文章编号:1671-9352(2007)04-0006-04

改进的7轮AES-192的碰撞攻击

张闻宇,张海纳
(山东大学 数学与系统科学学院,山东 济南 250100)

摘要:对7轮AES-192的碰撞攻击进行了改进.改进的碰撞攻击是基于Gilbert和Minier的攻击过程并且利用了一些AES-192的密钥特性.改进的攻击可以使用2^{123}字节的存储通过大约2^{120}次加密运算来恢复主密钥,此过程比Gilbert和Minier的攻击过程提高了2^{24}倍而只需增加2^8倍的存储量.如果保持存储量不变,改进的攻击过程需要大约2^{127}次加密运算.

关键词:AES;碰撞攻击;区分器
中图分类号:TP300 **文献标识码**:A

Improved collision attack on 7 round AES-192

ZHANG Wen-yu and ZHANG Hai-na
(School of Math. And System Sci., Shandong Univ., Jinan 250100, Shandong, China)

Abstract: An improved collision attack on 7 round AES-192 is given. This attack is based on the result of Gilbert and Minier and the utilization of some properties of AES-192 key schedule. The improved attack can recover the main key by about 2^{120} encryption operations and 2^{123} bytes of memory. Compared with Gilbert-Minier's attack, the time complexity of this attack decreases 2^{24} times with 2^8 times increase in memory. When the same memory is used as Gilbert-Minier's attack, the time complexity is about 2^{127} encryption operations.

Key words: AES; collision attack; distinguisher

0 引言

Advanced Encryption Standard(AES)是明文分组为128位密钥长度为128,192或者256位的对称密码算法.AES-192的密钥长度为192位,总共有12轮.目前有很多对AES-192的分析结果[1~5],最好的分析结果是针对7轮的AES-192.本文我们针对7轮AES-192的碰撞攻击进行了改进.对AES的碰撞攻击最早由H. Gilbert和M. Minier提出[2],他们采用2^{115}字节的存储通过大约2^{144}次运算来恢复主密钥.本文中改进的碰撞攻击使用2^{123}字节的存储通过大约2^{120}次运算来恢复主密钥,此过程比Gilbert和Minier的攻击过程提高了2^{24}倍而只需增加2^8倍的存储量.如果保持存储量不变,我们的攻击过程需要大约2^{127}次运算.

本文的内容分为以下几个部分:首先我们对AES-192算法进行简单描述,然后是改进的碰撞攻击的过程,接下来我们对改进的碰撞攻击的过程进行进一步的优化,最后是本文的结论.

1 对AES-192算法的描述

AES-192的128位分组 $\boldsymbol{Y}$ 可以表示成4×4的方阵 $\boldsymbol{Y}=(Y_{i,j})$:

收稿日期:2007-03-06
基金项目:国家自然科学基金重点资助项目(90604036);国家杰出青年基金资助项目(60525201);国家973计划资助项目(2007CB807902)
作者简介:张闻宇(1979-),男,博士研究生,主要研究方向:对称密码的分析与设计.

$Y_{0,0}$	$Y_{0,1}$	$Y_{0,2}$	$Y_{0,3}$
$Y_{1,0}$	$Y_{1,1}$	$Y_{1,2}$	$Y_{1,3}$
$Y_{2,0}$	$Y_{2,1}$	$Y_{2,2}$	$Y_{2,3}$
$Y_{3,0}$	$Y_{3,1}$	$Y_{3,2}$	$Y_{3,3}$

AES 的轮变换对 128 位的中间状态进行下面四个基本变换:

- 字节替换(ByteSub,BS):当前状态以字节为单位通过 AES 的 S 盒.
- 行移位(ShiftRow,SR):当前状态的第 i 行循环左移 i 个字节,$i=0\cdots3$.
- 列混合(MixColumn,MC):当前状态的每一列与 4×4 的列混合矩阵相乘.
- 密钥异或(AddRoundKey,ARK):当前状态与轮密钥按字节异或.

AES-192 由初始密钥异或,11 轮轮变换,以及最后一轮不包含列混合的轮变换组成.

AES-192 的轮密钥采用下面的密钥方案生成.192 位的密钥扩展 K 成一组密钥 $W_0, W_1, \cdots W_{51}$,每个 W_i 由 4 个字节组成.$W_0\cdots W_5$ 直接由 K 初始化,$W_i, i=6\cdots51$ 通过下面步骤生成:

$$\text{if } i \bmod 6=0 \quad W_{i-1}=\text{SubByte}(\text{RotByte}(W_{i-1}))\oplus\text{Rcon}[i/6],$$

$$W_i=W_{i-6}\oplus W_{i-1}.$$

其中 RotByte(W)将 W 循环左移 1 个字节,Rcon[i] = ($RC[i]$,0,0,0),这里 $RC[i]$是 x^{i-1}在 $GF(2^8)$中的取值.第 r 轮的轮密钥 K^r 由 $W_{4r+i}, i=0\cdots3$ 组成,我们也把 K^r 作为 4×4 的方阵 $K^r_{i,j}$处理.

