文章编号:1674-2869(2011)06-0094-04

一种混沌序列加密算法的密码分析

蔡 琼,彭 涛,叶 杨
(武汉工程大学 计算机科学与工程学院,湖北 武汉 430074)

摘 要:对一种基于 Logistic 混沌映射的序列加密算法进行安全性分析,此混沌序列具有前几个值对混沌初态的低位比特变化不敏感的信息泄漏规律,无法抵抗基于选择明文的密钥分割攻击,对此加密算法进行改进,使得密钥的吻合度分布趋向于随机化,能有效抵抗密钥分割攻击.

关键词:信息泄漏;分割攻击;吻合度
中图分类号:TN918.1 **文献标识码**:A **doi**:10.3969/j.issn.1674-2869.2011.06.022

1 混沌序列加密算法

由于混沌映射所具有的许多类似随机的性质和密码学中的混淆和扩散等性质相似,所以出现了很多混沌加密算法,本文分析的混沌序列密码算法使用的是 Logistic[1] 映射.

$$f(x)=\mu x(1-x),x\in[0,1],\mu\in[3.5699456,4] \tag{1}$$

当 $x\in[0,1],\mu\in[3.5699456,4]$ 时,Logistic 映射具有混沌效应.然而由于实数在计算机中以有限的精度实现,对于每次迭代产生的 x 可以表示如下:

$$x^{(n)}=\sum_{i=0}^{n-1}\frac{x_i}{2^i}$$

其中 n 表示精度.

明文分组长度是 64 bit,密钥是混沌的初始控制参数 x_0 和 μ.该加密算法如下四步:

a. 初始化,以初态 x_0 和控制参数 μ 迭代 N_0 次,得到 ω.即 $\omega=f_\mu^{N_0}(x_0)$.

b. 以 ω 为初态迭代 70 次,并取出每次迭代得到的二进制数 x_i^n 的第 k 位,得到一个 70 位的二进制随机序列 $\{x_{i(k)}^n\}_{i=1}^{70}$,将此随机序列分为两部分.

$$A_j=\{x_{i(k)}^n\}_{i=1}^{64},\ D_j=\sum_{i=0}^{5}2^{5-i}x_{i(k)}^n$$

其中 A_j 为 64bit 分组,D_j 为小于 64 的整数.

c. 加密明文分组,明文分组 M_j 对应的密文分组 $C_j=(M_j\ll D_j)\oplus A_j$.然后把密文块做一个映射,$\varphi(C_j)=c_j+c_{j+1}+\cdots+c_{j+7}$,$D^*=D_j+\varphi(C_j)\ \mathrm{mod}64$.

d. 如果所有的明文分组都被加密则加密结束,否则 $\omega=f^{D^*+70}(\omega)$,然后转到 **b** 继续加密.

2 加密系统的信息泄露规律以及攻击

虽然文献[2]对该加密系统进行了改进,但文献[3]指出了该加密算法对密钥的分割攻击存在安全隐患.加密算法步骤 **a** 实质上是为了掩盖混沌初态,来增加系统的安全性,但是如果以迭代之后的 ω 为初态,以参数 μ 产生的混沌序列,与以 x_0 为初态经过迭代之后产生的混沌序列是一致的.这样就可以把 ω 视为 x_0 的等效密钥,只要完成了对 $\{\omega,\mu\}$ 的攻击就完成了对加密系统的攻击.

在选择明文攻击条件下,选取第一个 64 bit 明文分组为全零分组,即 $M_1=(0,0,0,\cdots,0)$,C_1 为对应的密文分组,则由 $C_j=(M_j\ll D_j)\oplus A_j$ 知 $C_1=A_1$.即当第一个 64 bit 明文分组为全零时,其对应的密文分组就是随机序列的前 64 bit 值 $\{x_{i(k)}^n\}_{i=1}^{64}$.下面分析由 $\{x_{i(k)}^n\}_{i=1}^{64}$ 恢复等效密钥 $\{\omega,\mu\}$.

定理 1[4] 设 $x_0,x_1,x_2,\cdots$ 是利用混沌变换 $f(x)=\mu x(1-x)$,$0<x<1$ 由 m 精度的初值 x_0 产生的 m 精度小数序列,x_i' 是 x_i 的 n 精度小数,则在 x_i' 给定时,x_{i+1}' 至多有 5 种变化,且 $2^n x_{i+1}'$ 的可能取值范围是仅与 x_i' 有关的连续的整数.

