A Chaotic Cryptosystem based on a Finite-state Baker's map and its Security Analysis

Naoki Masuda† and Kazuyuki Aihara‡

†, ‡*Graduate School of Engineering, The University of Tokyo, Tokyo 113-8656 Japan*
‡*CREST, Japan Science and Technology Co.(JST), Saitama 332-0012 Japan*
†masuda@sat.t.u-tokyo.ac.jp
‡aihara@sat.t.u-tokyo.ac.jp

Abstract— Various cryptosystems utilizing chaotic maps have already been proposed. We proposed a chaotic cryptosystem by constructing a finite-state baker's map in the previous paper. In the present paper, we explain this cryptosystem, and analyze its security chiefly by simulation. Some theoretical comments for security analysis are also accompanied.

I. Introduction

Various cryptosystems based on deterministic chaos have already been presented. Among them are ones utilizing chaos synchronization and/or chaos control methods. As an example, the sender and receiver share the parameter values of the chaotic map used for the carrier as the secret key. The receiver reconstructs the exact carrier by synchronization technique to extract the transmitted message.

There are other types of chaos-based cryptosystems: the stream cipher which employs chaos to generate a key, and the block cipher which transforms plaintexts directly by a chaotic map. The stream type generates a random-looking key stream by iteratively performing chaotic map. The security depends on the characteristics of the random-looking key stream. Its statistical property has been examined [1, 2]. On the other hand, the block type divides the message into blocks, and transform each block by performing a chaotic map iteratively [3, 4, 5]. A block must be long enough, and the property of chaotic transform is again important for security. There are both digital and analog versions of these types, but some of them[3, 4] were already broken with differential cryptoanalysis owing to their strong local linearity[6, 8, 7].

In our previous paper [8], we first decrypted a chaos-based digital block cipher [4] with a two-dimensional cut map. The weakness of this cryptosystem comes from strong linearity of the cut map and mixed-use of digital and analog representations. We then proposed another chaos-based block cipher which overcomes these difficulties. The new cryptosystem profits from a one-to-one transformation on a finite set. It is realized by discretizing a tent map with a special truncation. This cryptosystem has improved theoretical security as shown in [8] and as will be shown in the present paper.

In the present paper, we first review the cryptosystem based on a finite-state baker's map and its theoretical analysis to determine the sufficient iteration number. Next, we show by simulation that a much smaller iteration number is satisfactory for practical use. The discussion part deals with theoretical suggestions.

II. Cryptosystem based on a finite-state baker's map

A. Construction of the cryptosystem

We review the cryptosystem proposed in [8] with some generalization in the state space.

We use a modification of a tent map to transform plaintexts into ciphertexts. The uniqueness of decryption would be lost with a simple application of the tent map because the tent map is two-to-one mapping. Accordingly, we discretize the plaintext space (P), the ciphertext space (C) and the transformation so that we can achieve a one-to-one finite-state baker's map.

We put

$$P = C = \{x = M^{-1}X; X \in \mathbf{N}, 1 \le X \le M\}$$

for $M \ge 2$. One-dimensional tent map (Fig. 1) is defined by

$$f_a(x) = \begin{cases} \frac{x}{a} & (0 < x \le a), \\ \frac{x-1}{a-1} & (a < x \le 1), \end{cases}$$

$$f_a^{-1}(x) = ax \quad \text{or} \quad 1 + (a-1)x.$$

Next, we define a modification of $f_a(x)$ by

$$\tilde{f}_a(x) \equiv \frac{|\{x' \in P | f_a(x') < f_a(x))| + 1}{M}.$$

where $|\cdot|$ indicates the cardinality of a set. This function is naturally interpredted as the ascending order of $f_a(x)$ in $\{f_a(x')|x' \in P\}$, followed by normalization.

