第 57 卷 第 5 期 2008 年 5 月
1000-3290/2008/57(05)/2737-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.5,May,2008

一种基于混沌的带密钥 hash 函数的碰撞问题及分析*

王继志[1)] 王美琴[2)] 王英龙[1)]

1)(山东省计算中心,济南 250014)

2)(山东大学密码技术与信息安全教育部重点实验室,济南 250100)

(2007 年 6 月 26 日收到;2007 年 9 月 17 日收到修改稿)

指出了一类基于混沌映射构造带密钥单向 hash 函数算法的碰撞问题,并对其产生的机理进行了初步分析,给出了数字化混沌序列非奇异的定义,证明了数字化混沌序列非奇异的充要条件,并分析了变参数离散混沌动力系统数字化后序列的周期性.分析结果表明这类算法产生碰撞的原因是其对混沌映射的数字化导致混沌序列的奇异性,因此必须谨慎选择混沌映射的数字化方法以保证混沌序列的非奇异性.

关键词:混沌,带密钥散列函数,碰撞,非奇异性

PACC:0545

1. 引 言

混沌是一种动力学行为,混沌现象表面上看起来是随机的、不可预测的,但实际上却是按照严格而且常常是简单的规律发生变化的一种自然现象,可以利用简单的数学表达式产生复杂的混沌行为.因此,混沌的这种性质在现代密码学中具有重要的应用价值.目前,已有很多文献提出了基于混沌映射构造带密钥的单向 hash 函数的算法[1—5].其中文献[1]提出了一种基于混沌神经网络的带密钥的单向 Hash 函数构造方法.该方法通过使用以混沌分段线性函数作为输出函数的神经网络和基于时空混沌的密钥生成函数实现明文和密钥信息的混淆和扩散.然而,通过仔细考察,发现该算法比较容易构造明文对,使得明文对的 hash 值在同一密钥下发生碰撞,不满足 hash 函数的抗碰撞性;也比较容易构造密钥对,使得对同一明文的 hash 值发生碰撞,不满足对密钥的敏感性.

本文首先指出该算法所存在的问题,对产生该问题的原因进行了初步分析,给出了混沌序列非奇异的定义,分析结果表明保证数字化混沌序列的非奇异性是避免该问题产生的方法.

2. 碰撞问题

2.1. 原算法概述

文献[1]中的算法将 256 位的明文块映射为 128 位的 Hash 值,其中密钥为 128 位.映射采用混沌神经网络,具有输入和输出两层结构,输入层具有 8 个节点,输出层具有 4 个节点.具体算法如下:

1)256 位的明文块分成 32 个 8 比特的数据,其中每 4 个 8 比特的数据为一组,记为 $P_{0,0}\ P_{0,1}\ P_{0,2}\ P_{0,3}\cdots P_{7,0}\ P_{7,1}\ P_{7,2}\ P_{7,3}$ 共 8 组.

2)每组 4 个 8 比特数据 $P_{i,0}\ P_{i,1}\ P_{i,2}\ P_{i,3}\ i=0,1,\cdots,7$,通过固定权值 $[1/2^8\ \ 1/2^{16}\ \ 1/2^{24}\ \ 1/2^{32}]$,即

$$P_i = P_{i,0}/2^8 + P_{i,1}/2^{16} + P_{i,2}/2^{24} + P_{i,3}/2^{32}$$

转化为[0,1]之间的小数.

3)将 $P_i\ i=0,1,\cdots,7$ 分别输入 8 个输入层节点,其节点的传递函数为

$$f(x,Q)=\begin{cases} x/Q, & 0\leqslant x<Q,\\ (x-Q)/(0.5-Q), & Q\leqslant x<0.5\\ (1-Q-x)/(0.5-Q), & 0.5\leqslant x<1-Q,\\ (1-x)/Q, & 1-Q\leqslant x\leqslant 1, \end{cases} \tag{1}$$

* 山东省自然科学基金(批准号:Y2006A27)资助的课题.

其中 Q 取 1/3,迭代次数取 40.

