第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0135—03 文献标识码：A 中图分类号：TP309

多路并行 S 盒替代操作指令研究

戴紫彬，孟 涛，陈 韬，张永福
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：在分析 DES, AES, IDEA 等 41 种分组密码算法结构的基础上，研究了 4×4, 6×4, 8×8, 8×32 4 种常用 S 盒替代的操作特征和 S 盒的实现方式。提出一种可高效、灵活地完成 4 种常用 S 盒替代操作的专用 S 盒运算指令、配置指令模型，给出了专用 S 盒指令的超长指令字(VLIW)扩展指令模型，设计并实现了 S 盒替代的硬件单元，并对专用 S 盒操作指令执行效率进行了分析。
关键词：分组密码；S 盒；查找表；超长指令字

Research of Multiple Parallel Substitution Box Instruction

DAI Zi-bin, MENG Tao, CHEN Tao, ZHANG Yong-fu
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Based on the analysis of 41 popular block ciphers, the paper researches the features of 4 of kinds of popular substitution boxes, which are 4×4, 6×4, 8×8 and 8×32, and analyzes the realization mode of the substitution boxes. It describes special instructions, which can perform 4 kinds of popular substitution boxes quickly and flexibly, extends the usage of special instruction to the VLIW structure instruction, and designs the hardware module of the substitution box. Performance of special instructions are analyzed by comparing it with other instructions.
【Key words】 block ciphers; substitution box; look up table; VLIW

S盒(substitution box)是许多分组密码算法中唯一的非线性部件[1-2]，它的密码强度决定了整个密码算法的安全强度，其工作速度决定了整个算法的制乱速度。专用密码处理器作为一个高速、灵活的实现方式已被广泛认可，它的指令集包含较多的运算指令，这些运算指令的灵活性与执行效率，在一定程度上决定了系统处理数据的灵活性与速度。对于分组密码专用处理器，S盒操作指令的使用频率非常高，所以，S盒操作指令的设计是指令集设计的关键之一。

1 分组密码算法中的 S 盒

1.1 分组密码算法中 S 盒的结构与特征

通过对DES、AES、IDEA等 41 种分组密码算法[3]分析可知，有 30 种算法使用了S盒替代操作，分别是 8×8, 8×32, 4×4, 6×4, 13×8, 13×8, 12×8, 10×8, 3×64, 6×2 共计 10 种不同类型的S盒，10 种S盒中为 2 种以上不同算法所使用的仅有 4×4, 6×4, 8×8, 8×32 型 4 种S盒，其他 6 种不同类型的S盒查表操作可以采用以上 4 种S盒查表操作或逻辑运算实现。

执行 4×4, 6×4, 8×8, 8×32 S 盒替代操作时，无论查找表的输入有多少位，其输出位宽都是 4 bit 的整数倍，同时，分组密码处理的每个支路往往将多个 S 替代操作并置，将支路输入分为多个操作字，分别进行查表操作，查表操作的输入小于 64 bit，输出都为 32 bit。例如，DES 算法将输入的 48 bit 数据分为 8 个 6 bit，分别进行 6×4 查表操作，输出 32 bit；AES 加密算法将 128 bit 数据分为 4 个支路，每个支路的 4 B 分别进行 8×8 查找表操作，每个支路输出为 32 bit。

根据加解密处理所使用的 S 盒是否相同，分组密码使用的 S 盒可分为 2 种：(1)加解密处理使用的 S 盒相同，如 DES 算法；(2)加解密处理使用的 S 盒不同，如 AES 算法。

根据每一轮操作使用的 S 盒是否相同，分组密码使用的 S 盒的可分为 2 种：(1)每轮操作使用相同的 S 盒，如 DES、AES、SAFER＋；(2)每轮操作使用不同的 S 盒，如 Serpent，该算法第 1 轮～第 8 轮使用不同的 S 盒。