定理 2[5] 设函数 $f(x)=\mu x(1-x)$,$\mu,\mu+\delta\in(3.5699456,4]$,$x,x+\varepsilon\in[0,1]$,则:

$$|f_\mu(x)-f_{\mu+\delta}(x+\varepsilon)|\leqslant 4|\varepsilon|+\frac{1}{4}|\sigma|.$$

证明:由于函数 $f(x)$ 在 $[0,1]$ 是连续可导的,则由拉格朗日中值定理知,存在

收稿日期:2011-01-06

作者简介:蔡 琼(1961-),女,湖北武汉人.副教授,硕士.研究方向:网络数据库及数据挖掘.

$$\xi_\mu\in[x,x+\varepsilon],\eta_{x+\delta}\in[\mu,\mu+\delta]$$

使得

$$f_\mu(x)-f_\mu(x+\varepsilon)=\frac{\partial}{\partial x}f_\mu(x)|_{x=\xi_\mu}\cdot|\varepsilon| \quad (2)$$

$$f_\mu(x+\varepsilon)-f_{\mu+\delta}(x+\varepsilon)=\frac{\partial}{\partial\mu}f_\mu(x)|_{\mu=\eta_{x+\delta}}\cdot|\delta| \quad (3)$$

将(2)、(3)两式相加得到

$$|f_\mu(x)-f_{\mu+\delta}(x+\varepsilon)|=\frac{\partial}{\partial x}f_\mu(x)|_{x=\xi_\mu}\cdot|\varepsilon|+\frac{\partial}{\partial\mu}f_\mu(x)|_{\mu=\eta_{x+\delta}}\cdot|\delta|$$

再由 $\left|\frac{\partial}{\partial x}f_\mu(x)\right|=|\mu(1-2x)|<4$

$$\left|\frac{\partial}{\partial\mu}f_\mu(x)\right|=|x(1-x)|=\left|\frac{1}{4}-\left(1-\frac{1}{2}\right)^2\right|<\frac{1}{4}$$

得到:$|f_\mu(x)-f_{\mu+\delta}(x+\varepsilon)|\leqslant 4|\varepsilon|+\frac{1}{4}|\delta|$

定理 1、2 说明,Logistic 混沌映射具有如下性质:输入的低位变化对输出的高位影响不大,而上述加密系统中的实际用来加密的二进制流,是由混沌映射反复迭代产生的,这就导致了混沌序列具有前几个值对混沌初态和参数的低位比特变化不够敏感的性质;由随机序列的产生方式知,当输入发生轻微变化时,输出几乎不变.从为了定量刻画这种性质,引入吻合度的概念.

定义[5]　设 k 和 k' 分别是某密码算法的正确密钥和试验密钥,$\{b_i\}_{i=1}^{\infty}$ 和 $\{b_i'\}_{i=1}^{\infty}$ 分别是它们产生的随机序列,则称 $\max\{t:\forall i,1\leqslant i\leqslant t,b_i=b_i'\}$ 为 k' 的吻合度.

将 $\{\omega^n,\mu^n\}$ 的吻合度记为 t_n,要从理论上精确分析 t_n 的分布规律是困难的.文献[4]用模拟分析方法给出了密钥为 64 bit,算法的吻合度分布的统计规律.

表 1　T_{16} **的分布规律**

Table 1　Regularities of distribution of T_{16}

T_{16}	<=8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	>=26
个数	98	72	116	193	314	398	459	559	589	626	583	598	569	517	490	398	349	301	2771

一般地有:$p(t_8\geqslant 9)=0.992\ 4$,$p(t_{16}\geqslant 9)=0.990\ 2$,$p(t_{24}\geqslant 9)=0.989\ 3$,$p(t_{32}\geqslant 29)=0.980\ 0$,$p(t_{40}\geqslant 37)=0.988\ 3$,$p(t_{48}\geqslant 46)=0.986\ 0$.

