PAPER ⟨Special Issue on Cryptography and Information Security⟩

A Secret Key Cryptosystem Using a Chaotic Map

Toshiki HABUTSU†, Yoshifumi NISHIO†, *Associate Members*, Iwao SASASE† *and* Shinsaku MORI†, *Members*

SUMMARY In this paper we propose a new secret key cryptosystem using a chaotic map. This system is based on the characteristics of chaos that the small variations of parameters make the results of recursive calculations on chaotic maps quite different. By appropriately setting the calculation times and selecting a parameter as a secret key, we can make a useful cryptosystem whose distribution of ciphertexts is uniform distribution $U(0, 1)$ and the results of the computation for two slight different keys are relatively independent.

1. Introduction

Random oscillations of the solutions in deterministic systems, which are described by differential or difference equations, are called chaos[1]. Recently many types of chaos-generating systems have been proposed and analyzed in various fields. Especially, chaotic behavior of solutions in some types of one-dimensional difference equations

$$X_{n+1}=F(X_n) \qquad X_n \in [0, 1] \tag{1}$$

is investigated in detail[2]. One-dimensional discrete maps F generating chaotic solutions are called chaotic maps.

Chaotic solutions have the following features.

1. If a parameter (the shape of F) varies slightly, the solution obtained by recursive computation of chaotic map from the same initial point, eventually becomes quite different.
2. If an initial point X_0 varies slightly, the solution obtained by recursive computation of chaotic map with the same parameter, eventually becomes quite different.
3. Solution starting from almost all X_0 in $[0, 1]$ wanders in $[0, 1]$ at random and its distribution is uniform.

Therefore, if one doesn't know both the exact parameter and the exact initial point, he cannot expect the motion of the chaotic solution.

In this paper, we propose a secret key cryptosystem using a one-dimensional map F generating chaos. This system is based on recursive calculations on a chaotic map as $X_n=F^n(X_0)$. We use a parameter α of the map for a secret key, and a point p in an interval $[0, 1]$ for plaintext. The encryption function is n-times composite of F^{-1} and the decryption function is n-times composite of F. Therefore, the encryption and the decryption are achieved by only repeating a very simple calculation.

Generally, F is m to one map, so one plaintext has m^n ciphertexts and any one of m^n ciphertexts can be deciphered only using the secret key. Therefore, senders can selects the ciphertexts by any arbitrary random generator.

Moreover, if times of composite is large enough, it is expected that ciphertext variations act at random and are independent of key variations. This is suitable for the performance of the cryptosystem.

The security of our cryptosystem is relies on these two points mentioned above.

Though the study on chaos have been continued for about a quarter of a century, the effective application of chaos for engineering has hardly proposed without generating pseudo random sequences[3]. Therefore, our study seems to be significant in points of the positive application of chaos for engineering.

2. Construction of a Secret Key Cryptosystem Using the Tent Map

As an example of chaotic maps, we use the tent map which is one of the most popular and the simplest chaotic maps.

2.1 Preliminaries

Figures 1(a) and 1(b) show the tent map and the inverse tent map. These maps transform an interval $[0, 1]$ into itself and contain only one parameter α, which presents the location of the top of the tent. These maps are described as follows.

$$F: \begin{cases} X_{k+1}=\dfrac{X_k}{\alpha} & (0 \leqq X_k \leqq \alpha) \\ X_{k+1}=\dfrac{X_k-1}{\alpha-1} & (\alpha < X_k \leqq 1). \end{cases} \tag{2}$$

$$F^{-1}: \begin{cases} X_{k-1}=\alpha X_k \\ \quad\text{or} \\ X_{k-1}=(\alpha-1)X_k+1. \end{cases} \tag{3}$$

F is two to one map and F^{-1} is one to two map.

Manuscript received February 14, 1990.
Manuscript revised April 12, 1990.

† The authors are with the Faculty of Science and Technology, Keio University, Yokohama-shi, 223 Japan.

Therefore, F^n is 2^n to one map and F^{-n} is one to 2^n map. Since $X=F(F^{-1}(X))$ is always satisfied, $X=F^n(F^{-n}(X))$ is always satisfied.

The distribution of the sequences obtained by iterating the tent map is uniform distribution $U(0, 1)$[3].

2.2 The Cryptosystem

(1) Secret Key

The parameter α is a secret key.

(2) Encryption

(i) Set an initial point as a plaintext p, where $0<p<1$, $p\neq\alpha$.

