第27卷 第4期 计 算 机 工 程 2001年4月
Vol.27 №4 Computer Engineering April 2001
·安全技术· 文章编号：1000—3428(2001)04—0132—03 文献标识码：A 中图分类号： TP309;TP312

MARS算法和RC6算法分析

王 镭，陈克非
（上海交通大学计算机科学与工程系，上海200030）

摘 要：介绍了入围AES第二轮的MARS算法和RC6算法，通过对这两个算法的研究和比较，分析分组加密算法设计特点和趋势，供研究者参考。

关键词：AES(advanced encryption standard)；DES(data encryption standard)；数据相依旋转

Analysis on MARS and RC6 Encryption Algorithms

WANG Lei，CHENG Kefei
(Department of Computer Science and Engineering, Shanghai Jiaotong University，Shanghai 200030)

【Abstract】In this paper , authors introduce MARS and RC6 encryption algorithms which enter the second round of AES . By analysing and comparing these two algorithms , we find some features and tendency of designing symmetric block cipher for researchers

【Key words】AES(advanced encryption standard)；DES(data encryption standard)；Data dependent rotation

随着计算机的普及和网络技术的迅猛发展，分组加密算法有了更广泛的应用，对分组加密算法的要求也越来越高。在这种情况下，众多研究者提出了各种各样的算法。但是，使用不同的加密算法进行通信会带来诸多不便。于是，有必要寻求和确立数据加密标准。

在1972-1974年间，美国国家标准局公开征求对密码体制的联邦注册，这最终导致了DES的出现，它已成为世界上最广泛使用的密码体制。尽管针对DES的争论相当激烈，但对DES最中肯也是最致命的批评是其秘钥长度太短。事实上，当穷举秘钥成为可能时，DES已走到了生命的尽头。

针对DES的缺点，人们提出了三重DES算法。尽管它在安全性上有很大提高，但是，三重DES太慢了，而且它的明文和密文长度也太短，不能适应将来的发展。所以，三重DES只能是一个过渡性算法。

这样，1997年NIST公开征求AES作为2001年以后的数据加密标准。同时，NIST通告了对AES的几点要求如下：

· 分组长是128比特，秘钥长是128比特，192比特和256比特。
· 加密速度比三重DES快。
· 在Intel Pentium Pro和其他硬件及软件上均能高效运行。
· 算法设计的灵活性较好。如能接受其他的密码长度，能在各种平台上实现。
· 无32位处理器不易实现的操作。
· 算法的设计思想尽可能简单。

AES的征集通告发出后，许多国家，企业和个人都提交了自己的方案。1998年8月，AES召开第一次候选会议，结果有15个算法入围。1999年3月，AES召开第二次候选会议， 5个算法入围。2001年AES将从这5个算法中最后选出1个成为新的数据加密标准。MARS算法和RC6算法就是其中的两个算法。

1 MARS算法

MARS算法是由IBM公司提供的一个候选算法，其整体构架如图1所示。

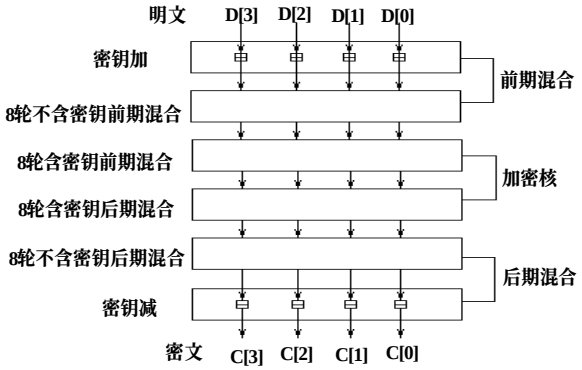

图1 MARS算法构架

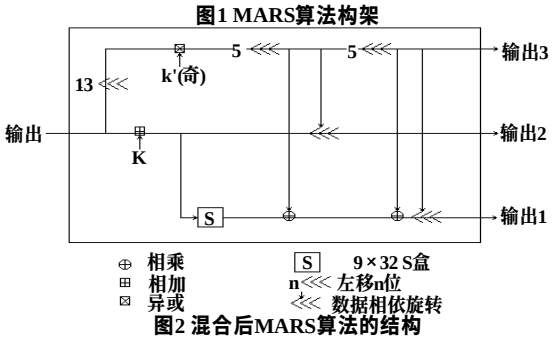

图2 混合后MARS算法的结构

算法可分成3部分：

第一阶段包括明文与子密钥相加和8轮无子密钥的type-3 Feistel混合。通过对明文的快速变换，大大提高了选择明文攻击的难度。因为攻击者想绕过第一阶段直接对加密核进行线性或差分攻击几乎不可能，无法得到加密核的输入。

