一种基于Hierarchy LUT的可重构S-box实现方法

方　震，赵　伟，刘　勇
（中国电子科技集团公司第五十八研究所，江苏 无锡 214035）

摘　要： 基于查找表方法构建的Substitution box（S-box）在可重构分组密码实现中广泛使用，然而因消耗的资源过大，其面积利用效率低。为提高可重构S-box面积利用效率，提出一种基于4R/1W存储结构的分层查找表（Hierarchy LUT），构建可重构S-box。所提出的4R/1W存储结构能减少存储单元的例化数量，提高存储密度。在40nm CMOS工艺下，实现基于Hierarchy LUT的可重构S-box，其面积利用效率得到改善，对比Table Lookup Unit（TLU）和Memory Sharing的可重构S-box方案，效率分别提高了51.76%和6.88%。

关键词： 可重构；S-box；4R/1W；Hierarchy LUT
中图分类号： TN46　　**文献标志码：** A　　DOI:10.16157/j.issn.0258-7998.222891

中文引用格式： 方震，赵伟，刘勇. 一种基于Hierarchy LUT的可重构S-box实现方法[J]. 电子技术应用，2023，49(1)：41-44.
英文引用格式： Fang Zhen，Zhao Wei，Liu Yong. A scheme of the reconfigurable S-box based on Hierarchy LUT[J]. Application of Electronic Technique，2023，49(1)：41-44.

A scheme of the reconfigurable S-box based on Hierarchy LUT

Fang Zhen，Zhao Wei，Liu Yong
(No.58 Research Institute of China Electronics Technology Gruop Corporation，Wuxi 214035，China)

Abstract： The S-box based on LUT is widely used in the reconfigurable block cipher. It is not efficient in area for the expended resources. In this paper, the Hierarchy LUT architecture based on 4R/1W memory unit is proposed to compose the reconfigurable S-box. The 4R/1W can reduce the numbers of the storage unit in the reconfigurable S-box. The proposed Hierarchy LUT is applicable for different sets of ciphers and it is implemented under 40 nm CMOS technology to compare with similar work. The comparison result shows that the proposed Hierarchy LUT gains 6.88% to 51.76% resource efficiency improvement.

Key words： reconfigure；S-box；4R/1W；Hierarchy LUT

0 引言

通信领域中，高吞吐量的加密和解密技术一直是研究的重点。分组密码算法在高速、海量数据加密解密应用中广泛使用。为使分组密码达到高的性能，通常采用硬件加速。专用集成电路（ASIC）虽然性能高，但是在算法切换、参数可变的应用中缺乏灵活性。可重构架构技术则可在一定程度上弥补短板，平衡高性能和灵活性，有利于分组密码算法硬件加速应用，进而通过优化分组密码算法实现。分组密码算法主要包括逻辑运算、算数运算[1]、置换处理[2]、字节替换（S-box）[2-3]。S-box作为分组密码算法的非线性处理单元，在分组密码算法中发挥着重要的作用。一般而言，不同的分组密码算法，S-box的结构都有所不同，这也是分组密码算法的瓶颈所在。因而S-box的性能和面积的优化成为了分组密码算法主要研究目标。

S-box的构建方法通常有两种：一是基于逻辑结构的构建方法，二是基于查找表结构的方法。第一种方法主要基于真值表生成或基于生成规则的逻辑运算。例如Product of Sums(POS)[4]、Positive Polarity Reed-Muller form(PPRM)[5]、Binary Decision Diagram(BDD)[6]采用两级逻辑实现，或者采用GF(2^8)、GF((2^4)^2 [7]或者GF(((2^2)^2)^2)[8]有限域运算逻辑实现。虽然逻辑构建实现占用资源较少，但缺乏灵活性，不能适配不同的S-box结构。此外S-box综合时会产生很大的累积资源占用。第二种方法基于查找表。通常将存储单元用于Look Up Table(LUT)，存储字节替换表。由于存储单元中的字节替换表可以很方便地更新，这种方法被广泛应用于分组密码的可重构实现[2-3,9-10]。相比与基于逻辑的方法，其缺点是需要占用更多的硬件资源，特别是在支持几种不同的S-box操作时[3]。为了减少面积的资源消耗，文献

[2]提出由多个子系统组成存储系统，谋求性能和资源的平衡，实用效果有限。

基于上述问题，本文提出了一种4R/1W存储结构，并基于此存储单元构建分层查找表（Hierarchy LUT），以节省资源消耗，提高面积利用效率。

1 可重构S-box存储单元改进

在基于查找表的实现中，S-box的数据信息存储在一个基本的存储单元中。这些存储单元的数量会随着输入输出位宽、并行端口数量的增加而急剧增大。因此需要分析影响存储单元开销的因素。

