

文章编号:1001-9081(2010)09-2398-03

基于双混沌动态参数的单向散列算法

刘宴兵, 吕淑品, 唐浩坤

(重庆邮电大学 通信与信息工程学院, 重庆 400065)

(ljshupin@163.com)

摘要:结合双混沌系统以及传统散列函数的优点,提出一种新的带密钥单向散列函数的构造方法。该方法将帐篷映射和 Logistic 混沌映射结合组成双混沌系统生成混沌序列,作为动态参数代替传统散列算法中的固定参数参与轮函数的运算并生成散列摘要。结果表明,所提方法具有较大的密钥空间,很好的单向性,初值和密钥敏感性。

关键词:混沌; 散列函数; 动态参数; 单向性; 敏感性

中图分类号: TP309.2 文献标志码:A

One-way hash algorithm based on chaotic coupled dynamic parameters

LIU Yan-bing, Lü Shu-pin, TANG Hao-kun

(School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Combining the advantages of chaotic coupled system and conventional one-way hash algorithm, a new keyed one-way hash function was presented. In the proposed approach, chaotic coupled system was made by Tent map and Logistic chaotic map, which produced chaotic data as dynamic parameters that replaced the fixed parameters of conventional hash function. The experimental results show that this method has large key space, strong one-way property, and sensitivity to the initial conditions and keys.

Key words: chaotic; hash function; dynamic parameter; one-way property; sensitivity

0 引言

近年来利用混沌特性构造散列函数成为国内外研究的热点。文献[1]采用双混沌系统构造单向散列函数,但用消息分组直接参与混沌迭代,算法复杂度大大增加,安全性却没有很明显的提高;文献[2]采用二维传统混沌系统构造函数,并且采用消息分组迭代,对于较短的消息可以提高速度,但是当文件较大时,速度就会受到限制;文献[3]利用交叉耦合映象格子的方法构造函数,现有的这些混沌散列函数很少借鉴传统密码学理论的设计思路;文献[4]利用帐篷映射构造散列函数,借鉴了传统散列函数的优点,但是低维单混沌映射过于简单,可能存在潜在的动力学攻击;文献[5]利用了传统密码学中的经典理论,但是基于分组密码的 S-Box 结构,复杂且效率低,速度受到了很大限制,另外将初始迭代次数作为密钥的一部分,使密钥空间和运算速度处于矛盾地位。以上文献都推动了混沌散列函数的研究。

针对现有混沌散列算法的不足,本文结合传统散列函数和混沌映射的优点,提出基于双混沌系统动态参数的 Hash 算法 (Chaotic Coupled System-Secure Hash Algorithm1, CCS-SHA1)。本文算法采用帐篷映射和 Logistic 混沌映射组成双混沌系统生成混沌序列作为动态参数,并利用传统散列函数作为算法的核心参与散列计算。结果表明本文算法具有很好的单向性、置乱性、初值和密钥敏感性。

1 理论基础

1.1 混沌系统

混沌是非线性确定系统的外在复杂表现,是一种貌似随

机的非随机现象。混沌系统表现为对初始值和系统参数的敏感性、白噪声的统计特性和混沌序列的遍历特性^[6]。Tent 映射和 Logistic 映射是两个被广泛使用的混沌系统。

Tent 映射也叫帐篷映射^[4],是一个分段线性映射 (Piecewise Linear Chaotic Map, PWLCM), 定义如下:

$$X_{n+1} = \begin{cases} X_n/a, & 0 \leq X_n < a \\ (1 - X_n)/(1 - a), & a \leq X_n < 1 \end{cases} \quad (1)$$

