A Hash Function Construction Based on A One Dimensional Logistic Map

Yang Liu
College of Information Engineering
College of Information Engineering, Dalian University
Dalian, China
e-mail: lykx2001@163.com

Liyan Wang*
College of Information Engineering
College of Information Engineering, Dalian University
Dalian, China
e-mail: wly1963@163.com

Abstract—In this paper , a new Hash Function based on one dimensional logistic mapping is constructed , and the control parameter and iteration numbers of piecewise linear chaotic map is produced by the Logistic map. Let the iteration consequence make a linear change, one way scattered functions has a good flexibility and anti-collision by explanation. It can be found that the function that is constructed in this paper has good randomicity and collision-avoided. Through the computer simulation experiment, it indicates that the proposed algorithm can satisfy the performance requirements of hash function. From the theoretical analysis and computer simulation experiment, this arithmetic meets the various needs of the Hash functions, and it has the features of high efficient ,flexible, high operability and good reliability. So it can be widely used in digital signature and authentication system.

Keywords- chaotic dynamical systems; Hash function; one-dimensional Logistic chaotic map

I. INTRODUCTION

The rapid development of computer and Internet technology bring us into the era of information. With the rapid development of e-commerce,people lay more emphasis on how to ensure the safety of trade,which leads the establishment of information system to the indispensible infrastructure in the various area.

The traditional Hash functions,for example, MD5,SHA.etc.produces Hash value by multi-round the logical exclusion , operation or password iterations. In 2005,X.Wang[1-2] made a breakthrough in the collision study of Hash functions and discovered the traditional Hash functions which was once considered safe ,for example. MD5 、 SHA-1 , RIPEMD,etc. exists some unkown drawbacks .It makes it urgent to find the new and safe task of Hash functions .Chaos is a very complex phenomenon in nonlinear system, which has the basic features including the sensitivity to parameter and starter,the innate features of traditional cryptology, and unpredictable features of the long-term evolution chaos sequence.More and more people pay most attention to the Chaotic Cryptology which has a vast potential for future development.

Yi[3] proposed a Hash function construction based on tent map.Xiao Di ,Liao Xiaofeng etc.[4] proposed a one-way Hash function construction based on variable parameter chaotic mapping. You Zhongsheng and Liu Feng[5] proposed a Hash function method of construction based on Logistic mapping.In this paper,we will use one-dimensional Logistic mapping as fragment component P which is piece linear mapping, which produces a new arithmetic to constitute one-way hash function. For the safty of Hash function method, it consists some shortage of MD5、SHA-1and RIPEMD[8-10], so a new Hash function construction is necessary.

II. CHAOTIC DYNAMICAL SYSTEM

A. *One-dimensional Logistic mapping*

The definition of one-dimensional Logistic mapping is $x_{n+1} = \lambda x_n(1-x_n) \quad \lambda \in (0,4), x_n \in [0,1]$

It has shown that[6]Logistic mapping is chaos and sensitive to initial condition.The sequence $\{x_k\}_{k=0}^{\infty}$ is aperiodic and convergence,when the parameter $\lambda \in [3.569946, 4]$.

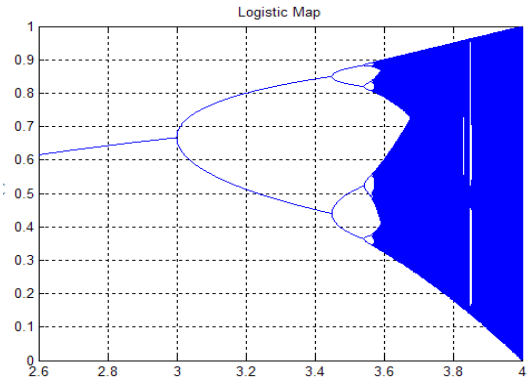

Figure 1. The bifurcation diagram of a one-dimensional Logistic mapping

B. *One-dimensional piecewise linear chaotic mapping*

The definition of one-dimensional piecewise linear chaotic mapping is

$$X(t+1) = F_p(X(t)) = \begin{cases} X(t)/P, & 0 \le X(t) < P \\ (X(t)-P)/(0.5-P), & P \le X(t) < 0.5 \\ (1-X(t)-P)/(0.5-P), & 0.5 \le X(t) < 1-P \\ (1-X(t))/P, & 1-P \le X(t) < 1 \end{cases}$$

where, $X \in [0,1]$, $P \in (0,0.5)$ .As shown in Fig .2.2 to the graph when P=0.324.

