文章编号 1004-924X(2010)09-2101-08

基于轨道扰动的混沌单向散列函数设计

李佩玥[1,2],古 力[3],隋永新[1],杨怀江[1]
(1.中国科学院 长春光学精密机械与物理研究所 应用光学国家重点实验室,吉林 长春 130033;
2.中国科学院 研究生院,北京 100039;3.南开大学 信息技术科学学院,天津 300071)

摘要:在分析针对数字混沌提出的伪随机扰动策略和变参数补偿策略的基础上,提出了基于轨道扰动的混沌单向散列函数设计方法。首先,将消息填充为 64 byte 的整数倍,以提高短消息散列的安全性;然后,选取 64 byte 的固定扰动向量,并将明文信息与固定扰动向量一起映射至数字混沌系统相空间的扰动空间;最后,将扰动空间内的元素输入至数字混沌系统进行多次混沌迭代,并在迭代结果中取出 160 bit 作为最终散列值。该算法选用 Logistic 映射作为混沌映射,计算复杂度比高维混沌映射低,而轨道扰动的思想使得该算法比一般的低维混沌映射安全性更高。研究表明,该算法对初值极其敏感,且具有很好的混乱和扩散性质及较高的抗碰撞性。该算法采用 256 bit 定点数运算,更易于软硬件实现。

关 键 词:单向散列函数;混沌映射;轨道扰动
中图分类号:TP391;TP311 **文献标识码**:A **doi**:10.3788/OPE.20101809.2101

Design of chaotic one-way hash function based on orbit perturbation

LI Pei-yue[1,2], GU Li[3], SUI Yong-xin[1], YANG Huai-jiang[1]

(1. *State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130033, *China*;
2. *Graduate University of Chinese Academy of Sciences, Beijing* 100039, *China*;
3. *College of Information Technology Science, Nankai University, Tianjin* 300071, *China*)

Abstract: On the basis of analysis on the pseudo-random perturbation policy and Variable Parameter Compensation(VPCM) policy for digital chaotic system, a method to design the chaotic one-way hash function based on the orbit perturbation is proposed. In order to improve the security of short message hashing, the message is padded to be a multiple of 64 byte. Then, the length fixed perturbation of 64 bytes length is chosen, and the perturbation together with the padded message are mapped to the perturbation space of digital chaotic system. Finally, the digital chaotic system is iterated multiple times by using the elements of the perturbation space as inputs, and a hash value with 160 bit length is extracted from the results. The proposed algorithm uses the logistic mapping as the chaotic mapping, of which the computational complexity is lower than the one that has a reasonable high dimension. As the orbit perturbation is introduced the algorithm, its security is higher than that of common one. The results indicate that the algorithm is sensitive to the initial message comparatively and shows good

收稿日期:2010-05-10;**修订日期**:2010-07-26.
基金项目:国家 973 重点基础研究发展规划项目(No. 2007CB311201)

confusion and diffusion properties. Moreover, the fix-point operations with 256 bits are used in the proposed algorithm, and it is easy to be completed by software or hardware.

Key words: one-way hash function; chaotic mapping; orbit perturbation

1 引　言

单向散列函数是数字签名与认证、数据完整性检测等应用中必不可少的工具之一，其功能是将任意长度的消息压缩为固定长度的散列值，其压缩过程既可以看作是数学意义上的压缩变换，亦可以与物理学中耗散系统随时间的演化过程相对应。

混沌系统是一种比较典型的能量耗散系统。混沌变换所具有的混合、对参数和初值极端敏感等基本特性与密码学中“扩散”和“混乱”两个基本密码设计原则有着天然的联系。“混沌密码学”于 20 世纪 80 年代提出，此后，在密码学领域掀起了一次关于混沌密码的研究热潮[1-3]。2005 年，王小云等人提出了针对传统散列算法的模差分攻击方法，此后，用混沌系统构造散列函数成为了一个新的研究热点。

近年来，国内有越来越多的人投入到了混沌散列函数的研究领域，混沌散列函数的设计方法也层出不穷[4-9]。2006 年，王继志等人在文献[10]中分析了一类基于混沌映射构造散列函数方法的碰撞缺陷，并提出了基于混沌映射的单向散列函数构造方法应注意的几个问题。通过对已掌握文献的分析发现，在其思想的影响下，目前在混沌散列函数的设计过程中主要存在以下两种趋势：