其中 a 为 Tent 映射中的混沌控制参数, X 为系统输入初值, n 为迭代次数, X_{n+1} 为混沌输出值。

Logistic 映射^[7] 定义为:

$$x_{n+1} = \mu x_n (1 - x_n); x_n \in [0, 1] \quad (2)$$

当 $\mu \in [3.57, 4]$ 时, Logistic 映射即出现混沌现象,产生的混沌序列具有很好的类噪声特性,终值的分布比较均匀,而且无任何规律,它的输入值和输出值都分布在 0 ~ 1 上,而帐篷映射的参数取值范围较广,且变量密度较稳定。

1.2 散列函数 SHA1

SHA1 是基于 Merkle-Damgard^[8] 迭代结构的散列函数。能将任意长度的消息转换为一个 160 位的消息摘要。SHA1 有如下特性:不可以从消息摘要中复原信息;两个不同的消息不会产生同样的消息摘要。

SHA1 算法中共有 85 个固定参数^[4], 其中 5 个是寄存器初值:

$$H_0 = 0x67452301$$

$$H_1 = 0xEFCDAB89$$

$$H_2 = 0x98BADCFE$$

$$H_3 = 0x10325476$$

$$H_4 = 0xC3D2E1F0$$

收稿日期:2010-03-16;修回日期:2010-05-10。

基金项目:重庆市自然科学重点基金资助项目(CSTC2009BA2024; CSTC2009BA2053);信息网络安全公安部重点实验室开放课题(C09608)。

作者简介:刘宴兵(1971-),男,四川遂宁人,教授,博士,主要研究方向:无线网络安全、网格计算;吕淑品(1986-),女,河南驻马店人,硕士研究生,主要研究方向:无线网络安全;唐浩坤(1977-),男,重庆人,讲师,主要研究方向:无线网络安全。

其余 80 个是每步运算中使用的工作参数 $T_x^{[4]}$, 描述如下:

$$T_x = \begin{cases} 0x5A82799, & 1 \leq x \leq 20 \\ 0x6ED9EBA1, & 21 \leq x \leq 40 \\ 0x8F1BBCDC, & 41 \leq x \leq 60 \\ 0xCA62C1D6, & 61 \leq x \leq 80 \end{cases}$$

在 SHA1 算法中, 这些参数参与每一步的迭代运算, 首先将 5 个初始值注入对应寄存器中, 然后参数 T_1 到 T_{80} 将分别参与算法的第 1 步到第 80 步的运算。这些预先固定的参数在运算中主要起到置乱的作用, 对于抵抗差分分析没有任何效果。

2 CCS-SHA1 散列算法构造

根据 Tent 映射和 Logistic 映射的特点, 将二者结合, 构造出新的双混沌系统, 由此得到取值范围广且混沌效果好的输出序列, 作为传统散列函数的动态参数参与迭代运算。

作为散列算法中的动态参数要满足以下条件: 1) 取值范围广; 2) 分布均匀, 保证随机性; 3) 密钥空间大, 才能保证算法的安全。为此需要进行参数截取和位移控制, 截取参数是为了得到分布广的序列值, 因为 Logistic 映射的输入输出范围是 0~1; 位移控制是为了扩大密钥空间, 从而增强算法的安全性。图 3 是算法的系统流程, 详细算法步骤如下。

1) 将混沌控制参数 a , 帐篷映射系统初值 $x_1(0)$, 及 Logistic 系统初值 $x_2(0)$ 和位移参数 s 作为密钥 $K = (a, x_1(0), x_2(0), s)$, s 为 2 位 2 进制数, 取值空间为 0~3。

对双混沌分别进行迭代 n 次。其中双混沌系统结构如图 1。

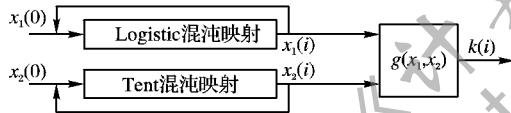


图 1 CCS 构造图

$$k(i) = g(x_1(i), x_2(i)) = \begin{cases} x_1(i), & x_1(i) > x_2(i) \\ x_2(i), & x_1(i) \leq x_2(i) \end{cases} \quad (3)$$