根据并行输入数据各个子分组所使用的 S 盒是否相同，分组密码使用的 S 盒可分为 2 种：(1)并行输入数据每一子分组使用的 S 盒都相同，如 AES；(2)并行输入数据各子分组使用不同的 S 盒，如 DES 算法。

1.2 S 盒实现方式分析

从硬件实现角度划分，S 盒的实现方式主要有 2 种：(1)基于逻辑电路的实现方式，即用逻辑硬件的布线来完成布尔函数所描述 S 盒操作，对于固定函数来说，其占用资源较少，但运算速度较慢，而对于多类型的 S 盒操作来说，不具可配置性；(2)基于查找表(Look Up Table, LUT)的实现方式，将 S 盒替代表存储在 RAM 或 ROM 中，操作数作为读地址，这种方法占用较多存储单元，但运算速度快，最主要的是它具有可配置性，能满足当前多种密码运算的需要，并且当芯片不进行配置时它本身不带有任何算法信息，使得芯片本身具有更好的安全性。

从指令级实现角度划分，可分为基本指令实现与专用指令实现。通用处理器基本指令的组合能够完成 S 盒替代操作，例如：4 条 32 bit 数据路径上的 MIPS 指令 Shr、And、Shr 和 Load 的顺序执行，就可以完成一个 8×8 的 S 盒操作，这种方法浪费了大量指令周期，从而降低了密码算法的处理速度；采用专用指令可以节省指令周期，有效提高数据处理速度，但它需要有相关硬件的支持，当 n 和 m 较大时，会占用一定量的面积。

作者简介：戴紫彬(1966－)，男，教授、博士，主研方向：信息安全；孟 涛，硕士研究生；陈 韬，讲师；张永福，博士生导师
收稿日期：2007-04-25 **E-mail：**daizb2004@126.com

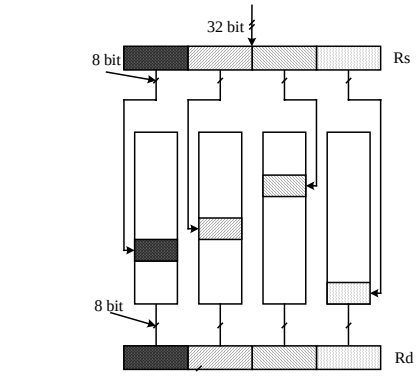
2　专用 S 盒操作指令及硬件单元设计

2.1　S 盒运算指令的设计

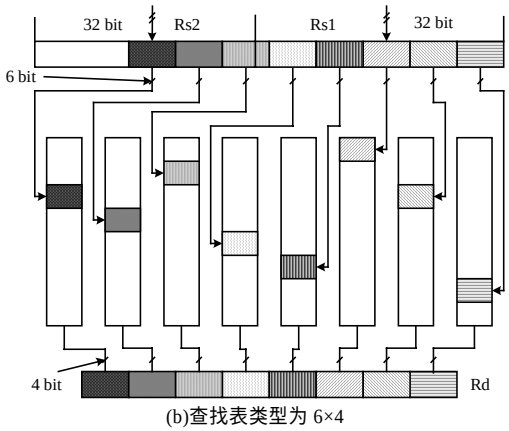
通过对 S 盒替代操作特征的研究可知，完成特定的 S 盒替代操作，执行过程中要有指定操作类型、操作页面的控制信息，即要求在指令模型中，要有标识操作类型、操作页面的参数，以及两个源操作数、一个目的操作数，由此可得 S 盒替代指令基本模型为

