一种混沌映射密码算法的安全性分析*

钟黔川
(西昌学院,四川 西昌 615013)

【摘 要】近年来有许多基于迭代混沌映射的密码系统被提出,但它们中很少能抵抗选择明文攻击、选择密文攻击或者已知明文攻击。本文分析了参考文献[14]中存在的一些缺陷并且攻破它。参考文献[14]主要思想在于使用变长扩展密钥(最大128位)构造四个一维混沌映射的初值和迭代次数,获取初值和迭代次数的过程是有限整数问题,存在致命缺陷,不具抗攻击性,本文使用选择密文/明文攻击方法在很短时间内就能恢复变长扩展密钥。

【关键词】混沌加密;混沌映射;分组密码
【中图分类号】TP301.6 【文献标识码】A 【文章编号】1673-1891(2011)04-0047-04

1 引言

在过去的许多年里,提出了很多基于一维混沌映射的加密系统[1-7],但在提出后不久大多数又不约而同的被成功攻击[8-13]。Pareek等提出了一种基于多重一维映射的新混沌加密算法。为了避免可能的攻击,他们使用了变长扩展密钥,将明文分成变长分组。同时,随机从多个一维混沌映射中选择一个混沌映射来进行迭代,加密时随机从会话密钥中选取部分值作为混沌迭代的次数,主要算法描述如下:

在算法中,最大为128位的密钥被分为多个8bit为单位的块,每块称作会话密钥:

$$K=K_1K_2K_3K_4\cdots K_{16}(\text{密钥}) \quad (1)$$

明文/密文被分成多个8bit为单位的块,每块的长度是变化的:

$$P=\underbrace{P_1P_2}_{C_1}\underbrace{P_3P_4}_{C_2}\cdots\underbrace{P_n}_{C_n}(\text{明文}) \quad (2)$$

$$C=\underbrace{C_1C_2}_{C_1}\underbrace{C_3C_4}_{C_2}\cdots\underbrace{C_n}_{C_n}(\text{密文}) \quad (3)$$

在表1中四个一维混沌映射用整数进行了编号(映射号N):

表1 四个一维混沌映射的映射号、迭代表达式、混沌映射参数

混沌映射	映射号r(N)	迭代表达式	混沌映射参数
Logistic 映射	0	$X_{n+1}=\lambda X_n(1-X_n)$	$\lambda=3.99$
Tent 映射	1	$X_{n+1}=\begin{cases}\lambda X_n & \text{If } X_n<0.5\\ \lambda(1-X_n) & \text{If } X_n\geq 0.5\end{cases}$	$\lambda=1.97$
Sine 映射	2	$X_{n+1}=\lambda\sin(X_n)$	$\lambda=0.99$
Cubic 映射	3	$X_{n+1}=\lambda X_n(1-X^2_n)$	$\lambda=2.59$

开始的时候,每个混沌映射的初始值(IC)都是一样的,统一由会话密钥产生:

$$R=\sum_{i=1}^{16}(K_i/256) \quad (4)$$

$$IC=R-[R] \quad (5)$$

一个动态表DT1被建立如表2所示,混沌映射的初值(IC)在每块明文/密文加密/解密时被更新。在表2中初始时用'3839384B4A44534457453233'作为密钥(K)来产生初值(IC):

表2 动态表DT1

映射号(N)	初值(IC)
0	0.101562
1	0.101562
2	0.101562
3	0.101562

另一个动态表DT2被建立如表3所示。随机数由线性同余随机数发生器(LCG)产生如下等式所示:

$$Y_{n+1}=(aY_n+c)\bmod m, \quad (6)$$

其中参数a,c和m分别取5,1和16,Y_0由如下等式产生:

$$Y_0=[IC\times 10^2] \quad (7)$$

B,N和IT的值由Y_{n+1}产生,在表3中列出了其值的变化:

$$B=Y_{n+1} \quad (8)$$

$$N=Y_{n+1}\bmod 4 \quad (9)$$

IT=((Y_{n+1}mod16)+1)个会话密钥密钥的进制表示。

表3 动态表DT2

在分组中的块号(B)	映射号r(N)	映射中的迭代次数(IT)
3	3	75
0	0	56
1	1	57
6	2	83
15	3	75
-	-	-
-	-	-

收稿日期:2011-09-01
*基金项目:国家自然科学基金资助项目(项目编号:60671033)。
作者简介:钟黔川(1970-),男,重庆江津人,讲师,博士研究生,主要研究领域为信息安全、混沌密码、数字水印技术。