对于上面描述的 AES-192 的密钥方案,我们有以下两个性质.Lucks 在[3]中介绍了这样的性质:如果我们知道第 7 轮的密钥 K^7,即 $W_{28}, W_{29}, W_{30}, W_{31}$,我们可以得到第 6 轮的前两列密钥:

$$W_{24}=\text{SubByte}(\text{RotByte}(W_{29}))\oplus W_{30}\oplus\text{Rcon}[5],$$

$$W_{25}=W_{30}\oplus W_{31}.$$

我们可以按如下方式[6]推导 $W_i, i=6\cdots51$:

$$\begin{aligned}
&W_6=W_0\oplus f_6(W_5),\\
&W_7=W_1\oplus W_6=W_0\oplus W_1\oplus f_6(W_5),\\
&\vdots\\
&W_{24}=W_0\oplus f_6(W_5)\oplus f_{12}(W_{11})\oplus f_{18}(W_{17})\oplus f_{24}(W_{23}),\\
&W_{25}=W_1\oplus f_{12}(W_{11})\oplus f_{24}(W_{23}),\\
&\vdots\\
&W_{28}=W_0\oplus W_4\oplus f_6(W_5)\oplus f_{12}(W_{11})\oplus f_{18}(W_{17})\oplus f_{24}(W_{23}),\\
&W_{29}=W_1\oplus W_5\oplus f_{12}(W_{11})\oplus f_{24}(W_{23}).
\end{aligned}$$

其中 f_i 在密钥方案中定义.从以上推导的过程我们可以得到下面的性质:

$$W_4=W_{24}\oplus W_{28},\ W_5=W_{25}\oplus W_{29}.$$

在下一节描述的碰撞攻击过程中,将用到上述两个性质来进行选择明文的划分和攻击过程的改进.

2 改进的 AES-192 的碰撞攻击

这一节我们首先简要描述 H. Gilbert 和 M. Minier 在[2]中建立的用于 7 轮碰撞攻击的区分器,然后描述我们的改进的碰撞攻击过程,关于原始的碰撞攻击的更多细节请参阅[2].

在[2]中,基于 3 轮 AES 变换中存在的字节碰撞,作者建立了 4 轮的区分器用于进行 7 轮碰撞攻击.本节基于[2]我们建立类似的区分器,可以描述为:对于 Y^5 的第 2 列 4 个字节,我们可以进行逆变换得到 $Y^4_{0,1}=\text{SubByte}^{-1}[(0E\cdot Y^5_{0,1}\oplus0B\cdot Y^5_{1,1}\oplus0B\cdot Y^5_{2,1}\oplus09\cdot Y^5_{3,1})\oplus\omega^5_{0,1}]$,此处 $\omega^5_{0,1}$为 K^5 通过列混合的逆变换之后对应位置的字节值.简记 $0E\cdot Y^5_{0,1}\oplus0B\cdot Y^5_{1,1}\oplus0D\cdot Y^5_{2,1}\oplus09\cdot Y^5_{3,1}$为 $f^c(y)$.通过对 $y=0,1,16$ 时函数 $f^c(y)$对 c 碰撞

的检测来判断字节碰撞是否发生,并且这种检测操作的运算量少于一次 AES 的加密操作.下面我们分两部分详细描述的改进的碰撞攻击过程.

2.1　对碰撞攻击过程的改进

选择 2^{32} 的明文 Y^0,使其满足:$Y^0_{0,1}$, $Y^0_{1,2}$, $Y^0_{2,3}$, $Y^0_{3,0}$ 取遍所有可能值,Y^0 的其它字节为常数值.加密这些明文得到 2^{32} 的密文,我们的改进攻击按照下面过程进行(如图 1 所示).

图 1　改进的 7 轮 AES-192 的碰撞攻击

Fig.1　The improved collision attack on 7 round AES-192

(1) 猜测 4 字节密钥 $K^0_{0,1}$, $K^0_{1,2}$, $K^0_{2,3}$, $K^0_{3,0}$,与明文 Y^0 的对应字节异或,再猜测 4 字节密钥 $K^1_{0,1}$, $K^1_{1,1}$, $K^1_{2,1}$, $K^1_{3,1}$(即 W_5),记所猜的 8 字节密钥为 K_{top},这样我们可以得到 Y^2 的第 2 列的值.将 2^{32} 明文进行如下划分使得所得 2^{24} 子集合满足下列条件:

◆ y 取遍 0 到 255 的所有值,三元字节向量组 c 为常数值,并且一组 c 值对应一个子集合.

◆ Y^2 的其它 12 个字节为常数值且对所有的子集合都相等.

从上面划分的 2^{24} 个子集合中选择 2^{16} 个,进行下一步.

(2) 猜测 $K^7_{0,2}$, $K^7_{0,3}$, $K^7_{1,1}$, $K^7_{1,2}$, $K^7_{2,0}$, $K^7_{2,1}$, $K^7_{3,0}$, $K^7_{3,3}$ 的所有可能取值,部分解密最后一轮,再猜测 2 字节密

钥 $\omega_{2,3}^6, \omega_{3,2}^6$,对所有猜测的密钥字节预计算 $f^c(y)$的右半部分(记为 f_r),其中 $y = 0\cdots15$,将计算结果存入临时表格.基于这些不同 c 值对应的表格,根据所有猜测的密钥计算$(f_r^c(y)\oplus f_r^{c^*}(y))_{y=0\cdots15}$并将结果按顺序存入一个表格.预计算部分所需存储为 $2^{80}\cdot2^4\cdot2^{31} = 2^{115}$字节.同样的预计算过程也可以对 $f^c(y)$的左半部分(记为 f_l)进行,所需存储量大小相同.

