基于时滞混沌系统的带密钥Hash函数的设计与分析

徐 杰[1]，杨娣洁[1]，隆克平[1,2]

(1. 电子科技大学光互联网和移动信息网络研究中心 成都 611731; 2. 北京科技大学计算机与通信工程学院 北京 海淀区 100083)

【摘要】提出了一种基于时滞混沌系统的带密钥Hash函数算法，该算法利用时滞混沌系统非线性动力学特性，将需要传送的明文信息调制在时滞混沌迭代的轨迹中，并通过HMAC-MD5算法计算得出Hash值，Hash值的每个比特都与需传送的明文信息相关。该算法使Hash值对明文信息及时滞混沌迭代初始条件的微小变化高度敏感。理论分析和仿真结果均表明，该算法在保证Hash值的混乱性和散布性的同时，由于其混沌特性的加入而增大了参数空间，并且混沌Hash值与初始明文信息之间的非线性关系可以有效地抵御线性分析。因此，本文设计的基于时滞混沌系统的Hash函数算法具有很好的安全性、抗碰撞性和抗攻击能力，在数字签名等认证技术领域有很好的应用前景。

关 键 词 数字签名； Hash函数； HMAC-MD5； 时滞混沌系统

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.03.024

Design and Analysis of a Cryptographic Hash Function Based on Time-Delay Chaotic System

XU Jie[1], YANG Di-jie[1], and LONG Ke-ping[1,2]

(1. Research Center for Optical Internet and Mobile Information Networks, University of Electronic Science and Technology of China Chengdu 611731;
2. School of Computer Science and Communication Engineering, University of Science and Technology Beijing Haidian Beijing 100083)

Abstract An algorithm of cryptographic hash function based on time-delay chaotic system is presented in this paper. In this algorithm, initial message is modulated into time-delay chaotic iteration, and the Hash value can be calculated by a HMAC-MD5 algorithm. Thus, every bit of this Hash value is correlative with initial message, and this Hash value is very sensitive to micro changes of the initial message or the initial condition of chaotic system. By theory analyses and simulations, we obtain that the Hash value has irregularity and diffusion properties, and the parameter space is augmented because of the properties of chaos. The nonlinear relation between hash value and initial message can be effectively against linear analysis. Therefore, this Hash function based on time-delay chaotic system can get better anti-attack and anti-collision capacity.

Key words digital signature; Hash function; HMAC-MD5; time-delay chaotic system

网络数据的完整性时刻都会受到威胁，为了确认收到的信息在传输过程中没有被攻击者插入、篡改或删除，以公钥密码、数字签名等为代表的加密安全技术已得到广泛的研究和应用。单向Hash函数作为数字签名等安全技术中的一个关键环节，目前有MD2、MD5、SHA等标准。文献[1-2]公布了对MD4、MD5、HAVAL-128、RIPEMD、SHA-1等Hash函数的碰撞攻击方法，对国际上通行的Hash函数给出了快速寻找碰撞攻击的方法，从理论上证明了基于MD5和SHA-1等算法的电子签名有被伪造的可能性。所谓碰撞，是指不同的初始文本对应的Hash映射结果相同，即发生了多对一映射。为了提高网络信息的安全性，保证数字签名的真实性，设计新的、更安全的单向Hash函数十分必要。

由于混沌系统具有初始值敏感性、遍历性和伪随机性等特点，近年来利用混沌方法构造Hash函数迅速成为新的研究方向和热点。目前国内外主要的研究方法是在原有算法的基础上，结合混沌系统构造出新的高可靠性、高安全性的Hash函数。文献[3]提出了基于前馈-反馈非线性数字滤波器构建带密钥的Hash函数。文献[4]则研究了分段线性混沌映射的Hash函数构造方法。文献[5]提出了基于RBF神经网络和混沌映射构造Hash函数的方法。Wx文献[6]提出了利用耦合混沌映射方法构造Hash函数。文献

收稿日期：2010－04－12； 修回日期：2010－11－23

基金项目：教育部长江学者计划、国家杰出青年科学基金(60725104)；国家973计划(2007CB310706)；国家863计划(2008AA011002，2009AA01Z215，2009AA01Z254)；国家自然科学基金(60873263，60932002，60932005)；教育部新世纪人才计划、四川省青年基金(09ZQ026-032)

作者简介：徐 杰(1981－)男，博士，主要从事网络与信息安全、密码与保密通信等方面的研究.