一个分组中B块明文/密文被加密/解密，用初值IC使混沌映射迭代IT次。新值X(X_{new})被用于产生明文/密文，加密/解密如下等式所示：

$$C_i=(p_i+[X_{new}\times 10^5]\bmod 256) \quad (10)$$

$$p_i=(C_i+256-([X_{new}\times 10^5]\bmod 256)) \quad (11)$$

mod 256

在动态表DT1中映射N的初值IC由加密/解密每一块明文/密文以后新得到的X，也就是X_{new}来更新。

当动态表DT2完全耗尽，令IC=X_{new}，由等式(6)，(7)，(8)和(9)得到新的值填充它，更详细的内容请阅读参考文献[14]。

2 原文中的一些缺陷

Pareek等没有使用双精度数而使用单精度数进行计算，使密钥空间大大缩小。单精度数的数字精度大约是2^{-20}，在参考资料[14]的算法中混沌映射的初值和迭代次数的组合根本不能经受遍历穷举攻击。从表4可见，只有定义每一步的迭代值为单精度和初值IC=0.1015625，才能得到表4第三列所示的新迭代值，如果用双精度数显然得不到这些值。

表4 使用密钥'3839384B4A44534457453233'对明文'cha'加密的映射N初值IC、迭代次数IT、新迭代值X_{new}

映射N的初值IC	映射N的迭代次数IT	映射N的迭代值(X_{new})
0.101562	75	0.503917
0.503917	75	0.577983
0.577983	75	0.207845

从等式(10)、(11)可以看出，原算法中迭代混沌映射产生的二进制序列与密钥有关，而不依赖明文的机制容易造成信息泄露和导致算法遭受选择明文攻击[13]。

下面讨论的是混沌映射的初值和迭代次数是有限整数，这更是原算法存在的致命缺陷。

3 攻击IC，分组的块数(B)和映射N的迭代值IT

比较典型的穷举攻击方法有：

唯密文攻击(Ciphertext only attack)：密码分析者仅知道一些密文，而对明文一无所知。这种攻击手段所需信息是最少的，但也是难度最高的手段之一。

已知明文攻击(Known plaintext attack)：密码分析者知道一些密文以及对应明文，但不知道密钥。在这种情况下，如果密文和明文具有比较确定的对应关系的话，密码分析者就很容易通过替换、查找、类推、猜测等手段破译密文。

选择明文攻击(Chosen plaintext attack)：密码分析者能够临时访问加密机，因此能够任意选择一个明文字符串x，并可构造相应的密文字符串y，一个密码系统比较容易受到这类攻击。

选择密文攻击(Chosen Ciphertext attack)：密码分析者能够临时访问解密机，因此能够任意选择一个密文字符串y，并可构造相应的明文字符串x，一个密码系统比较容易受到这类攻击。

下面的讨论中，根据著名的Kerchoff's准则，我们假定密码分析者知晓除密钥以外的所有事情。尽管对128位密钥进行穷举攻击需要2^{128}次测试，我们将在下面分析从密钥(K)获取初值(IC)和一个分组的块数(B)的过程存在致命缺陷，结果就是密钥空间锐减为2^{16}。在这种情况下，很容易就能获取初值IC和一个分组的块数(B)，继而通过很少的运算时间就穷举出迭代次数IT，从而完整的恢复密钥K。

从密钥中获取初值IC是通过等式(4)和(5)。R可能的值只能是0，1/256，2/256，…，16*255/256，这样IC的可能值也就只能是0，1/256，2/256，…255/256，256/256–[256/256]，257/256–[257/256]，258/256–[258/256]，…，16*255/256–[255/256]，IC可能的取值是重复的。原因在于，当R为0，256/256，512/256…，15*256/256时，我们得到同样的IC值，都是0，R其余的值也有同样的规律。因此IC可能值只有0，1/256，2/256…，255/256。R和IC的关系如图1所示：

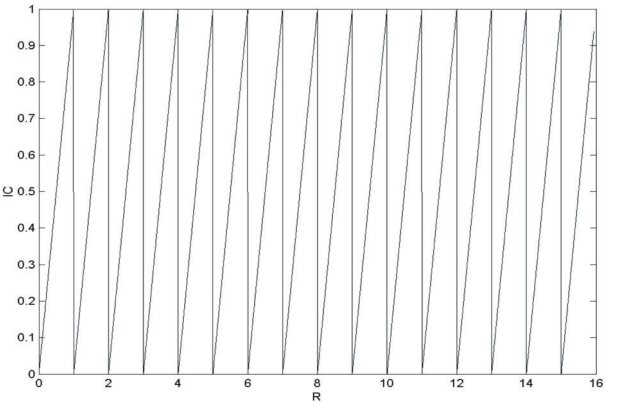

图1 R和IC的关系

我们定义K_{rl}作为第一个将要恢复的会话密钥，K_{rl}可能的值只能是0，1，2，3…，255。K_{rl}和IC可能取值的组合数最大只能是256*256=2^{16}。由于这个取值过程原因，总的密钥搜索空间从2^{128}下降到2^{16}。