例如，一个经典的分组密码算法Advanced Encryption Standard(AES)，每轮需要16个相同的S-box，传统的S-box查找表的实现如图1所示，16个RAM存储块用来存储相同的查找表信息，每个RAM块都有独立的读写端口。因为每个RAM块存储的信息都一样，可以共用输入端口，将其换成图2所示的结构，用触发器来存储查找表信息。这些触发器存储结构共用一个输入端口，而输出端口则通过多路选择器选择输出。

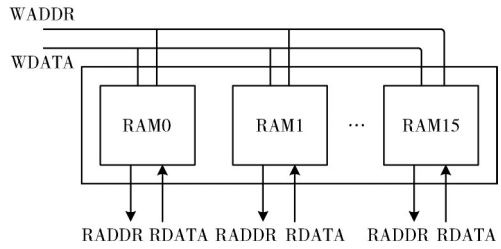

图1 重复RAM块存储查找表

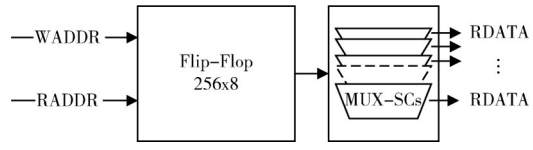

图2 寄存器储存查找表

基于此思路，本文提出一个定制的4R/1W(4个读端口，1个写端口)存储单元，用来减少整体存储的面积开销。如图3所示，该电路基于6管SRAM结构，包括1对写信号线（WBL和WBLB）以及4个单端的读信号线（RBL_1、RBL_2、RBL_3、RBL_4）。每个读信号线都由两个NMOS组成，以M7和M8组成的读端口为例，M7的漏极连接M8的源极，M8的漏极接到读信号端口。其他三个读端口结构相同。这种存储结构可以同时接收4路彼此独立的读信号，获取4个地址的数据，而无需额外例化3个存储单元，因而有很高的存储密度。

用来存储S-box的RAM存储单元所占用的面积占据总面积的相当大的比重。以AES算法为例，尽管IP vendors提供的RAM存储器经过优化，占用很少的资源，但在AES算法中需要16个RAM单元存储S-box，这些累计存储单元

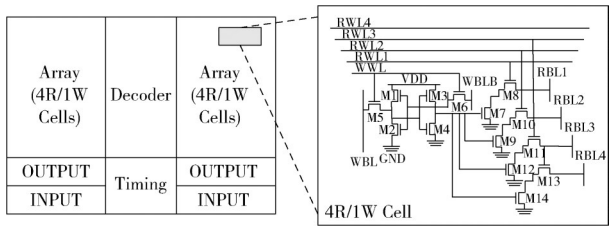

图3 4R/1W存储单元结构

面积开销则不容忽略，如图4所示。通过主从触发器搭建的存储的结构虽然能够减少重复的存储面积的占用，但是其输出端口中的选择器占用的资源却很大。而采用本文提出的4R/1W结构的存储器则占用很小的资源开销。

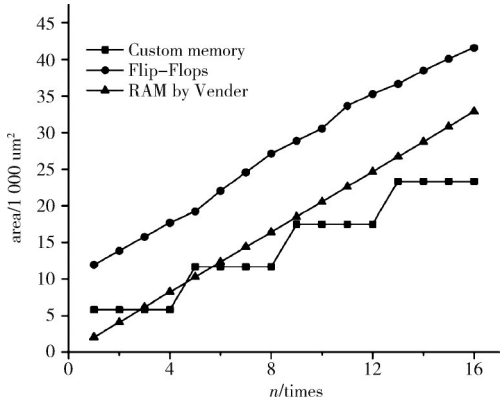

图4 各类存储在电路中面积开销

2 可重构S-box查找表改进

S-box有四个主要的特性，分别为输入位宽、输出位宽、S-box的数量和每轮并行端口数量。不同的S-box结构，四个特性有着较大的差异。为便于表述，在本文中定义了AW、DW、N、m四个参数：AW为地址最大位宽，DW为数据最大位宽，N为最大的S-box数量，m为最大并行端口数量。表1展示了几个常用的分组密码加密算法，其中RU参数表征加解密处理的性能[2]。分组密码算法的S-box结构不一样，其对应的一些参数也各不相同。

当AW、DW、N和m四个参数变化时，分组密码算法的面积开销大有不同。如果只有一个读端口，则会大大

表1 不同算法中S-box性能及特性表

Algorithm	RU	AW/位	DW/位	N/个	m/个
AES	10	8	8	16	1
Blowfish	22	8	32	1	4
Camellia	9	8	8	1	4
CAST128	16	8	32	1	8
DES	11	6	4	1	8
GOST	26	4	4	1	8
KASUMI	2	9	9	1	1
SEED	2	8	8	4	2