(1) 将消息映射到参数空间而非相空间

这一点是比较容易理解的，因为将从物理意义上讲，消息映射到参数空间实现了混沌系统在不同吸引子之间的跳跃[11]，既延长了轨道周期，又使得跳跃过程难以预测；而将消息映射到相空间则会产生一条固定的轨道，若取该轨道上的其他点作为初值迭代，仍会得到同样的一条轨道，进而产生碰撞[10]。

(2) 低维混沌系统很难保证混沌散列函数的安全性

其原因主要是：高维混沌系统的相空间要比低维混沌系统的相空间复杂得多，而密码学又是以“扩散”与“混乱”为基本原则，故而高维映射因其复杂而为首选，低维映射因其简单而很难保证安全。

以上两点固然有其合理的一面，但由此带来的问题却是不可忽略的：

(1) 散列运算速度降低

复杂数字混沌系统在迭代过程中需要进行大量的乘加运算，且常需要以通过增加迭代次数的方式来提高散列函数的安全性，这些因素都严重降低了散列函数的运算速度。

(2) 高维混沌系统的轨道不可控

参数是控制确定性系统产生混沌行为的主要因素，而目前对高维数字混沌系统在参数控制下的运动行为是很难精确描述的。将消息映射到参数空间会导致高维混沌系统的迭代轨道变得不可控制，尽管在一定程度上增加了散列函数的复杂性，但却为其埋下了安全隐患。

本文扩展了周红等人在流密码设计过程中提出的 m 序列扰动[13]的思想，将轨道扰动的概念引入到混沌散列函数的设计过程中。以低维数字混沌系统为迭代映射，将消息映射至其相空间的扰动空间，在改善数字混沌系统动力学特性退化的同时，提高了散列函数的运算速度和安全性。

2 混沌轨道扰动

数字混沌系统是连续混沌系统在计算机上的实现，但其动力学特性与连续混沌系统相比却存在着非常严重的退化，造成这种现象的原因主要是混沌轨道的有限精度表示产生的量化误差。由于混沌系统存在极端的初值敏感性，这种微小的误差在混沌系统的作用下会被不断放大，并不断产生新的量化误差，从而导致数字化混沌轨道以一种非常复杂和不可捉摸的方式偏离系统的真实轨道[11]。

文献[11]中指出，在 ω bit 实现精度下，无限周期的连续混沌系统数字化后的最大周期和平均周期都远远小于有限精度下的状态数 2^{ω}，且存在大量的短周期轨道。所以，要将混沌系统应用于

密码函数的设计过程中，必须首先考虑数字混沌系统的特性退化问题。

目前，有两种方法可以有效地解决这个问题：混沌轨道扰动[13-16]和变参数补偿（VPCM）[17]。从物理意义上讲，混沌轨道扰动的方法实际上是VPCM法的一种平均化的简化版本[11]，本文即是将混沌轨道扰动的思想引入至混沌散列函数的设计之中。

2.1　混沌轨道扰动思想

文献[13]用 m 序列对数字化混沌系统实施扰动以克服有限精度效应，并研究了 m 序列的阶数、扰动幅度以及扰动分布对有限精度混沌系统输出信号的特性造成的影响. 图 1 所示为无扰动时混沌系统的映射关系。

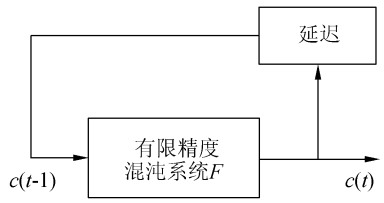


图 1　无扰动时混沌系统的映射关系

Fig. 1　Chaotic map without perturbation

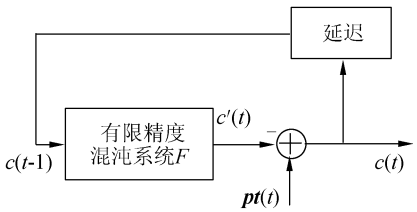


图 2　加入序列后的混沌映射

Fig. 2　Chaotic map with perturbation

设 $d(t)$ 为 m 序列，$c(t)$ 为明文序列，F 为有限精度的数字混沌系统，图 2 所示为序列的扰动过程，即 $c(t)=\boldsymbol{pt}(t)-c'(t)$，其中扰动向量为