2) 对混沌系统输出结果进行处理, 若 $x_1(i) > x_2(i)$, 则输出 $k(i) = x_1(i)$, 若 $x_1(i) \leq x_2(i)$, 则输出 $k(i) = x_2(i)$ 。

3) 将输出数据转化为 IEEE 16 进制字符串 S , $S = \text{num2hex}(k)$, 截取 $k(i)$ 转化的 16 进制数的后 8 位, 即 $S = S(:, 9:16)$ 。在密钥空间内, 选取初值, 对双混沌系统循环迭代 5000 次, 得到的算术值分布情况如图 2 所示。

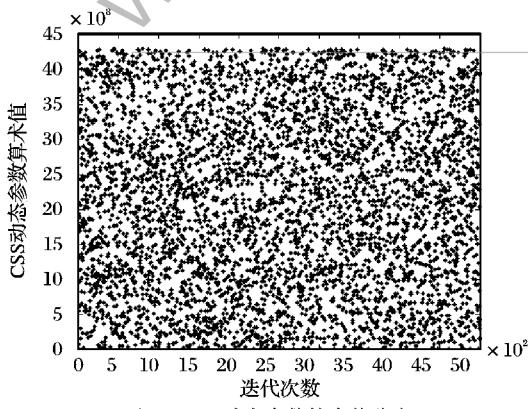


图 2 CCS 动态参数算术值分布

4) 从处理过的混沌序列中, 随机取 85 个不同的动态参

数, 依次右移 s 位。

5) 移位后的结果分别赋给 H_0, H_1, H_2, H_3, H_4 和 $T_1 \sim T_{80}$, 替代 SHA1 中固定参数参与运算。

6) 将 SHA1 中的固定参数替换为动态参数后, 在散列算法中沿用 SHA1 算法的轮函数、迭代结构以及消息分组, 填充和扩展模式。

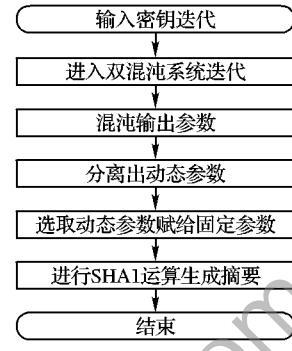


图 3 CCS-SHA1 构造流程

3 仿真实验及性能分析

3.1 双混沌序列的自相关分析

自相关函数表示在取两个任意不同的 n 值时, 对应的混沌序列输出之间的相关程度。自相关系数越接近 1, 就越相似, 反之随机性就越好。实验中对文献 [4] 中单个帐篷映射进行分析, 与本文双混沌系统产生的混沌序列进行比较。

定义最大自相关长度 $Mlag = 100$, $m = -Mlag:Mlag$; 当混沌控制参数 a 在 $[0.49, 0.51]$ 时, 两者的自相关系数均为 0, 即都有很好的随机性和不相关性;

但是当混沌控制参数 a 在 $[0, 1]$ 取其他值时, 结果如图 4。

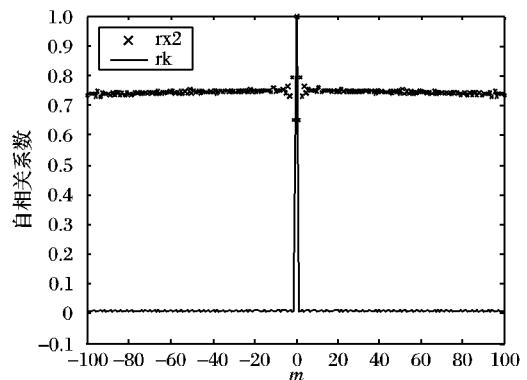


图 4 自相关分析对比

图 4 中: $rx2$ (叉形线) 表示文献 [4] 中单个帐篷映射输出序列的自相关系数; rk (实线) 表示本文提出的双混沌系统产生混沌序列的自相关系数。

实验得出, 此时本文构造的双混沌系统产生的随机序列自相关系数远小于文献 [4] 中的自相关系数, 即本文提出的双混沌系统产生的随机序列有更好的混沌性和不相关特性, 保证了动态参数的随机性。