(ii) Calculate n-times composite of the inverse map, $C=F^{-n}(p)$, in a recursive way, and send this value C to the receiver. On each computation, select one of two equations of F^{-1} in Eq. (3) in any arbitrary way. In short, one plaintext has 2^n ciphertexts and one of 2^n ciphertexts is sent to the receiver.

(3) Decryption

Calculate n-times composite of the map, $F^n(C)$, in a recursive way and recover the plaintext p.

$$p=F^n(C)=F^n(F^{-n}(p)). \qquad (4)$$

Note that only α is required for this computation. The information about which of two equations is used for each encryption process (F^{-1}), is not necessary for the decryption process. Any one of 2^n ciphertexts, even when the coin-flipping is used in the encryption process, is deciphered whithout fail.

The encryption and the decryption are achieved by repeating a simple calculation. They require n times multiplications.

3. Discussions

3.1 Requirements for Parameters

(1) Secret Key and Plaintext Size

Figures 2(a) and 2(b) show the distribution of the ciphertexts for different parameters. When α is near 0, the distribution of ciphertexts is narrow as in figure 2(a) and eavesdroppers have larger probability of the achievement for attacking the key. Similarly, α must not be near 1. However when α is around 0.5 as in figure

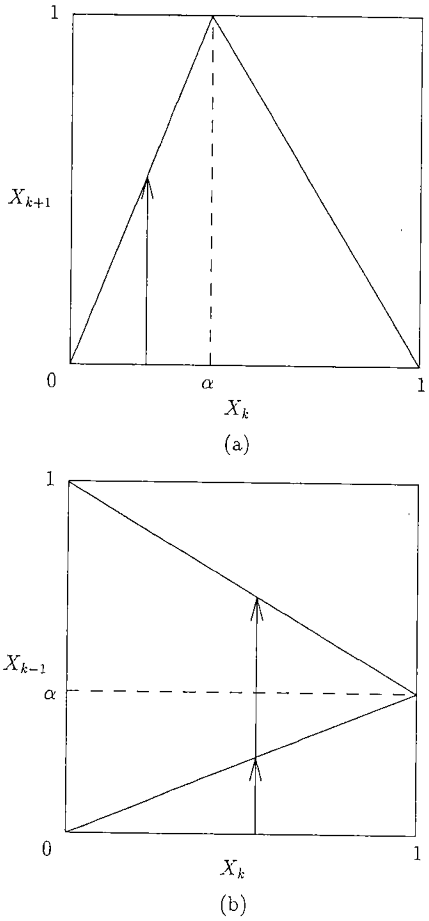


Fig. 1 (a) Tent map.
(b) Inverse tent map.

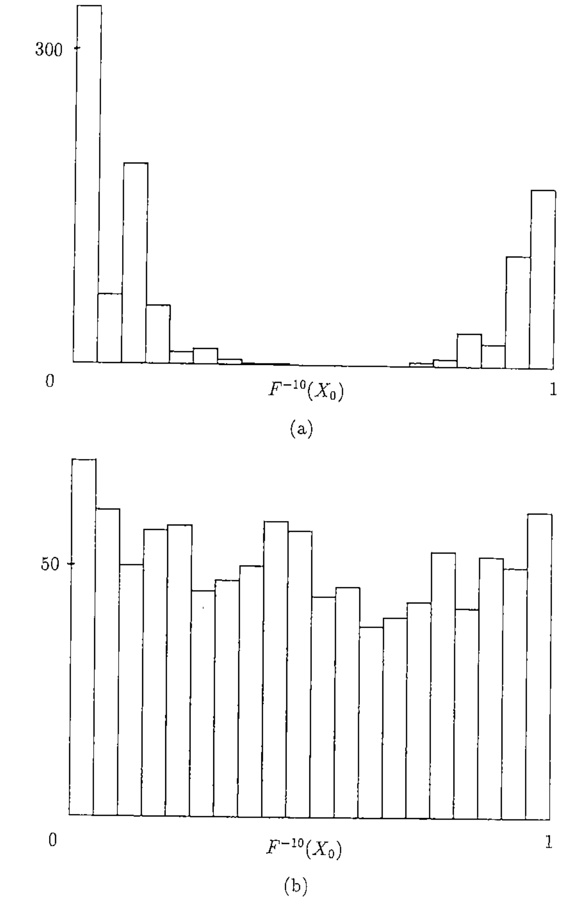


Fig. 2 The histogram of $F^{-10}(X_0)$ in 20 intervals $(i/20, (i+1)/20)$, $i=0, \cdots, 19$.
(a) $\alpha=0.11X_0=0.2356$
(b) $\alpha=0.46X_0=0.2356$