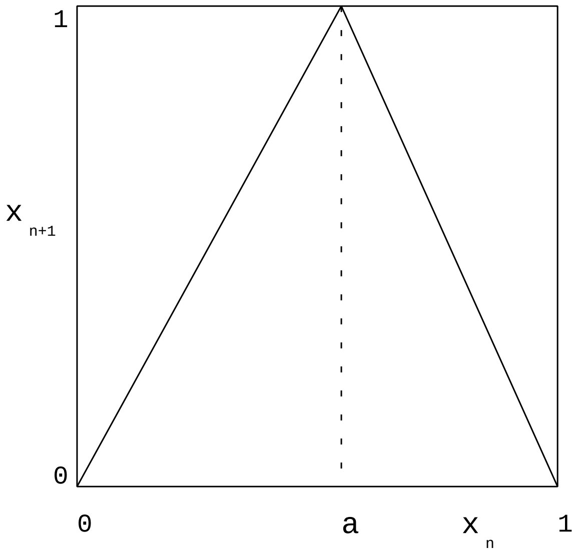

Figure 1: Tent map: $x_{n+1} = f_a(x_n)$.

If $x_1 < a < x_2$ and $f_a(x_1) = f_a(x_2)$, we put

$$\tilde{f}_a(x_1) + M^{-1} = \tilde{f}_a(x_2). \qquad (1)$$

$\tilde{f}_a$ maps P to P in a one-to-one manner.

We redefine the space and the transform on an integer space for practical use. We write $X = Mx, Y = My, A = Ma$, and

$$\begin{aligned} P' &= C' = \{X; X \in \mathbf{N}, 1 \le X \le M\}, \\ K' &= \{A; A \in \mathbf{N}, 1 \le A \le M\}. \end{aligned}$$

P' , C' and K' denote the plaintext space, the ciphertext space and the key space, respectively. The cryptosystem is defined by

$$\begin{aligned} e_A : P' \to C', &\qquad e_A(X) = \tilde{F_A}^n(X)(\text{encryption rule}), \\ d_A : C' \to P', &\qquad d_A(X) = \tilde{F_A}^{-n}(X)(\text{decryption rule}), \end{aligned}$$

where

$$\tilde{F_A}(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, & (1 \le X \le A), \\ \left\lfloor \frac{M}{M-A}(M - X) \right\rfloor + 1, & (A < X \le M) \end{cases}$$

consistent with the definition of $\tilde{f}_a(x)$[8]. $\lfloor z \rfloor$ and $\lceil z \rceil$ denotes round-off and round-up of z, respectively.

The decryption function is given by

$$\tilde{f}_a^{\,-1}(y) = x' \text{ s.t. } f_a(x') \text{ is the } My \text{ th smallest.}$$

We put

$$X_1 = \left\lfloor M^{-1} A Y \right\rfloor, X_2 = \left\lceil (M^{-1}A - 1)Y + M \right\rceil .$$

It follows that

$$\begin{aligned} f_a(M^{-1}X_1) &\le M^{-1}Y < && f_a(M^{-1}(X_1 + 1)), \\ f_a(M^{-1}X_2) &\le M^{-1}Y < && f_a(M^{-1}(X_2 - 1)). \end{aligned}$$

We denote by $m(y)$ the number of $x \in P$ which is included in $[0, x_1] \cup [x_2, 1]$. We showed that (i) $m(y) = Y$ or (ii) $m(y) = Y + 1$ holds [8]. When (i) holds,

$$\tilde{F_A}^{-1}(Y) = \begin{cases} X_1, & (\frac{X_1}{A} > \frac{X_2 - M}{A - M}), \\ X_2, & (\frac{X_1}{A} \le \frac{X_2 - M}{A - M}), \end{cases}$$

and when (ii) holds, simple calculation leads to $\tilde{F_A}^{-1}(Y) = X_1$.

B. Sensitive dependence on plaintexts and keys

We evaluate the iteration number n such that a pair of next plaintexts is encrypted into a pair of totally different ciphertexts. How the minimum difference (= the unity in the integer notation) between two next plaintexts expands can be decomposed into the following three processes.

