对5轮Square的中间相遇攻击

王 哲,张文英
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:Square分组密码算法是美国数据加密标准AES算法的前身,它的分组长度、主密钥长度和轮密钥长度都是128比特。文中给出了一个4轮的Square区分器。通过这个区分器找到Square第三轮的密文可以在某些条件下用比较少的参数来表示,减少攻击的运算量。运用这个区分器成功地实现了对5轮Square的中间相遇攻击。这个攻击比其他的攻击的准备阶段和空间复杂度在花费上都少,攻击的先前准备阶段的时间复杂度为2^{34},空间复杂度为2^{72},攻击的时间复杂度为2^{72}。

关键词:Square分组密码;Square分析;中间相遇密码分析
中图分类号:TN918.1 **文献标识码**:A **文章编号**:1673-629X(2011)06-0132-04

Meet-in-Middle Attack on 5-Round Square

WANG Zhe, ZHANG Wen-ying
(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: Square block ciphers algorithm is the data encryption standard AES algorithm predecessor, the size of block, masterkey and round keys of it are all 128-bit. This article employs a four round distinguisher. Through the distinguisher find out that the third cipher of Square can use some few constants under conditions, to decrease the attack's computations. Use this distinguisher to accomplish a meeting-in-middle attack for five-round Square. This attack is faster than other attacks at the expense of an increase in the complexities of memory and precomputation. The attack's precomputation stage of time complexity is 2^{34} and space complexity is 2^{72}, time complexity of the attack is 2^{72}.

Key words: Square block cipher; Square analysis; meeting-in-middle cryptanalysis

0 引 言

分组密码具有速度快、易于标准化和便于软件实现的特点,通常是信息与网络安全中实现数据加密、数字签名、认证及密钥管理的核心体制,它在计算机通信和信息系统安全领域有着最广泛的应用。分组密码的设计和分析是两个既相互对立又相互依存的研究方向,正是由于这种对立促进了分组密码的飞速发展。一般地,对整个R轮密码实施攻击是非常困难的,减少密码的迭代轮数,用某种攻击方法对密码的低轮变形进行分析,由分析的结果可以反映出该密码抵抗这种攻击的能力。对加密体系进行分析,可以衡量密码系统的安全性,促使人们设计出更加安全和更加高效的密码系统,对信息安全具有重要的意义。

Square分组密码[1]是由Joan Daemen, Lars Knudsen和Vincent Rijmen设计发明的。它是美国数据加密标准AES算法的前身。

对Square最有名的攻击当数Boomerang相关攻击[2],它运用了7轮的Boomerang区分器,再加上一轮去恢复全部的密钥,分析的数据复杂度为2^{123}。基于Square算法的设计者运用Square攻击,对6轮的Square进行成功的攻击[1]分析复杂度为2^{72}。但是由于目前计算机计算能力所限,这些攻击在实践上仍是不可行的。在文中,借鉴中间相遇技术和Square方法[3,4]构造一个4轮区分器去攻击5轮的Square,攻击复杂度小于已有结果中的复杂度。

1 Square分组密码的描述

本节介绍Square的算法结构和轮密钥生成算法。

Square算法的分组和主密钥、轮密钥都是128bit。数据处理都是以矩阵形式进行的(每个字节都是在有限域$GF(2^8)$[4],每个x_i都代表一个字节)。如

$X = (x_0, x_1, \cdots, x_{15}) =$

x_0	x_1	x_2	x_3		$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$
x_4	x_5	x_6	x_7	=	$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$
x_8	x_9	x_{10}	x_{11}		$x_{3,1}$	$x_{3,2}$	$x_{3,3}$	$x_{3,4}$
x_{12}	x_{13}	x_{14}	x_{15}		$x_{4,1}$	$x_{4,2}$	$x_{4,3}$	$x_{4,4}$

收稿日期:2010-10-31;**修回日期**:2011-02-02
基金项目:山东省自然科学基金项目(Y2008g01)
作者简介:王 哲(1986-),女,山东聊城人,硕士,研究方向为密码分析;张文英,博士后,副教授,研究方向为密码分析、布尔函数。