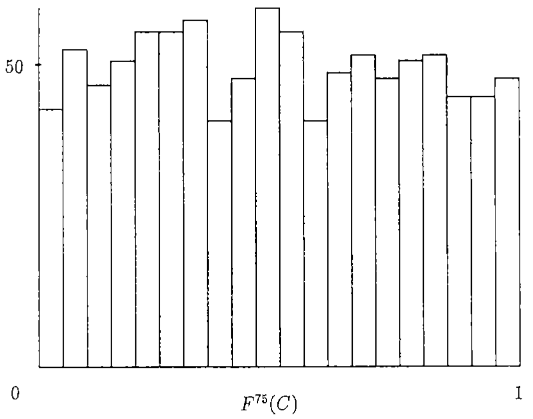


Fig. 3 The histogram of plaintexts obtained from the same ciphertext for 1,000 keys ($C=0.3987$) : 20 intervals ($i/20$, $(i+1)/20$), $i=0, \cdots, 19$.

2(b), the distribution of the ciphertexts is uniform enough. Therefore, we assume that a should be in $0.4<a<0.6$.

The key space size and the plaintext size are required 64 bits for the defense against brute force attack. If the significant digit is 20, both of the key space size and the plaintext size are about 64 bits.

(2) Times of Mapping : n

We determine n so as to make the plaintexts obtained by deciphering the same ciphertext using slight different keys a and $a+\Delta a$, quite different. That is, we determine n so as to satisfy the following two conditions.

(i) If one chooses some keys and computes plaintexts by deciphering a ciphertext, the distribution of the plaintexts for respective keys is uniform distribution $U(0, 1)$.

(ii) If one changes the keys chosen in (i) slightly, the distribution is independent of the distribution in (i).

If these two conditions are satisfied, attackers cannot even expect the plaintext, as far as they do not know the accurate key.

Figure 3 shows the distribution of plaintexts obtained from a ciphertext for 1,000 keys, where $n=75$. It is shown that the distribution is consistent with uniform distribution $U(0, 1)$. Therefore, condition (i) is satisfied.

In order to test the condition (ii), we use χ^2 test. The concept of the methods is as follows. Further details about the test of independence are in Ref. (4).

(i) Divide the interval $[0, 1]$ into l class intervals.

(ii) Compute the N pairs of $F_a^n(C)$ and $F_{a+\Delta a}^n(C)$, and make $l \times l$ contingency table (frequency$=k_{ij}$).

(iii) Compute

$$\chi^2=N\left(\sum_{i=1}^{l}\sum_{j=1}^{l}\frac{k_{ij}^2}{\sum_{j=1}^{l}k_{ij}\cdot\sum_{i=1}^{l}k_{ij}}-1\right). \qquad (5)$$

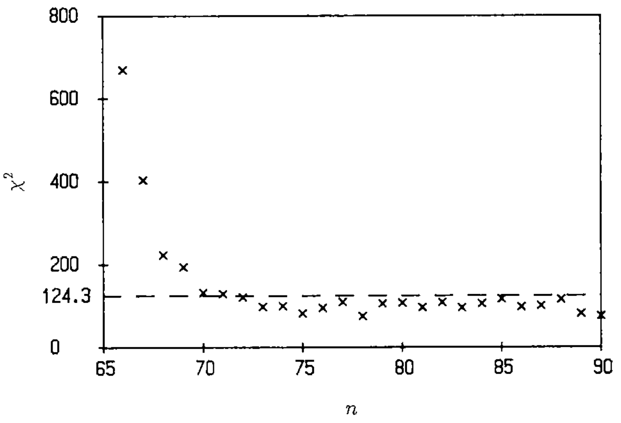


Fig. 4 The results of χ^2 test ($\chi^2_{100}(0.05)=124.3$).

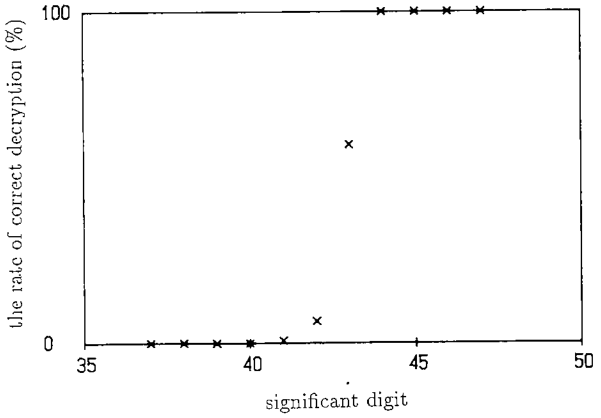


Fig. 5 The rate of correct decryption (Computer simulation : 1,000 samples).