1. The distance of the unity increases to be twice.
2. The distance grows exponentially to the order of the plaintext space.
3. $\tilde{f}_a$ is furthermore iterated enough times to be almost independent.

We denote by n_1, n_2, n_3 the iteration numbers for (1), (2) and (3) to hold, respectively. We restrict the key space within $0.5 < a < 0.6$ for a theoretical reason.

We theoretically estimated $n_1 = 4.3 \log_{10} M, n_2 = 3.4 \log_{10} M$ and $n_3 = 15$ [8]. As a whole, $n = n_1 + n_2 + n_3 = 7.7 \log_{10} M + 15$ is sufficient.

The discrepancy-growing process for the two next keys (with the same plaintext) consists of three steps similar to those for plaintexts. The calculation leads to the same results as that for plaintexts: $n \sim 7.7 \log_{10} M + 15$.

Simulation results show $n \sim 4 \log_{10} M + 15$ is sufficient in practical use[8].

C. Characteristics of the proposed cryptosystem

Some of the representative characteristics of the proposed cryptosystem are as follows.

- Implementation is easy because the map is simple. Especially, rounding is tractable for digital computers.
- We are utilizing chaotic properties based on the tent map. Strictly speaking, our finite-state baker's map is not identical to the tent map, and the discrepancy grows exponentially in the course of iteration.

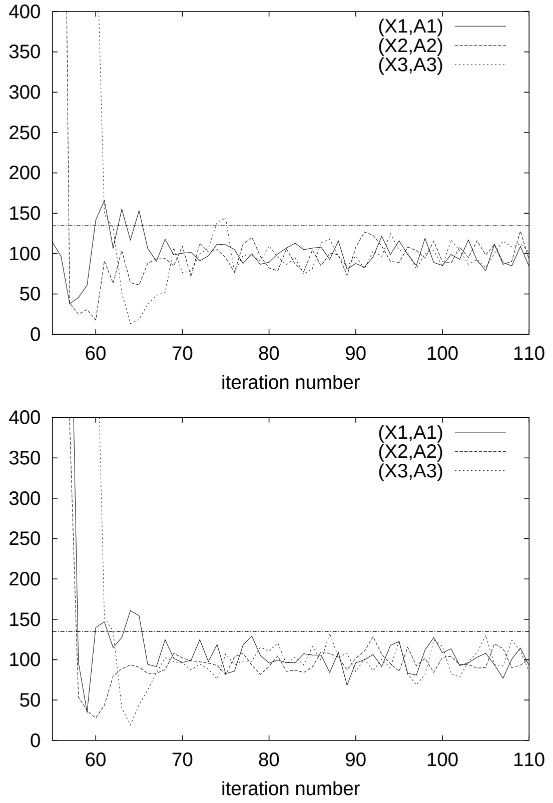

Figure 2: The result for the uniformity test in terms of plaintexts (U-P, upper) and keys (U-K, lower). $M = 10^{20}, S = 1200, l = 100$. Three pairs of initial plaintext and key are tried: $\{(X_1, A_1), (X_2, A_2), (X_3, A_3)\} = \{(85483497692351461897, 54364810590829182407),$ $(38267471053192397610, 51238969610352216109),$ $(60821277239516496944, 59494081732494216993)\}$. The level of significance 0.01 ($\chi^2_{99}(0.01) = 134.7$) is also shown.

- M can be any integer larger than/equal to 2. Taking the calculation complexity into account, $M = 2^s$ is appropriate.

III. Simulation analysis

In this section, we examine the uniformity and the independence of ciphertexts by computer simulations. The uniformity assures the diffusion property of the cryptosystem, and the independency assures sensitive dependence on a key-value or a plaintext-value. The statistical uniformity/independence test is designed with the conventional χ^2 test [3, 4]. We examine the uniformity and the independence in terms of both plaintexts (test U-P, I-P) and keys (test U-K, I-K). The tests are designed as follows:

1. the uniformity test (U-P , U-K)

   (a) Divide the interval [1,M] into l consecutive intervals with the same length. The i th interval is denoted by I_i.