4)128 位密钥分为 4 个 32 位整数,除以 2^{32} 量化为[0,1]之间的小数 k_1 k_2 k_3 k_4,按下式进行迭代:

$$x_1(i+1) = (1-\varepsilon)g(x_1(i)) + \varepsilon g(x_4(i)),$$
$$x_2(i+1) = (1-\varepsilon)g(x_2(i)) + \varepsilon g(x_1(i)),$$
$$x_3(i+1) = (1-\varepsilon)g(x_3(i)) + \varepsilon g(x_2(i)),$$
$$x_4(i+1) = (1-\varepsilon)g(x_4(i)) + \varepsilon g(x_3(i)),$$

其中 $\varepsilon = 1/3$,g 为 Logistic 映射 $x(i+1) = 4x(i)(1-x(i))$.

连续取 10 个每隔 30 步迭代的系统状态值,其中前 8 个 4 维状态值作为输入层神经元到输出层神经元的连接权值 W,其后的 2 个 4 维状态值分别作为阈值矢量 Θ 和控制参数矢量 Q.

5)输出层 4 个节点的输出按下式计算:

$$c = f(\mathrm{mod}(wU + \Theta, 1), Q),$$

其中,U 为输入层的输出,迭代 40 次.

将 4 个输出层输出连接起来即为 128 位 hash 值.

2.2. 构造明文对碰撞

首先考察神经元传递函数 $f(x,Q)$ 的性质.

命题 1 $f(x,Q) = f(1-x,Q)$.

证明 当 $0 \leqslant x < Q$ 时,显然 $1-Q < 1-x \leqslant 1$,所以

$$f(x,Q) = x/Q,$$
$$f(1-x,Q) = (1-(1-x))/Q = x/Q,$$

因此

$$f(x,Q) = f(1-x,Q).$$

当 $Q \leqslant x < 0.5$,$0.5 \leqslant x < 1-Q$,$1-Q \leqslant x < 1$ 时,同样可证 $f(x,Q) = f(1-x,Q)$.

因此命题 1 得证.

命题 2 若有两组 4 个 8 比特的数据 a_0 a_1 a_2 a_3 和 b_0 b_1 b_2 b_3,满足

$$a_0/2^8 + a_1/2^{16} + a_2/2^{24} + a_3/2^{32} = 1 - (b_0/2^8 + b_1/2^{16} + b_2/2^{24} + b_3/2^{32}), \quad (2)$$

则明文对 a_0 a_1 a_2 a_3 $P_{1,0}$ $P_{1,1}$ $P_{1,2}$ $P_{1,3}$ … $P_{7,0}$ $P_{7,1}$ $P_{7,2}$ $P_{7,3}$ 和 b_0 b_1 b_2 b_3 $P_{1,0}$ $P_{1,1}$ $P_{1,2}$ $P_{1,3}$ … $P_{7,0}$ $P_{7,1}$ $P_{7,2}$ $P_{7,3}$ 在同一密钥 K 下得到的 hash 值相等.

该命题的证明是显然的.根据命题 1,两个明文在步骤 3)中得到的一次迭代值是完全相同的,因此 40 次迭代值也是完全相同的,由于输出层的输出只与密钥、输入层的输出有关,显然在同一密钥 K 下得到的 hash 值相等.

(2)式很容易满足,例如,$a_0 = 64$,$a_1 = a_2 = a_3 = 0$,$b_0 = 192$,$b_1 = b_2 = b_3 = 0$,满足(2)式.

2.3. 构造密钥对碰撞

首先考察 Logistic 映射的性质.

对于映射 $g(x) = 4x(1-x)$,显然有

命题 3 $g(x) = g(1-x)$.

命题 4 若两个 32 位整数 a 和 b,满足

$$a/2^{32} = 1 - b/2^{32},$$

则密钥对 a k_2 k_3 k_4 和 b k_2 k_3 k_4 在同一明文下,得到的 hash 值相等.

该命题的证明是显然的.两个密钥在步骤 4)中得到的一次迭代值是完全相同的,因此得到的参数 W,Θ 和 Q 也是完全相同的,所以在同一明文下得到的 hash 值相等.

