一种优化 DES 算法

陈　良
（广东省公安司法管理干部学院技术系，广州 510232）
E-mail：liangchen816@hotmail.com

摘　要　论文简要介绍 DES 算法及其实现上影响速度的原因。对 S-盒代替和 P-盒置换进行了分析和优化，将其合并为 SP-盒。将 S-盒代替表和 P-盒置换表进行了分析和优化，将其合并为 SP-盒变换表。这一优化并未改变 DES 的计算结果，因而并未改变 DES 的安全性。同时，取消了原算法 S-盒代替中对 S-盒输入的与和移位操作；取消了 P-盒置换的与和移位操作。将原来的 S-盒输入，即，SP-盒的输入作为索引，直接从 SP-盒变换表中取得 SP-盒的输出，即，原来的 P-盒置换的输出。因而，节省了 CPU 的计算时间，提高 DES 的实现速度。

关键词　DES 算法　优化　S-盒代替　P-盒置换

文章编号 1002-8331-（2004）06-0074-03　**文献标识码** A　**中图分类号** TP309

An Optimizing DES Algorithm

Chen Liang
（Guangdong Institute of Public Security and Justice，Guangzhou 510232）

Abstract：At first，this paper introduces the algorithm of DES（Data Encryption Standard）and the reason of its low calculating speed.Then it analyzes and optimizes the substitution of S-box and replacement of P-box，then combine both operations to generate SP-box；analyzes and optimizes the table of substitution of S-box and the table of replacement of P-box，and combines both tables to generate the table of SP-box.The optimizing process does not change the calculating result so that the security of DES is not changed.At the same time，cannels the AND and SHIFT opertions in S-box and P-box.According to the index which is the original input of S-box，that is，the input of SP-box，we can directly get the output of SP-box from the table of SP-box，that is，the original output of P-box.So the time of calculating of CPU is saved and the calculating speed of DES is higher than that of its origin.

Keywords：DES algorithm，optimizing，substitution of S-box，replacement of P-box

1　引言

数据加密标准（Data Encryption Standard，DES），作为 ANSI 的数据加密算法（Data Encryption Algorithm）和 ISO 的DEA-1，成为一个世界范围内的标准已经 20 多年了[1]。它很好地抗住了多年的密码分析，除可能的最强有力的敌手外，对其他的攻击仍是安全的。

由于 DES 算法框图是为了清晰地说明加密和解密的原理，直接按照 DES 算法框图实现，加密和解密的速度很慢。因而论文提出优化 DES 算法以提高其实现速度。

2　DES 算法简介

2.1　DES 描述

DES 是一个分组加密算法，它以 64-位为分组对数据加密[2]。64-位一组的明文从算法的一端输入，64-位的密文从另一端输出。DES 是一个对称算法：加密和解密用的是同一算法（除密钥编排不同以外）。

密钥的长度为 56 位（密钥通常表示为 64 位的二进制数，但每个 8 的倍数位用于奇偶检验被忽略掉）。密钥可以为任意 56 位的数，且随时可更换。有一些密钥是弱密钥，但可以很容易地避免。所有的安全都依赖于密钥。

简单地说，算法只不过是加密的两个基本技术——混乱和扩散的组合。DES 基本组建分组是这些技术的一个组合（先代替后移位），它基于密钥作用于明文，这是众所周知的轮（Round）。DES 有 16 轮，这意味着要在明文分组上 16 次实施相同的组合技术（见图 1）。此算法使用了标准的算术和逻辑运算。

2.2　算法概要

DES 对 64-位的明文分组进行操作。通过一个初始置换，将明文分组分成左半部分和右半部分，各 32-位长。然后进行 16 轮完全相同的运算，这些运算被称为函数 f，在运算过程中数据与密钥结合。经过 16 轮后，左、右半部分合在一起经过一个末置换（初始置换的逆置换），这样该算法就完成了。