第二阶段是整个加密算法的核心部分，加密核包括16轮由密钥控制的type-3 Feistel混合。前8轮使用前期方式而后8轮使用后期方式是为了确保加密和解密的对称性。

作者简介：王 镭(1978～)，男，硕士生，主研方向为数据加密与安全技术；陈克非，博导
收稿日期：2000-09-13

第三阶段与第一阶段类似。它大大提高了选择密文攻击的难度，使攻击者无法得到加密核的输出。

在16轮由密钥控制的type-3 Feistel混合中，MARS算法用E盒作为Feistel网络的f函数,其结构如图2所示。

可以说，E盒是MARS算法的核心函数，而MARS算法的基本设计思想在E盒的设计中得到了充分的体现。这就是，综合各种不同的加密操作，通过精巧的设计和科学的安排，使得每种操作的加密效果最大化，从而达到整个算法的性能最优化。从下面对E盒的分析中可以比较清楚地看到这一点。

· DES的f函数以S盒为其绝对中心，在选择明文的攻击下，那些不强的操作就可能被"过滤"，攻击将集中于S盒（如差分攻击法）。而在E盒中，包容了乘法，S盒与数据相依旋转3种很强的非线性操作，它们相互作用，大大增加了攻击者的难度。

· 我们知道，当两个32比特数作32比特乘法时，乘数的低位比高位对结果有更大的影响。所以，设计者将输入左移13比特作为乘数，使得乘数的低位和S盒的输入（输入的低9位）错开。这样，S盒起到了保护乘法操作的弱点的作用，同时也保证了输出1和输出3的无关性。

· 我们知道，当两个32比特数作32比特乘法时，结果的高位具有最强的加密效果，因为它们是由乘数的绝大多数位决定的。所以，在乘法和数据相依旋转的组合中，取乘法结果的高位作为旋转量（通过左旋5比特）。

· 为了保证3个输出尽可能相互独立，相互之间运算很少，虽然有数据相依旋转，但这种操作对第二操作数只取低5比特参与运算。除此之外，只有输出 3 到输出 1 的异或，设计者巧妙地安排了两次异或，起到了相互抵消的作用。

· 因为数据相依旋转和乘法对输入比特的0，1分布的位置相当敏感，所以保持13位的旋转量，可以保证每轮E盒的表现迥然不同，给攻击者进一步增加困难。

· 最后，我们可以看到，在3条输出线中，输出2相对较弱，据此，设计者安排了在type-3 Feistel网络中不把输出2作为下个E盒的输入（加密核的前期方式中，使用输出1作为下个E盒的输入，后期方式中，使用输出3作为下个E盒的输入）。

2 RC6算法

RC6算法是在RC5算法的基础上设计的，下面分别是RC5和RC6算法的程序(RC6提交AES的算法参数是32比特/16轮)。

RC5加密算法(参数为w/r)

```
输入：存有明文的2个w比特的寄存器A，B
      轮数r
      w比特的轮密钥数组S[0,1,...2r+1]
输出：密文存在A，B中
程序：A=A+S[0]
      B=B+S[1]
      for i=1 to r do
      {
      A=[(A⊙B<<<B]+S[2i]
      B=[(B⊙A)<<<A]+S[2i+1]
      }
```

RC6加密算法(参数为w/r)

```
输入：存有明文的4个w比特的寄存器A，B，C，D
      轮数r
      w比特的轮密钥数组S[0,1,...2r+3]
输出：密文存在A，B，C，D中
程序：B=B+S[0]
      D=D+S[1]
      for i=1 to r do
      {
        t=[B × (2B+1)]<<<1gw
        u=[D × (2D+1)]<<<1gw
        A=[(A⊙t<<<u]+S[2i]
        C=[(C⊙u)<<<t]+S[2i+1]
        (A,B,C,D)=(B,C,D,A)
      }
      A=A+S[2r+2
      C=C+S[2r+3]
```