SBOX.TYPE.PAGE Rd, Rs1 , Rs2

其中，功能字段 TYPE 指示 S 盒替代表类型，可选择的值为 8×8, 8×32, 6×4, 4×4。图 1 以 8 ×8、6×4 为例，给出了 S 盒查表操作指令功能示意图。当查找表类型为 8×8 时，该指令将输入的 32 bit 源操作数分为 4 B，每个字节独立进行 8×8 的 S 盒查表，4 次查表动作一次完成，输出的 32 bit 数据送入目的寄存器；当查找表类型为 6×4 时，该指令将输入的第 2 个源操作数的低 16 bit 与第 1 个 32 bit 源操作数拼装成为一个 48 bit 数据，分为 8 个 6 bit 数据，并行执行 6×4 的 S 盒查表，输出的 32 bit 数据送入目的寄存器。功能字段 PAGE 指示 S 盒查表的页面号，通过赋不同的值，实现分页查表。设计实现 8×8 S 盒查表指令支持 2 页、8×32 S 盒查表指令支持 2 页、6×4 S 盒查表指令支持 4 页、4×4 S 盒查表指令支持 16 页。



(a)查找表类型为 8×8



(b)查找表类型为 6×4

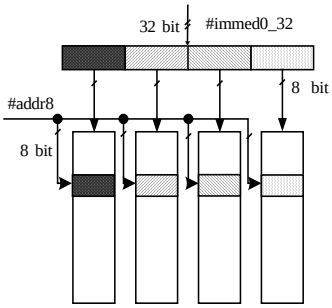
图 1　S 盒查表操作指令功能示意图

2.2　S 盒配置指令的设计

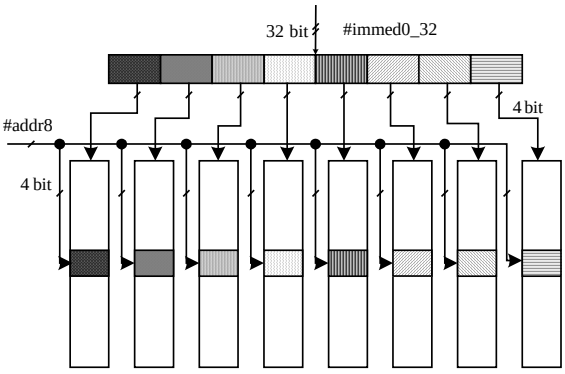
S 盒查表操作指令使用前需先配置 S 盒替代表，本文设计了专用的配置指令，其基本模型为

CFG _ SBOX.TYPE.PAGE　#addr8, #immed0_32

其中，TYPE、PAGE 的意义同上；#addr8 为存储空间的地址；#immed0_32 为 32bit 的配置数据。图 2 以 8×8, 4×4 为例，给出了配置 S 盒查表指令的功能示意图，当配置 8×8 查找表时，32 bit 的立即数分为 4 B，以#addr8 为写地址，每个字节写入相应的存储单元中；当配置 4×4 查找表时，32 bit 的立即数分为 8.5 B 数据，以#addr8 中有效的 4 bit 数据为写地址，将每个半字节写入相应的存储单元中。



(a)配置 8×8 查找表



(b)配置 4×4 查找表

图 2　S 盒配置指令功能示意图

2.3　专用 S 盒指令的 VLIW 扩展

当前常用分组密码算法的分组宽度已达 128 bit，算法中的大部分操作可并行执行，例如：AES 算法的 S 盒的查找表为 8×8，每个查找表的内容都相同，则当以 32 bit 为处理位宽时，是可以多路并行执行的，其操作如图 3 所示，其中 T 代表 8×8 的查找表。

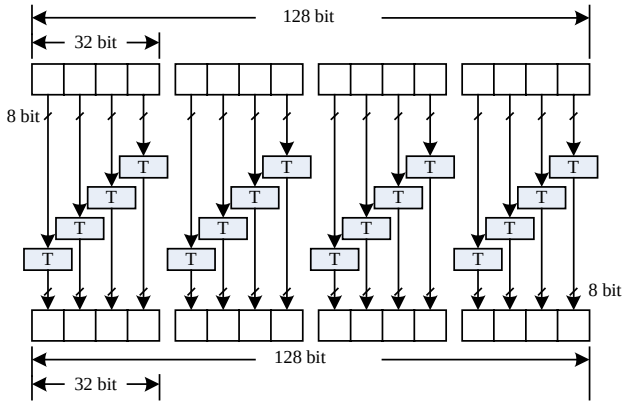


图 3　AES 中多路并行执行的 S 盒操作

因此，为了支持多路并行的 S 盒操作，可将 S 盒操作指令扩展为 VLIW 结构的指令，其指令槽个数为 4，格式如图 4 所示，在 VLIW 结构硬件支持下，则可以高效地处理常用的分组密码算法中的可并行 S 盒操作。