为了恢复K_{rl}和IC，我们需要一个分组的两块连续的明文，这两块连续的明文通过初值IC和同样的迭代次数IT加密。最简单的方法是使用明文/密文

的最开始几块。在这部分，我们定义P_1，P_2，P_3和C_1，C_2，C_3分别表示加密/解密文件中连续的最开始的三个明文/密文。由等式(7)，针对LCG(线性同余随机数发生器)的种子值(Y_0)的可能取值只能是0，1，2，3…，99。根据等式(6)从Y_0导出的Y_1的可能取值只能是0，1，2，3…，15。由等式(7)，第一个分组的块数(B_f)是Y_1。B_f的值(等于Y_1)除了0和1，都大于等于2，混沌映射号的可能取值是四个混沌映射之一。由于在第一个分组中有两个连续的明文块P_1，P_2，它将满足上面的要求。当Y_1=0，Y_{n+1}={0，1，6，15，12，13，2，11，8，9，14，7，5，10，3}，其中0≤n≤15。如果Y_1=1，Y_{n+1}={1，6，15，12，13，2，11，8，9，14，7，5，10，3，0}，其中0≤n≤15。由于Y_1=0表示第一个分组的块数是0，换句话说，没有明文/密文块被加密或者解密。结果是，当Y_1=0，1时，加密/解密文件中第一、第二分组的块数都分别是1，6，第二分组的映射号是2(6模4)，也就是使用sine映射。在这种情况下，我们也取一个分组的两块连续的明文块，不同之处仅仅在于我们将使用第二个分组最开始的两个明文块来恢复(IC，k_{r1})。因此，我们能测试所有的(IC，k_{r1})检查是否分别用Logistic映射，Tent映射，Sine映射，Cubic映射加密P_1，P_2得到同样的C_1，C_2，同时测试是否用Sine映射加密P_2，P_3得到同样的C_2，C_3。为了检查所给的(IC，k_{r1})对是否是合法的，P_1分别用logistic映射，tent映射，sine映射或者Cubic映射加密成密文C_1，根据每个映射相应的迭代表达式使用系统参数λ和初值IC迭代k_{r1}次，迭代的最后值作为加密P_2的初值，然后P_2分别用每个映射相应的迭代表达式加密成密文C_2，使用系统参数λ和初值IC迭代k_{r1}次，这种测试重复检测的所有的IC和k_{r1}。

下面的伪代码说明这个过程。

输入

P_1，P_2，P_3和C_1，C_2，C_3

输出

IC和k_{r1}

Begin

For each possible value of i(256 values)，IC=i/256.0

For each possible value of Kr1(256 values)

Iterate logistic map Kr1 times starting from IC (express as X1[0])

Compute the ciphertext C11 of P_1

Iterate logistic map Kr1 times starting from X1 [Kr1]

Compute the ciphertext C12 of P_2，

If C11=C_1 and C12=C_2 then print IC，Kr1，1

Iterate tent map Kr1 times starting from IC (express as X2[0])

Compute the ciphertext C21 of P_1

Iterate logistic map Kr1 times starting from X2 [Kr1]

Compute the ciphertext C22 of P_2，

If C21=C_1 and C22=C_2 then print IC，Kr1，2

Iterate sine map Kr1 times starting from IC (express as X3[0])

Compute the ciphertext C31 of P_1

Iterate logistic map Kr1 times starting from X3 [Kr1]

Compute the ciphertext C32 of P_2，

If C31=C_1 and C32=C_2 then print IC，Kr1，3

Iterate logistic map Kr1 times starting from IC (express as X4[0])

Compute the ciphertext C41 of P_1

Iterate logistic map Kr1 times starting from X4 [Kr1]

Compute the ciphertext C42 of P_2，

If C41=C_1 and C42=C_2 then print IC，Kr1，4

Iterate sine map Kr1 times starting from IC (express as X5[0])

Compute the ciphertext C51 of P_2

Iterate logistic map Kr1 times starting from X5 [Kr1]

Compute the ciphertext C52 of P_3，

If C51=C_1 and C52=C_3 then print IC，Kr1，5

Next Kr1

Next i

End

当程序执行完毕，我们将得到正确的IC和K_{r1}。恢复其余的会话密钥是非常容易的，所需的明文/密文对等于每个其余明文/密文分组的第一块密文长度乘2。为了恢复会话密钥K_{r2}，需要密文C_1对应的明文P_1或者基于上面描述的被选择的密文C_{r2}对应的明文P_{r2}(r2表示第二分组的第一块)。我们迭代混沌映射j次(0≤j≤255)。为了检查j是否等于第二个被恢复的会话密钥K_{r2}，相应的混沌映射被迭代256次，并且比较每次迭代值对应的密文是否等于C_{r2}，如果相等，K_{r2}的值被恢复。但迭代过程可能不会结束以准备下一步的基于动态表DT2中初值。为了恢复其余的会话密钥，这个过程被重复。随着这种攻击的进行，密钥中会话密钥的顺序用等式(9)可以恢复。