If this value is smaller than the upper 5 % point of χ^2 of which the number of the degrees of freedom is $(l-1)\times(l-1)$, the independence is not rejected using the level of significance 0.05.

Figure 4 shows times of mapping n versus χ^2, where $l=11$, $N=1{,}000$ and $\Delta a=10^{-20}$. Because the upper 5% point of χ^2_{100} is 124.3, the independence is not rejected when $n \geqq 73$.

From these discussions mentioned above, we determine that the times of mapping n is 75.

(3) Ciphertext

If we take the infinite significant digit, it is clear that the decryption process has no error. However, digital computer's memory is finite, so computation error always exist.

Figure 5 shows the rate of the correct decryption versus the significant digits obtained by computer simulation. Since the times of composite of inverse map is 75, the cipher space size is 20 digits+75 bits (42.58 digits). Actually, computation error is accumulated by each step, so some more digits are required. As a result, if 44 digits is taken for the significant digits, the decryption process is always correct.

3.2 Composite of Map

The tent map is piecewise linear map, therefore n-times composite of the tent map is also piecewise linear map. It is described by 2^n-segment piecewise linear function. However, eavesdroppers cannot obtain the exact form of this function and they cannot even expect the plaintext without the information about complete form of the function. This is the basis of the security of our cryptosystem.

If other chaotic maps which are not piecewise linear are taken for this cryptosystem, composite maps are not described by simple function. It can be considered that the degree of security is higher.

4. Conclusions

We have proposed a new secret key cryptosystem using a chaotic map. In the case that we use the tent map as a chaotic map, we verify that correct decryption is achieved by appropriate setting of the significant digit. In the proposed system, a plaintext has 2^n ciphertexts and one of 2^n ciphertexts is sent to the receiver. Even if the ciphertext is chosen by any arbitrary way, the receiver can obtain the plaintext only using the secret key.

Furthermore, in the case that the times of mapping is 75, we verify that the results of the computation for two slight different keys are relatively independence.

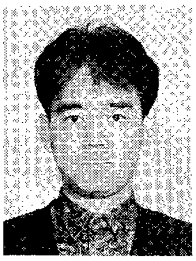
References

(1) J. M. T. Thompson and H. B. Stewart : "Nonlinear Dynamics and Chaos", John Wiley & Sons, Chichester (1986).

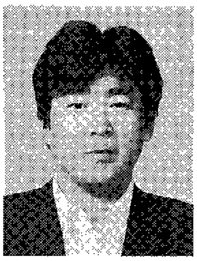
(2) P. Collet and J. P. Eckmann : "Iterated Maps on the Interval as Dynamical Systems", Birkhäuser, Boston (1980).

(3) S. Oishi and H. Inoue : "Pseudo-random number generators and chaos", Trans. IECE Japan, **E65**,9, pp. 534-541 (Sept. 1982).

(4) G. K. Bhattacharyya and R. A. Johnson : "Statiscal Concepts and Methods", John Wiley & Sons, Tronto (1977).



Toshiki Habutsu was born in Tokyo, Japan, in 1967. He received the B. E. degree in Electrical Engineering from Keio University, Yokohama, Japan in 1989. He is presently a master student in the Department of Electrical Engineering, Keio University. His research interests are in cryptography and secure communication systems.



Yoshifumi Nishio was born in Ise, Japan, in 1966. He received the B. E. and M. E. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1988 and 1990 respectively. He is presently a doctoral student in the Department of Electrical Engineering, Keio University. His research interest is in nonlinear circuit technology.

Iwao Sasase was born in Osaka in 1956. He received the B. E., M. E., and Ph. D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1979, 1981 and 1984, respectively. From 1984 to 1986 he was a Post Doctoral Fellow and a Lecturer of Electrical Engineering at University of Ottawa, Canada. He is now an Assistant Professor of Electrical Engineering At Keio University, Japan. His research interests include modulation and coding, communication theory, and satellite communications. He received 1984 IEEE Communications Society Student Paper Award (Region 10), 1988 Hiroshi Ando Memorial Young Engineer Award, and 1988 Shinohara Memorial Young Engineer Award. Dr. Sasase is a member of IEEE.

Shinsaku Mori was born in Kagoshima, Japan in 1932. He received the B. E., M. E., and Ph. D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1957, 1959 and 1965, respectively. Since 1957, he has been engaged in research at Keio University, mainly on nonlinear circuit theory and communication engineering. He is now a Professor of Keio University. He is a member of IEEE.