3.2 算法密钥空间分析

算法的安全性要靠足够大的密钥空间来保持, 密钥 $K = (a, x_1(0), x_2(0), s)$, 混沌控制参数 a , 帐篷映射系统初值 $x_1(0)$ 及 Logistic 系统初值 $x_2(0)$ 由于受有限字长效应影响, 只能在有限范围内取值, 且都是双精度浮点数, 长度为 64 比特。根据 IEEE-754 标准, 双精度浮点数的有效小数位为 15~16 位, 而混沌控制参数 $a, x_1(0)$ 和 $x_2(0)$ 取值范围是 $(0, 1)$,

因此它们取值空间为 10^{15} 。由于 SHA1 算法中位移参数 s 为 170 比特, 其相应的密钥空间为 2×10^{170} 。综合起来, 算法的密钥空间为 $10^{15} \times 10^{15} \times 2^{170} = 2^{270}$ 。本文算法的密钥空间远大于现有暴力破解能力的边界值, 且大于文献[4] 中的密钥空间。强大的密钥空间很好地保证了其算法强度。

3.3 算法的单向性和碰撞性分析

本文算法由两部分组成, 产生动态参数的双混沌系统和 SHA1 的核心迭代结构。由于 SHA1 是成熟的散列算法, 单独使用情况下均证明有良好的单向性。使用其作为本文算法的迭代结构, 使得攻击者即使知道密钥也无法由散列摘要恢复出明文的任何信息。而双混沌系统的引入则进一步提高了本文算法的抗碰撞能力。原 SHA1 算法由于参数固定, 对于差分碰撞攻击抵御能力较弱。本文算法中每一步迭代都会随初始密钥改变而改变, 攻击者如果没有掌握密钥 k , 将无法知道寄存器初值和工作参数, 攻击方将无法找到攻击点。

4 算法的安全性分析

混乱与扩散是设计密码的 2 条基本指导原则^[9], 对散列函数同样适用, 扩散是将每一位明文的影响尽可能地作用到较多的输出散列密文位中去; 同时, 还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的散列密文位中去。其目的是有效隐藏明文的统计特性, 这也就是混沌系统的初始条件敏感依赖性。混乱是指散列密文和明文之间的统计特性的关系尽可能地复杂化, 这也就是混沌映射通过迭代, 将初始域扩散到整个相空间。通过混乱和扩散, 可以有效地抵抗统计和差分攻击。因此理想带密钥散列的散布效果应该是明文的细微变化将导致结果的每比特都以 50% 的概率变化^[10]。

平均变化比特数:

$$\bar{B} = \frac{1}{N} \sum_{i=1}^N B_i \quad (4)$$

平均变化概率:

$$P_{\text{SHA1}} = (\bar{B}/|H|) \times 100\% \quad (5)$$

B 的均方差:

$$\Delta B = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (B_i - \bar{B})^2} \quad (6)$$

P 的均方差:

$$\Delta P_{\text{SHA1}} = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (B_i/|H| - P_{\text{SHA1}})^2} \times 100\% \quad (7)$$

其中: N 为统计次数, B_i 为第 i 次测试结果的变化比特数, $|H|$ 为算法的 hash 值长度, 此处 SHA1 的 hash 摘要为 160 位, 所以 $|H| = 160$ 。