Square 算法是一个 8 轮 SPN 分组密码算法,它有 9 个轮密钥,其中第一个为白化密钥。Square 每一轮的 F 函数结构由四个部分组成:乘矩阵 M,S 盒运算 S,矩阵转置 T,加密钥。

乘矩阵 M 运算,是指明文矩阵和 M 矩阵相乘。其中 M $\begin{pmatrix}02 & 03 & 01 & 01\\01 & 02 & 03 & 01\\01 & 01 & 02 & 03\\03 & 01 & 01 & 02\end{pmatrix}$ 计算为:

$$\begin{pmatrix}b1\\b2\\b3\\b4\end{pmatrix}=\begin{pmatrix}02 & 03 & 01 & 01\\01 & 02 & 03 & 01\\01 & 01 & 02 & 03\\03 & 01 & 01 & 02\end{pmatrix}\begin{pmatrix}a1\\a2\\a3\\a4\end{pmatrix}$$

M 运算是一个线性操作。上面矩阵乘法是在有限域 $GF(2^8)$ 上。

S 盒运算是:

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$		$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	$b_{1,4}$
$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	S 盒	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$	$b_{2,4}$
$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	→	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$	$b_{3,4}$
$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$		$b_{4,1}$	$b_{4,2}$	$b_{4,3}$	$b_{4,4}$

$S:b_{i,j}=S(a_{i,j})$。S 盒替换是让输入矩阵的每个字节分别进入 S 盒,即是把每个字节放进 S 盒里进行变换。这里的 S 盒与 AES 中 S 盒相同。其中 S 盒是一个非线性置换。

矩阵转置 T 运算就是指把所得到的矩阵进行转置,$b_{i,j}=a_{j,i}$ 即矩阵的行变成矩阵的列。

a	b	c	d	→	a			
					b			
					c			
					d			

加密钥运算是指将经过前三步运算得到的矩阵与轮密钥组成的矩阵进行相应的异或得到密文,即 $b_{i,j}=(a_{i,j})\oplus rk_{i,j}$。

每一轮进行这四个运算后,一共进行 8 轮,便可以得到密文。

再来看 Square 密码的密钥编排。

Square 密钥编排与 AES-128 密钥编排非常相似。图 1 为 Square 密钥编排的结构图。

设 $rk^0,rk^1,\cdots,rk^8$ 为 9 个 128 比特的轮密钥,rk^0 为主密钥。任一轮密钥 rk^i 都是按 4 × 4 的矩阵排列。rk^i_j 代表第 i 轮密钥的第 j 行。轮密钥生成函数公式如下:

$rk_0^{i+1}=rk_0^i\oplus \mathrm{rotl}(rk_3^i)\oplus C_i$,$rk_1^{i+1}=rk_1^i\oplus(rk_0^{i+1})$,

$rk_2^{i+1}=rk_2^i\oplus(rk_1^{i+1})$,$rk_3^{i+1}=rk_3^i\oplus(rk_2^{i+1})$

其中,C_i 是一个常数,它是由先前 C_{i-1} 生成的。

Square 加密的总体结构为:

$\mathrm{Square}[rk]=F[rk^8]\circ F[rk^7]\circ F[rk^6]\circ F[rk^5]\circ F[rk^4]\circ F[rk^3]\circ F[rk^2]\circ F[rk^1]\circ R[rk^0]\circ M^{-1}$

解密和加密的结构基本上是一样的,只是把密钥使用顺序颠倒过来。

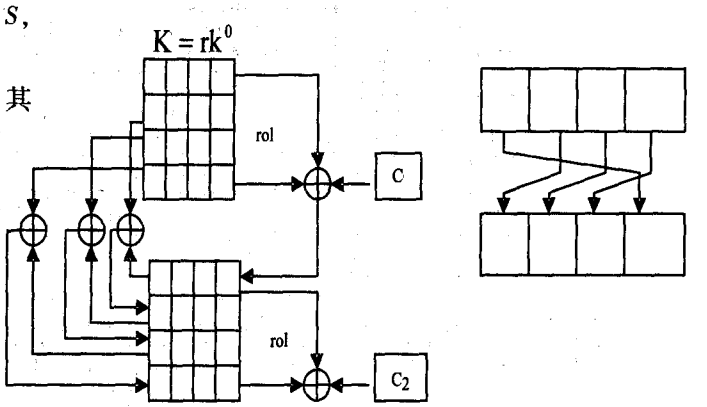

图 1　Square 的密钥编排方案及 rol 运算

2　4 轮 Square 区分器

Square 攻击方法最初是由 Square 密码的设计者提出的。它对于低轮数类似 Square 的矩阵密码都是有效的,随后 N. Ferguson 等人和 H. Gilbert 等人分别利用动态规划和生日悖论的技巧推广了 Square 攻击,后来又有人来研究一种新的 Square 攻击[5]。它是已知攻击 AES 算法—Rijdael 最有效的攻击方法之一。

