

超立方体法在 SM4 算法 S 盒中的应用

王 悦, 李树国

(清华大学 微电子技术研究所, 北京 100084)

摘 要: S 盒是商用密码算法 SM4 中最耗时的一部分, 因此构造高性能的 S 盒具有重要意义. 为了显著减少 SM4 算法进行加解密运算的延时, 我们引入了 N 维超立方体法构造 S 盒, 在硬件电路的实现上, 相比于传统 S 盒的查表法延时缩短 6%, 面积减少 17%. 此方法同时适用于其它对称加密算法中的 S 盒变换, 具有可借鉴性.

关键词: SM4; S 盒; 查表法; N 维超立方体法

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)07-0010-04

The Application of Hypercube Method in S Box of SM4

WANG Yue, LI Shu-guo

(Microelectronics Technology Institute, Tsinghua University, Beijing 100084, China)

Abstract: SBOX is the most time consuming part in block cipher SM4 algorithm, so it's of great importance to construct a S box of high performance. In order to reduce latency of encryption algorithms in SM4, We introduce the N-dimensional hypercube method to construct SBOX, the delay reduced six percent and the area reduced seventeen percent Compared with the traditional S box using look-up table method. what's more, this method is portable that it can apply to SBOX transformations of other algorithms.

Key words: SM4; SBOX; look-up table method; N-dimensional hypercube method

1 引言

SM4 算法是一种商用无线局域网分组密码算法^[1], SM4 与 DES^[2]、AES 算法一样, 核心都是 SBOX 的分组对称密码算法^[3]. S 盒是 SM4 算法中唯一的非线性运算, 它作用于每一轮的加解密运算和密钥扩展, 直接决定了密码算法的性能. S 盒相当于一个八比特输入, 八比特输出的布尔函数, 布尔函数目前多采用代数化简法和卡诺图化简法^[3], 当输入变量多达八比特时, 这两种化简方法变得极其复杂, 为此国内外很多人都致力于布尔函数化简方面的研究. 本文采用 N 维超立方体法化简布尔函数. 传统的立方体法以迭代形式在计算机上实现^[4], 即从最小项(0-立方体)形成布尔函数开始, 迭代形成(1-立方体)、(2-立方体)等等, 直至不可能再化简

为止. 此算法运算速度很慢, 且需要大量的存储单元^[5], 显然不适于硬件实现. 目前有人采用将立方体展开成平面图的方式对逻辑变量观察^[6], 然而当输入变量个数达到八位后, 图形同样也会变得非常复杂, 不易得出最简输出结果. 当引入 N 维超立方体的简化模型后, 通过对 N 维超立方体简化模型的分析, 即可清晰的看出逻辑变量之间的关系, 将相邻、相对的点化成线、面、体的形式, 从而减少输入逻辑变量的个数, 得到输出结果. 由此我们把对 S 盒的研究转化为 N 维超立方体布尔函数化简的研究.

2 SM4 的加解密算法

说明文输入为 $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$, 密文输出为 $(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$, 轮密钥为 rk_i . 则本算法的加密变换为^[1]

收稿日期: 2013-09-21; 修回日期: 2013-11-01

基金项目: 国家“八六三”计划项目(2012AA012402); 国家自然科学基金项目(61073173); 清华大学自主研发计划(2011Z05116)

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), i = 0, \dots, 31.$$

定义反序变换 R 为 $R(A_0, A_1, A_2, A_3) = (A_3, A_2, A_1, A_0)$,

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}).$$

其中轮函数 F 为

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk).$$

其中 T 是一个可逆变换,由非线性变换 τ 和线性变换 L 复合而成,即 $T(\cdot) = L(\tau(\cdot))$.

τ 由 4 个并行的 S 盒构成.

本算法的解密变换与加密变换结构相同,不同的仅是轮密钥 rk_i 的使用顺序.

加密时轮密钥的使用顺序为 $(rk_0, rk_1, \dots, rk_{31})$.

解密时轮密钥的使用顺序为 $(rk_{31}, rk_{30}, \dots, rk_0)$.