[7]构建了基于保守混沌系统的单向Hash函数。文献[8]提出了基于耦合映像格子混沌模型的Hash函数算法。文献[9]在对复合离散混沌系统和由两个混沌映射构成的特殊复合离散混沌系统分析的基础上，建立了基于复合离散混沌系统的带密钥的Hash算法。文献[10]提出了基于二维超混沌映射的单向散列函数构造方法，但其抗碰撞性还不能达到较好的效果。文献[11]提出了基于时空混沌系统构造Hash函数的方法，但在明文填充时，仅仅填充了一些字符而并未加入明文的任何消息，仍然容易产生碰撞。但所有这些成果都推动了混沌Hash函数的研究，具有积极的意义。

在对研究现状深入分析的基础上，本文设计了基于时滞混沌系统构造带密钥的Hash函数算法。该算法利用时滞混沌系统的敏感性和遍历性，将明文消息逐比特地调制在时滞混沌系统的迭代轨迹中，并以关联了所有明文信息的一组混沌序列，结合带密钥的Hash函数HMAC-MD5认证算法，计算得出单向Hash值。理论分析和仿真实验均表明，该算法在保证了散列值的混乱性和散布性的同时，因混沌特性的加入而增大了参数空间，并使HMAC-MD5认证算法的抗穷举性得到了很大的提升，进一步增强了算法的安全性和抗碰撞性。

1 时滞混沌的系统研究

本文基于时滞混沌系统的非线性动力学特性设计Hash函数算法，该混沌系统根据时延系数的不同可以表达为不同维数的映射，系统方程表示为：

$$u_n = a\sin^2(u_{n-N} + b) \tag{1}$$

式中，a和b是实参数；u_n是系统n时刻的状态，其状态集合称为状态空间；u_0为初始状态是初始状态；N是系统维数。

系统(1)可通过如下变量转换为：

$$\boldsymbol{X}_n = (x_n^{(1)} = u_{n-N}, \cdots, x_n^{(N)} = u_n)^{\mathrm{T}} \tag{2}$$

得到的N维系统方程为：

$$\boldsymbol{X}_{n+1} = T(\boldsymbol{X}_n, a, b): \begin{cases} x_{n+1}^{(1)} = x_n^{(2)} \\ \quad\vdots \\ x_{n+1}^{(N-1)} = x_n^{(N)} \\ x_{n+1}^{(N)} = a\sin^2(x_n^{(1)} + b) \end{cases} \tag{3}$$（3）

由式(3)可知系统在参数空间内具有对称性和周期性：

$$T^p(-\boldsymbol{X}_n, -a, -b) = -T^p(\boldsymbol{X}_n, a, b) \tag{4}$$（4）

$$T^p(\boldsymbol{X}_n, a, b + k\pi) = T^p(\boldsymbol{X}_n, a, b) \tag{5}$$（5）

因此，根据该混沌系统的对称和周期特性，将研究的区域仅限制在参数空间(a,b)的$a>0$且$b\in[0,a]$的范围内。

同时，从系统方程式(3)的sin函数性质可知，该系统还具备有界性：

$$\forall(N,n)\in N^2, \forall(a,b)\in R^2, \forall \boldsymbol{X}_0 \in R^N, \left\|\boldsymbol{X}_n\right\|_\infty \leqslant a \tag{6}$$

可见，在任何参数和任何初始条件下，系统的所有状态轨迹都是有界的，对于混沌特性的控制和应用是非常有利的。

文献[12-14]中，已对该时滞混沌系统的非线性动力学特性进行了深入研究。在系统参数空间内，通过对系统的稳定性研究，得到了该系统从稳定状态到混沌状态的分岔演变过程，对系统的稳定性控制和应用中的参数选取有重要作用。在系统状态空间内，已经研究了系统吸引域(或吸引盆)随参数变化的演变过程，以及作为吸引域边界的不变流形和作为混沌吸引子(或奇怪吸引子)边界的临界流形的特性。同时并且，由不同初始条件而引起的系统多稳定态的特性也在研究中得到了验证。