According to the reference[4],the iterative system is chaotic,and the output sequence $\{X(t)\}$ is traversal on [0,1],the autocorrelation function is of the form to δ .The Frobenius-Perron operator[7] of the invariant distribution function $f^*(x)$ is

$$P_r(f^*(x)) = Pf^*(xP) + (0.5-P)f^*(P + x(0.5-P)) + (0.5-P)f^*(0.5 + (1-x)(0.5-P)) + Pf^*(1-xP)$$

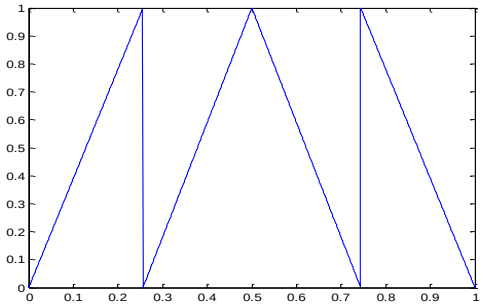

Figure 2. Piecewise linear chaotic mapping

the general solution $f^*(x)$ is 1 and the system is uniform distribution on [0,1].

entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. HASH FUNCTION CONSTRUCTION BASED ON ONE-DIMENSIONAL LOGISTIC MAP

C. *Algorithm description*

The keyword is $\{x_0, y_0\}$,the parameter P of the piecewise linear function is determined by last iteration,different locations of the original text bit and one-dimensional Logistic mapping iteration. So we conclude the basic method of the Hash functions construction with keywords which based on the CBC operating mode of the block cipher. It includes 4n times cycling. In every numeration, the parameter P of the piecewise linear function changes. The iterative tracing point x_n 、 x_{2n} 、 x_{3n} 、 x_{4n} change into binary number by linear transformation, and then it takes a 32-bit respectively. Finally we combine them together to form a 128-bit information abstract. The concret arithmetic as it is:

*1) Changing the pending text according to byte-oriented ASCII code into figures.Linear transformation is the number from 0 to 1.*The whole text produces a large arrays,denoted by C, the array length is the text of bytes n ,according to one-dimensional Logistic mapping, we take $\lambda = 3.78$.

2) The procedure of iteation is as follows:

Step 1 : let $P_1 = (\frac{C_1 + y_0}{4}) \in (0, 0.5)$,then $x_1 = F_{P_1}(x_0)$, $y_1 = \log istic(y_0)$.

Step 2-n :

Let $P_i = (\frac{C_i + x_{i-1}}{4} + y_{i-1})/3 \in (0, 0.5)$,then

$x_i = F_{P_i}(x_{i-1})$,

$y_i = \log istic(y_{i-1}), i = 2,3,4,\mathrm{L}\ n$.

Step $n+1$-$2n$:

Let $P_i = (\frac{C_{2n-i+1} + x_{i-1}}{4} + y_{i-1})/3 \in (0, 0.5)$,then

$x_i = F_{P_i}(x_{i-1})$,

$y_i = \log istic(y_{i-1}), i = n+1, n+2, \mathrm{L}\ ,\ 2n$.

Step $2n+1$-$3n$:

Let $P_i = (\frac{C_{i-2n} + x_{i-1}}{4} + y_{i-1})/3 \in (0, 0.5)$,then

$x_i = F_{P_i}(x_{i-1})$, $y_i = \log istic(y_{i-1})$,

$i = 2n+1, 2n+2, \mathrm{L}\ , 3n$.

Step $3n+1$-$4n$:

Let $P_i = (\frac{C_{4n-i+1} + x_{i-1}}{4} + y_{i-1})/3 \in (0, 0.5)$,then

$x_i = F_{P_i}(x_{i-1})$, $y_i = \log istic(y_{i-1})$,

$i = 3n+1, 3n+2, \mathrm{L}\ , 4n$.

3) Taking $x_n, x_{2n}, x_{3n}, x_{4n}$ from results iterative sequence, and using linear transform into binary number. We extract 32-bit from the fractional part respectively, and combin them together to be the 128-bit Hash value.

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

D. Text simulation

Suppose that the plaintext is "Then, we analysis the Hash Function that we constructed, and find the Hash Function has good randomization and collision-avoided. Theoretical analysis and computer simulation indicate that the proposed algorithm can satisfy the performance requirements of hash function. It can be widely used in digital signature and authentication system."

To initialize $\{x_0=0.333333, y_0=0.3242527\}$,then using MATLAB simulation software to simulate experiments following the next 6 conditions

C 1：Take the original plaintext and keys.

C 2：substitute $x_0=0.333333$ to $x_0=0.333333+1*10^{-16}$.

C 3： Change the original plaintext's initial letter T into t.

C 4：Change the original plaintext's word analysis into analysic.

C 5：Change the period in the end of the original plaintext into comma.

C 6： Get rid of the first comma in the text.