Square 攻击基本思想[6~9]如下:

Square 攻击主要建立在以下两个重要概念 Λ 集平衡性之上的一种选择明文攻击[10,11]。

(1) Λ 集是一个包含 2^8 个状态的集合,这些状态在某个字节(称为活动字节)上两两互异(因而遍历字节所有的可能值),而在其他字节(称为非活动字节)的位置则完全相同,即对任意状态 $A,B\in\Lambda$ 有:

$$\begin{cases}A_{i,j}\neq B_{i,j}, & \text{若}(i,j)\text{ 位置上是活动字节}\\ A_{i,j}=B_{i,j}, & \text{若}(i,j)\text{ 位置上是非活动字节}\end{cases}$$

(2) 对包含 2^8 个状态的集合 P,某个位置 (i,j) 上的字节是平衡的当且仅当所有状态在该位置上的字节的异或结果为 0,即字节 (i,j) 是平衡的,$\sum_{A\in P}A(i,j)=0$。

受文献[5]中的建立明文和密文之间含有若干参数的函数关系思想的启发,得到了 Square 分组密码两个性质,并根据此性质给出了一个四轮区分器。

性质 1. 给定一个有 256 个元素的明文集合,使得其中只有一个字节是活动的,其余字节都是非活动的,即所有明文仅在一个字节处不同,该字节遍历所有 256 种可能,其余相同位置的字节都相同,对上述 256 个明文分别加密三轮运算后,所得密文集合在任何一个字节都是平衡的,即对 256 个密文处于同一位置的字节求和,结果都是 0。

证明:

图 2 所示的是在第一轮只有第一个字节是其活动

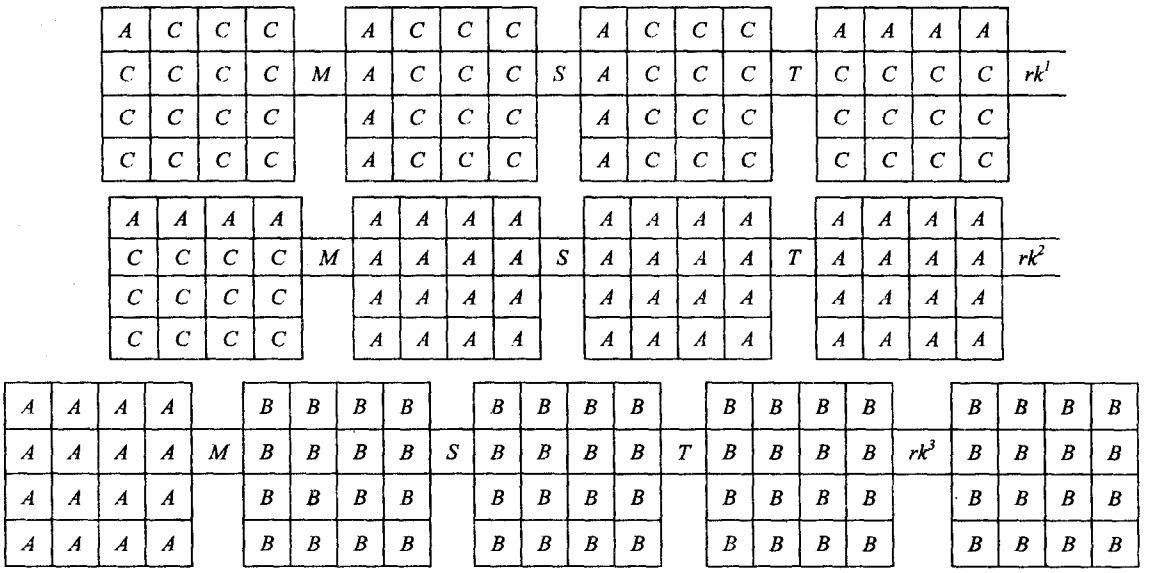

图 2 三轮 Square 运算过程

字节，其它 15 个字节都是非活动的，可视为常量。经过三轮的运算得到的密文所有的字节都是活动的。在图中 A 所表示的是活动的字节，B 是代表平衡的字节，C 代表常量。