初置敏感测试: 在明文空间内随机选取一段进行测试, 然后改变明文中任 1 比特的值, 得到另一结果, 比较差别的比特数, N 次比较的结果如表 1 所示。

表 1 CCS-SHA1 算法初值敏感测试

迭代次数	\bar{B}	ΔB	$P/\%$	$\Delta P/\%$	B_{\max}	B_{\min}
256	80.3725	6.4098	50.23	5.2916	99	62
512	79.5686	6.2785	49.73	4.9162	95	62
1024	80.1765	6.3292	50.11	5.2917	97	60
2048	80.1451	6.7327	50.09	5.0412	97	60
总平均	80.0656	6.4375	50.04	5.1351	97	61

密钥敏感性测试: 任意改变密钥的 1 比特值, N 次比较后的结果如表 2 所示。

表 2 CCS-SHA1 算法密钥敏感测试

迭代次数	\bar{B}	$\Delta P/\%$	ΔB	$P/\%$
256	80.2134	5.3152	6.3548	50.23
512	80.5765	5.1392	6.2517	49.73
1024	80.0123	4.9371	6.0149	50.11
2048	78.6245	5.0426	6.5431	50.09
总平均	79.8611	5.1085	6.2911	50.04

由仿真结果可见, 本文算法的平均变化比特数接近 80, 平均变化概率变化率都接近 50%, 已经非常接近理想值, 表明它充分和均匀地利用了密文空间。 ΔB 和 ΔP 标志散列混乱和散布性质的稳定, 越接近 0 就越稳定, 本文的结果都很小, 初值和密钥的极端敏感以及平均稳定的散布特性使攻击者无法得到有用的统计信息, 为抵御已知密文攻击和差分现行政策提供了保证。

5 结语

本文结合帐篷映射和 Logistic 映射的优点生成动态参数替代原有固定参数参与运算, 采用成熟散列算法作为散列迭代的核心进行迭代。结果表明: 双混沌系统产生随机性很好的动态参数, 本文算法具有很大的密钥空间、良好的单向性和初始敏感性, 原始数据每比特的变化将引起摘要近 50% 比特改变, 具有理想的明文雪崩特性和密钥敏感性; 并且采用成熟的散列算法作为迭代的核心, 具有较高的数据处理能力和安全性。

参考文献:

- [1] SONG Y R, JIANG G P. Hash function construction based on chaotic coupled map network [C]// The 9th International Conference for Young Computer Scientists. Washington, DC: IEEE Computer Society, 2008: 2752–2758.
- [2] ZHANG Q H, ZHANG H. One-way hash function construction based on conservative chaotic systems [C]// 2009 Fifth International Conference on Information Assurance and Security. Washington, DC: IEEE Computer Society, 2009: 403–405.
- [3] 赵耿, 袁阳, 王冰. 基于交叉耦合映象格子的单向 Hash 函数构造 [J]. 东南大学学报, 2009, 39(4): 728–732.
- [4] 郭伟, 曹杨. 基于混沌动态参数的散列函数 [J]. 通信学报, 2008, 29(10): 93–100.
- [5] GUO XIAN-FENG, ZHANG JIA-SHU. Keyed one-way hash function construction based on the chaotic dynamic S-Box [J]. Acta Physica Sinica, 2006, 55(9): 4442–4449.
- [6] AUSLOOS M, DIRICKX M. The Logistic map and the route to chaos [M]. New York: Springer-Verlag, 2006.
- [7] 张雪锋, 范九伦. 基于分段 Logistic 混沌映射的单向 Hash 函数 [J]. 武汉大学学报, 2008, 54(5): 588–592.
- [8] MERKLE R C. A certified digital signature [C]// Advances in Cryptology – CRYPTO’ 89 Proceedings. New York: Springer-Verlag, 1989: 218–238.
- [9] 韦鹏程, 张伟, 廖晓峰. 基于双混沌系统的带秘密密钥散列函数构造 [J]. 通信学报, 2006, 27(9): 29–30.
- [10] YANG B, LI Z M, ZHENG S H, et al. Hash function construction based on coupled map lattice for communication security [C]// Global Mobile Congress 2009. Barcelona: [s. n.], 2009: 1–7.