通过这些研究通过上述研究，可发现该系统所产生的混沌吸引子始终有界，并且受参数控制，对于该系统的实际应用非常有利。通过研究得到了该系统通向混沌的方法，对于混沌序列的选取和控制十分重要。

2 基于时滞混沌迭代的带密钥Hash函数设计原理

在对时滞混沌系统非线性动力学研究的基础上，本文设计了一种基于该混沌系统的带密钥Hash函数算法。该算法的基本思路是将明文消息M以字符为单位读取，经线性变换量化处理得到离散的明文序列$C(k)$，该明文序列$C(k)$通过时滞混沌系统进行逐字节的迭代，从而得到一组离散时滞混沌序列，对其进行带密钥Hash函数运算，即可获得定长的时滞混沌Hash值。该算法的基本设计原理如图1所示。

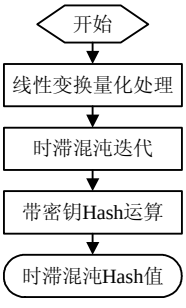


图1 基于时滞混沌迭代的带密钥Hash函数构造原理图

该Hash算法主要分为3个步骤，具体描述如下：

1) 进行明文线性变换量化处理。具体方法为：对明文信息$M(k)$以字符为单位进行ASCII编码，得到明文信息$M(k)$的ASCII编码序列Asc($M(k)$)，其中k=1, 2,…, K，K为$M(k)$的长度。由于ASCII码序列的值域范围为[0,255]，因此通过ASCII编码，明文消息$M(k)$的值域量化至[0,255]之间，利用线性公式$C(k)=g+0.001\mathrm{Asc}(M(k))$对Asc($M(k)$)进行线性变换，$g$为取值范围在[12,12.545]之间的一个常数，于是得到符合时滞混沌迭代参数所要求的值域范围[12,12.8]的离散序列$C(k)$。

2) 对离散序列$C(k)$进行时滞混沌迭代，计算离散时滞混沌序列。时滞混沌系统(1)的一维系统为：

$$x_{n+1}=a\sin^2(x_n+b) \tag{7}$$

（7）

利用该一维系统对离散序列$C(k)$按顺序进行K轮混沌迭代，其中k=1, 2,…, K；1≤n≤N，N为每轮时滞混沌迭代的次数；a和b为每一轮时滞混沌迭代参数。通过对混沌系统(1)的非线性动力学特性的研究可知[14]，当$a\in$[12.000,12.800]，$b\in$[0.000,0.300]时，该系统具有稳定的混沌吸引子，混沌序列具有很好的类噪声特性，为构造具有较高防伪造性和抗碰撞性的Hash函数提供了有效保证。具体计算方法为：1) 第1轮迭代，令$a=C(1)$，选定任意一个初值x_1，b为常量，经时滞系统(7)的N次迭代后，可得到与$C(1)$相关的迭代结果x_{N+1}^0；2) 第2轮迭代，，令$a=C(2)$，以第一轮时滞混沌迭代的迭代结果以第1轮时滞混沌迭代的迭代结果x_{N+1}^0为初值x_1，b为固定常量，经一维时滞系统N次迭代后，可得到与$C(1)$和$C(2)$相关的迭代结果x_{N+1}^1；以此类推，至第K轮迭代时，令$a=C(K)$，以第(K–1)轮时滞混沌迭代的迭代结果x_{N+1}^{K-2}为初值x_1，b为固定常量，得到N次迭代后与$C(1)$，$C(2)$，$C(3)$，…，$C(K)$均相关的离散时滞混沌序列$(x_i^{K-1})(i\in[1,N+1])$，如表1所示。

表1　离散时滞混沌序列

迭代轮次	A	初值x_1	离散时滞混沌序列				
第1轮	$C(1)$	任意	x_1^0	x_2^0	…	x_N^0	x_{N+1}^0
第2轮	$C(2)$	x_{N+1}^0	x_1^1	x_2^1	…	x_N^1	x_{N+1}^1
第3轮	$C(3)$	x_{N+1}^1	x_1^2	x_2^2	…	x_N^2	x_{N+1}^2
…	…	…	…	…	…	…	…
第K轮	$C(K)$	x_{N+1}^{K-2}	x_1^{K-1}	x_2^{K-1}	…	x_N^{K-1}	x_{N+1}^{K-1}