Using the hexadecimal number to show Hash consequence by simulation. As follows:

C 1：9D94174FA1F311DDB6925A2EDE111ECE

C 2：51006A678C7425087B82AC4660C45178

C 3：292CCD0A6DD2ADFC26920113948E70B1

C 4：47630AAC0B1B9D30234E29517A47B88D

C 5：937628741DA4B09BCB26C4DF55061C7A

C 6：74BA1F7B16CDE3E7E428837ACD562E19

Using 0,1 graphical sequences to show drawn Hash value, as shown in the Fig .3.

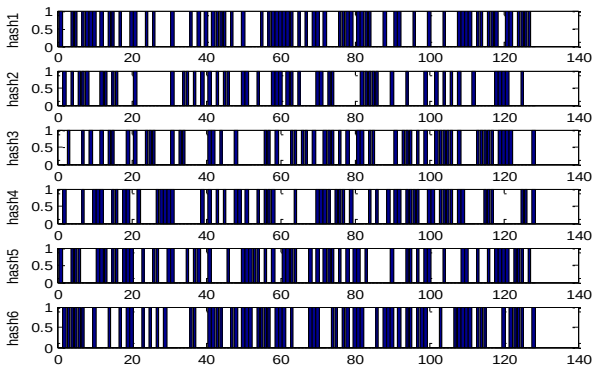

Figure 3. The Hash values in different conditions

As it is shown from the simulation result, the one-way Hash performance of this arithmetic is favourable, the subtle change of the original text or secret key will bring great change to the final result.

IV. THE ANALYSIS OF THE SAFETY

A. The statistic analysis of the chaos and scattering nature

Two basic principles of design code are Chaos and scattering .The uniform distribution of hash value is one of the most important requirements of the hash function.As it is same with the Hash functions, in order to scatter the Hash value evenly in the cryptogram space, we should make the Hash value irrelevant to the content of the corresponding plaintext in the procedure of producing Hash value, but we should have the highly sensitivity to the plaintext. That is to say, every bit of the Hash value has the relationship with the plaintext information M, and it is very sensible to the plaintext information M and the subtle change of the initial value. To the binary representation of the consequence, every bit has only two possibilities including 0 and 1, so the diffusion effect of the ideal Hash value is that the subtle change of the initial value should lead to the 50% variation in every bit of the Hash value.

We take a proclaimed in writing from it, then we evaluate its Hash functions. Changing one bit in the proclaimed in writing into changed after the Hash functions, and comparing the two Hash values to produce changed bit value. Before comparing, we should define the four statistical value:

The average number of bit: $\overline{B}=\frac{1}{n}\sum_{i=1}^{N}B_i$,

The average probability of change：

$P=(\overline{B}/128)\times 100\%$,

The square error of B：

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

The mean square error of P：

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

After comparing 2048 times, we will see the corresponding values distribution of bit, as shown in the Fig .4.

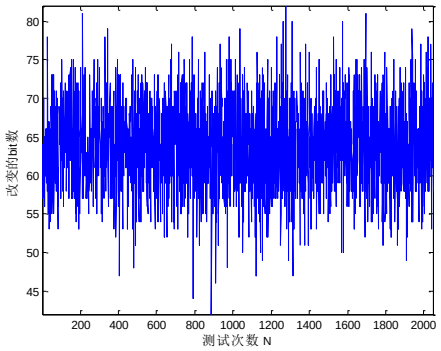

Figure 4. the changeable number distribution of bit

Apparently, the change of proclaimed in writing one bit causes the Hash value whose actual change of bit number was intensively distributed the nearby of ideal condition

changeable number 64, it shows that the arithmetic has the powerful capacity of chaos and diffuse.

By N=256,512,1024,2048 times comparation, we take notes of this arithmetic's empirical data.As it is shown in Table I.

TABLE I. THE CHANGE BIT OF AVERAGE HASH VALUE AND THE CORRESPONDING LISTING

	N=256	***N=502***	***N=1024***	***N=2048***	mean
$\overline{B}$	63.9102	64.0156	64.0029	63.9912	63.9800
P	49.93%	50.01%	50.00%	49.99%	49.983%
ΔB	5.3266	5.3624	5.6097	5.6406	5.4848
ΔP	4.16%	4.19%	4.38%	4.41%	4.285%

From the data in Table I, we can see that the average changeable bit of chaos Hash value based on this text arithmetic and the average change probability of each bit all nearly come to the ideal condition of 64 bit and 50%,it has made full use of the ciphertext space,the every little change of the plaintext,the change of ciphertext produce the equiprobable average distribution in statistics. the statistical consequence guarantee the aggressors can't forge other plaintext and ciphertext when we know some plaintext and ciphertext, ΔB and ΔP both very small,it shows that our arithmetic has the stable and very capable capacity to the chaos and diffusivity of plaintext, so our one-way Hash functions satisfy the safety requirements from this text.