在每一轮（见图 2）中，密钥位移位，然后再从密钥的 56 位中选出 48 位。通过一个扩展置换将数据的右半部分扩展成 48 位，并通过一个异或操作与 48 位密钥结合，通过 8 个 S-盒将这 48 位替代成新的 32 位数据，再将其置换一次。这四步运算构成了函数 f。然后，通过另一个异或运算，函数 f 的输出与左半部分结合，其结果即成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复 16 次，便实现了 DES 的 16 轮运算。

假设 B_i 是第 i 次迭代的结果，L_i 和 R_i 是 B_i 的左半部分和右半部分，K_i 是第 i 轮的 48-位密钥，且 f 是实现代替、置换及

作者简介：陈良，学士学位，硕士，主要研究方向为应用密码学、计算机网络及计算机网络安全。

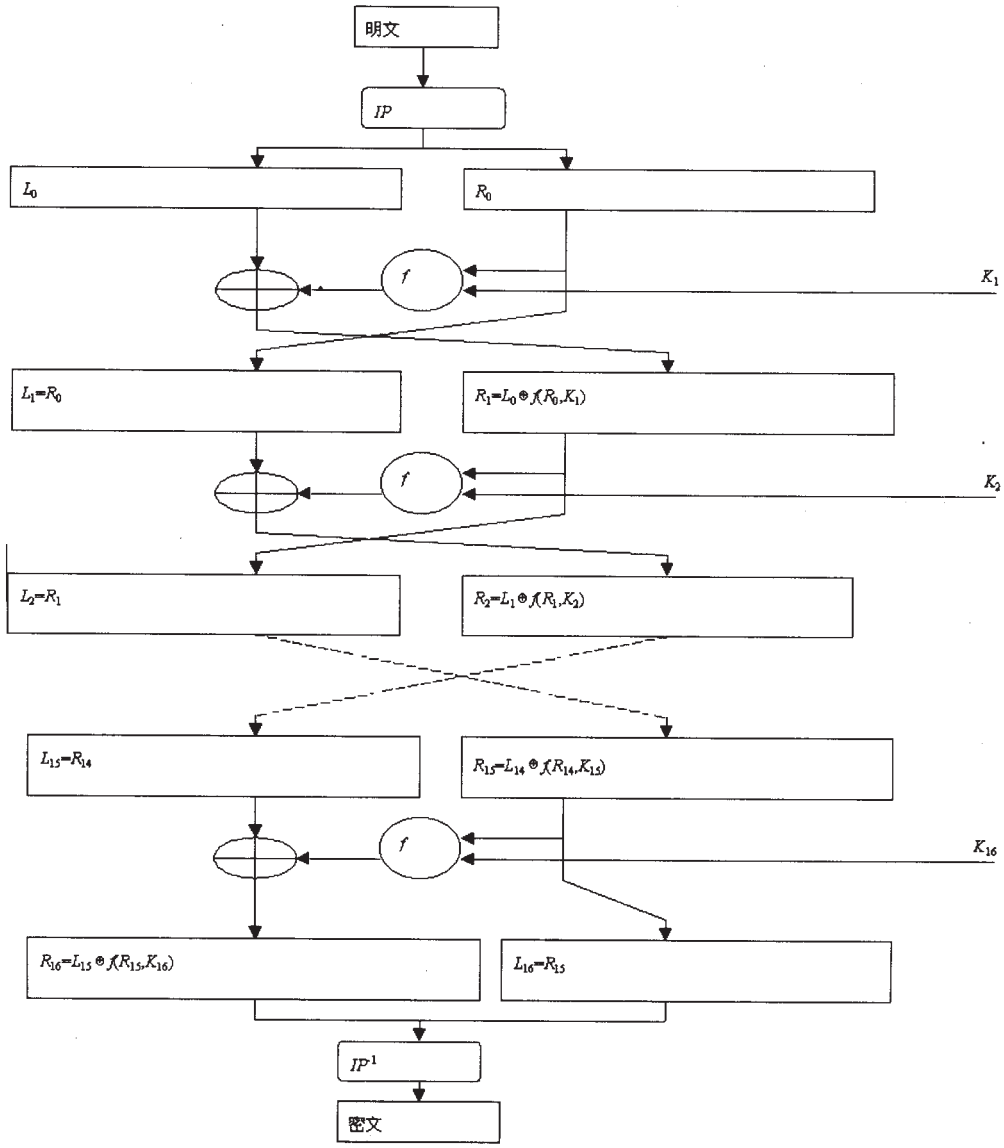

图 1　DES 算法

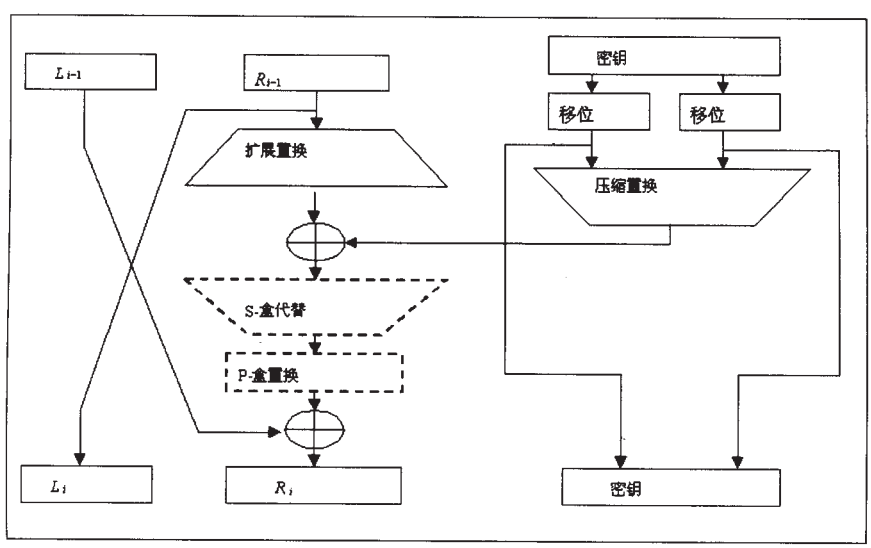

图 2　DES 的一轮

密钥异或等运算的函数，那么一轮就是：

$$L_i=R_i-1$$

$$R_i=L_{i-1} \oplus f(R_{i-1},K_i)$$

2.3　DES 解密

在经过所有的代替、置换、异或和循环移动之后，您也许认为解密算法与加密算法完全不同，且也如加密算法一样有很强