3. 分 析

从上文的分析可以看出,原算法不满足抗碰撞性和密钥敏感性,主要是在从二进制数向小数的转换过程中,由于混沌映射的对称性,导致不同的二进制数映射为同一小数,从而产生 hash 值的碰撞.

下面推广到一般情况,分析该问题是如何产生的以及如何避免.

3.1. 前提条件

下面主要研究形如(3)式的一维离散混沌系统

$$x_{n+1} = f(x_n, \mu),\ n = 0,1,2,\cdots,\quad x \in R \text{ 且 } x \in [a,b], \quad (3)$$

其中,μ 为参数,R 为实数集.

如果在迭代过程中,参数 μ 恒定不变,则称(3)式为定参数离散混沌动力系统;否则,称(3)式为变参数离散混沌动力系统.

在基于(3)式构造密码算法时,需要将明文的二进制数转换为有限精度的实数,反过来说也就是离散混沌系统的数字化,以生成混沌序列.一般的方法是采用线性变换,如用 m bit 二进制数表示实数 x_n,即在区间[a,b]上等间隔的选择 2^m 个离散点,分别用 0,1,2,…,2^m-1 表示.例如,用 0 表示 a,用 1 表示 $a+(b-a)/2^m$,用 2 表示 $a+2(b-a)/2^m$,以此类推,用 2^m-1 表示 $a+(2^m-1)(b-a)/2^m$.若用

y_n 表示数字化后的数值，则

$$x_n = a + y_n(b-a)/2^m. \tag{4}$$

将(4)式代入(3)式得

$$y_{n+1} = g(y_n,\mu) = \left[\frac{2^m}{b-a}\left(f\left(a+\frac{y_n(b-a)}{2^m},\mu\right)-a\right)\right], \tag{5}$$

其中，[ ]表示取整运算.

由于 y_n，y_{n+1} 是 m bit 二进制整数，而(5)式右边一般是浮点运算，因此计算的最后结果需要取整(如果直接用浮点数进行运算，取有限精度就相当于这里的取整运算).

观察(5)式可以看出，其产生序列的方法与一级 q 元反馈移位寄存器的结构是类似的，如图 1 所示.

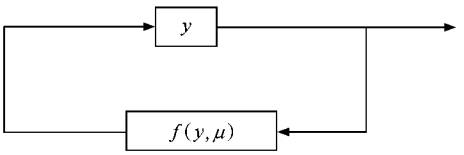

图 1　一级反馈移位寄存器

下面，以反馈移位寄存器的观点来考察(5)式.

3.2. 非奇异性

对于数字化定参数离散混沌动力系统

$$y_{n+1} = g(y_n,\mu), n = 0,1,2,\cdots, \quad y_n \in \{0,1,2,\cdots,2^m-1\}, \tag{6}$$

从任何一个初值 y_0 出发，通过(6)式的迭代运算，可以得到序列 $y_0, y_1, y_2, \cdots$，因此至多迭代 2^m 次，必有

$$y_{i+k} = y_i.$$

这样，从 y_i 到 y_{i+k-1} 就构成了一个循环序列，其周期为 k. 如果把 y 的每一个取值看作一个状态，可得到如图 2 所示的状态转移图.

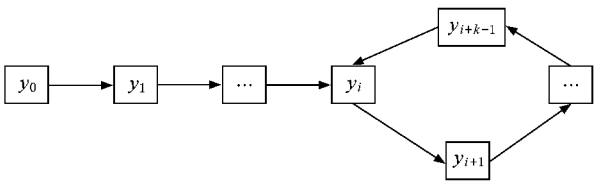

图 2　状态转移

从图 2 可以看出，文献[1]中算法之所以存在碰撞问题，就是因为它所产生的数字化混沌序列的状态图存在分枝点，即对于 y_i，存在两个先导节点 y_{i-1} 和 y_{i+k-1}，使得

$$g(y_{i-1},\mu) = g(y_{i+k-1},\mu),$$

从而导致最后的 hash 值存在碰撞.