增加面积的开销。为尽可能减小面积的开销，适当增大可读的端口数量、AW 和 DW。但要注意，因为读写控制逻辑会占用一定的资源，过多的读写端口同样会引起面积开销增大。

基于上节提出的 4R/1W 存储单元，本节提出一个分层查找表 Hierarchy LUT，如图 5 所示。Hierarchy LUT 包括 4 个 32 端口存储器以及输入输出控制逻辑。其中 32 端口的存储器由 8 个 4R/1W 存储单元组成，它们共用一个写数据线。

Hierarchy LUT 可以根据 S-box 的结构来配置重构输入输出位宽，进而重构电路。根据输入输出的位宽，可以提供 6 种不同的查找表模式，如图 6 所示。

Mode1：工作于 4 个 256×8 的多端口模式。

Mode2：工作于 2 个 256×16 的多端口模式。

Mode3：工作于 1 个 512×16 的多端口模式。

Mode4：工作于 1 个 256×32 的多端口模式。

Mode5：工作于 1 个 1024×8 的多端口模式。

Mode6：工作于 2 个 512×8 的多端口模式。

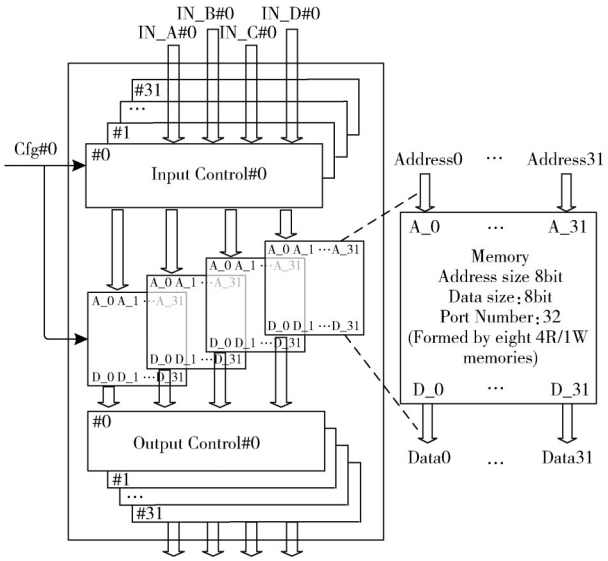

图 5　分层查找表结构

3　对比实现

本文在 40 nm CMOS 工艺下，通过 Synopsys IC compiler 工具进行综合，实现 Hierarchy LUT 构造可重构 S-box，结果如表 2 所示，面积利用率为 1.724。与之对比的是基于 Table Lookup Unit(TLU)[2]和 Memory Sharing[3]的可重构 S-box 结构。

基于 TLU 结构的 S-box 是可重构加解密处理器的一个主要部分。为了提供并行的数据端口，TLU 结构提供比较大的输入输出位宽，存储深度达 1 024，其基本结构是由单端口的存储单元组成的。本文提出的基于 Hierarchy LUT 结构的 S-box，减少了存储器的冗余，具有较高的存储密度，与 TLU 结构相比，面积利用效率从 1.136 提高到 1.724，性能提升 51.76%。

基于 Memory Sharing[3]触发器结构的可重构 S-box，适用于 AES、DES 及 Serpent 的算法。该结构有 16 个端口，其占用的面积很小，但是此结构不够灵活，且并行度不高，最大输入输出位宽为 8 位，而且在数量多的端口情况下，因其端口数据选择器控制占用较多的资源，面