$$\boldsymbol{pt}(t)=(-1)^{d(t)}\sum_{i=2}^{n}2^{-i}d(t-i+1)\ 。$$

通过对 m 序列的扰动过程进行分析，可以得到以下结论：

（1）m 序列扰动是一种相空间的轨道扰动。根据文献[12]对改善 PWLCM 的动力学特性的分析可知，这种扰动策略对于改善数字化混沌的动力学特性退化问题的效果较好。

（2）从物理意义上讲，混沌轨道扰动的目的是利用混沌系统极端初值敏感性的特性，有效地避免了在混沌映射的迭代过程中产生一条固定的相空间轨道，既克服了数字混沌系统的短周期问题，又增大了基于轨道预测混沌序列的难度

2.2　扰动强度与 Lyapunov 指数

定义 1：对于实现精度为 w bit 的数字混沌系统，若对迭代过程中轨道的最低 l bit 进行扰动，则定义 l 为混沌轨道扰动的扰动强度。

定义 2：对于实现精度为 w bit 的数字混沌系统，无轨道扰动时，在 Lyapunov 指数 λ 的影响下，每次迭代均会导致轨道的最低 l_{eq} 位发生变化，定义为的等效扰动强度。

文献[12]对 l_{eq} 的估计值为[1.44λ]，文献[11]则将其修正为[2.89λ]。从等效 Lyapunov 指数的定义出发，本文认为文献[12]的估计值更为准确，故而采用文献[12]中的结论，即 $l_{eq}=[1.44\lambda]$。

定义 3：对于实现精度为 w bit 的数字混沌系统，加入强度为 l 的轨道扰动后，迭代过程中误差的平均放大速率 λ_{eq} 定义为 l 的等效 Lyapunov 指数。

在非线性动力学系统的长期演化过程中，Lyapunov 指数 λ 决定了在吸引域内相邻轨道沿该方向平均发散（$\lambda>0$）或收敛（$\lambda<0$）的快慢程度。假设混沌映射的一个正的 Lyapunov 指数为 λ_1，那么初始误差为 Δc 的两个信号经过 n 次混沌迭代后的平均误差变为 $e^{n\lambda_1}\Delta c$。

在加入强度为 l 的轨道扰动后，初始误差为 Δc 的两个信号经过一次混沌迭代后的误差为 $2^l\Delta c$，由等效 Lyapunov 指数的定义易知：$2^l=e^{\lambda_{eq}}$，即 $\lambda_{eq}=l\ln 2$。

对以上结果进行分析，可以得到以下结论：

（1）对于实现精度为 w bit 的数字混沌系统（Lyapunov 指数为 λ），在未进行轨道扰动时，在迭代过程中若要使 w bit 的信息完全消失，则平均迭代次数为 $n_1=w\ln 2/\lambda$。

（2）对于实现精度为 w bit 的数字混沌系统，加入强度为 l 的轨道扰动后，在迭代过程中若要使 w bit 的信息完全消失，则平均迭代次数为 $n_2=w\ln 2/\lambda_{eq}$，即 $n_2=w/l$。

（3）为了保证混沌系统的动力学特性，扰动强度 l 不应过大。

定义 4：在轨道扰动过程中，若扰动序列

$\{\varepsilon_i\}_0^\infty$ 的扰动对象为数字混沌系统的状态变量，则称所有扰动序列构成的集合 E 称为数字混沌系统相空间的扰动空间。

基于轨道扰动的混沌散列函数的设计，即是将明文消息映射至数字混沌系统相空间的扰动空间，根据扰动强度合理选择迭代次数，并最终在相空间取出散列结果。

3　算法设计

基于轨道扰动的混沌散列算法以 Logistic 映射为混沌映射，将任意长度的明文消息压缩为 160 bit 的散列值。算法以 byte 为单位处理明文消息，处理过程采用 256 bit 的定点数实现，即迭代过程中的变量均以 $0.b_{256}b_{255}b_{254}\cdots b_2b_1$ 的形式表示。算法描述如下：