当分组的块数为0表示没有迭代，因此第一个会话密钥(K_1)不能用这种方法恢复。为了找出K_1，K(0≤j≤255)作为K_1通过等式(4)和(5)用其余的会话密钥被计算K次(K_2,K_3…,Kn,n表示密钥的长度)。为了验证k是否等于第一个会话密钥(K_1)，等式(4)和(5)被执行256次并且算出的IC的每一个值和我们推出的正确的IC值进行比较。

为了验证上述攻击方法的有效性，在2.4GHZ、内存为256MB的Pentium Ⅴ机器上我们使用的是c++程序语言编写的恢复程序，执行时间少于20秒，其中K=3245A7BB4D596F3E88922A53，在例子中完整的密钥被恢复。

很明显上面我们使用了用选择密文攻击的方法恢复出完整的变长密钥，类似的也可以使用选择明文攻击方法，两者不同之处仅仅在于怎样选择明文/密文。

4 结论

总之，基于我们提出的攻击方法，参考文献[14]的混沌密码算法不能经受已知明文选择明文攻击以及选择密文攻击。实验表明我们提出的攻击所用的运算时间很少。其实要想克服攻击，只要将等式(10)产生的密文反馈到下一步混沌映射所需的初值、系统参数和迭代次数中，使初值、系统参数和迭代次数取值空间保持不变就可以了。

注释及参考文献：

[1]Baptista M S.Cryptography with chaos.Phys.Lett.A,1998,240:50-54.

[2]Wong W K,Lee L P,Wong K W.A modified chaotic cryptographic method.Comput Phys Commun,2000,138:234-236.

[3]Wong K W.A fast chaotic cryptography scheme with dynamic look-up table.Phys.Lett.A,2002,298:238-242.

[4]Wong K W,Ho S W,Yung C K.A chaotic cryptography scheme for generating short ciphertext.Phys.Lett.A,2003,310:67-73.

[5]Pareek N K,Patidar V,Sud K K.Discrete chaotic cryptography using external key.Phys.Lett.A,2003,309:75-82.

[6]Xiang T,Liao X F,Tang G P,Chen Y,Wong K W.A novel block cryptosystem based on iterating a chaotic map.Phys.Lett.A,2006,349:109-115.

[7]Yu W W,Cao J D.Cryptography based on delayed chaotic neural networks.Phys.Lett.A,2006,356:333-338.

[8]G.Álvarez,F.Montoya,M.Romera,G.Pastor.Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value.Chaos,Solitons and Fractals,2005,23:1749-1756.

[9]Yong Chen,Xiaofeng Liao.Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm.Phys.Lett.A,2005,342:389-396.

[10]G.Álvarez,F.Montoya,M.Romera,G.Pastor.Cryptanalysis of dynamic look-up table based chaotic cryptosystems.Phys.Lett.A,2004,326:211-218.

[11]G.Álvarez,F.Montoya,M.Romera,G.Pastor.Cryptanalysis of an ergodic chaotic cipher.Phys.Lett.A,2003,311:172-179.

[12]G.Álvarez,F.Montoya,M.Romera,G.Pastor.Cryptanalysis of a discrete chaotic cryptosystem using external key.Phys.Lett.A,2003,319:334-339.

[13]徐淑奖,王继志.一类改进的混沌迭代加密算法[J].物理学报,2008,57(1):37-41.

[14]N.K.Pareek a,b,Vinod Patidar a,K.K.Sud.Cryptography using multiple one-dimensional chaotic maps.Communications in Nonlinear Science and Numerical Simulation,2005,10:715-723.

Cryptanalysis on the Cryptography of the Chaotic Maps

ZHONG Qian-chuan

(Xichang College, Xichang, Sichuan 615013)

Abstract: Recently many chaotic cryptosystems based on the iterative equation have been proposed, but many of them can't resist the chosen ciphertext attack, chosen plaintext attack and known plaintext attack. In this letter, we analyze the existing problems of cryptography using multiple one-dimensional chaotic maps [14] presented by Pareek et al. and break it. This cryptosystem uses an external secret key of variable length (maximum 128-bits) to obtain the initial condition and number of iterations of four one-dimensional chaotic maps, but this way exists weaknesses of deriving the initial condition by using finite integer problem allowing for attack. So, the external secret key of variable length can be recovered with a little time using the chosen ciphertext attack or chosen plaintext attack.

Key words: Chaotic cryptosystem; Chaotic map; Block cipher