设$\{\omega,\mu\}$为正确的密钥,若同时穷举密钥中两个数的高 n bit,则 $t_n\geqslant t$ 吻合度的试验密钥的个数期望为 2^{2n-1},且吻合度 $t_n\geqslant t$ 的试验密钥中包含 $\{\omega^n,\mu^n\}$的概率为 $p(t_n\geqslant t)$.当试验密钥$\{\omega'^n,\mu'^n\}$与$\{\omega^n,\mu^n\}$不相等时,可认为由$\{\omega'^n,\mu'^n\}$产生的的序列与乱数序列相互独立,因而$\{\omega'^n,\mu'^n\}$产生的序列的吻合度 $t_n\geqslant t$ 的概率近似为 2^{-t},而由模拟试验知,$\{\omega^n,\mu^n\}$的吻合度 $t_n\geqslant t$ 的概率相对于 2^{-t}要大得多.据此就可将随机试验密钥$\{\omega'^n,\mu'^n\}$和$\{\omega^n,\mu^n\}$区分开.由上述模拟实验结果可知,利用已知明文采取先攻击高位密钥再攻击低位密钥的方法对这两个密码算法进行分割攻击,即依次攻击 k^8,k^{16},k^{24},k^{32},k^{40},k^{48},每次选取前者的候选密钥,可最终获得正确密钥,而不漏掉正确密钥的概率为:

$$p=p(t_8\geqslant 1)p(t_{16}\geqslant 9)p(t_{24}\geqslant 19)p(t_{32}\geqslant 29)p(t_{40}\geqslant 37)p(t_{48}\geqslant 46)=0.92\ 4\times 0.990\ 2\times 0.989\ 3\times 0.980\ 0\times 0.988\ 3\times 0.986\ 0\approx 0.928\ 4$$

即该加密系统是不安全可破的.

3　改进办法

针对上述问题,若要确保吻合度分布的合理性才能避免上述分割攻击,需引入比特矩阵.由于随机序列任然具有前几个比特对混沌初态和参数的低位比特变化不够敏感的性质,所以改变随机序列[6]的产生方式.

算法中,以初态 x_t 和参数 μ 迭代 100 次,并取出每次迭代得到的二进制数 x_i^n 的第 k 位,得到二进制序列$\{x_{i(k)}^n\}_{i=1}^{100}$,将此序列排列成一个 10×10 的矩阵 $\boldsymbol{M}_{10\times 10}$,并取二进制序列最后的 16bit 序列$\{x_{i(k)}^n\}_{i=85}^{100}$,表示为一个整数 N_i,最后计算 $\boldsymbol{M}^{N_i}$,将迭代之后的矩阵按行排列为二进制比特串:

$$\boldsymbol{M}_{10\times 10}=\underbrace{B_1B_2\cdots B_{64}}_{A_{j1}}\underbrace{B_{65}B_{66}\cdots B_{70}}_{A_{j2}}\underbrace{B_{71}B_{72}\cdots B_{100}}_{A_{j3}},B_i\in\{0,1\}$$

如果上式将 100 位比特串划分为 A_{j1}、A_{j2}、A_{j3}.其中将 A_{j2}表示为对 64 取模的整数 D_j.

将明文块 P_j 循环右移 D_j,获得一个新的块 P_j',对新的块 P_j'通过与 A_{j1}异或得到密文 C,然后执行下述操作:

$$C_j=P_j'\oplus A_{j1},f_1=(f(A_{j1})+f(A_{j3}))\bmod 64$$

$$C_j'=s(C_j,f_1)\oplus A_{j3},f_2=(f(A_{j1})+3f(A_{j3}))\bmod 64$$

$$C_j''=s(C_j',f_2)\oplus A_{j1}$$

其中,$s(c,n)$ 表示把 c 循环左移 n 位.

$$f(A)=\sum_{i=0}^{7}A_i$$

如果所有的明文块加密完毕则结束,否则执行下述操作,然后转至步骤(b).

$$D^*=D_j+f(C_j'')\bmod 64$$

$$\omega=f^{D^*+70}(\omega)$$

4 改进后的安全性分析

改进之后随机序列的产生方式改为在之前的随机序列基础上增加矩阵[7]的取模幂乘.然而增加矩阵幂乘运算会减慢加密的速度,采用以下算法,其法时间复杂度为 $O(\log_2^n)$(n 为矩阵迭代指数):

由于矩阵乘法具有结合律,如 $\boldsymbol{A}^4=\boldsymbol{A}^2\cdot\boldsymbol{A}^2$,因此有如下结论:当 n 为偶数时,$\boldsymbol{A}^n=\boldsymbol{A}^{(n/2)}\cdot\boldsymbol{A}^{(n/2)}$;当 n 为奇数时,$\boldsymbol{A}^n=\boldsymbol{A}^{(n/2)}\cdot\boldsymbol{A}^{(n/2)}\cdot\boldsymbol{A}$,($n/2$ 取整),依次递归计算,并在计算过程中不断对 2 取模,避免高精度运算.