3 N 维超立方体法构造 S 盒

3.1 立方体法简介

3.1.1 传统立方体法

每一个最小项自身就是一个 0-立方体,两个相邻最小项组成的子集称为 1-立方体,类似的,如果任意两个 $(N-1)$ 立方体彼此相邻,那么这两个 $(N-1)$ 立方体组合成一个 N 立方体, $N \geq 1$. 对于任意集合 $M(f)$,如果 $M(f)$ 包含 $N-1$ 立方体的一些子集,并且这些子集不被其它 $N+1$ 集包含,那么这个 $N-1$ 立方体就称为基本 $N-1$ 立方体.

我们可以根据上述定义,由最小项 0-立方体,迭代生成 $N-1$ 立方体,由此得出布尔函数化简后的输出项.此方法适用于软件实现,然而在硬件电路中,由于迭代次数多,因此延时长、面积大,不适于硬件实现.

因此,我们根据 SM4 算法硬件电路的需要,采用观察法对 N 维超立方体进行研究,来化简布尔函数.

3.1.2 采用观察法对三变量布尔函数化简

首先将布尔逻辑函数表示为“与-或”表达式,每一个与项(乘积项)可用一个立方体与之对应,许多个与项的集合可用复合立方体与之对应, N 个变量与 N 维超立方体相对应^[3].

某个函数的变量个数为 $N = 3$,变量分别为 A_1, A_2, A_3 .立方体结构示于图 1.

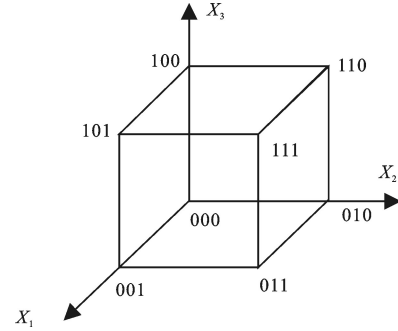


图 1 三变量布尔立方体

输入变量有 $2^3 = 8$ 种组合,对应于图一立方体的八个顶点.

依据立方体的特点有:

相邻的两个点可以合并为棱,相邻且平行的两个棱可以合并为面,相对的两个面可以简化为体^[3].

例如相邻的两个点 000 和 001,分别对应输入变量 $\tilde{A}_1 \tilde{A}_2 \tilde{A}_3$ 和 $\tilde{A}_1 \tilde{A}_2 A_3$,相邻的两个点可以合并为一条棱 $00x(\tilde{A}_1 \tilde{A}_2)$,即 $\tilde{A}_1 \tilde{A}_2$; x_1 坐标轴方向的棱 $00x(\tilde{A}_1 \tilde{A}_2)$ 和 $01x(\tilde{A}_1 A_2)$ 可以合并为一个面,即两条棱对应四个点 000($\tilde{A}_1 \tilde{A}_2 \tilde{A}_3$),001($\tilde{A}_1 \tilde{A}_2 A_3$),010($\tilde{A}_1 A_2 \tilde{A}_3$),011($\tilde{A}_1 A_2 A_3$),合并成面 $0xx(\tilde{A}_1)$,对应变量 $\tilde{A}_1$;相对的两个面可以合并成一个体,如图 1,上下平行的两个面分别对应变量 $\tilde{A}_1$ 和 A_1 , $\tilde{A}_1$ 和 A_1 合并后即为图示立方体,为 1.

3.2 N 维超立方体与 S 盒

3.2.1 N 维超立方体的形成

低维空间对应图形的形成:在平面几何中有一点 A ,如果把点 A 沿着水平方向一段距离到点 B ,就形成了 A, B 两点之间的线段,这一直线段就是“一维”空间;如果“一维”线段端点 A, B 沿着线段垂直方向移动一段相同的距离,形成了一个正方形矩形面,称为“二维”空间;正方形沿着三维方向移动一段相同的距离,构成一个立方体,称为“三维”空间.

高维超立体的形成与低维空间对应图形形成的过程相似.一个立方体沿着垂直方向(第四维方向)移动同样的距离,形成一个“四维超立体”.以此类推.

3.2.2 N 维超立方体的简化模型

含有 N 个变量的输入对应 N 维超立方体.