现在，我们来分析一下两个算法的异同：

· 同RC5一样，RC6是一个非常简洁的算法，这可以说是它的最大特点。

· 自从1995年提出RC5算法以来，对该算法的分析和攻击的研究五花八门。尽管到目前为止，还没有找到实用的攻击方法，但是对RC5的理论上的攻击主要基于旋转量不是基于寄存器内所有位这一弱点。RC6算法的设计阻止了这类攻击。增加了32比特的整数乘法，由乘积决定旋转量，这使得旋转量基于寄存器内所有位。

· 与RC5不同，RC6并未将输入分在两个寄存器内直接进行运算，而是将输入分到了4个寄存器内，这是因为AES要求分组长度为128比特，又不支持64位的操作所致。同时，这一变化也使得旋转量由更多的输入比特决定。

· RC5的设计思想是充分利用处理器能够高效实现的操作（如旋转）。可以说，RC6算法完全秉承了这一思想，在RC6中，除了旋转之外还加入了32比特的乘法操作，这是因为现今的计算机已经能高效地实现乘法操作了。整数乘法具有很强的"扩散"能力，由乘积决定旋转量使得RC6可以比RC5进行更少的轮数而比RC5有更高的安全性。

3 MARS算法和RC6算法的比较

(1)设计思路

可以说，MARS算法基本上没有跳出DES的框架，它主要是使用非平衡的Feistel网络。E盒的设计的确相当精巧，虽然略显繁琐，但正是这种非常细节化的设计，保证了算法抵抗目前比较流行的差分攻击法和现行攻击法的良好性能，也保证了将来可能找到的攻击方法几乎必将繁琐无比。RC6算法的设计思路和MARS算法刚好相反，追求简洁，主要是大量使用数据相依旋转。因为其前身RC5算法能抵抗目前所知道的所有攻击方法，RC6的安全性还是有相当保障的。

(2)加密技术运用

两个算法都将乘法和数据相依旋转结合，并且都用加密效果最强的乘法结果高位作旋转量。两个算法都使用了白化技术，白化技术所需开销极小（一般是加或异或）而产生的加密效果很强（令攻击者得不到核心部分的输入输出，而使攻击难度大增），所以在分组加密算法中得到普遍使用。同入围AES的大多数算法一样，MARS算法使用S盒。鉴于人们担心S盒存在陷门，AES规定必须公开S盒的设计原理，MARS有公开的S盒生成算法，用户可以自己生成S盒。RC6算法没有使用S盒，带来的好处是不需要存放查找表。

(3)安全性

就目前的分析，对RC6算法最有效的攻击是强力攻击。当然，由于分组长度和密钥长度都至少是128比特，穷举法并不可行。对20轮的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。而对MARS算法，

用线性分析法至少需要2^{128}个明文，用差分分析法至少需要2^{190}个明文。

(4)实现

RC6算法和MARS算法加密一个分组的耗费差不多，都约在600个时钟周期左右（32位机）。在目前流行的PC上，一个时钟周期执行2-3条指令，如果调度算法比较好的话，加密速度约为300-400clocks/block。容易计算，如果在奔腾Ⅲ450上运行，加密速度约为1.1M-1.5Mblocks/sec，也就是17.6M-20Mbytes/sec，可以说相当快了。

另外，如果RC6算法或MARS算法成为AES标准，因为分组加密算法在网络时代的基础性作用，下一代的计算机就极可能为该算法专门设计一条或几条指令集成于CPU中（类似于MMX指令），这样，实现速度将会提高很多。

值得一提的是，与大多数加密算法不同，RC6算法在加密过程中不需要查找表，加之算法中的乘法运算也可以用平方代替，所以该算法对内存的要求很低。这使得RC6特别适合在单片机上实现。比如IC卡，它内部集成的高速缓存代价高昂，算法所需的内存少，就能大大降低制作成本。

4 小结

可以说，入围AES第二轮的5个算法代表了国际上分组加密算法的最高水平。通过对MARS算法和RC6算法的分析和比较，我们可以看到优秀分组加密算法的共性:

· 有自己独特的设计思路和风格;

· 较好地使用各种新的加密技术;

· 对目前流行的攻击方法有相当强的抵抗能力，并能在理论上给出分析和证明;

· 在软硬件各种平台上能高速运行，现在研究加密算法不仅包括算法本身的研究，如何在硬件上高效实现，如何使代码效率更高，如何提高并行性都是重要的研究内容。

参考文献

1 http://csrc.nist.gov/encryption/aes/

2 MARS-A Candidate Cipher for AES.IBM Coperation,1998-07

3 Rivest R L.RC6-block Cipher.1998-08

※※※

(上接第62页)