显然，对于某一离散混沌映射来说，其全部状态转移可能是由几个类似图 2 的状态转移图构成的. 那么是否存在状态转移是由有限个彼此没有公共顶点的圈所构成的情况，也就是说状态图中不存在分枝节点 如果存在，满足这一要求的充要条件是什么，下面来讨论这一问题.

首先类似于反馈移位寄存器非奇异的定义[6]，给出离散混沌映射数字化序列非奇异的定义.

定义 1　如果一个离散混沌映射数字化后的序列状态图是由有限个彼此没有公共顶点的圈所构成，则称此离散混沌映射数字化后的序列是非奇异的，否则称之为奇异的.

定理 1　一个离散混沌映射数字化后序列非奇异的充要条件是对于 $x \neq y$，$x, y \in \{0,1,2,\cdots,2^m-1\}$，定参数数字化离散混沌映射 $g(x,\mu)$，方程

$$g(x,\mu) - g(y,\mu) = 0$$

无解.

证明　必要性.

根据非奇异的定义，状态图是由有限个圈构成的，即状态图不存在分枝点，也就是说不存在两个点 x, y，且 $x \neq y$，使得 $g(x,\mu) = g(y,\mu)$，即方程 $g(x,\mu) - g(y,\mu) = 0$ 无解.

充分性.

由于方程 $g(x,\mu) - g(y,\mu) = 0$ 无解，也就是说不存在两个不同的离散点，使得他们映射到同一个点，也就是状态图中不存在分枝节点，所以序列是非奇异的.

证毕.

推论 1　如果一个离散混沌映射 $f(x_n,\mu)$ 数字化时，所取的离散点中存在 $x_i, x_j, i \neq j$，使得 $f(x_i,\mu) = f(x_j,\mu)$，则该离散混沌映射数字化后是奇异的.

该推论的证明是显然的. 因为若存在 $x_i, x_j, i \neq j$，使得 $f(x_i,\mu) = f(x_j,\mu)$，则必有数字化后的函数 $g(x_i,\mu) = g(x_j,\mu)$，因此该函数产生的序列是奇异的.

再回到文献[1]的算法. 根据推论 1，显然存在不相等的离散点，使得神经元的传递函数 $f(x,Q)$ 相等，即该离散混沌映射数字化后是奇异的. 因此可以

把数字化混沌序列是否奇异作为一个判定条件，即若数字化混沌序列是奇异的，则比较容易构造不同的明文，使得它们的迭代值相等.

下面以一个简单的分段线性映射为例来说明如何选择离散点以保证数字化混沌序列的非奇异性.

分段线性映射

$$x_{n+1} = f(x_n,\mu) = \begin{cases} 1 + \mu x_n, x < 0, \\ 1 - \mu x_n, x \geqslant 0, \end{cases} \tag{7}$$

取参数 $\mu = 2$，$x_n \in [-1,1]$，得到如图 3 所示的迭代结果，可以看出在区间 $[-1,1]$ 中有明显的混沌现象发生.

下面对该离散混沌映射进行数字化.

首先采用线性变换.

假设用 7bit 二进制数表示 x_n，用 y_n 表示，则 $y_n \in \{0,1,2,\cdots,127\}$，也就是说需要在区间 $[-1,1]$ 之间选择 128 个离散的点. 如果按下式等间隔进行选取：

$$x_n = 2y_n/128 - 1,$$

则存在 $y_n = 1$ 和 $y_n = 127$，使得

$$\begin{aligned} f(2 \times 1/128 - 1, 2) &= 1 + 2(2 \times 1/128 - 1) \\ &= -124/128, \\ f(2 \times 127/128 - 1, 2) &= 1 - 2(2 \times 127/128 - 1) \\ &= -124/128, \end{aligned}$$

即

$$f(2 \times 1/128 - 1, 2) = f(2 \times 127/128 - 1, 2).$$

根据推论 1，可得该映射数字化后的序列是奇异的. 因此该方法是不可行的.