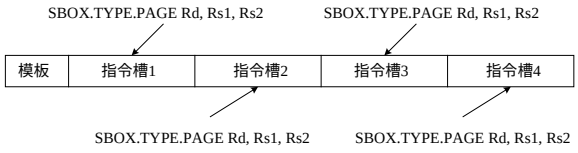


图 4　专用 S 盒指令的 VLIW 扩展指令格式

2.4 S 盒硬件单元设计

为支持专用 S 盒操作指令的执行，本文设计了 S 盒运算单元。由专用 S 盒操作指令所要完成的功能可得，S 盒运算单元的结构应当满足：

Address_Width=max{8,8,4,8}=8

Data_Width=Gcd(8,32,4,4)=4

其中，Address_Width 为地址线宽度；Data_Width 为数据线宽度。可见，S 盒硬件单元内部基本的 LUT 结构应是 8×4 结构；分组密码处理中往往将分块数据同时送入多个 S 盒进行查表操作，多个 S 盒查表输出为 32 bit 的整数倍，因此 S 盒单元内部 8×4LUT 的数目应当是 8 的整数倍；考虑到在分组密码算法中经常会有多个不同的 S 盒查找表，部分密码算法加解密结构 S 盒替代表不同。因此，S 盒的内部 8×4LUT 的数目最终确定为 16，图 5 给出了 2 个 LUT 组合的电路示意图。对于 4×4 查找表模式和 6×4 查找表模式，其读写地址小于 8 bit，因此其高位需要页面号来填补构成 8 bit 的读写地址，当应用于 4×4 查找表模式时，页面选择(Page)为 4 bit，当应用于 6×4 查找表模式时，页面选择(Page)为 2 bit。对于 8×8 模式而言，输出为一个 S 盒替代表查表结果，对于 4×4、6×4 两种模式，输出为两个 S 盒替代表查表输出，而在 8×32 模式下，输出仅为 S 盒替代表输出 32 bit 的一个字节。

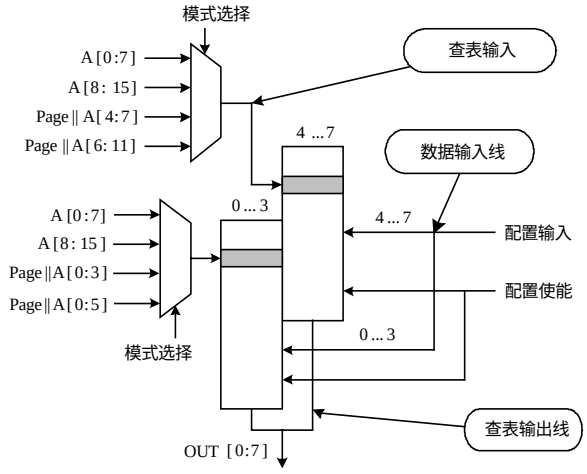


图 5　2 个最小 LUT 的组合电路

笔者采用 Verilog 语言实现了 S 盒运算单元，用 NC_Verilog 对本设计进行了功能仿真。由仿真结果分析可知 S 盒运算单元的功能无误，能有效地支持专用 S 盒指令的执行。

