, Paul D Franzon. Chip-package Co-implementation of a triple DES Processor[J]. IEEE Transactions on Advanced Packaging, 2004, 27(1): 194-202.

作者简介:

高娜娜 女, 1975年生, 北京科技大学信息学院博士研究生, 主要研究方向: 密码算法、集成电路设计. E-mail: nana_gao@163.com

李占才 男, 1962年生, 副教授, 硕士生导师, 主要研究方向: 信息安全、集成电路设计