的混乱效果。恰恰相反,经过精心选择各种操作,获得了这样一个非常有用的性质:加密和解密可以用相同的算法。

DES 使得用相同的函数来加密或解密每个分组成为可能,二者的唯一不同之处是密钥的次序相反。这就是说,如果各轮的加密密钥分别是 $K_1,K_2,K_3,\cdots,K_{16}$ 那么解密密钥就是 $K_{16},\cdots,K_3,K_2,K_1$。为各轮产生密钥的算法也是循环的。密钥向右移动,每次移动个数为 0,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1。

3 DES 优化算法

3.1 计算子密钥

当用 DES 算法加密大于 64 位的明文时,由于加密每个 64 位明文在 16 轮中所用的 16 个子密钥是相同的,所以可以先计算出 16 个子密钥。这样就不需要在每个 64 位明文加密过程中重复计算,节约了计算时间。

3.2 将 S-盒代替与 P-盒置换合并为 SP 盒代替

(1)S-盒代替

压缩的子密钥与扩展后的数据块做异或后,要对得到的 48 位结果再做一次代替操作。代替由 8 个代替盒(S-盒)来完成。每个 S-盒有 6 位输入和 4 位输出,一共有 8 个不同的 S-盒。48 位输入被分成 8 个 6 位,每个 6 位输入一个单独的 S-盒,如图 3[1]。