B. The analysis of anti-collision

Collision, it means that we can get the same Hash mapping consequences from Different starter. So it has another mapping, we test this arithmetic's capability of anti-collision through following experiment[4-5]：we select a plaintext randomly from the information plaintext space , and then we get the Hash value, then we store it in the form of ASCII code. We change and choose the 1bit value in information plaintext randomly. Comparing the two Hash value, if the two Hash value of the same position has the same ASCII code, it means one times collision, we count the times of collision, then using the formula $d = \sum_{i=1}^{N} |t(e_i) - t(e_i')|$ to calculate the absolute diversity factor of two Hash value. e_i is the i th ASC II code of original Hash value, e_i' is the i th ASC II code of the new Hash code . Function t is the thing that changing the ASCII code into corresponding decimal system value. We can see it obviously in the secret key,the biggest same ASCII code is 3 in the same position, this means the degree of collision is very low. In addition, the absolute difference degree of the two Hash value is as the Table II shows.

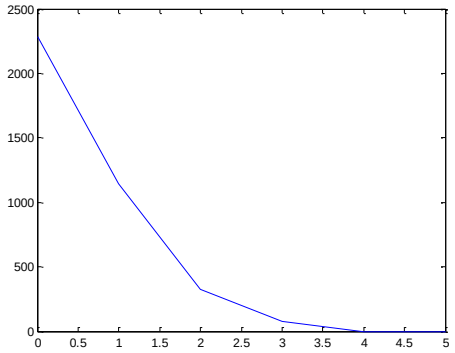

Figure 5. the distribution of the ASCII code which has the same value

TABLE II. THE ABSOLUTE DIVERSITY FACTOR OF THE TWO HASH VALUE

Absolute diversity factor	Maxium diversity factor	Minimum diversity factor	Average diversity factor	Average diversity factor/ character
D	2272	746	1465	91.5885

C. The analysis of flexibility

The arithmetic in this text has preferable flexibility, it can meet the needs in various circumstances. For example, making the Hash value from 128 status to 160 or 256 status, we only need to increase the extractive bit, in this way can we change the length of Hash value.

V. CONCLUSION

We give a one-way Hash function construction algorithm based on compound chaos mapping. This arithmetic uses piecewise linear chaos mapping model with parameter P, using the output of one dimensional Logistic mapping as the segmentations parameters of the segmentation map, and we give a new arithmetic which constructs one way scattered functions. Let the iteration consequence make a linear change. Our one way scattered functions has a good flexibility and anti-collision by explanation. We can see it from the theoretical analysis and computer simulation experiment that this arithmetic meets the various needs of the Hash functions, and it has the features of high efficient ,flexible, high operability, good reliability and a good potential of actual operation.

REFERENCES

[1] X.Wang,D.Feng,X.Lai,H.Yu. Collisions for Hash Functions MD4,MD5,HAVAL-128and RIPEMD[J]. Rump Session of Crypto'04 E-print,2004.

[2] X.Wang,X.Lai,D.Feng etc.. Cryptanalysis of the Hash Functions MD4 and RIPEMD[J],in: Proceedings of Eurocrypt'05, Aarhus,Denmark,2005,pp.1-18.

[3] Yi X. Hash function based on chaotic tent maps[J]. IEEE Transactions on Circuits and Systems-II: 2005,52(6):354-357.

[4] Xiao D,Liao X F,Deng S J. One-way hash function construction based on the chaotic map with changeable-parameter[J]. Chaos,Solitons & Fractals, 2005,24(1):65-71.

[5] S.Z.You,F.Liu.The Hash function construction based on Logistic map. Computer Science,2006,33(4):106-107.

G.X.Hu,Y.Wang.Reseach on digital image encryption method based on hybrid chaotic system.Journal of computer Applications, 2010, 30(5):1209-1211.

[6] Lasota A,Mackey M. Probabilistic Properties of Deterministic Systems[M]. New York: published by the press syndicate of the university of Cambridge. 1985: 32-76.

[7] X. Wang , D. Feng , X. Lai, H. Yu. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD[J]. Rump Session of Crypto'04 E-print, 2004.

[8] X.Wang,X.Lai,D.Feng etc.. Cryptanalysis of the Hash Functions MD4 and RIPEMD[J]. in:Proceedings of Eurocrypt'05, Aarhus, Denmark,2005,1-18.

[9] Wang SH, Shan PY. Security analysis of a one-way hash function based on spatiotemporal chaos. Chin Phys B 2011,20:090504–090507.