3) 对离散时滞混沌序列$(x_i^{K-1})(i\in[1,N+1])$进行HMAC-MD5运算，获得定长的混沌Hash值。具体方法为：① 令离散时滞混沌序列(x_i^{K-1})为HMAC-MD5算法的输入消息，即$M=(x_i^{K-1})$，其中$i\in[1,N+1]$；② 采用列为“00110110”重复排列任意次的ipad序列与通信双方约定的密钥Key进行异或运算，得到序列S_0，并采用序列为“01011100”“01011100”重复排列任意次所构成的opad序列与通信双方约定的密钥Key进行异或运算，得到序列S_1；③ 将序列S_0与输入消息M拼接构成离散序列$G_0=(M|S_0)$，对G_0进行MD5运算，得到长度为128 bit的Hash值$H_0=H[G_0]_{\mathrm{MD5}}$；④ 将序列$S_1$与所得的Hash值$H_0$拼接构成离散序列$G_1=(H_0|S_1)$，对$G_1$进行MD5运算，得到长度为128 bit的Hash值$H_1=H[G_1]_{\mathrm{MD5}}$。$H_1$即为最终的时滞混沌Hash值。

3　混沌Hash函数性能分析

3.1　密钥敏感性分析

为了分析基于所设计的Hash函数算法对密钥的敏感性，针对文本信息进行Matlab仿真实验，并将密钥仅做10^{-6}的改动，分析所得的Hash值的差异。取初始文本信息为：

As a phenomenon of culture, festivals bear the weight of human civilization. China makes no exception. Chinese traditional festivals contain and incarnate the distillation of Chinese traditional culture. However, since the Opening and Reform, Chinese traditional festival culture has encountered with an unprecedented challenge. Through analyzing the phenomenon of the invasion, the thesis reveals the economic and ideological reasons for its birth and development in China and summarizes its great effects on Chinese society. Meanwhile, the thesis also points out the limits of the invasion by exploring its reasons from the historical and realistic aspects. Thus it can be seen that the western festival culture cannot replace the status of Chinese traditional festival culture in China for ever.

基于初始密钥和经10^{-6}改动后的密钥，分别进行本文设计的时滞混沌Hash函数运算，所得Hash值用十六进制表示如下。

初始密钥的Hash值为：

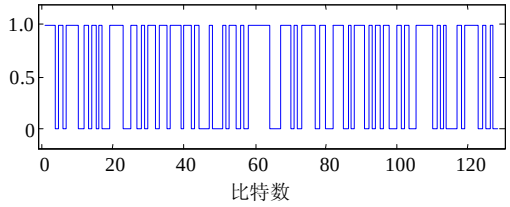
eb953cd6dda22d7e3af675d594fa8bd4

改动后密钥的Hash值为：

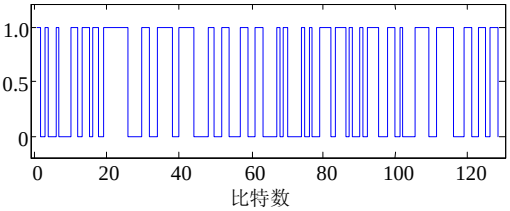
a46dbf8679e198cc2853ba5c68f3e336

将上述Hash值用二进制序列图形化表示，如图2所示。

以上仿真结果表明，本文所设计的Hash函数算法对密钥具有很高的敏感性，即使密钥存在微小的差异，也会产生截然不同的Hash值。



a. 利用初始密钥产生的时滞混沌Hash值二进0、1颁图



b. 利用初始密钥1/1000000的密钥产生时滞混沌Hash值二进0、1颁图

图2 密钥存在10^{-6}差异时的Hash值二进制对比结果

3.2 混乱与散布性质统计分析

Hash函数的设计必须遵循混乱和散布两个重要原则，尽量做到相关明文对应的Hash值不相关。对于结果的二进制表示，每bit比特只有0或者1两种可能，所以理想Hash值的散布效果应该是，初值的微小变化将导致结果的每bit比特都以50%的概率变化。因此，考察Hash认证函数的混乱与散布性质，即考察算法在明文发生l bit变化情况所引起Hash密文结果变化的比特数。