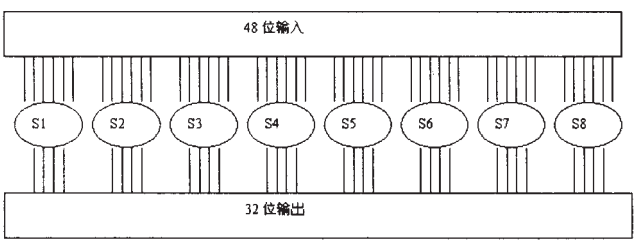

图 3 S-盒代替

每个 S-盒为一个 4 行 16 列的表,盒中的每个元素为 4 位的数字。由 6 位输入来决定将盒的那一行那一列的元素作为输出[1]。如表 1 S-盒代替表。

表 1 S-盒代替表(以 S1 为例,S2-S8 类同)[1]:

s1 :14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7;
0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8;
4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0;
15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13;

将输入的 6 位分别标记为 b1,b2,b3,b4,b5,b6,则 b1 和 b6 连接起来构成一个 2 位的二进制数,为 0 到 3,对应于表 1 中的行号。而中间的 4 位连接起来构成一个 4 位的二进制数,为 0 到 15,对应于表 1 中的列号。

例如,设 S-盒的 6 位输入为 110011,第一位和最后一位为 11 对应于 S-盒的第 3 行,中间 4 位为 1001 对应于同一个 S-盒的第 9 列。若为 S6 的输入,则输出为 S6 的第 3 行第 9 列 14 即,1110。

S-盒代替是 DES 中关键的一步。算法中的其他操作都是线性的,容易分析,而 S-盒的非线性决定了 S-盒的安全性。

(2)P-盒置换

S-盒的 32 位输出再经过 P-盒置换,将这 32 位做一次移位操作。表 2 给出了 P-盒置换。例如,位 21 移到位 4,而位 4 移到位 32[1]。

(3)S-盒代替与 P-盒置换合并

将 S-盒和 P-盒合并为一个 SP-盒,如图 4。

表 2 P-盒置换表

16,7,20,21,	29,12,28,17,	1, 15,23,26,	5, 18,31,10
2, 8,24,14,	32,27, 3,9,	19,13,30, 6,	22,11,4, 25

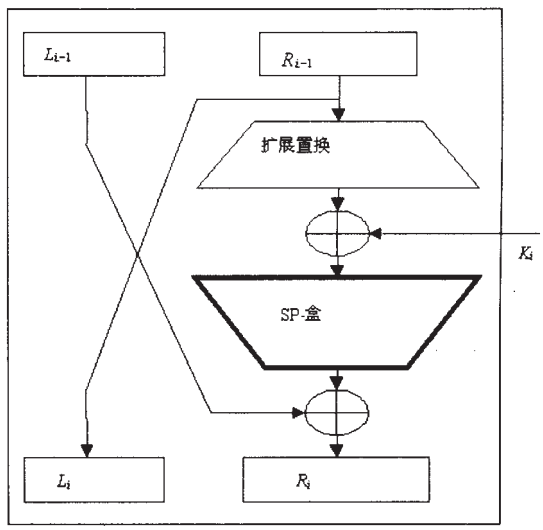

图 4 优化后 DES 的一轮

将 S-盒代替表和 P-盒置换表合并为一个 SP-盒变换表。

表 3 SP-盒变换表(以 SP1 为例,SP2-SP8 类同)

sp1 :0x40410000,0x00000000,0x00400000,0x40410100,
0x40400100,0x00410100,0x00000100,0x00400000,
0x00010000,0x40410000,0x40410100,0x00010000,
0x40010100,0x40400100,0x40000000,0x00000100,
0x00010100,0x40010000,0x40010000,0x00410000,
0x00410000,0x40400000,0x40400000,0x40010100,
0x00400100,0x40000100,0x40000100,0x00400100,
0x00000000,0x00010100,0x00410100,0x40000000,
0x00400000,0x40410100,0x00000100,0x40400000,
0x40410000,0x40000000,0x40000000,0x00010000,
0x40400100,0x00400000,0x00410000,0x40000100,
0x00010000,0x00000100,0x40010100,0x00410100,
0x40410100,0x00400100,0x40400000,0x40010100,
0x40000100,0x00010100,0x00410100,0x40410000,
0x00010100,0x40010000,0x40010000,0x00000000,
0x00400100,0x00410000,0x00000000,0x40400100