3.1　消息填充

为了提高对短消息计算散列值的安全性，需要首先将明文消息 M 填充为 64 byte 的整数倍，填充方法是在消息后面填充 0×80，并将原始消息的字节长度以小端在前模式填充至最后 4 个字节。设填充后的消息长度为 n，填充后的消息为 $M=m_0m_1m_2\cdots m_{n-1}m_{n-1}$，其中 m_i 表示填充后消息的第 i 个字节，$i\in[0,n-1]$。

消息扰动 $\varepsilon_m(r)$ 为 256 bit 定点数，且该定点数的 $b_{201}-b_{208}$ 为 m_r，其余各位均为 0。

3.2　选择固定扰动向量

在任意伪随机序列中选取 64 byte 作为算法的固定扰动向量 $\boldsymbol{P}$，本算法的 $\boldsymbol{P}$ 为[66 65 98 110 108 99 107 120 71 97 72 65 79 127 70 92 98 107 82 97 118 85 118 87 109 90 69 84 67 66 109 107 85 71 86 70 78 71 106 80 64 114 111 69 81 110 123 76 118 95 81 75 85 126 116 111 128 90 124 108 96 105 94 127]，p_i 表示向量中 $\boldsymbol{P}$ 的第 i 字节，其中 $i\in[0,63]$。

固定扰动 $\varepsilon_p(r)$ 为 256 bit 定点数，且该定点数的 $b_{193}-b_{200}$ 为 $p_{(r\bmod64)}$，其余各位均为 0。

3.3　开始迭代

Step 1：令迭代次数为 $r=2n$，选取迭代初值 $x(0)$，将其用 256 bit 定点数表示如下：

$$x(0)=0.0123456789ABCDEFFEDCBA9876543210\underbrace{000\cdots000}_{32个0}$$

Step 2：迭代次数 r 满足 $1\leqslant r\leqslant n$ 时，迭代过程如下：

$$x'(r-1)=(x(r-1)+\varepsilon_p(r-1)+\varepsilon_m(r-1))\bmod 1 \tag{1}$$

$$x(r)=4x'(r-1)(1-x'(r-1)), \tag{2}$$

Step 3：迭代次数 r 满足 $n<r\leqslant2n$ 时，迭代过程如下：

$$x'(r-1)=(x(r-1)+\varepsilon_p(r-1)+\varepsilon_m(2n-r))\bmod 1, \tag{3}$$

$$x(r)=4x'(r-1)(1-x'(r-1)). \tag{4}$$

(4) 将最终迭代值 $x(2n)$ 的 b_1-b_{160} 作为散列结果输出。

4　安全性分析

4.1　文本散列结果

取初始文本 1 为“Cryptographic hash function is the basic technique for information security and plays an important role in modern cryptography. A hash function H takes a long string of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint.”

文本 2 将文本 1 的首字符 C 改为 D，文本 3 将文本 1 中的 is 改为 Is，文本 4 在第一个句号的后面加个空格，文本 5 将文本 1 的 output 改为 putput，文本 6 将文本 1 的最后一个句号去掉。分别计算文本 1～文本 6 的散列值，图 3 所示为各个散列值的 0～1 分布图，用十六进制表示如下：

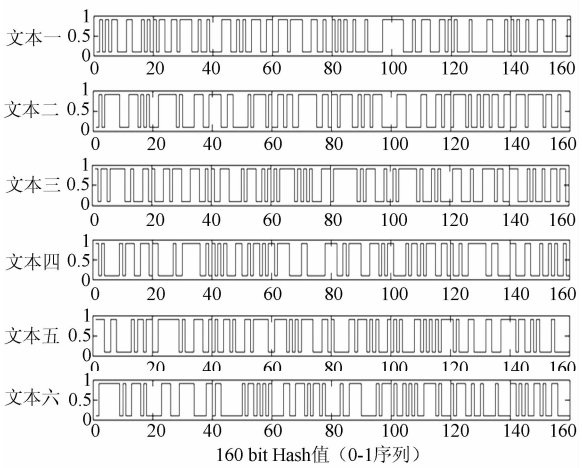


图 3　文本散列结果 0～1 分布图

Fig. 3　0-1 distribution figures of hash result

文本 1：5631566f24394e6778c95220fe271a8418548c43
文本 2：5f1d47e873cc17a6cfcdbcb7070636f4b6677d90
文本 3：b7c8d1b8e5385cabea8eff5c4bf450e23d9c526d
文本 4：a0b9d827e55196b78607978eb0b5cd27e618c4a5
文本 5：e60b67f4729a37cf578d06ea2a1aaf4618fb2840
文本 6：7f4e838f86c05aa19d682782e953d172421a9a61