3　专用 S 盒操作指令执行效率分析

本文主要在 RISC 结构和 VLIW 结构下，对 S 盒操作指令的执行效率进行了分析。

RISC 结构下，采用 32 位 MIPS 指令集为基本指令集(BIS)；文献[4-5]提出了并行 S 盒查表指令 Ptlu，将加入 Ptlu 指令的基本指令集称为 Ptlu 扩展指令集(PIS)；将加入本文所提出的专用 S 盒运算指令的基本指令集，称为专用 S 盒扩展指令集(SIS)。假设寄存器有两读一写的 32 bit 端口，BIS、PIS、SIS 三者执行 DES、AES、MARS、Serpent 算法一轮中 S 盒操作所用指令条数的比较，如表 1 所示。

表 1　RISC 结构下的执行效率比较

密码算法	查找表类型	输入/bit	输出/bit	BIS 所需指令/条	SIS 所需指令/条	PIS 所需指令/条
DES	6×4	48	32	36	1	24
AES	8×8	128	128	84	4	4
MARS	8×32	32	128	12	4	4
Serpent	4×4	128	128	140	4	96

由表 1 可知，在 32 bit 数据路径上，与通用指令相比，专用 S 盒运算指令执行 4 种类型的查找操作的效率都较高；与 Ptlu 相比，执行 8×8、8×32 查表操作的效率相同，但执行 6×4、4×4 查找表操作时，专用 S 盒运算指令有较大的优势。

在 VLIW 结构下，数据路径为 128bit，VLIW 的指令槽为 4，寄存器有 8 读 4 写的 32 bit 端口，将扩展的专用 S 盒运算指令(ES)与扩展的 Ptlu(EP)进行比较，完成 S 盒操作所用时钟周期的比较如表 2 所示。

表 2　VLIW 结构下的执行效率比较

密码算法	查找表类型	输入/bit	输出/bit	ES 所需时钟	EP 所需时钟
DES	6×4	48	32	1	8
AES	8×8	128	128	1	1
MARS	8×32	32	128	1	1
Serpent	4×4	128	128	1	24

由表 2 可知，在多路并行的情况下，执行 8×8、8×32 查表操作时，扩展的专用 S 盒运算指令与扩展的 Ptlu 指令效率相同，但在执行 6×4、4×4 查找表操作时，扩展的专用 S 盒运算指令仍有较大的优势。

4　结束语

本文提出了一种适用于 4×4, 6×4, 8×8, 8×32 4 种查找表的专用 S 盒操作指令模型，并将其扩展为 4 指令槽的 VLIW 指令，设计并实现了支持专用 S 盒指令的 S 盒运算单元。经分析仿真结果知，此单元能够支持专用 S 盒高效、灵活地完成 4 种常用类型的 S 盒操作，当执行 4×4 模式的操作时，可配置 16 页查找表；执行 6×4 模式的操作时，可配置 4 页查找表；执行 8×8 模式的操作时，可配置 2 页查找表；执行 8×32 模式的操作时，可配置 2 页查找表。通过与通用指令、Ptlu 指令的比较可知，在 32 bit 的 RISC 结构中以及在 128 bit 的 VLIW 结构中，都能较大程度地提高处理 S 盒操作的速度。

参考文献

[1] 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, 27(3): 446-449.

[2] 李声涛. 分组密码中 S 盒的设计与分析[D]. 长沙, 湖南: 国防科技大学, 2004.

[3] Elbirt A J. Reconfigurable Computing for Symmetric-key Algorithms[D]. Massachusetts, USA: Electrical and Computer Engineering Department, University of Massachusetts Lowell, 2002.

[4] Fiskiran A M, Lee R B. Fast Parallel Table Lookups to Accelerate Symmetric-key Cryptography[C]//Proceedings of the International Conference on Information Technology Coding and Computing, Embedded Cryptographic Systems Track. Las Vegas, Nevada, USA: [s. n.], 2005.

[5] Fiskiran A M, Lee R B. On-chip Lookup Tables for Fast Symmetric-Key Encryption[C]//Proceedings of IEEE 16th Int'l Conf. on Application-specific Systems, Architectures, and Processors. Piscataway, NJ, USA: [s. n.], 2005.