密码算法RC5和RC6的分析和比较

何文才[1,2] 牛晓蕾[1] 刘培鹤[2] 杜鹏[1] 张媛媛[1]

1西安电子科技大学通信工程学院 陕西 710071

2北京电子科技学院通信工程系 北京 100070

摘要：RC5和RC6都是安全、简单、高效的分组密码算法，且参数可以灵活设置。本文详细地对RC5/6-w/r/b的加解密算法进行了介绍，并对它们的密码特性进行了分析和比较。

关键词：RC5；RC6；分组密码

0 引言

著名的RC系列密码算法是由RSA公司设计的，目前的最新版本是RC6。RSA公司是RSA算法和MD5的设计者。作为AES(Advanced Encryption Standard)的侯选算法RC6是在RC5的基础上改进的，其目的是为了更好地符合AES的要求。RC5设计简单，运算速度快，使用灵活，易于软硬件实现。RC6不但继承了RC5的这些优点，同时可以抵抗任何已知的攻击，满足AES的安全要求。RC6对RC5的改进主要有两个方面：一是RC6不再使用64位工作寄存器，而是使用4个32位寄存器；二是RC6中增加了32bit的整数乘法，整数乘法是一种非常高效的扩散方法，RC6利用这种乘法计算迭代轮数，所以它的加密轮数与所有明文有关，不像RC5只与较低位的明文有关，这使得RC6具有更快的扩散性，从而具有更可靠的安全性。

1 算法

迭代分组密码算法RC5和RC6实际上是由w、r、b三个参数确定的加密算法，参数确定之后记为 RC5/6-w/r/b。其各个参数的含义和取值如表1所示。

表1 RC5/6-w/r/b中各个参数的含义和取值

参数	含义	RC5/RC6的取值
w	字的长度，以位为单位	16，32，64
r	迭代次数	0，1，2，…255
b	密钥长度，以字节为单位	0，1，2，…255

Rivest推荐的RC5安全版本是RC5-32/12/16，满足AES最低安全要求的RC6版本是RC6-32/20/b(对b没有要求)。

RC5和RC6用到的基本运算有：

a+b 模2^w整数加

a-b 模2^w整数减

a⊕b 逐位异或

a×b 模2^w乘法运算

a<<<b 循环左移w位的字a，移动位数由b的低lg w位决定

a>>>b 循环右移w位的字a，移动位数由b的低lg w位决定

注：RC5未用ab即模2^w整数乘运算。

1.1 RC5算法

1.1.1 RC5密钥扩展

RC5共需要2r+2个子密钥，所以要进行密钥扩展，其中每一轮迭代需要2个子密钥，迭代之外还需要2个子密钥。

RC5算法密钥扩展过程的伪代码表示

```
S[0]=Pw
for i=1 to t-1 do
S[i]=S[i-1]+Qw
Output(S[0],S[1],……S[t-1])
输入8bit,长度为b的用户密钥 K[0],k[1],……K[b-1]
```

转换K[0],k[1],……K[b-1]为数组长度为c,比特数为w的数组L[0],L[1],……L[c-1]

密钥数组L与初始数组S随后将混合，以产生最终的子密钥数组，S在混合时，较大的数组要进行三轮操作，对较小的数组则可能操作更多次，伪码表示如下：

```
i=j=x=y=0
do 3×max(t,c)times:
S[i]=(S[i]+x+y)<<<3; X=S[i]; i=(i+1)mod t
L[j]=(L[j]+x+y)<<<(x+y); Y=L[j]; j=(j+1) mod c
```

其中c=[b×8/w]，方括号表示取整运算。

Pw和Qw为一字长的常量，称为“魔术常量(Magic Constants)”，计算公式为：

Pw=Odd[(e-2)2^w] 其中 e=2.718281828459……(自然对数底)

Qw=Odd[(Φ-1)2^w] 其中 Φ=1.618033988749……(黄金分割比)=$\frac{1+\sqrt{5}}{2}$

作者简介：何文才(1956-)，男，教授，西安电子科技大学密码学专业兼职硕士研究生导师，北京电子科技学院科研处处长，研究方向：信息安全、编码理论、无线数据加密通信等。牛晓蕾(1983-)，女，西安电子科技大学密码学专业硕士研究生，研究方向：信息安全。

Odd[x] 表示与 x 最接近的奇数。

当 w 分别为 16、32、64 时，常数 Pw、Qw 的值如表 2 所列。

表 2　常数 Pw、Qw 取值表（16 进制）

W	Pw	Qw
16	0xB7E1	0x9E37
32	0xB7E15163	0x9E3779B9
64	0xB7E151628AED2A6B	0x9E3770B97F4A7C15