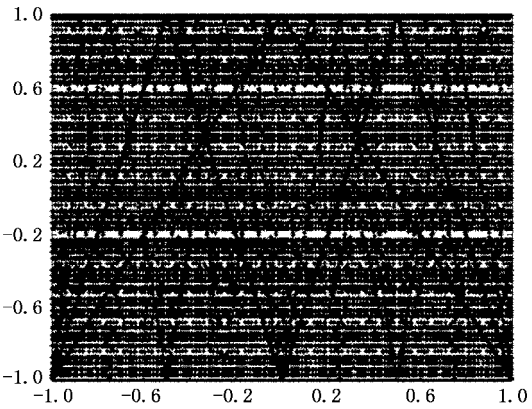

图 3 分段线性映射

由于该函数是关于 $x = 0$ 对称的，下面给出另外一种取点的方法：

$$\begin{aligned} x_n &= \frac{2(y_n + 0.5)}{128} - 1, y_n < 64, \\ x_n &= \frac{2y_n}{128} - 1, y_n \geqslant 64 \end{aligned} \tag{8}$$

该方法采用分段线性变换，避开了使 $f(x_i,\mu) = f(x_j,\mu)$ 的点，因此是可行的. 如图 4 所示，(b) 是 (a) 的局部放大.

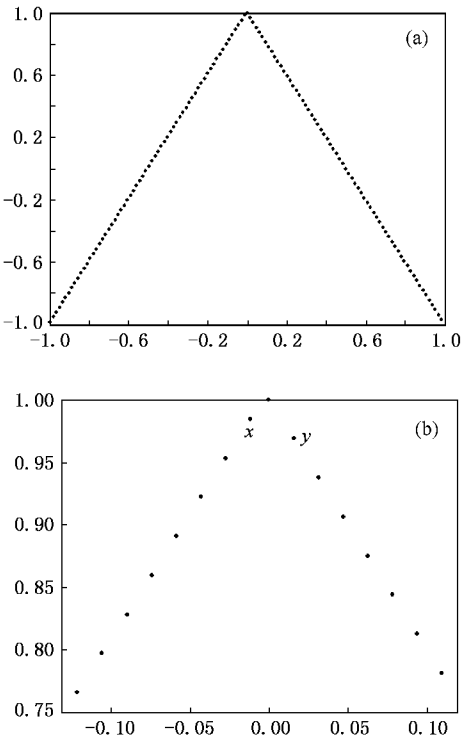

图 4 数字化映射取点

根据 (5) 式，由于最后结果要进行取整运算，如果只是在选取离散点时避开了使 $f(x_i,\mu) = f(x_j,\mu)$ 的点，仍不能保证数字化后的序列是非奇异的. 例如，如图 4(b) 所示的 x，y 两点，如果这两点的函数值之差小于 $(b-a)/2^m = 1/64$，则取整运算后，这两个点可能取整为同一个整数，导致序列奇异. 因此要保证类似这两点的函数值之差大于选取离散点的间隔距离，才能保证取整运算后，取整为不同的整数，即需满足

$$|f'(x,\mu)| \geqslant 2,$$

其中 f' 表示 f 的一阶导数.

那么对于导数的绝对值小于 2 的分段线性映射函数，是不是数字化后的序列肯定是奇异的？答案是否定的，因为可以选择 f 的多次迭代作为一次迭代. 例如，假设 $|f'(x,\mu)| = k < 2$，取 n 次迭代作为一次迭代，即

$$\underbrace{f(f(\cdots f(f(x))))}_{n\text{个}f},$$

求其一阶导数

$$\underbrace{f'(\underbrace{f(\cdots f(x))}_{n-1\text{个}f})\cdot f'(\underbrace{f(\cdots f(x))}_{n-2\text{个}f})\cdot\cdots\cdot f'(n)}_{\text{共}n\text{个}} = k^n,$$

对于 $k>1$，则总可以找到一个 n，使得 $k^n \geqslant 2$.

但是在具体的数字计算中发现，分段线性映射函数本身满足该条件，多次迭代作为一次迭代，可能会导致原先不相等的离散点反而相等，情况比较复杂.