混乱与散布性质的统计数字特征可由以下数据描述：

1) 平均变换比特数 $\overline{B}=\frac{1}{N}\sum_{n=1}^{N}B_n$；

2) 平均变换率 $P=(\overline{B}/128)\times 100\%$；

3) B的均方差 $\Delta B=\sqrt{\frac{1}{N-1}\sum_{n=1}^{N}(B_n-\overline{B})^2}$；

4) P的均方差 $\Delta P=\sqrt{\frac{1}{N-1}\sum_{n=1}^{N}(B_n/128-P)^2}$。

其中，N为统计次数；B_n为第n次测试时的变换比特数。

基于这种思想基于上述思想，本文设计的基于时滞混沌系统的Hash函数的混乱与散布性的分析统计数据计算方法为：1) 取一段长度为 K 的原始明文，通过Hash函数，计算出该段明文的Hash值H；2) 在该段明文的第一个字符的ASCII码上加1，得到一段新的明文，计算出新明文的Hash值H''，并比较H与H''的变换比特数，得到B_1；3) 在原始明文的第二个字符的在原始明文的第2个字符的ASCII码上加1，得到一段新的明文，计算出新明文的Hash值H'''，并比较H与H'''的变换比特数，得到B_2；4) 以此类推，最终得到B_1，B_2，B_3，…，B_{n-2}，B_{n-1}，B_n；5) 得到B_n序列后，计算出上述描述混乱与散布性质的统计数据。

本文分别对明文长度 K 为250、500、1 000、6 500个字符的文字信息进行Hash函数性能统计数据运算，结果如表2所示。

表2 混沌Hash函数混乱与散布性质的统计数据

统计次数N	平均变换比特数 $\overline{B}$	B的均方差 ΔB	平均变换率 P /(%)	P的均方差 ΔP
250	64.288 0	5.880 1	50.22	0.045 9
500	64.081 5	5.713 2	50.06	0.044 6
1 000	64.002 0	6.132 1	50.00	0.047 9
6 500	63.836 5	5.598 8	49.87	0.043 7

从表2可知，即使初始明文有微小的变化，本文设计的时滞混沌Hash函数算法，都将导致Hash值有将近一半的位变化。平均变化比特数和每比特平均变化率都分别趋近于理想状态下的64 比特和bit和50%。可见，本文算法相当充分和均匀地利用了明文空间，明文的任何扰动，使得密文在统计上产生接近等概率的均匀分布，从统计效果上保证了攻击者无法在已知一些明文密文对的情况下伪造其他的明文密文。同时并且，△B与△P都很小，表明算法对明文的混乱与散布能力强而稳定。

4.3 抗碰撞性分析

抗碰撞性是衡量Hash函数性能的又一重要指标。对Hash函数的碰撞分析，可以通过每次改变明文的任何一个bit比特位，对得到的Hash值在相同位置出现相同十六进制值的情况进行统计分析，从而计算其碰撞率。本文分别对250、500、1 000和6 500次明文bit比特位的改变进行测试，得到Hash值在相同位置出现相同十六进制值的碰撞概率，如表3所示。总平均碰撞率为6.45%，可见，多次测试的碰撞率都非常低，说明本文算法具有很强的抗碰撞性。

表3 混沌Hash函数碰撞率

比特位改变次数	碰撞率/(%)
250	6.79
500	6.27
100	6.46

6 500	6.26

4 结 论

本文所设计的基于时滞混沌系统的带密钥Hash函数算法，利用时滞混沌系统的非线性动力学特性，将需要传送的明文信息逐字节地调制在时滞混沌迭代的轨迹中，使产生的Hash值的每个比特都与需要传送的明文信息相关。在带密钥的Hash函数运算过程中，采用HMAC-MD5算法，对密钥进行两次异或运算，加深了攻击者破译的难度。

理论分析和仿真结果表明，本文设计的Hash函数算法对密钥有高度的敏感性，即使密钥的微小变化都将导致所得到的Hash值产生巨大的变化。可见该算法能有效地抵御线性分析，并具有更大的密钥空间和更高的安全性。并且，在混乱与散布统计分析以及抗碰撞性分析中，各项性能测试结果都趋近于理想值，表明该算法对明文的混乱与散布能力强而稳定，且具有很强的抗碰撞性。因此，本文设计的基于时滞混沌系统的Hash函数算法具有很好的安全性和抗碰撞性，在数字签名、数字水印等认证技术中具有很好的应用前景。

本文研究工作得到电子科技大学青年基金(L080101jx0815)的资助，在此表示感谢。

参 考 文 献

[1][1]WANG Xiao-yun, FENG Deng-guo, LAI Xue-jia, et al. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD[C]//Rump Session of Crypto’04, California: Cryptology ePrint Archive, 2004.