当超立体大于六维时,随着坐标维数的增大,超立体结构也变得越来越复杂,表示出来也越来越困难,因此需要将抽象的 N 维超立方体空间进行适当

的变换。

要把四维超立体变换成一种“简化的四维超立体”,任选一对相邻平行的两个立方体,将这一对立方体沿着第四维方向背向平行移动,使这两个立方体之间离开一段距离,形成两个独立的立方体,每一个立方体用一个圆环套起来,在两个圆环之间用两条平行的直线连接起来,就是四维超立体变换后的“简化的四维超立体”模型,如图2所示。这条平行的直线既表示将这两个独立的立方体连接成为一个整体,又代表一束8条直线的棱(两个立方体对应的8个顶点之间的连接线)。

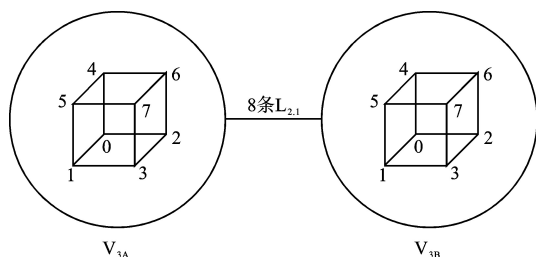


图2 简化的四维超立体

同理,任选一对相邻平行的四维超立体,将这两个四维超立体沿着第五维方向背向离开一段距离,形成两个独立的四维超立体;再按上述办法将两个四维超立体变换成相等距离的“两个四维超立体”,形成两层空间,第二层空间是一个大矩形面,矩形面上四个顶点,每一个顶点就是一个三维立方体,这就是简化后的“五维超立体”模型。

依此类推,一个 N 维超立方体中的任意一层超立体都是相邻平行的“2个 $(N-1)$ 维超立体”组合成的。

3.2.3 N 维超立方体的化简方法

对超立体模型采用差值法化简。

差值法化简 N 维超立方体模型:函数的 N 维超立方体中某一子形体空间中有 2^q 个相邻最小项,有 q 种“编号差”,即 q 个 R_i ,从 2^q 个最小项中任取一个最小项展成 N 位二进制码,消去 q 个 R_i 所对应位的取值,余下位的取值(“0”或“1”)对应位以“原变量”或“反变量”的乘积就是 2^q 个最小项合并后的结果。

3.2.4 N 维超立方体法对 S 盒的化简

由于 S 盒的输入变量为 8 比特,因此考虑 $N=8$ 对应的 8 维超立体情况。

依据上述对“简化的超立体”模型分析, $N=8$ 对应的超立体模型如图3所示。

对图3的左下角 0_3 图放大如图4所示。

举例如下:

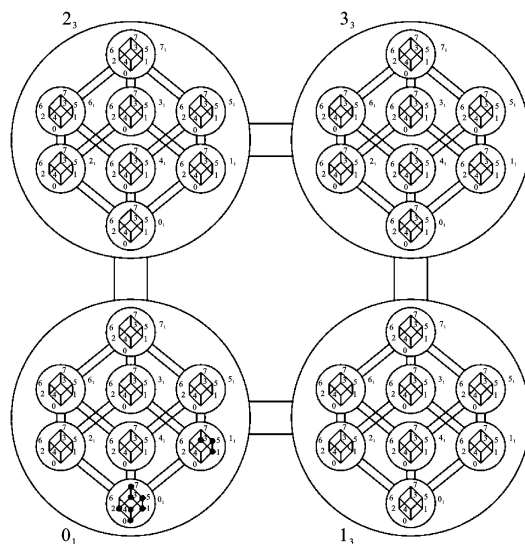


图3 简化的八维超立体

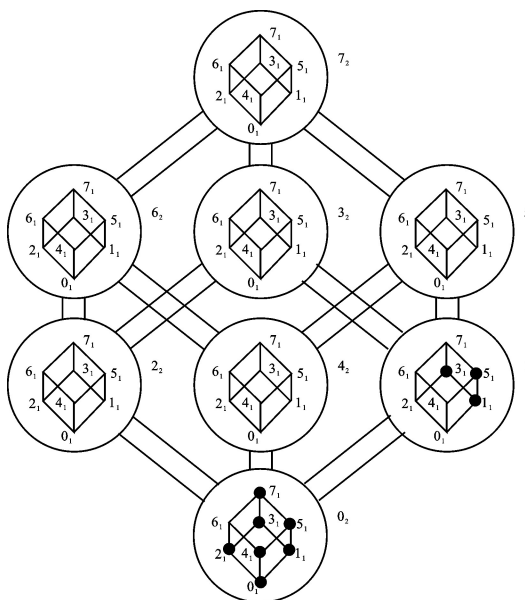


图4 放大图

由 SM4 的 S 盒表格可以看出,当输入为 00 时,输出为 d6。遍历 S 盒,便可确定输出的每一位关于输入的逻辑表达式。

本文仅拿 S 盒的第一行举例。输出最高位 $y[7_1]$ 对应的输入为 {00, 01, 02, 03, 04, 05, 07, 09, 0b, 0d}, 写成表达式的形式为:

$$y[7_1] = \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2 \& \sim X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2 \& \sim X_1 \& X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& X_2 \& \sim X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& X_2 \& X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& \sim X_2 \& \sim X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& X_2 \& \sim X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& X_2 \& X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& X_2 \& X_1 \& X_0$$

$\sim X_5 \& \sim X_4 \& \sim X_3 \& X_2 \& X_1 \& X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& \sim X_2 \& \sim X_1 \& X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& \sim X_2 \& X_1 \& X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& X_3 \& X_2 \& \sim X_1 \& X_0.$

将每一个输入用黑点标记在图三八维超立方体图形上. 为表示方便, 将输入分层表示, X_7, X_6 为最外层的两个元素, X_5, X_4, X_3 为中间层的三个元素, X_2, X_1, X_0 为最底层元素.

$y[7_1] = \{0, 0, 0; 0, 0, 1; 0, 0, 2; 0, 0, 3; 0, 0, 4; 0, 0, 5; 0, 0, 7; 0, 1, 1; 0, 1, 3; 0, 1, 5\}.$

(1) 对 $\{0, 0, 0; 0, 0, 1; 0, 0, 2; 0, 0, 3\}$, 有: $R_{(3,1)} = 0, R_{(3,2)} = 0, R_{(2,1)} = 0, R_{(2,2)} = 0, R_{(2,3)} = 0, R_{(1,1)} = 1, R_{(1,2)} = 2.$

注: $R_{(i,j)}$ 代表第 i 层, j 坐标下相邻两个点之间的差值.

取此类中的一个数: $\{0, 0, 0\}$, 表示成表达式形式 $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2 \& \sim X_1 \& \sim X_0$, 消去最底层分别代表 2, 1 的两个变量, 即 X_1, X_0 , 余下位即为合并后的结果:

$\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2$

(2) 同理对 $\{0, 0, 0; 0, 0, 1; 0, 0, 4; 0, 0, 5\}$, 有 $R_{(3,1)} = 0, R_{(3,2)} = 0, R_{(2,1)} = 0, R_{(2,2)} = 0, R_{(2,3)} = 0, R_{(1,1)} = 1, R_{(1,3)} = 4.$

取此类中的一个数: $\{0, 0, 0\}$, 表示成表达式形式 $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2 \& \sim X_1 \& \sim X_0$, 消去最底层分别代表 4, 1 的两个变量, 即 x_2, x_0 , 余下位即为合并后的结果: $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_1.$

(3) 对 $\{0, 0, 1; 0, 0, 3; 0, 0, 5; 0, 0, 7\}$, 同理有合并后的结果为 $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_0.$

(4) 对 $\{0, 0, 1; 0, 0, 5; 0, 1, 1; 0, 1, 5\}$, 有: $R_{(3,1)} = 0, R_{(3,2)} = 0, R_{(2,1)} = 1, R_{(2,2)} = 0, R_{(2,3)} = 0, R_{(1,1)} = 0, R_{(1,2)} = 0, R_{(1,3)} = 4.$

合并后的结果为: $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_1 \& \sim X_0$

(5) 对 $\{0, 0, 1; 0, 0, 3; 0, 1, 1; 0, 1, 3\}$, 有 $R_{(3,1)} = 0, R_{(3,2)} = 0, R_{(2,1)} = 1, R_{(2,2)} = 0, R_{(2,3)} = 0, R_{(1,2)} = 2$

合并后的结果为 $\sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_2 \& \sim X_0.$

(6) 综合上述化简, 有 $y[7_1] = \sim X_7 \& \sim$

$X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_2 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_1 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_3 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_1 \& \sim X_0 + \sim X_7 \& \sim X_6 \& \sim X_5 \& \sim X_4 \& \sim X_2 \& \sim X_0.$

经过此种方法可以得到化简后的逻辑表达式.