另外，对于不是分段线性的情况，如抛物线映射

$$x_{n+1} = 1 - 4(x_n - 0.5)^2, x_n \in [0,1],$$

在 $x_n = 0.5$ 时，无论迭代多少次，其一阶导数都等于 0，这时可以采用不等间隔取点，即斜率 f' 大的地方取的间隔小，斜率 f' 小的地方取的间隔大，只要函数值的区间距离大于 $1/f'$ 个选取离散点的区间距离，仍可以保证取整运算后不会取整为同一整数.

根据上述结论，(7)式采用(8)式的取点方法，经计算(最后取整运算采用四舍五入)可得，其状态图是由 2 个周期为 36 的圈，1 个周期为 35 的圈，1 个周期为 18 的圈，1 个周期为 3 的圈，共 5 个圈构成的，如下：

1)0,1,3,7,15,31,63,127,2,5,11,23,47,95,66,124,8,17,35,71,114,28,57,115,26,53,107,42,85,86,84,88,80,96,64(周期 35).

2)4,9,19,39,79,98,60,121,14,29,59,119,18,37,75,106,44,89,78,100,56,113,30,61,123,10,21,43,87,82,92,72,112,32,65,126(周期 36).

3)6,13,27,55,111,34,69,118,20,41,83,90,76,104,48,97,62,125(周期 18).

4)12,25,51,103,50,101,54,109,38,77,102,52,105,46,93,70,116,24,49,99,58,117,22,45,91,74,108,40,81,94,68,120,16,33,67,122(周期 36).

5)36,73,110(周期 3).

这说明上述方法是有效的，数字化后的混沌序列是非奇异的.

然而上述方法仍然可能存在短周期现象，这对密码算法来说是有害的，最好是能生成全字长的 M 序列，以避免算法陷入到短周期. 如何生成 M 序列还需要进一步研究.

3.3. 变参数离散混沌映射的周期

文献[1]中的算法是将明文作为迭代初值，密钥作为控制参数，而文献[5]中的算法采用相反的做法，即将密钥作为迭代初值，明文作为控制参数，因此有必要考察变参数离散混沌映射的周期性，以防止混沌序列陷入到短周期序列中.

考察下述变参数离散混沌动力系统：

$$x_{n+1} = f(x_n,\mu_n),\ n = 0,1,2,\cdots$$
$$\mu_{n+1} = g(\mu_n),$$

如果 μ_n 是周期为 P_g 的序列，对于任意 μ_m，定参数离散混沌序列 $x_{n+1}=f(x_n,\mu_m)$ 均为非奇异的，周期均为 P_f，且对于任意两个参数，其数字化序列皆不是移位等价的，则有下述定理.

定理 2　根据上述前提条件，对于变参数离散混沌动力系统数字化后序列的周期 P，有

$$P = mP_g, m \text{ 为自然数且 } 1 \leqslant m \leqslant P_f.$$

证明　对于变参数离散混沌映射可以转化为 P_g 个定参数离散混沌映射函数，如下式所示：

$$x_{n+1} = f(x_n,\mu_0), n \bmod P_g = 0,$$
$$x_{n+1} = f(x_n,\mu_1), n \bmod P_g = 1,$$
$$x_{n+1} = f(x_n,\mu_2), n \bmod P_g = 2,$$
$$\cdots$$
$$x_{n+1} = f(x_n,\mu_{p_g-1}), n \bmod P_g = P_g - 1.$$

下面先证 $P = mP_g, m$ 为自然数. 用反证法.

假设 $P \bmod P_g = k,\ k\neq 0$，则不失一般性

$$x_0 = x_P,$$
$$x_1 = x_{P+1},$$

所以

$$f(x_0,\mu_0) = f(x_p,\mu_k) = f(x_0,\mu_k).$$

由于 $k\neq 0, \mu_0 \neq \mu_k$，上式与条件中对于任意两个参数，其数字化序列皆不是移位等价矛盾.

所以 $k = 0$.

下面证明 m 的范围为 $1\leqslant m\leqslant P_f$.

$m\geqslant 1$ 是显然的.