过后CMTS用随机算法产生一AK，用CM的公 钥采用RSA算法加密AK，把加密后的AK发给CM。

CM和CMTS 都从AK通过HASH(实际是SHA函数)算法得到一个KEK(key encryption key)和两个消息验证KEY。(HMAC_KEY_U，HMAC_KEY_D)。

(3)CM 向 CMTS 发 送 TEK(Traffic Encryption Key) 请 求 数 据包。

(4)CMTS使用HMAC_KEY_U验证HAMC摘要正确与否。如果正确返回KEY reply。否则发回KEY拒绝的消息。最后CM用HMAC_KEY_D验证CMTS发来数据包的HMAC摘要。用KEK做密钥用DES算法解密得到TEK。

3.2.3 BPI+ 的DOCSIS MAC 数据包格式

MAC 数据包包括以太网数据包和MAC 包头。在MAC包头中有用来设置BPI+的参数的EHDR部分。CM和CMTS之间传递的数据包是采用TEK作为密钥用DES算法加密的。MAC包头不加密。以太数据包的前12个Bytes表示以太网/802.3 的目标地址和原地址，不加密。便于CMTS 对CM数据包实施基于IP地址的包过滤。从CM向CMTS发送的上行数据包中，有用来表示数据包的QoS ID字节，通过CM的QoS ID 可以在CMTS 对CM设置最小和最大带宽，防止非法用户独占网络带宽。

4 DOCSIS 安全措施仍然存在的漏洞

在DOCSIS BPI+中采用了一定的保护措施，对于用户来说保证了在CM和 CMTS 之间数据的安全传输，对于Cable 运营商来说，保证了只有合法登记的CM才能加入到网络中来，防止了服务的窃取。对于Cable 网络的内容提供者来说保证了只有付费的用户才能使用其服务。保证了应用服务的安全。由于在用户的UPSTREAM 数据包中有QoS SID ，对数据、语音等各种服务增加了质量保证，也在一定程度上防止了某些用户霸占带宽，保证了整个网络的正常运行，保证了网络的安全。但是也不能认为Cable 是安全的网络设备。一个用户可以通过在家制造噪音或者独占大部分的网络带宽导致整个Cable网络瘫痪。下面是一些对Cable网络可能存在的威胁，这些威胁都是源于DOCSIS 中的网络连接漏洞。BPI+对这些攻击没有提供有效的防范措施。

(1)CPE系统的安全

由于所有和同一CMTS 相连的CM的用户都处于同一子网，因此如何防止对运行Microsoft Windows 操作系统 的使用TCP/IP NetBios(NBT) 和System Message Block (SMB) 协议的文件系统的非法访问成为很重要的一个问题。因为黑客只要知道的机器名或者地址，就会对机器发动网络攻击或进行非法访问。由于NBT 名字服务广播只使用UDP 的137 端口，因此如果CMTS 支持包过滤，就可以在CMTS 把NBT 广播包过滤掉。否则只有用户关掉NBT服务。

(2)仿冒DHCP服务器

由于CM 在注册过程中要通过DHCP 服务器获得IP地址，CM和CPE设备可以从首先作出响应的任何DHCP服务器获得IP地址。仿冒的DHCP Server 的应答会导致网络用户不能得到服务。

(3)CPE 设备假冒CM，盗用网络服务

对于这类攻击要求CMTS能区分CM和CPE 设备。

(4)假冒SNMP 管理者

由于DOCSIS 只要求SNMPv1， SNMPv1只提供了很少的安全保护。因此可能发生SNMP 管理者被假冒现象，盗用网络服务或者破坏整个网络。对于这类攻击要求CMTS和CM 厂商支持SNMP v2 或SNMP v3。

本文所讨论的安全措施只适用于Cable 接入网络。如果通信的数据离开接入网络，进入Internet ，数据就会经受Internet上的各种网络攻击的威胁。如果要保证安全通信的数据离开接入网络，就要采取高层的安全解决方案，如应用层对E-mail的加密或者采用SSL 算法对Web传输加密。

参考文献

1 有线电视技术一交互式有线电视业务传输系统.国际标准参考资料

2 冯登国,裴定一 编.密码学导引.1999

3 www.Cablelabs.com 中DOCSIS 标准接口规范