这种性质是攻击 Square 的基础。利用这个区分器攻击 4 轮的 Square，对第 4 轮的密钥进行猜测，解密后得到第三轮的输出，如果密钥正确，则第三轮的输出和为 0。此性质是判断密钥正确与否的关键依据。

以下根据这个性质来分析 Square 每一轮加密的时候的参数。

a_{11}	C	C	C		$2a_{11}+m1$	m_{12}	m_{13}	m_{14}
C	C	C	C	M	$a_{11}+m2$	m_{22}	m_{23}	m_{24}
C	C	C	C		$a_{11}+m3$	m_{32}	m_{33}	m_{34}
C	C	C	C		$3a_{11}+m4$	m_{42}	m_{43}	m_{44}

演示一个 4 轮的 Square 的加密过程。在这个加密的过程中舍去了白化密钥。用 $a_{i,j}$ 表示明文的第 i 行、第 j 列。在对明文进行第一轮的 M 运算时，可以得到如上图的结果。

进而再进行 S、T 和加密运算，一轮密文得到的矩阵为：

$s(2a_{11}+m1)+rk^1_{11}$	$s(a_{11}+m2)+rk^1_{12}$	$s(a_{11}+m3)+rk^1_{13}$	$s(3a_{11}+m4)+rk^1_{14}$
M_{12}	M_{22}	M_{32}	M_{42}
M_{13}	M_{23}	M_{33}	M_{43}
M_{14}	M_{24}	M_{34}	M_{44}

在这里定义 $mi(1\le i\le 4)$ 为常数，$M_{i,j}(1\le i\le 4, 2\le j\le 4)$ 为进行 S 盒后加密完的常数。

$$c_1=s(2a_{11}+m1)+rk^1_{11}, c_2=s(2a_{11}+m2)+rk^1_{12},$$
$$c_3=s(2a_{11}+m3)+rk^1_{13}, c_4=s(2a_{11}+m4)+rk^1_{14}$$

则
$$C^2_{11}=s(2c_1+3M_{12}+M_{13}+M_{14})+rk^2_{11} \quad (1)$$
$$C^2_{21}=s(2c_2+3M_{22}+M_{23}+M_{24})+rk^2_{21} \quad (2)$$
$$C^2_{31}=s(2c_3+3M_{32}+M_{33}+M_{34})+rk^2_{31} \quad (3)$$
$$C^2_{41}=s(2c_4+3M_{42}+M_{43}+M_{44})+rk^2_{41} \quad (4)$$
$$C^3_{11}=s(2C^2_{11}+3C^2_{21}+C^2_{31}+C^2_{41})+rk^3_{11} \quad (5)$$

其中 C^2_{11}、C^2_{21}、C^2_{31}、C^2_{41} 含有 rk^2_{11}、rk^2_{21}、rk^2_{31}、rk^2_{41} 的常量。

性质 2. 根据上面所展示的 5 个公式得出，取仅有一个字节活动的明文集合，让该字节遍历 0 到 255。其它的字节都是非活动的即为常量。加密三轮后，得到密文 $(C^3_{11}, C^3_{12}, \cdots, C^3_{44})$。对于把 a_{11} 映射到 C^3_{11} 函数，只需要 9 个参数就可以完全确定由 a_{11} 映射到 C^3_{11} 的函数关系了。这 9 个参数是 c_1、c_2、c_3、c_4、C^2_{11}、C^2_{21}、C^2_{31}、C^2_{41}、rk^3_{11}。