(3) 对应于上述预计算过程,猜测 $K_{0,0}^7, K_{1,0}^7, K_{2,3}^7$或 $K_{2,3}^7$之一,$K_{3,1}^7$或 $K_{3,2}^7$之一,共 4 字节密钥,我们可以对 $y = 0\cdots15$ 计算 $f_l^c(y)$,再计算$(f_l^c(y)\oplus f_l^{c^*}(y))_{y=0\cdots15}$并在预计算得到的表格中查询是否有同样的取值.如果对 $y = 0\cdots15$ 所计算的值都相等,则对其它所有的值进行上述计算,如果都相等,则返回此时对应的所有猜测的密钥.此过程的时间复杂度少于 $2^{64}\cdot2^{32}\cdot2^{31} = 2^{127}$次 AES 变换.同样的攻击过程对于另外的预计算过程也可以进行,复杂度相同.

上述攻击过程就是从所有 2^{32}可能取值中随机选取 2^{16}个测试所得结果是否相等的过程,根据生日假设,此碰撞测试过程中发生碰撞的概率大约为$\frac{1}{2}$,故攻击成功的概率为$\frac{1}{2}$.

2.2 攻击过程的进一步优化

对于上面描述的改进的碰撞攻击过程,我们可以进行进一步的优化,使得存储与时间复杂度通过权衡达到最优,优化过程为:

(1) 在上面攻击过程的第 2 步,我们可以猜测 W_{30}, W_{31}的所有可能值,此时我们可以得到 $W_{29} = W_5\oplus W_{30}\oplus W_{31}$,继而根据密钥方案得到 W_{24}, W_{25},再猜测 $K_{0,0}^7, K_{1,0}^7, K_{2,0}^7$或 $K_{3,0}^7$之一共 3 字节密钥,我们可以对$y = 0\cdots15$ 计算 $f_l^c(y)$,存入临时表格,再根据不同 c 值对应的表格计算$(f_l^c(y)\oplus f_l^{c^*}(y))_{y=0\cdots15}$并将结果按顺序存入一个表格.此时预计算部分所需存储为 $2^{88}\cdot2^4\cdot2^{31} = 2^{123}$字节.

(2) 猜测 $\omega_{2,3}^6, \omega_{3,2}^6, K_{3,0}^7$或 $K_{2,0}^7$之一共 3 字节密钥,根据预计算过程中猜测的密钥,我们可以对 $y = 0\cdots15$ 计算 $f_r^c(y)$,然后计算$(f_r^c(y)\oplus f_r^{c^*}(y))_{y=0\cdots15}$并在预计算得到的表格中查询是否有同样的取值存在.如果对 $y = 0\cdots15$ 所计算的值都相等,则对其它所有 y 的值进行上述计算,如果都相等,则返回此时对应的所有猜测的密钥.此过程的时间复杂度少于 $2^{64}\cdot2^{24}\cdot2^{31} = 2^{119}$次 AES 变换.考虑到预计算的时间复杂度大约等于 2^{119}次 AES 变换,所以攻击过程的总复杂度为 2^{120}次 AES 变换.

上述优化的攻击过程可以使用 2^{123}字节存储和 2^{120}次加密运算恢复主密钥.攻击过程的成功概率为$\frac{1}{2}$.

3 结论

本文给出了改进的 7 轮 AES-192 的碰撞攻击.我们的攻击可以使用 2^{123}字节的存储通过大约 2^{120}次加密运算来恢复主密钥,此过程比 Gilbert 和 Minier 的攻击过程提高了 2^{24}倍而只需增加 2^8 倍的存储量.如果保持存储量不变,我们的攻击过程需要大约 2^{127}次加密运算.

参考文献:

[1] N Ferguson, J Kelsey, B Schneier, et al. Improved cryptanalysis of rijndael, selected areas in cryptography 2003[M]. Ottawa: Springer-Verlag, 2004.

[2] H Gilbert, M Minier. A Collision Attack on 7 rounds of rijndael, the third advanced encryption standard candidate conference[M]. New York: Springer-Verlag, 2000.

[3] S Lucks. Attacking seven rounds of rijndael under 192-bit and 256-bit keys, the third advanced encryption standard candidate conference [M]. New York: Springer-Verlag, 2000.

[4] M Minier. A three rounds property of the AES, advanced encryption standard-AES: 4th international conference[M]. Berlin: Springer-Verlag, 2005.

[5] W Phan. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES)[J]. Information Processing Letters, 2004, 91(1):33 ~ 38.

[6] F Armknecht, S Lucks. Linearity of the AES key schedule[M]. Berlin: Springer, 2005. 159 ~ 169.

(编辑:李晓红)