4.1 初值敏感性分析

对混沌系统的初始条件进行微小变化,通过统计产生的二值序列中相应位置上的 1 和 0 的值的变化情况,计算相应的序列位变化率.位变化率的定义如下:

$$T=\frac{n'}{n}$$

其中 n 为序列长度,n'为初始条件进行微小改变后生成的二值序列与原序列比较,相应位变化的个数.取 $\mu=3.659\ 6$,比较随机序列的前 70 位得到的结果表 2 所示.

表 2 序列变化率

Table 2 Sequence rate

混沌系统初始条件	0.3	0.4	0.5	0.6	0.7
变化后的初始条件	0.300 001	0.400 001	0.500 001	0.600 001	0.700 001
原混沌系统位变化率	0.485 7	0.5	0.442 9	0.500 1	0.485 6
改进后位变化率	0.571 4	0.628 6	0.600 3	0.514 3	0.582 3
改进后相对于原随机序列的变化率	0.557 1	0.5	0.601 2	0.314 3	0.552 7

由表 2 可知,改进后的混沌系统比原系统有更好的初值敏感性,对于第一个全零的明文分组有:$C_1=(M\ll D_1)\oplus A_1$,知 $C_1=A_1$,但是从上表得知改进后的系统使得随机序列有了平均 50%以上的变化率,需要穷举至少 $C_{70}^{35}\approx 2^{70}$ 次才能恢复随机序列,对密钥的分割攻击的计算复杂度为 $C_{70}^{35}\cdot 2^{60}\approx 2^{130}$,有效地抵抗了密钥分割攻击.

4.2 密钥吻合度分析

取 $\mu=3.659\ 6$,密钥为 64 bit,随机选取 10 000个密钥统计得到如图 1～4 所示的吻合度分布图,其中虚曲线代表改进之后的吻合度分布,实线代表之前的吻合度分布.改进之后的吻合度分布趋向于随机化,即 $p(t_m\geqslant t$ 趋向于 2^{-t},故改进之后使得基于密钥的分割攻击变得无效.

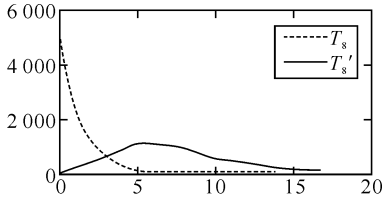

图 1 T_8 的分布规律

Fig. 1 Regularities of distribution of T_8

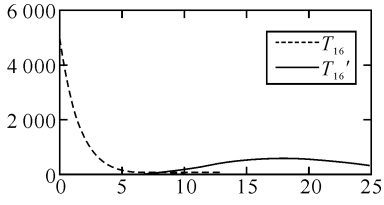

图 2 T_{16} 的分布规律

Fig. 2 Regularities of distribution of T_{16}

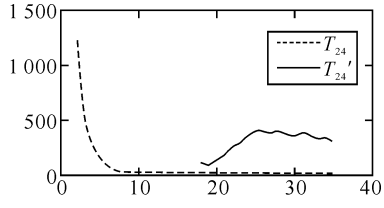

图 3 T_{24} 的分布规律

Fig. 3 Regularities of distribution of T_{24}

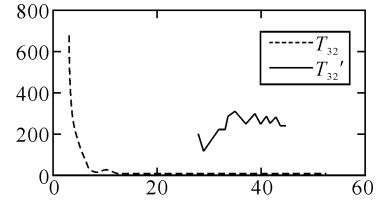

图 4 T_{32} 的分布规律

Fig. 4 Regularities of distribution of T_{32}

4.3 对于选择明文攻击

假设 P_z 与明文块长度相同(64 位),且全为 0,相应的密文为 C_z,则有下式(a);假设 P_s 与明文块长度相同(64 位),且第一位为 0,其他全为 1,相应的密文为 C_s,则有

$$s(s(s(P_z,D_j)\oplus A_{j1},f_1)\oplus A_{j3},f_2)\oplus A_{j1}=C_z s$$

$$(s(A_{j1},f_1)\oplus A_{j3},f_2)\oplus A_{j1}=C_z \tag{4}$$

$$s(s(s(P_s,D_j)\oplus A_{j1},f_1)\oplus A_{j3},f_2)\oplus A_{j1}=C_s \tag{5}$$

由式(4)和式(5)无法推导出 A_{j1},A_{j3},穷举 $2^{64}\cdot 2^{64}\cdot 64\cdot 64=2^{140}$ 次方可列举全部的组合.