对于任意 μ_m，定参数离散混沌序列 $x_{n+1} = f(x_n,\mu_m)$ 只有 P_f 个状态，那么从初值 x_0 出发，最理想的情况就是把 P_f 个状态遍历一遍，再回到 x_0，也就是 $m = P_f$.

所以 $1\leqslant m\leqslant P_f$.

证毕.

从定理 2 可以看出，变参数混沌序列的周期主要是由控制参数序列的周期性决定的，这表明应用该方法设计密码算法时，关键的是参数序列的迭代函数，而不是初始状态的迭代函数.

4. 结 论

本文对文献[1]中的算法进行了仔细地考察,指出其中存在的碰撞问题,并从一般情况出发,得出了一个判定条件,即若数字化后的混沌序列是奇异的,则比较容易构造明文对,使得它们的迭代值相同.

同时对定参数混沌映射的数字化及变参数混沌映射的周期进行了讨论.对于定参数离散混沌映射,其数字化时需要注意两个问题:一是要避开使得映射函数值相等的离散点;一是所选取的离散点中函数值接近的任意两个点,取整运算后不能取整为同一个整数,如果映射函数不满足这个条件,可以把多次迭代作为一次迭代,使得该条件满足.但也可能出现映射函数本身满足该条件,多次迭代作为一次迭代反而不满足该条件,情况比较复杂,需要具体分析.

对于变参数离散混沌映射函数,其数字化后的序列周期,主要是由参数序列的迭代周期决定的,因此在设计密码算法时要重点关注于参数序列迭代函数的选取.

[1] Liu G J, Shan L, Dai Y W, Sun J S, Wang Z Q 2006 *Acta Phys. Sin.* **55** 5688 (in Chinese) [刘光杰、单 梁、戴跃伟、孙金生、王执铨 2006 物理学报 **55** 5688]

[2] Liu J D, Yu Y M 2007 *Acta Phys. Sin.* **56** 1297 (in Chinese) [刘建东、余有明 2007 物理学报 **56** 1297]

[3] Wei P C, Zhang W, Liao X F, Yang H Q 2006 *Journal on Communications* **27**(9) 27 (in Chinese) [韦鹏程、张 伟、廖晓峰、杨华千 2006 通信学报 **27**(9) 27]

[4] Li H D, Feng D G 2003 *Chinese Journal of Computer* **26** 460 (in Chinese) [李红达、冯登国 2003 计算机学报 **26** 460]

[5] Sheng L Y, Li G Q, Li Z W 2006 *Acta Phys. Sin.* **55** 5700 (in Chinese) [盛利元、李更强、李志炜 2006 物理学报 **55** 5700]

[6] Xiao G Z, Liang C J, Wang Y M 1985 *The theory and applications of pseudo-random sequence* (Beijing: National defence industry press) 39 (in Chinese) [肖国镇、梁传甲、王育民 1985 伪随机序列及其应用(北京 国防工业出版社)第 39 页]

The collision of one keyed hash function based on chaotic map and analysis*

Wang Ji-Zhi[1)] Wang Mei-Qin[2)] Wang Ying-Long[1)]

1) (*Shandong Computer Science Center*, *Jinan* 250014, *China*)

2) (*Key Laboratory of Cryptography & Information Security Ministry of Education*, *Jinan* 250100, *China*)

(Received 26 June 2007; revised manuscript received 17 September 2007)

Abstract

The collision of a keyed hash function based on chaotic map is pointed out. Its principle is analyzed in theory. The definition of the nonsingularity is presented based on analyzing digital discrete chaotic sequence. The necessary and sufficient conditions for the nonsingularity is deduced. The period of digital discrete chaotic sequence with variable parameter is discussed. The result shows that the singulartiy of chaotic sequence leads to the collision of the hash function. So the digital method of chaotic map must be chosen carefully to ensure the nonsingularity of chaotic sequence.

Keywords: chaos, keyed hash function, collision, nonsingularity

PACC: 0545

* Project supported by the Natural Science Foundation of Shangdong Province, China (Grant No. Y2006A27).