1.1.2　RC5 加密算法

输入：2w bit明文,轮数r及密钥S[0],S[1], ……S[2r+1]

输出：2w bit密文

加密算法过程的伪代码表示：

```
Input(A,B)
A=A+S[0]
B=B+S[1]
for i=1 to r do
A=((AB)<<<B)+S[2i]
B=((BA)<<<A)+S[2i+1]
Output(A,B)
```

其中初始的 A、B 分别为要加密的两个比特数为 w 的明文，输出的 A、B 分别为加密好的两个比特数为 w 的密文。

1.1.3　RC5解密算法

RC5 的解密过程很容易由加密过程推导出来，伪代码表示为：

```
Input(A,B)
for i=r downto 1 do
B=((B-S[2i+1])>>>A)+A
A=((A-S[2i])>>>B)+B
A=A-S[0]
B=B-S[1]
Output (A,B)
```

其中初始 A、B 中的数据就是已经加密了的比特数为 w 的数据，最终的 A、B 中的数据为解密后的比特数为 w 的数据。

1.2　RC6算法

RC6 算法也包括密钥扩展算法、加密算法和解密算法三部分。

1.2.1　RC6密钥扩展

RC6 的子密钥生成过程与 RC5 的相同，但子密钥的个数为2r+4。

1.2.2　RC6加密算法

RC6 用 4 个 w 位的寄存器 A、B、C、D 来存放输入的明文和输出的密文。

输入：明文，存放在 4 个 w 位输入寄存器 A、B、C、D 中

循环次数 r

w位密钥S[0],S[1],……S[2r+3]

输出：密文，也存放在寄存器 A、B、C、D 中

加密算法过程的伪代码表示：

```
Input(A,B,C,D)
B=B+S[0]; D=D+S[1]
for i=1 to r do
t=(B×(2B+1))<<<lg w
u=(D×(2D+1))<<<lg w
A=((A⊕t)<<<t)+S[2i]
C=((C⊕u)<<<u)+S[2i+1]
(A,B,C,D)=(B,C,D,A)
A=A+S[2i+2]; C=C+S[2i+3]
Output(A,B,C,D)
```

其中初始的 A、B、C、D 分别为要加密的四个比特数为 w 的数据，最终的 A、B、C、D 分别为加密好的四个比特数为 w 的数据。

1.2.3　RC6 解密算法

输入：密文，存放在 4 个 w 位输入寄存器 A、B、C、D 中

循环次数 r

w位循环密钥S[0],S[1],……S[2r+3]

输出：明文，也存放在寄存器 A、B、C、D 中

RC6 解密算法过程的伪代码表示：

```
Input(A,B,C,D)
C=C-S[2i+3]; A=A-S[2i+2]
for i=1 to r do
(A,B,C,D)=(D,A,B,C)
u=(D×(2D+1))<<<lg w
t=(B×(2B+1))<<<lg w
C=((C-S[2(r-i)+3])>>>t)⊕u
A=((A-S[2(r-i)+2])>>>u)⊕t
D=D-S[1] B=B-S[0]
Output(A,B,C,D)
```

其中初始的 A、B、C、D 分别为已经被加密的四个比特数为 w 的数据，最终的 A、B、C、D 分别为解密后的四个比特数为 w 的数据。

2　优缺点分析

2.1　RC5的安全性分析

RC5 最显著的两个特点是算法简单和数据确定移位。从混淆和扩散性出发，逐比特异或部件与(mod 2^w)加法部件的组合存在明显漏洞，比如当a 和b对应分量不同时，ab =a+b。移位是算法中惟一的非线性运算，Rivest认为，正是这个非线性运算使得对该算法的线性分析和差分分析都很困难。对 RC5，目前还没有特别有效的攻击法，大部分的研究还只在理论上，一般都基于旋转的次数与输入的明文数无关。

RC5 设计之初，RSA 试验室曾经花费了相当的时间来分析 64 位分组的 RC5 算法，分析结果表明：在 5 轮循环后统计

特性看起来非常好。在8轮循环后，每一个明文位至少影响一个循环移位。如果进行差分分析，对5轮循环需要2^{24}个已知的明文，对10轮循环需要2^{45}个已知的明文，事实上，6轮循环后差分分析就是安全的了，Rivest推荐至少12轮，甚至可能是16轮。

2.2 RC6的安全性分析

作为RC5强化版的RC6通过引入乘法运算来决定循环移位次数的方法，对RC5进行改进，弥补了RC5在扩散速度上的不足，并且RC6中的非线性部分是由多个部件共同实现的，这都大大增强了RC6的安全性。但是，RC6算法的所有安全性都依赖于“数据的循环移位”，而没有任何其他安全保护，这是RC6的安全隐患，也是它未被采纳为AES的原因之一。