对以上数据进行统计分析可知，相对于文本 1 的散列值，文本 2～文本 6 的散列值分别变化了 80、80、82、73、81 bit。可见消息中任何细微的差异，都会导致散列结果发生较大的变化，由此说明该算法具有很高的初值敏感性。

4.2　混乱与扩散性质的统计分析

为了隐藏明文消息的冗余度，Shannon 提出了混乱与扩散的概念。对一个二进制表示的散列值而言，每比特只有 1 或 0 两种可能，因此理想的敏感值应保证任何明文的轻微改变将导致散列结果的每一比特都以 50% 的概率变化。为了更加形象的说明本算法的混乱与扩散性质，本文定义以下 4 个统计量。

平均变化比特数：$\overline{B}=\frac{1}{N}\sum_{i=1}^{N}B_i$

平均变化概率：$\overline{P}=(\overline{B}/160)\times 100\%$

B 的均方差：$\Delta B=\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(B_i-\overline{B})^2}$

P 的均方差：

$$\Delta P=\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(B_i/128-P)^2}\times 100\%$$

本文采取以下的测试方法对本算法的混乱与扩散性质进行统计分析：从明文空间中随机选取任意长度的明文消息并求其散列结果，然后随机修改明文消息中的任一比特并求得另一散列结果，比较两个散列结果求出变化的比特数 B_i，一共进行 N 次类似测试。图 4 所示为当 $N=2\ 048$ 时 B_i 的分布图，其中横坐标表示测试次数，纵坐标表示比特变化数 B_i。当 N 分别为 128、256、512、1 024、2 048 时，得到表 1 所示的统计数据。

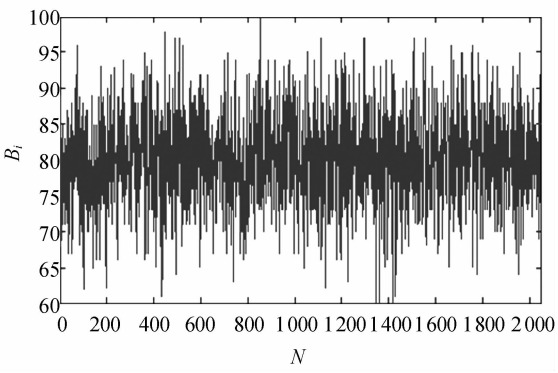


图 4　$N=2\ 048$ 时的比特数变化分布图

Fig. 4　Distribution figure of bit changed when $N=2\ 048$

由表 1 中的数据可以看出，本算法的平均变化比特数 $\overline{B}$ 和平均变化概率非常接近理想状态下的 80 bit 和 50%，此数据充分的说明了本算法具有很好的混乱和扩散性质，从统计效果上保证了攻击者在已知一些明文消息与散列结果的情况下，无法得到任何散列结果分布的有用信息。本算法的 ΔB 和 ΔP 均很小，说明了算法对明文消息的混乱与扩散能力十分稳定。

表 1　混乱与扩散的统计数据

Tab. 1　Statistic of confusion and diffusion

指标	N					均值
	128	256	512	1 024	2 048	
$\overline{B}$	79.906 3	80.168 0	79.974 6	80.117 2	80.017 6	80.036 7
$\overline{P}$(%)	49.94	50.10	49.98	50.07	50.01	50.02
ΔB	6.718 7	6.474 6	6.383 8	6.476 1	6.192 9	6.449 2
ΔP(%)	4.20	4.05	3.99	4.05	3.87	4.032
$B_{i\max}$	95	95	97	102	100	97.8
$B_{i\min}$	67	63	61	58	60	61.8