   (b) Compute S ciphertexts $\tilde{F}^n_A(X)$, $\tilde{F}^n_A(X+1)$, ... , $\tilde{F}^n_A(X+S-1)$ for U-P (or $\tilde{F}^n_A(X)$, $\tilde{F}^n_{A+1}(X)$, ... , $\tilde{F}^n_{A+S-1}(X)$ for U-K) and count the frequency k_i that ciphertexts are included in I_i.

   (c) Evaluate the χ^2 statistics given by Eq. (2) under the null hypothesis that ciphertexts distributes uniformly; the degree of freedom for the χ^2 statistics is $l - 1$.

$$\chi^2 = \sum_{i=1}^{l}(k_i - \frac{S}{l})^2/\frac{S}{l}. \qquad (2)$$

2. the independence test (I-P , I-K)

   (a) Generate l intervals in the same way as the uniformity test.

   (b) Compute S pairs of ciphertexts ($\tilde{F}^n_A(X_1)$, $\tilde{F}^n_A(X_1+1)$) , ... ($\tilde{F}^n_A(X_S)$, $\tilde{F}^n_A(X_S+1)$) for I-P (or ($\tilde{F}^n_{A_1}(X)$, $\tilde{F}^n_{A_1+1}(X)$) , ... ($\tilde{F}^n_{A_S}(X)$, $\tilde{F}^n_{A_S+1}(X)$) for I-K) and make a $l \times l$ contingency table. k_{ij} denotes the frequency that pairs are included in $I_i \times I_j$.

   (c) Evaluate the χ^2 statistics given by Eq. (3) under the null hypothesis that the ciphertexts originating from next two plaintexts (keys) are independent; the degree of freedom for the χ^2 statistics is $(l-1) \times (l-1)$.

$$\chi^2 = \frac{1}{S}\sum_{i=1}^{l}\sum_{j=1}^{l}\frac{(Sk_{ij} - \sum_{i=1}^{l} k_{ij} \cdot \sum_{j=1}^{l} k_{ij})^2}{\sum_{i=1}^{l} k_{ij} \cdot \sum_{j=1}^{l} k_{ij}}. \qquad (3)$$

The results of these tests are shown in Figs. 2 and 3. They indicate that the uniformity and the independence are satisfied for $n \geq 80$. $n = 80$ is much fewer than the value estimated by analytical investigations.

IV. Analytic suggestions

It is theoretically most important to clarify the role of discretization. On one hand, discretization results in the complicated computation in analytical sense. Rounding a continuous map is hard to describe by analytic functions because of the discontinuity. This fact covers an explicit expression of encryption rule, and at the same time, makes the theoretic security analysis difficult. On the other hand, any discretization produces a difference between the obtained obrit and the original continuous orbit. This slight discrepancy grows exponentially. As a result of iterations, our ciphertext can be a pseudo-orbit. Such maps can be