5 结 语

针对一个基于混沌设计的分组密码算法所产生的混沌序列具有前几个值对混沌初态的低位比特变化不敏感,无法抵抗在选择明文攻击条件下对密钥的分割攻击,提出了增加矩阵取模幂乘运算,并改进算法中参数的控制,由密钥吻合度分布

实验可知,可基本确保任意两个不同的试验密钥产生的乱数序列相互独立,并且对初始值的变化有更好的敏感性,使得改进之后的算法,能抵抗对密钥的分割攻击和选择明文攻击.

参考文献:

[1] Xiang T, Liao X F, Tang G P, et al. A novel block cryptosystem based on iterating a chaotic map[J]. Physics Letters A, 2006(349): 109 - 115.

[2] Wang King-yuan, Yu Cang hai. Cryptanalysis and improvement on a cryptosystem based on a chaotic map [J]. Computers and Mathematics with Applications, 2009 (57): 476 - 482.

[3] 张涛. 一个混沌分组密码算法的分析[J]. 计算机应用研究, 2010, 27(6): 2294 - 2296.

[4] 金晨辉. 一个基于混沌的分组密码算法的分析[J]. 中国工程科学, 2001, 3(6): 75 - 80.

[5] 金晨辉, 高海英. 对两个基于混沌的序列密码算法的分析[J]. 电子学报, 2004, 32(7): 1066 - 1070.

[6] 杨建华. 数列组的广义线性相关性[J]. 武汉工程大学学报, 2009, 31(12): 79 - 81.

[7] 胡端平, 唐超. 一致矩阵的特征性质[J]. 武汉工程大学学报, 2009, 31(5): 93 - 94.

Cryptanalysis of chaotic sequence cipher

CAI Qiong*, *PENG Tao*, *YE Yang

(School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan 430074, China)

Abstract: This paper analzsed the security of a cipher based on a map of the logistic chaos sequence. However, the information leakage that the first several chaotic states generated by this encryption system were not sensitive to the change of the low order of initial input, makes the encryption system can not to resist the divide-and- conquer attacks, under the chosen plaintexts condition. The improvement, which making the distribution of coincidence degree of the keys tends to randomize, can effectively resist the attacks.

Key words: information leakage; divide-and-conquer attacks; coincidence degree

本文编辑:陈小平

☆

(上接第 94 页)

[6] Marvell 88W8686 Data Sheet. Integrated MAC/ Baseband/RF Low Power SoC IEEE802. 11a/g/b [EB/OL]. http://www. datasheet ardhive. com / 88%20Mawell-datacheet. htul, 2007.

[7] Aam-linux-gcc cross-compilation sites [EB/OL]. http://www. codesourcery. com/sgpp/lite/arm/ portal/release, 644.

[8] Linux-2. 6. 28 Sourece sites[EB/OL]. http://www. kernel. org/pub/linux/kernel/v2. 6/linux-2. 6. 28. 9. tar. gz.

Design of WLAN adapter device driver based on SPI

***SHENG Li-li*[1], *WANG Zhong*[1], *WANG Chun-li*[1], *WANG Hao*[2]**

(1. School of Computer Science and Engineering, Wuhan Insitute of Technology, Wuhan 430074, China;
2. School of Electranic Information, Wuhan University, Wuhan 430072, China)

Abstract: This paper introduces the design and realization of the Marvell 88W8686 WLAN adapter Linux device driver. It can be used on Electrocardio monitoring instrument and Hand-held data acquisition system. To start with the work, the software and hardware embedded development framework is established. Next, the Linux kernel rebuild and net device driver research are accomplished. In addition, the Marvell 88W8686 adapter device driver is modified and cross-compiled. Finally the Marvell 88W8686 WLAN adapter device driver is immigrated from X86 structure to ARM. Furthermore, the embedded WLAN based on ARM platform is established.

Key words: ARM; embedded Linux; WLAN adapter; 802. 11g; device driver　　本文编辑:陈小平