攻击RC6的最好的方法是穷举法，穷举b字节的用户密钥或扩展密钥，但这种穷举法需要$\min\{2^{86},2^{1024}\}$次操作，理论上需要超过2^{704}字节的内存。如果对RC6进行中间相遇攻击，则需要2^{700}次计算，这样要恢复扩展密钥最少需要$\min\{2^{86},2^{704}\}$次操作。另外，RC6的加解密时间都与数据无关，这样可以有效地避免“时间攻击”。对RC6的差分分析和线性分析只有在迭代轮数较少时有效，对20轮循环的RC6，用线性分析法至少需要2^{155}个明文，用差分分析法至少需要2^{238}个明文。

2.3 RC5和RC6的性能比较

此外，与大多数分组密码不同，RC6在加密过程中不需要查表，乘法运算也可以用平方代替，所以该算法对内存的要求较低，这可以使得RC6可以方便地使用于IC卡等内存空间小的产品中，这一特点还使得RC6很适合用单片机来实现。

表3 RC5和RC6的性能比较

	RC5	RC6	原因分析
简洁性	更好	好	RC5和RC6用到的是常见的运算
扩散性	好	更好	RC6引入了整数乘法，提高了扩散
执行效率	更高	高	RC5的运算过程比RC6更简单
执行时间	更短	短	RC5迭代轮数只与部分明文有关
存储空间	更小	小	不论加密还是解密过程，RC5都比RC6更简洁
安全性	高	更高	RC6中采用乘法运算决定循环移位次数的方法弥补了RC5算法的漏洞
软硬件实现	容易	容易	都只用了常见的初等运算，有很好的适应性

3 结论与展望

RC5和RC6是两种新型的分组密码算法，它们的字长、迭代次数、密钥长度都可以根据具体情况灵活设置，运算简单高效，非常适合软硬件实现。但它们也有自己各自的优缺点，在实际应用中应根据实际需要选择。目前，RC5已经被RSA公司正式采纳并使用，如用在S/MAIL(用于能用s/mime的产品))、BSAFE(用于c++)、JSAFE(用于java)等软件中，还有几大手机厂家如Nokia，Motorala，Erison等的WAP手机的首选分组加密算法就是RC5。RC6也被广泛应用，如天网防火墙，Tak-C系列智能卡等。

参考文献

[1]RSA home page: http://www.rsasecurity.com/.
[2]NIST home page: http://www.nist.gov/.
[3]http://www.duozhao.com/lunwen/b411/lunwen_76605.html.
[4][美]William Stallings.著.Cryptography and Network Security Principles and practices,Third Edition Publishing House of Electronics Industry.
[5]李莉,张焕国.高级加密标准AES侯选之—RC6[J].通信保密.2000.
[6]http://theory.lcs.mit.edu/%7Erivest/rc6.pdfTheRC6BlockCipher.

Analysis and Comparison Between RC5 and RC6

He Wencai[1,2],Niu Xiaolei[1],Liu Peihe[2],Du Peng[1],Zhuang Yuanyuan[1]
1 College of Communication Engineering,Xidian University,Shanxi,710071
2 Beijing Electronic Science and Technology Institute, Beijing,100070

Abstract:RC5 and RC6 both are secure,simple and efficient block cipher.More,parameters can be set neatly.The paper introduces encryption and decryption of RC5/6-w/r/b in detail.The paper also analyses and compares cryptogram characteristic of RC5 and RC6.

Keywords:RC5;RC6;block cipher

[上接96页]

Secure Computing公司荣获全球最大资讯安全杂志《SC》的“读者信赖奖”和“2006年最佳奖提名”

近日，著名企业网关安全的领军企业，Secure Computing Corporation荣获全球最大信息安全杂志SC杂志‘2006年最佳奖”提名，并被列入SC杂志“读者信赖奖”20大类的100个入围名单。据悉，此次“读者信赖奖”评选结果是由SC杂志的九千多名读者评选产生。SC杂志是全球最大的信息安全杂志，出版时间已经十余年，拥有众多读者群，每月发行，全球发行量为10万份以上。SC杂志见解专业、成熟，观点权威，真知灼见，并以提供IT安全方面的有深度的、无偏见的新闻报道和综合分析为特色，以独立的产品测试和内容编辑深入研究为基础，为IT安全产品如何满足巨大的商业需求提出理论依据，并有助于IT安全的专业人员制定正确的安全决定。