4 DES 优化算法分析

(1)S-盒代替

速度慢的原因:要对输入的 6 位进行移位和与操作来获得 S-盒中的行号和列号,并进一步获得 S-盒的输出值。

解决方案:如果不对 S-盒的输入进行移位和与操作,即,用 S-盒的输入直接取得输出值。则处理器不需要移位和与操作,必然提高计算速度。要做到这一点。必须对 S-盒中的数值,即表 1,进行重新排序。分析 S-盒的输入,可以归纳出:

S-盒的第 0 行的输入为:0,2,4,……,30(二进制 0xxxx0)

S-盒的第 1 行的输入为:1,3,5,……,31(二进制 0xxxx1)

S-盒的第 2 行的输入为:32,34,36,……,62(二进制 1xxxx0)

S-盒的第 3 行的输入为:33,35,37,……,63(二进制 1xxxx1)

(下转 86 页)

4 实验结果与结论

通过对上面所检测的新闻视频片段播放后进行统计，口播帧一共出现了两次，分别在第 1~6 秒和第 91~119 秒之间，由此可见，上面的检测结果是正确的。除了这个实验之外，作者还对中央电视台一套节目的 2002 年 1 月 2 日的晚间新闻报道中的口播帧进行了检测，表 1 给出了实验结果。

表 1 基于规则分析检测口播帧算法的实验结果

节目名称		出现次数	误检数	漏检数	检出数	检出率
晚间	世界	8	0	1	7	87.50%
新闻	国内	7	0	0	7	100%
报道	体育	8	1	0	7	87.50%

（注：实验中尚未加入人脸检测和主持人话音识别的确认部分。）

实验结果表明，基于规则分析的口播帧检测算法在没有加入人脸检测模块和主持人话音识别模块的情况下进行实验，已经得到了较高的检测准确率，如果将这两个模块加入到算法中，检测结果的准确率还会得到进一步提高。由此可见，该检测算法是一种有效的口播帧检测算法。

（收稿日期：2003 年 3 月）

参考文献

1.马宇飞，白雪生.新闻视频中口播帧检测方法的研究[J].软件学报，2001，12（5）：377~382

2.Swanberg D，Shu C F，Jian R.Knowledge guided in video database [C].In：Nibblack W ed.IS&T/SPIE.San Jose，CA：SPIE，1993：13~14

3.Ariki Y，Saito Y.Extraction of TV news articles based on scene cut detection using DCT clustering[C].In：Delogne P ed.Proceedings of the International Conference on Image Processing Lausanne，Switzerland：IEEE Computer Society Press，1996：847~850

4.Gunsel B，Ferman A M，Tekalp A M.Video indexing through integration of syntactic and semantic features[C].In：IEEE Computer Society ed.Proceedings of the IEEE Workshop on Application of Computer Vision.Los Alamitos：IEEE Computer Society Press，1996：90~95

5.Hanjalic A，Lagendijk R L，Biemond J.Semi-Automatic news analysis，indexing and classification system based on topics preselection[C].In：Yeung，M M，Yeo B L，Bouman，C A eds.SPIE.San Jose，CA：SPIE，1999：3656：86~97

6.Huang Q，Liu Z，Rosenberg A.Automated semantic structure reconstruction and representation generation for broadcast news[C].In：Yeung M M，Yeo B L，Bouman C A eds.SPIE San Jose，CA：SPIE，1999：3656：50~62

7.于俊清.基于内容的视频摘要研究[D].博士学位论文.武汉：武汉大学，2002

（上接 76 页）

如果用输入的值作为输出的索引，就可以直接取得 S-盒的输出。即，将 S-盒的第 0 行的数值的存储索引由二维的（0，x）改为一维：0，2，4，……，30。将 S-盒的第 1 行的数值的存储索引由二维的（1，x）改为一维：1，3，5，……，31。将 S-盒的第 2 行的数值的存储索引由二维的（2，x）改为一维：32，34，36，……，62。将 S-盒的第 3 行的数值的存储索引由二维的（3，x）改为一维：33，35，37，……，63，其中，x 为 0，1，2，……，15。