4.3　抗生日攻击和碰撞攻击分析

由生日悖论可知，若散列函数输出的散列值为 N bit，那么只需测试 $N/2$ 个随机消息，即可以找到两个消息具有相同的散列值。基于生日悖论的生日攻击方法将攻击难度由 2^N 减小为 $2^{N/2}$。对于本文散列算法而言，如果对其进行生日攻击，

则 160 bit 的散列结果意味着需要对 2^{80} 个消息进行测试才可能找到一组碰撞，所以本算法对生日攻击有很强的免疫性。

关于散列算法碰撞特性的分析，目前尚无较好的测试方法。如果以散列结果的长度 160 bit 作为分析尺度，那么计算量则过于庞大，难以实现。目前，文献中使用较多的是小尺度的分析方法，如将分析尺度定为 8 bit 的分析方法为：取 1 byte 的明文消息计算散列值，并从散列结果中取出 8 bit。这样初值(明文消息)空间与终值(散列结果)空间相同，记终值空间中任一值对应初值空间中原像的个数为 k，并用 $n(k)$ 表示终值空间中具有 k 个原像的点的个数，则 $n(1)$ 越大，$n(0)$ 和其他各项越小，说明碰撞越小，散列函数抗生日攻击和碰撞攻击的能力越强。用终值空间与初值空间的测度之比来衡量碰撞发生程度，令

$$L=\frac{256-n(0)}{256}\ , \tag{5}$$

则 L 的值越接近 1，碰撞程度越低，等于 1 时，完全没有碰撞。

图 5 为本文算法的碰撞分布图，其中 $n(0)$ 至 $n(4)$ 分别为 83，109，48，13，3，当 $k>5$ 时，$n(k)=0$。易计算得 $L=0.675\ 8$，可见，本文算法的碰撞程度较低。

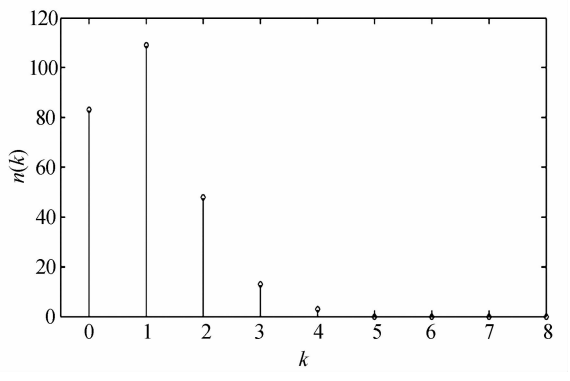


图 5　碰撞分布图

Fig. 5　Collision distribution

参数 L 的计算目前很难与其它算法进行比较，其主要原因是小尺度的分析方法只能对算法的抗碰撞特性进行定性的分析，属于算法具备一定抗碰撞能力的必要而非充分条件。但由于其可以灵活地通过改变初值空间和终值空间大小的方式控制分析尺度，并在各个尺度下得到算法抗碰撞分析的能力，故而测试结果有一定的实际意义。

4.4　抗中间相遇攻击分析

中间相遇攻击是生日攻击的一种变形，二者的不同之处在于：生日攻击试图在函数的定义域中找到两个散列值相同的消息，而中间相遇攻击则试图找到一个值，它分别在两个函数的定义域和值域中。

文献[10]中指出：当构造明文初值通过混沌映射进行迭代时，得到了一条相空间中的轨迹，但如果取相轨迹中的其他点作为初值，通过同样的混沌映射迭代，仍然可以得到同样的一条相轨迹，从而构造碰撞，其分析方法与中间相遇攻击的思想是基本一致的。

基于轨道扰动的混沌散列函数很好地解决了这个问题。在混沌迭代中加入扰动，使得混沌映射的无固定迭代轨道消息不同导致扰动强度的不同，从而产生了迭代轨道的差异，该差异在算法的迭代过程中被充分放大，并最终影响散列结果。消息中任何细微的差异，都会导致散列结果发生很大的变化。由于无固定的迭代轨道，所以本算法对基于相空间轨道的中间相遇攻击方法有很强的免疫性。

4.5　算法速度与灵活性分析

算法在实现过程中对消息进行了一定的填充，以增加短消息计算时的复杂度，同时，为了使消息的任何细微差异都能被充分放大，算法采用了双向迭代方法，即首先将填充后的消息正向输入迭代过程，然后再反向输入迭代过程，最终的输出作为散列值。