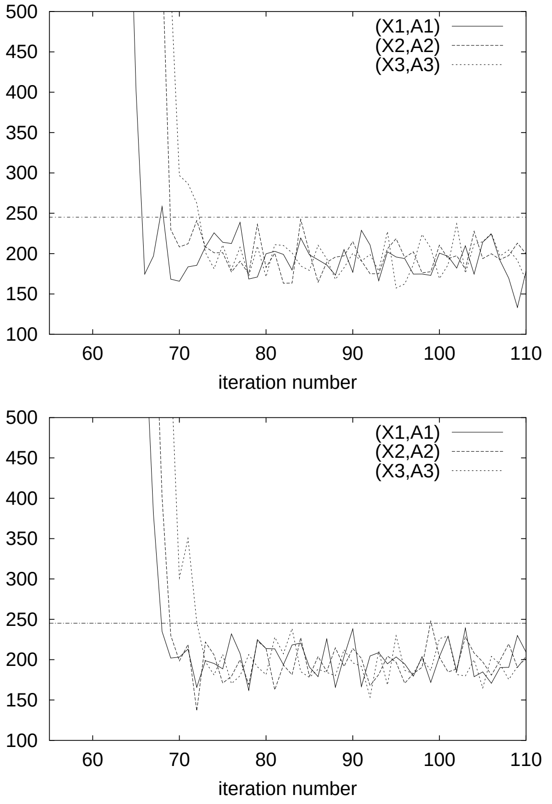

Figure 3: The result for the independence test in terms of plaintexts (I-P, upper) and keys (I-K, lower). $M = 10^{20}, S = 2000, l = 15$. The same three pairs as those in the uniformity test are used. The level of significance 0.01 ($\chi^2_{196}(0.01) = 245.0$) is also shown.

described by β-shadowing. β-shadowing is an approximation of a discretized map, and the discrepancy between the discretized map and the shadowed chaotic map is bounded from above [9]. A map which has β-shadowing has almost the same property as continuous chaotic map such as the sensitivity on initial conditions and randomness of almost every orbit [2, 9]. The relation between β-shadowing and the finite-state baker's map will be considered in the future paper.

In relation to this topic, any transform within a finite set is periodic. Simulation results show discretization of the logistic map results in many cycles with small periods. The attractive basins of such cycles are quite large [9]. These properties are not appropriate both for digital realization of chaos and for application of a chaotic map to cryptosystems. However, we do not suspect that the finite state baker's map has the fatal property described above because it is one-to-one, and no cycle is attractive.

The analysis of chaos from a discrete point of view will enable us to connect discrete maps to continuous maps when the precision of discrete maps goes to infty. When it is possible, the evaluation of chaotic properties is also advantageous to security analysis. The Kolmogorov entropy and the Liapunov exponent measure the rate at which information on initial conditions is lost in the course of iterations. The iteration number can be evaluated by these statistics of chaos so that sufficient security is ensured[5].

V. Conclusion

We have first reviewed the chaotic cryptosystem based on a finite-state baker's map and its security analysis. The presented cryptosystem avoids the piecewise linearity and analog representation, and it has reinforced security. We have next performed a simulation of security analysis based on the χ^2 test. The simulational results show that the uniformity and the independence are ensured for iteration numbers smaller than what is required theoretically. Finally, we have put some theoretical comments regarding to rounding, β-shadowing, cycles and dynamical systems.

References

[1] T. Kohda and A. Tsuneda,"Statistics of chaotic binary sequences", *IEEE Transactions on Information Theory*, Vol. 43, No. 1, pp. 104–112, 1997.

[2] T. Kohda and A. Tsuneda, "Stream cipher systems based on chaotic binary sequences", *SCIS96-11C*, 1996.

[3] T. Habutsu, Y. Nishio, I. Sasase and S. Mori, "A secret key cryptosystem by iterating chaotic map", *Proc. Eurocrypt'91*, pp. 127–140, 1991.

[4] M. Tsueike, T. Ueta and Y. Nishio "An application of two-dimensional chaos cryptosystem: E-mail with MIME", *Technical report of IEICE, NLP96–19*, pp. 61–66, 1996. (Japanese)

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", *Int. J. Bifurcation and Chaos*, Vol. 8, No. 6, pp. 1259–1284, 1998.

[6] E. Biham, "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91", *Proc. Eurocrypt'91*, pp. 532–534, 1991.

[7] Th. Beth, D. E. Lazic and A. Mathias, "Cryptanalysis of cryptosystems based on remote chaos replication", *Proc. Crypto'94*, pp. 318–331, 1994.

[8] N. Masuda and K. Aihara, "Chaotic cipher by finite-state Baker's map", *IEICE*, Vol. J82-A, No. 7, pp. 1038–1046, 1999. (Japanese)

[9] A. E. Jackson, "Perspective nonlinear dynamics", *Cambridge Univ. Press*, 1989.