[2][2]WANG Xiao-yun, FENG Deng-guo , LAI Xue-jia, et al. How to break MD5 and other Hash functions[C]// EUROCRYPT 2005. Aarhus, Denmark: Springer-Verlag, 2005: 19-35

[3][3]ZHANG Jias-hu, WANG Xiao-min, ZHANG Weng-fang. Chaotic keyed Hash function based on feed forward feed back nonlinear digital filter[J]. Phys Lett, 2007, A 362 A: 439-448.

[4][4]XIAO Di, LIAO Xiao-feng, DENG Shao-jiang. One-way Hash function construction based on the chaotic map with changeable-parameter[J]. Chaos, Solitons and Fractals, 2005, 24: 65-71.

[5][5]WEI Peng-cheng, ZHANG Wei, YANG Hua-qian, et al. Combining RBF neural network and chaotic map to construct Hash function[J]. Lecture Notes on Computer Science, 2006, 3973: 332-339.

[6][6]SONG Yu-rong, JIANG Guo-ping. Hash function construction based on chaotic coupled map network [C]//The 9th International Conference for Young Computer Scientists (ICYCS 2008). ChangSha, China: Inst of Elec, 2008: 2753-2758.

[7][7]ZHANG Qing-hua, ZHANG Han, LI Zhao-hui. One-way Hash function construction based on conservative chaotic systems[C]//Fifth International Conference on Information Assurance and Security 2009 (IAS ’09). Xi’an, China: IEEE Computer, 2009: 402-405.

[8][8]YANG Bo, LI Zhi-min, ZHENG Shi-hui, et al. Hash function construction based on coupled map lattice for communication security[C]//Global Mobile Congress 2009. Shanghai, China: IEEE Computer Society, 2009: 1-7.

[9][9]李红达, 冯登国. 复合离散混沌动力系统与Hash函数[J]. 计算机学报, 2003, 26(4): 460-464
LI Hong-da, FENG Deng-guo. Composite nonlinare discrete chaotic dynamical systemsand keyed Hash functions[J]. Chinese Journal of Computers, 2003, 26(4): 460-464.

[10][10] 彭飞, 丘水生. 基于二维超混沌映射的单向散列函数构造[J]. 物理学报, 2005, 54(10): 4562-4568.
PENG Fei, QIU Shui-sheng. One-way Hash function construction based on two-dimensional hyper-chaotic mappings[J]. Acta Phys Sin, 2005, 54(10): 4562-4568.

[11][11] 刘光杰, 单梁. 基于时空混沌系统构造Hash函数[J]. 控制与决策, 2006 , 21(11):1244-1248.
LIU Guang-jie, Shan Liang. Construction of Hash function based on spatiotemporal chaotic systems[J]. Control and Decision, 2006, 21(11): 1244-1248.

[12][12] XU Jie, CHARGÉ P, FOURNIER P D, et al. Chaos generator for secure transmission using a sine map and an RLC series circuit[J]. Science in China Series F: Information Sciences, 2010, 53(1): 129-136.

[13][13] XU Jie, LONG Ke-ping, FOURNIER P D, et al. Analysis of chaotic dynamics in two-dimensional sine square map[J]. Chinese Physics Letters, 2010, 27(2): 020504.

[14] XU Jie, LONG Ke-Ping, FOURNIER- PRUNARET DanieleD., TAHA Abdel-Kaddous, CHARGE Pascal, CChaotic haotic Dynamics dynamics in a Sine sine Square square Mapmap: High-Dimensional dimensional Case case (N⩾3)[J]. Chinese Physics Letters, 2010, 27(8): 080506.

编 辑 漆 蓉