4 实验数据分析

化简后的 S 盒, 在 smic 0.18 μm 工艺库下进行 DC 综合, 相比于传统的查表法, 面积和延时的比较结果如表 1 所示.

表 1 比较结果

S 盒的实现方法	面积	延时
查表法	1 500 门	1.6 ns
立方体法	1 250 门	1.5 ns

由上面比较表可以看出, 用立方体法实现的 SBOX, 面积缩短了 17%, 延时减少了 6%, 显著提高了 S 盒 的性能. 此方法同样适用于 AES 等对称算法的 S 盒中, 具有可借鉴性. SM4 的 S 盒前三行见表 2.

表 2 SM4 的 S 盒前三行

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62

参考文献:

- [1] 国家密码管理局. 无线局域网产品使用的 SMS4 密码算法[S]. 北京, 2006.
- [2] 王建华, 李金. 基于扰乱器对 DES 加密算法安全性提高的论证[J]. 微电子学与计算机, 2012, 29(10): 198-202.
- [3] 张冰. 逻辑函数的另一种化简方法—Q—M 化简法[J]. 新疆教育学院学报, 2003, 19(2): 85-88.
- [4] Fleisher H, Giraldi J, Phoenix R, et al. Minimizability of random boolean fuctions[J]. IEEE Transactions on Computers, 1989, 38(4): 593-595.
- [5] Zhu Youlian, Zhai Lifang. Research on multidimensional—cube simplification algorithm of logical functions[C]// Proceedings of the 4th World Congress on Intelligent Control and Automation, Shanghai, China, 2002.
- [6] 顾宗信. 利用立体展开图简化二值布尔函数[J]. 太原理工学院学报, 1980(3): 16-20.

(下转第 17 页)

- [2] Bei C D, Gray R M. An improvement of the minimum distortion encoding algorithm for vector quantization [J]. IEEE Trans. Communications, 1985, 33(10): 1132-1133.
- [3] Guan L, Kamel M. Equal-average hyperplane partitioning method for vector quantization of image data [J]. Pattern Recognition Letters, 1992, 13(10): 693-699.
- [4] Pan Z, Kotani K, Ohmi T. A unified projection method for fast search of vector quantization [J]. IEEE Signal Processing Letters, 2004, 11(7): 637-640.
- [5] Pan Z, Kotani K, Ohmi T. A generalized multiple projection axes method for fast encoding of vector quantization [J]. Pattern recognition Letters, 2005, 26(9): 1316-1326.
- [6] Pan Z, Kotani K, Ohmi T. Fast encoding method for vector quantization using modified L2-Norm pyramid [J]. IEEE Signal Processing Letters, 2005, 12(9): 609-612.
- [7] Chang C C, Hsieh Y P. A fast VQ codebook search with initialization and search order [J]. Information Sciences, 2012, 183(1): 132-139.
- [8] Lu Z M, Pan J S, Sun S H. Efficient codeword search algorithm based on Hadamard transform [J]. Electronics Letters, 2000, 36(16): 1364-1365.
- [9] Chu S C, Lu Z M, Pan J S. Hadamard transform based fast codeword search algorithm for high-dimensional VQ encoding [J]. Information Sciences, 2007, 177(3): 734-746.
- [10] 崔江涛, 李风华, 马建峰. 基于子空间三角不等式的高维码字搜索算法 [J]. 电子学报, 2011, 39(4): 940-945.
- [11] 乔阳, 潘志斌, 乔瑞萍, 等. 基于 Hadamard 变换和自适应顺序搜索的码字快速搜索算法 [J]. 微电子学与计算机, 2009, 26(1): 118-121.
- [12] 蔡光跃, 董恩清. 一种改进的基于 Hadamard 变换的快速码字搜索算法 [J]. 微电子学与计算机, 2007, 24(2): 154-156.

作者简介:

- 马肖肖 男, (1990-), 硕士研究生. 研究方向为图像编码.
- 潘志斌 男, (1963-), 博士, 教授. 研究方向为图像编码和模式识别.
- 李阳 男, (1987-), 硕士研究生. 研究方向为模式识别.
- 方洁 女, (1989-), 硕士研究生. 研究方向为视频编码.

(上接第 13 页)

作者简介:



王悦 女, (1992-), 硕士. 研究方向为信息安全.



李树国 男, (1963-), 教授、博士生导师. 研究方向为信息安全算法的数字大规模集成电路设计与实现.