3 密钥遴选的法则

判断密钥正确与否的标准，是攻击过程的重要依据。在介绍攻击过程之前，先举例说明密钥遴选的法则，即判断所猜测密钥正确与否的方法：

(1) 函数关系的寻找。以 $GF^4(2)\rightarrow GF(2)$ 的四元布尔函数 $f(x_1,x_2,x_3,x_4)=x_1x_2x_3x_4+x_1x_3+x_2x_4+x_1+x_4$ 为例说明，这里把 x_3，x_4 视为参数。当参数取遍所有可能的值时，f 函数在各固定参数值处的限制函数分别为：

$$f(x_1,x_2,0,0)=x_1, f(x_1,x_2,0,1)=x_2+x_1+1,$$
$$f(x_1,x_2,1,0)=0, f(x_1,x_2,1,1)=x_1x_2+x_2+1$$

这就是当参数取遍所有值时所对应的所有可能的函数。

(2) 猜测密钥，根据 (1) ~ (5) 式计算出“a_{11} 映射到 C^3_{11}”的函数关系，若该关系是上述五个式子之一，则认为所猜测密钥正确，否则认为错误，继续试其他的可能密钥值。

4　攻击过程

在这个部分中,给出一个对 5 轮 Square 的中间相遇攻击算法[12],这个算法基于对前面区分器 Square 性质的分析。在攻击的过程中,首先根据性质 2 准备好所有符合 $a_{11} \to C_{11}^3$ 的集合作为先前准备的明文集合,然后选择正确和合适的明文进行加密,得到密文。通过某些固定的密钥字节,对某些固定的密文集合进行解密,比较下得到的值是不是和先前准备的集合里面的值一样。如果一样的话,说明对密钥猜测正确。

具体步骤如下:

(1)数据离线预处理阶段:让参数取遍所有 $2^{9\times8}$ 种可能,分别得到参数取各数值时 C_{11}^3,用 a_{11} 表示时的表达式。得到一个 $a_{11} \to C_{11}^3$ 所有可能表达式的全体,将这些函数存入一个表格。

(2)求 C_{11}^1 的阶段:记 $K_{初始}$ 为白化密钥的初始密钥。猜测 $K_{初始}$ 第一个字节为 $K_{11}^{初始}$,选择使得用 $K_{初始}$ 加密后恰好在第一个字节取遍 0 ~ 255,该步需要 234 个明文,因为在第 2 ~ 4 字节都相同的概率为 2^{-24},在第一个字节 0 ~ 255 都被取遍的概率为 $(1-2^{-8})^n$,这里 n 指需要的在第 2 ~ 4 字节都相同的明文数,应用重要极限 $\lim\limits_{x\to0}(1+x)^{\frac{1}{x}} = e$ 可得 $(1-2^{-8})^{2^8} = [(1-2^{-8})^{-2^8}]^{-1} \sim \frac{1}{e}$,即若做28 次实验 0 ~ 255 中每个数值都被取到的概率约为 $\frac{1}{e}$,于是要使每个数字都被取到的期望大于 1,则实验次数应设为 210,则使取得 0 ~ 255 各值期望个数为 $2^2 \times \frac{1}{e}$ 大于 1。猜测 K_{11}^0、K_{21}^0、K_{31}^0、K_{41}^0,分别加密后得 C_{11}^1。把上述明文放进黑盒子加密 5 轮,得到密文。图 3 是求 C_{11}^1 的过程。

(3)求 C_{11}^4 的阶段:定义 K 最后为第五轮部分密钥组(K_{11}^4、K_{12}^4、K_{13}^4、K_{14}^4),搜索所有可能 K 最后的值。用 K 最后去解密第四轮的(C_{11}^5、C_{12}^5、C_{13}^5、C_{14}^5)。再进行转置和 S 盒运算,去获得 C_{11}^4。图 4 是求 C_{11}^4 的过程。

(4)如果以上所猜测 9 字节子密钥 K_{11}^0、K 最后都是正确的,则函数 $C_{11}^1 \to C_{11}^4$ 一定和 1 中先前准备阶段其中一个函数相同。根据 256 个 C_{11}^1 和第三步得到的相应 C_{11}^4,给出函数关系。若所得函数与先前准备阶段所得到的某个函数相同,则认为猜测的密钥就是要求的密钥。