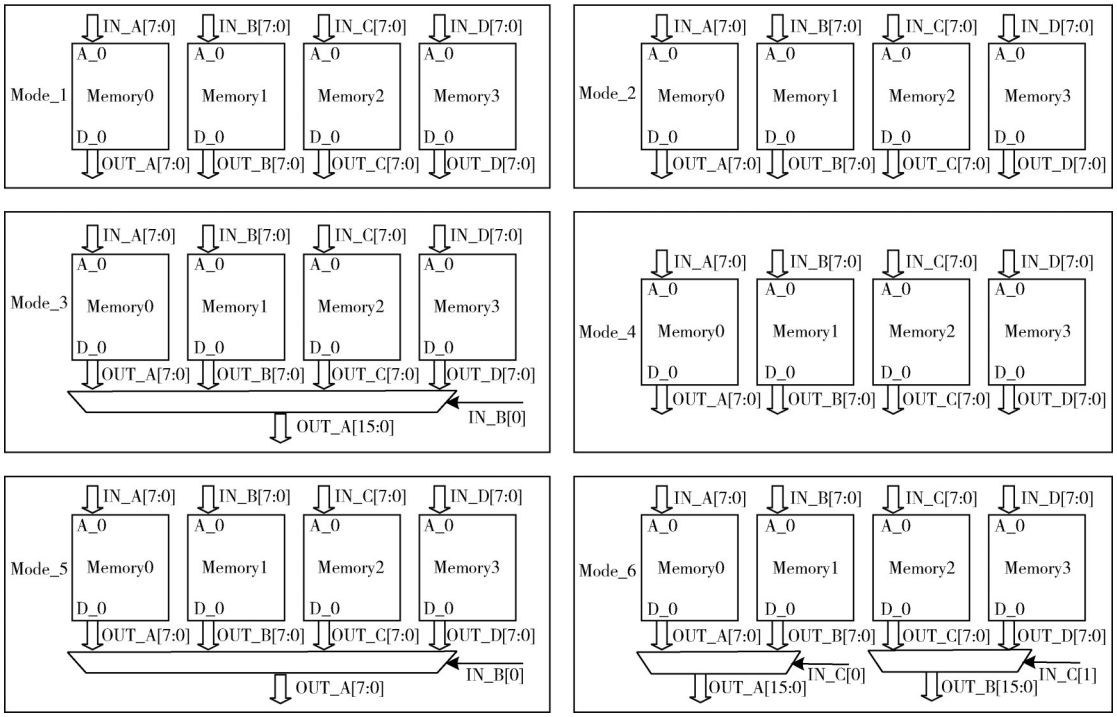

图 6　可重构 S-box 查找表模式

积会迅速增大。与之相比，本文提出的基于Hierarchy LUT结构的S-box，面积利用效率从1.613提高到1.724，性能提升6.88%。

表2　S-box面积利用率对比表

	TLU[2]	Memory Sharing[3]	Hierarchy LUT
存储单元结构	单口RAM	多口触发器	4R/1W
输入位宽	10	8	10
输出位宽	32	8	32
面积/mm^2	0.88	0.062	0.58
运算性能(Block/cycle)	1	0.1	1
面积利用率/((Block/cycle)/mm^2)	1.136	1.613	1.724

4 结论

本文提出了一种4R/1W存储结构，构建一种分层的查找表结构（Hierarch LUT），在40 nm CMOS工艺下，实现了可重构S-box设计。与Table Lookup Unit (TLU)和Memory Sharing触发器的可重构方案提出的结构相比，本文基于Hierarchy LUT结构的可重构S-box面积利用率得到有效改善，利用效率分别提高51.76%和6.88%。

参考文献

[1] DAI Z , WEI L , TAO M , et al. The research and design of parallel instruction targeted at substitution box[C]// 2009 IEEE 8th International Conference on ASIC (ASICON) , 2009:155-158.

[2] SAYILAR G, CHIOU D. Cryptoraptor: high throughput reconfigurable cryptographic processor [C]// 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD),2014:155-161.

[3] 高娜娜，王沁，李占才. 基于AES和DES算法的可重构S盒硬件实现[J]. 小型微型计算机系统，2006(3): 446-449.

[4] MORIOKA S, SATOH A. An optimized S-Box circuit architecture for low power AES design[C]// Proc. CHES, 2002: 172.

[5] SATOH A . A compact rijndael hardware architecture with S-Box optimization[C]// Asiacrypt , 2001.

[6] MORIOKA S, SATOH A. A 10-Gbps full-AES crypto design with a twisted BDD S-Box architecture[J]. IEEE Trans. Very Large Scale Integration (VLSI) Syst. 2004, 12(7): 686-691.

[7] MATHEW S K, SHEIKH F, KOUNAVIS M, et al. 53 Gbps native GF(24)2 composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors[J]. IEEE J Solid-State Circuits, 2011, 46(4): 767-776.

[8] AHMAD N, HASAN R, JUBADI W M. Design of AES S-box using combinational logic optimization[C]// 2010 IEEE Symposium on Industrial Electronics and Applications (ISIEA) ,696 - 699.

[9] WANG Y, HA Y. FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2013, 60(1): 36-40.

[10] ELBIRT A J, PAAR C. An instruction-level distributed processor for symmetric-key cryptography[J]. IEEE Trans. Parallel Distrib. Syst., 2005, 16(5):468-480.

（收稿日期：2022-04-20）

作者简介：

方震（1989-），男，学士，工程师，主要研究方向：通信与数字电路。

赵伟（1983-），男，硕士，工程师，主要研究方向：通信与数字电路。

刘勇（1979-），通信作者，男，博士，工程师，主要研究方向：通信与数字电路，E-mail：wxseugs@163. com。

扫码下载电子文档

版权声明