新的 S-盒（一维存储）为：

表 4 新的 S-盒代替表（以 S1′为例，S2′-S8′类同）

s1′：14，0，4，15，13，7，1，4，2，14，15，2，11，13，8，1，
3，10，10，6，6，12，12，11，5，9，9，5，0，3，7，8；
4，15，1，12，14，8，8，2，13，4，6，9，2，1，11，7，
15，5，12，11，9，3，7，14，3，10，10，0，5，6，0，13；
……

新的 S-盒以一维存储，用输入的 6 位值为索引，可以直接取得 S-盒的输出值。避免了对输入 6 位值进行移位和与操作，减小了 CPU 的计算开销，提高了速度。

（2）S-盒代替与 P-盒置换合并

合并的必要性：如果能从 S-盒的输入直接得到 P-盒的输出，不需要每圈都进行 P-盒的移位操作，就会节约 CPU 的计算时间。

合并的可能性：以上已经通过对 S-盒的重新排序，能够以 S-盒的输入为索引直接获得 S-盒的输出。又因为 S-盒的输出作为 P-盒的输入，它与 P-盒的输出对应关系是固定的。因而，可以以 S-盒的输入为索引直接得到 P-盒的输出。

设 S_{in} 为新的 S-盒的输入，S_{out} 为新的 S-盒的输出，S 为新的 S-盒变换函数，则，$S_{out}=S(S_{in})$。其中，S 为表 4 的对应关系。

设 P_{in} 为 P-盒的输入，P_{out} 为 P-盒的输出，P 为 P-盒变换函数，则，$P_{out}=P(P_{in})$。其中，P 为表 2 的对应关系。

又因为 $P_{in}=S_{out}$，所以 $P_{out}=P(P_{in})=P(S(S_{in}))=PS(S_{in})$。其中，$PS$ 为代替新的 S-盒和 P-盒的新的函数。问题是如何找到这个新的函数 PS（新的映射关系表）。

新的 S-盒中的 S1′作为 P-盒输入的 1 至 4 位，S2′作为 P-盒输入的 5 至 8 位，……，S8′作为 P-盒输入的 29 至 32 位。由 P-盒置换的含义和表 2 可以看出，P-盒的输出为：将 S1′的 1，2，3，4 位，即，P-盒输入的 1，2，3，4 位，移到 9，17，23，31 位。S2′的 1，2，3，4 位，即，P-盒输入的 5，6，7，8 位，移到 13，28，2，18 位……

例如，S1′的第一个值 14 的二进制形式为：1110 分别移至 9，17，23，31 位得到 0x40410000。

将新的 S-盒代替表和 P-盒置换表合并为一个 SP-盒变换表得到表 3，即为新的 SP-盒变换函数 PS。

5 结论

通过将 S-盒代替与 P-盒置换合并为 SP-盒，并导出新的映射关系表，表 3。可以用原来的 S-盒代替的输入，直接获得 P-盒置换的输出。避免了对 S-盒输入的每个 6 位进行移位和与操作来获得 S-盒输出的行号和列号。同时，不需要对 P-盒的输入进行移位操作。因此节约了 CPU 的计算时间，提高了 DES 算法的实现速度。

运行结果表明，在相同的计算机上加密速度约为 3.3MB/S。因而，较优化前的 0.04MB/S 提高了 80 多倍。同时，这一优化过程并未改变 DES 的计算结果，因而并未改变 DES 的安全性。（收稿日期：2003 年 3 月）

参考文献

1.李克洪，王大玲，董晓梅.实用密码学与计算机数据安全[M].沈阳：东北大学出版社，1997-10

2.[美]Bruce Schneier 著.吴世忠，祝世雄，张文政等译.应用密码学[M].机械工业出版社，2000-01