可见，算法的执行时间与填充后的消息长度成正比，每一字节消息的处理即是执行一次扰动运算和一次 Logistic 映射，共需执行两次乘法运算和三次加法运算，和其他类似算法相比是很快的。算法在实现过程中使用的是 256 bit 的定点数，在 Virtex 系列 FPGA 中，DSP Slice 模块可以在一个时钟周期内完成一次定点数的乘加运算，在 500 MHz 的时钟频率下，完成一次迭代仅需十几纳秒，所以其硬件实现效率也是很高的。

算法在使用过程中，可以通过改变定点数格式或散列结果的取值方法，灵活地控制散列结果的长度。和传统散列算法(MD5)相比，该算法能够更好地适应实际情况的需要。

5 结　论

本文从序列密码设计中 m 序列扰动的思想出发，分析了扰动强度与 Lyapunov 指数的关系，并将扰动空间的概念引入到混沌散列的设计过程中，最终提出了一种基于轨道扰动的混沌散列函数设计方法。这种方法将明文消息映射到相空间的扰动空间，实现了相空间中无固定轨道的迭代过程。研究结果表明，该算法的设计原理简单，且混沌映射的固有非线性动力学特性使得该算法的密码学特性较高，如明文消息的每比特变化均能引起散列结果中近 50％的比特发生改变，160 bit 的散列结果可以很好地抵抗生日攻击及对文献[10]分析方法的强免疫性等。256 bit 的定点数实现方法，既增大了数字混沌系统的状态空间，又使得算法易于硬件实现。在增加了算法安全性的同时，提高了算法的执行速度，这些特性使得该算法可以被广泛地应用在数据完整性校验、数字签名认证以及嵌入式网络安全设备中，大大提高了算法的实用性。

参考文献：

[1] 樊春霞，姜长生. 一种基于混沌映射的图像加密算法[J]. 光学 精密工程，2004，12(2)：179-184.
FAN CH X，JIANG CH SH. Image encryption based on discrete chaotic maps [J]. *Opt. Precision Eng.*，2004，12(2)：179-184. (in Chinese)

[2] 黄峰，冯勇. 利用图像分割思想的二维混沌映射及图像加密算法[J]. 光学 精密工程，2007，15(7)：1096- 1103.
HUANG F，FENG Y. Novel 2D chaotic map based on image segmentation and image encryption approach [J]. *Opt. Precision Eng.*，2007，15(7)：1096- 1103. (in Chinese)

[3] 李娟，冯勇，杨旭强，等. 三维可逆混沌映射图像加密及其优化算法[J]. 光学 精密工程，2008，16(9)：1738-1745.
LI J，FENG Y，YANG X Q，*et al*.. Invertible chaotic 3D map based image encryption and its optimized algorithm [J]. *Opt. Precision Eng.*，2008，16(9)：1738-1745. (in Chinese)

[4] 刘军宁，谢杰成，王普. 基于混沌映射的单向 Hash 函数构造[J]. 清华大学学报(自然科学版)，2000，40(7)：55-58.
LIU J N，XIE J CH，WANG P. One way hash function construction based on chaotic mappings [J]. *Journal of Tsinghua University (Sci & Tech)*，2000，40(7)：55-58. (in Chinese)

[5] 郭伟，曹杨，王小敏，等. 基于混沌动态参数的散列函数[J]. 通信学报，2008，10(29)：93-100.
GUO W，CAO Y，WANG X M，*et al*.. One-way hash function with chaotic dynamic parameters [J]. *Journal on Communications*，2008，10(29)：93-100. (in Chinese)

[6] 姜楠，杨德礼，王德高. 基于混沌理论的身份认证方案[J]. 吉林大学学报(理学版)，2008，46(7)：711-715.
JIANG N，YANG D L，WANG D G. Identity authentication scheme based on chaotic theory [J]. *Journal of Jilin University (Science Edition)*，2008，46(7)：711-715. (in Chinese)

[7] XIAO D，LIAO X F，WANG Y. Parallel keyed hash function construction based on chaotic neural network [J]. *Neurocomputing*，2009，72：2288-2296.