下面分析该步判断错误的概率:该步判断错误也就是虽然函数值相同,但所猜测密钥是错误的。下求两个函数完全相同的概率,两个函数完全相同也就是它们在 2^8 个点处的函数值都相同,而每点处函数值都有 2^8 种取法,所以在各点相同的概率都是 2^{-8},在所有 2^8 个点处的函数值都相同的概率是 $(2^{-8})^{256} = 2^{-2048}$,这是一个极小概率事件,认为极小概率事件不会发生,于是若函数与先前准备阶段的一个函数吻合,就认定所猜测的密钥正确。

(5)这样恢复了 K_{11}^4、K_{12}^4、K_{13}^4、K_{14}^4、K_{11}^0、K_{21}^0、K_{31}^0、K_{41}^0 和 $K_{11}^{初始}$ 9 个字节,共 72 比特,对于剩余的 56 比特可用穷尽搜索的方法获得。

复杂度分析:由 1 知攻击算法的存储复杂度为 2^{72},而猜测 K_{11}^4、K_{12}^4、K_{13}^4、K_{14}^4、K_{11}^0、K_{21}^0、K_{31}^0、K_{41}^0 和 K_{11}^1 所需的时间复杂度也是 2^{72},在 2 中明文准备的数据复杂度为 2^{34}。

5　结束语

文中给出了 Square 分组密码的两个性质,运用这两个性质攻击了 5 轮的 Square。先前准备阶段的时间复杂度为 2^{34},空间复杂度为 2^{72},攻击的时间复杂度为 2^{72},虽然只分析 5 轮的 Square,但是分析复杂度小,与以前的分析相比,易于实现。

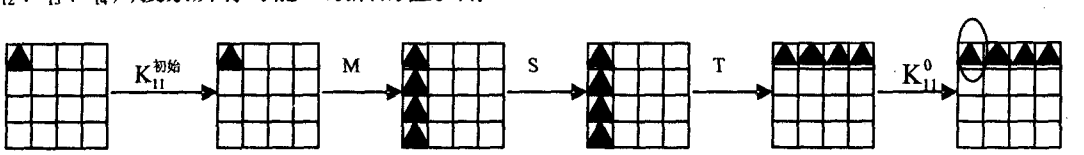

图 3　求 C_{11}^1 的过程

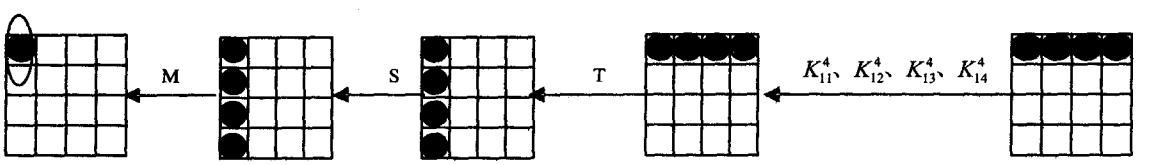

图 4　求 C_{11}^4 的过程

参考文献:

[1] Daemen J, Knudsen L, Rijmen V. The Block Cipher Square [C]//Fast Software Encryption 1997, Lecture Notes in Computer Science, 1267. [s. l.]: [s. n.], 1997: 149-165.

[2] Koo B, Yeom Y, Song J. Related-Key Boomerang Attack on Block Cipher Square [EB/OL]. 2010. http://eprint.iacr.org/.

[3] Demirci H, Selcuk A A. A Meet-in-the-Middle Attack on 8

(下转第 139 页)

3 实验结果分析

选择一篇英文文学作品作为测试语料,大小为4.83MB,选择其中长度为5-10个英文单词、短句作为模式串,总共选择5个,统计各模式串在测试语料中出现的总次数,占用CPU的时间,总的尝试次数和总的比较次数。实验环境为:CPU为Pentium(R),2.8 GHz,内存为1GHz,操作系统为Windows XP,编译环境为VC++ 6.0。实验数据如表5所示。

表5　算法比较

算法	CPU时间/ms	尝试次数	字符比较次数
BM算法	7182	265432828	272628876
BMLT算法	7378	259779857	264857429
QS算法	7424	251875392	256438952
改进算法	5612	219847372	220775265

从实验结果来看,改进算法较算法在占用时间、尝试次数和比较次数上效率都有不小的提高,其中占用CPU时间是BM算法的78.14%,总的尝试次数是BM算法的82.83%,总的字符比较次数是BM算法80.98%,而其他两种算法显然也没有本算法效率高。

4 结束语

对BM算法和现有的BM改进算法进行了简要的介绍,结合其各自的优点提出了一种新的BM改进算法。从理论分析和实验结果来看,改进后的BM算法的匹配次数和比较次数有所减少,匹配时间也缩短了。若将其应用到入侵检测系统的检测引擎中,可以提高系统检测的速度,改善系统性能。

文中主要从以下两个方面进行对BM算法优化:

(1)计算下次移动量时要同时考虑本次匹配的坏字符和本次匹配时模式串对应文本串后一个字符,比较这两个字符产生的跳转距离,选择较大的那个,从而扩大了一次最大移动量;

(2)在匹配过程中,纪录因子时,可能跳过此记录因子的一部分或全部,从而实现跳跃式比较,进而会减小此次匹配过程中的字符比较次数实现快速匹配。

参考文献:

[1] Desai N. Increasing Performance in High Speed NIDS[EB/OL]. 2002-03-15. http://www.linuxsecurity.com.

[2] 王永全.入侵检测系统(IDS)的研究现状和展望[J].通信技术,2008,41(11):139-143.

[3] Iheagwara C, Blyth A. Evaluation of the performance of ID systems in a switched and distributed environment: the RealSecure case study[J]. Computer Networks, 2002, 39(5): 93-112.

[4] 杨薇薇,廖　翔.一种改进的舰模式匹配算法[J].计算机应用,2006,26(2):318-319.

[5] Boyer R S, Moore J S. A fast string searching algorithm[J]. Communications of the ACM, 1977, 20(10): 762-772.

[6] 张红梅,范明钰.模式匹配BM算法改进[J].计算机应用研究,2009,26(9):3249-3252.

[7] 巫喜红,凌　捷.BM模式匹配算法剖析[J].计算机工程与设计,2007,28(1):29-31.

[8] 袁静波,郑吉森,丁顺利.一种BM模式匹配算法的改进[J].计算机技术与发展,2009,19(7):105-107.

[9] 杜　丰.入侵检测中BM模式匹配算法的研究和改进[D].杭州:浙江工业大学,2009.

[10] 顾　钧.基于网络入侵模式匹配的BM算法研究与优化[J].微计算机信息,2009,25:44-46.

[11] Daniel M S. A very fast substring search algorithm[J]. Communications of the ACM, 1990, 33(8):132-142.

[12] 章　张.基于层次分类的网络安全监管系统中串匹配算法的设计与实现[D].南京:南京理工大学,2004.

[13] 赵玲涛.基于内容的安全审计跟踪算法及其应用研究[D].上海:上海交通大学,2007.

(上接第135页)

-Round AES[C]//Fast Software Encryption 2008, Lecture Notes in Computer Science5086. [s.l.]:[s.n.],2008:116-126.

[4] Koblitz N. A course in number theory and cryptography[M]. New York:Springer-Verlag,1987.

[5] 韦宝典,刘东苏,王新梅.一种新Square攻击[J].西安电子科技大学学报(自然科学版),2003,30(4):473-476.

[6] 钟名富,胡予濮,陈　杰.分组加密算法SMS4的14轮Square攻击[J].西安电子科技大学学报(自然科学版),2008,35(1):105-109.

[7] Dunkelman O, Keller N, Shamir A. Improved Single-Key Attack on 8-round AES[EB/OL]. 2010. http://eprint.iacr.org/.

[8] Demirci H, Taskm I, Coban M, et al. Improved Meet-in-the-middle Attacks on AES[C]//Lecture Notes in Computer Science,5922. [s.l.]:[s.n.],2009.

[9] 王美一,唐学海,李　超,等.3D密码的Square攻击[J].电子与信息学报,2010,32(1):157-161.

[10] 李清玲,李　超.变种Camellia对Square攻击的安全性[J].应用科学学报,2006,24(5):485-490.

[11] 贺也平,吴文玲,卿斯汉.对于5轮Camellia密码的Square攻击[J].中国科学院研究生院学报,2001,18(2):177-180.

[12] 冯国登,吴文玲.分组密码的分析和设计[M].北京:清华大学出版社,2000.