[8] AMIN M，FARAGALLAH O S，EL-LATIF A A A. Chaos-based hash function (CBHF) for cryptographic applications [J]. *Chaos，Solitons and Fractals*，2009，42：767-772.

[9] 任海鹏，庄元. 基于超混沌 Chen 系统和密钥流构造单向散列函数的方法[J]. 通信学报，2009，30(10)：100-113.
REN H P，ZHUANG Y. One-way hash function construction based on Chen-type hyper-chaotic system and key-stream [J]. *Journal on Communications*，2009，30(10)：100-113. (in Chinese)

[10] 王继志，王英龙，王美琴. 一类基于混沌映射构造 Hash 函数方法的碰撞缺陷[J]. 物理学报，2006，55(10)：5049-5054.
WANG J ZH，WANG Y L，WANG M Q. The collision problem of one kind of methods for constructing one-way hash function based on chaotic map[J]. *Acta Physica Sinica*，2006，55(10)：5049-5054. (in Chinese)

[11] 王小敏. 非线性动力学滤波器设计及其在信息安全中的应用研究[D]. 成都：西南交通大学，2007.

WANG X M. *Design of nonlinear dynamic filter and its application in information security* [D]. Chengdu: Southwest Jiaotong University, 2007. (in Chinese)

[12] LI S J. *Analyses and new designs of digital chaotic ciphers*[D]. Xi'an: Xi'an Jiaotong University, 2003.

[13] 周红,凌燮亭.有限精度混沌系统的 *m* 序列扰动实现[J].电子学报, 1997,25(7):95-97.
ZHOU H, LING X T. Realizing finite precision chaotic systems via perturbation of *m*-sequences [J]. *Acta Electronica Sinica*, 1997,25(7):95-97. (in Chinese)

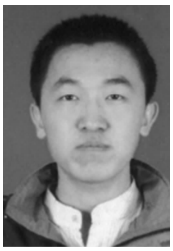
[14] CERMAK J. Digital generators of chaos[J]. *Phys. Lett. A*, 1996,214(3-4):151-160.

[15] SANG T, WANG R L, YAN Y X. Perturbance-based algorithm to expand cycle length of chaotic key stream [J]. *Electronics Letters*, 1998,34(9):873-874.

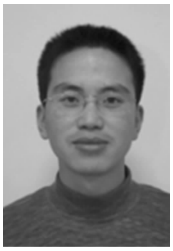
[16] SANG T, WANG R L, YAN Y X. Clock-controlled chaotic keystream generators [J]. *Electronics Letters*, 1998,34(20):1932-1934.

[17] HU H P, XU Y, ZHU Z Q. A method of improving the properties of digital chaotic system [J]. *Chaos Solitons & Fractals*, 2008,38:439-446.

作者简介:



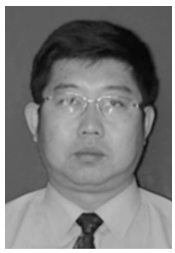
李佩玥(1985－),男,吉林磐石人,博士研究生,2007 年于吉林大学获得学士学位,主要从事网络信息安全、嵌入式系统、混沌散列函数等技术的研究。E-mail: Simon62900@yahoo.com.cn



古　力(1975－),男,四川隆昌人,讲师,1999 年、2002 年于东北师范大学分别获得学士、硕士学位,2004 年于中国科学院长春光学精密机械与物理研究所获得博士学位,主要从事混沌密码、信息安全等技术的研究。E-mail: guli@nankai.edu.cn

隋永新(1970－),男,吉林长春人,副研究员,硕士生导师,1993 年、1996 年于长春理工大学分别获得学士、硕士学位,2002 年于中国科学院长春光学精密机械与物理研究所获得博士学位,主要从事网络信息安全、光学信息融合及辐射定标技术等方面的研究。E-mail: suiyx@sklao.ac.cn

导师简介:



杨怀江(1966－),男,辽宁丹东人,研究员,博士生导师,1988 年于哈尔滨工业大学获得学士学位,1993 年于长春理工大学获得硕士学位,1996 年于北京理工大学获得博士学位,主要从事网络信息安全、光学信息融合及深紫外光刻技术的研究。E-mail: yanghj@sklao.ac.cn