On the Security of the Yi-Tan-Siew Chaotic Cipher

Shujun Li, Guanrong Chen, *Fellow, IEEE* and Xuanqin Mou

***Abstract*— This paper presents a comprehensive analysis on the security of the Yi-Tan-Siew chaotic cipher proposed in [1]. A differential chosen-plaintext attack and a differential chosen-ciphertext attack are suggested to break the sub-key K, under the assumption that the time stamp can be altered by the attacker, which is reasonable in such attacks. Also, some security Problems about the sub-keys α and β are clarified, from both theoretical and experimental points of view. Further analysis shows that the security of this cipher is independent of the use of the chaotic tent map, once the sub-key K is removed via the proposed suggested differential chosen-plaintext attack.**

***Index Terms*— chaotic cryptography, tent map, differential cryptanalysis, chosen-plaintext attack, chosen-ciphertext attack.**

I. Introduction

Since the 1990s, chaotic cryptography has attracted more and more attention as a promising way to design novel ciphers, and this research has become more intensive in recent years [2, Chap. 2]. To evaluate the security performance of chaotic ciphers and to clarify some design principles, cryptanalysis plays an important role.

This paper analyzes the security of the recently-proposed Yi-Tan-Siew chaotic cipher [1] and points out some defects existing in this cipher:

1) the sub-key K can be removed by a differential chosen-plaintext attack and a differential chosen-ciphertext attack, under the assumption that the time-stamp t can be altered by the attacker;
2) the sub-key β should not be contained in the secret key due to its poor contribution to the security of the cipher;
3) the noise vectors $\{U_j\}$ used in the encryption/decryption functions do not have a uniform distribution, which downgrades the security of the cipher by limiting the value of the sub-key α;
4) when the aforementioned differential chosen-plaintext (or chosen-ciphertext) attack is used, the security of the cipher is independent of the chaotic map, but depends on the mixture of three operations from different algebraic groups.

The first two defects mean that the claimed key (α,β,γ,K) collapses to be (α,γ). Note that the second and third defects were implicitly mentioned in Sec. III-B of [1] without convincing explanations. This paper will give a comprehensive analysis on all the four security defects.

The rest of this paper is organized as follows. The next section gives a brief introduction to the Yi-Tan-Siew chaotic cipher. Then, the first two defects of the cipher are discussed in Sec. III. The other two defects are analyzed in Secs. IV and V, respectively. The last section concludes the paper.

II. Yi-Tan-Siew Chaotic Cipher

This proposed cipher is a *time-variant* block cipher based on the chaotic tent map. Each block has $4n$ bits, and the encryption function changes as the iteration evolves. Given a plaintext $P=(P_1,\cdots,P_j,\cdots,P_r)$ and the corresponding ciphertext $C=(C_1\cdots,C_j,\cdots,C_r)$, where P_j and C_j are both $4n$-bit blocks, the cipher is described as follows.

- *The employed chaotic tent map* is an extended version of the normal skew tent map F_α:
$$G_{(\alpha,\beta)}: x_i=\begin{cases}F_\alpha(x_{i-1}), & \text{if } 0<x_{i-1}<1,\\ \beta, & \text{otherwise,}\end{cases} \tag{1}$$
where
$$F_\alpha: x_i=\begin{cases}x_{i-1}/\alpha, & 0\le x_{i-1}\le\alpha,\\ (1-x_{i-1})/(1-\alpha), & \alpha<x_{i-1}\le 1.\end{cases} \tag{2}$$
- *The secret key* was claimed to be a 4-tuple key (α,β,γ,K), where γ is used to generate a secret initial condition x_0 of $G_{(\alpha,\beta)}$ as follows:
$$x_0=F_\gamma^{4n}\left(\frac{10^{\lfloor\log_{10}t\rfloor}}{t}\right). \tag{3}$$
Here, t representes the current time-stamp transmitted over a public channel. Since γ is only used to generate x_0, the secret key can also be considered as (α,β,x_0,K). Based on the secret key, the following secret functions are calculated for the encryption/decryption procedures:
  1) *A sequence of $4n$-bit noise vectors* $U_j=(u_{4jn},u_{4jn+1},\cdots,u_{4jn+4n-1})$ $(j=0,1,2,\cdots,)$ are generated from the digital chaotic orbit[1] of the extended tent map $G_{(\alpha,\beta)}$ with the following rule:
$$u_i=\begin{cases}0, & 0\le x_i\le\alpha,\\ 1, & \alpha<x_i\le 1.\end{cases} \tag{4}$$
  2) *A sequence of secret permutations* w_{ji} $(j=0,1,2,\cdots;\ i=1,\cdots,n)$ are generated from U_j and the sub-key K, as follows: $V_j=(v_{j1},v_{j2},\cdots,v_{jn})=U_j\oplus K$, where each v_{ji}

This paper has been published in *IEEE Transactions on Circuits and Systems–II: Express Briefs*, vol. 51, no. 12, pp. 665-669, 2004, DOI: 10.1109/TCSII.2004.838657.

This research was supported by the Applied R&D Center, City University of Hong Kong, under Grants 9410011 and 9620004.

Shujun Li and Guanrong Chen are with the Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong, China.

Xuanqin Mou is with the School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, China.

Shujun Li is the corresponding author. Contact him via `http://www.hooklee.com`.

[1] In this paper, the term "digital chaotic orbit" is used to denote the orbit of a chaotic map realized in a digital computer [2, Chap. 2.5].

corresponds to a function w_{ji} that represents a permutation of four integers $\{1, 2, 3, 4\}$ (following Table 1 of [1]).

3) *A sequence of secret bit-permutation functions* $f_j = f_{jn} \circ \cdots \circ f_{j1}$ $(j = 0, 1, 2, \cdots)$ are generated as follows:

$$\begin{aligned} f_{ji}(X) &= f_{ji}(M_1, M_2, M_3, M_4) \\ &= [w_{ji}(M_1, M_2, M_3, M_4)] \lll 1, \end{aligned} \tag{5}$$

where $X = M_1 \times 2^{3n} + M_2 \times 2^{2n} + M_3 \times 2^n + M_4$ and "$\lll 1$" is the 1-bit circular left-shift operation.

4) *Another sequence of permutation functions* $f_j^{-1} = f_{j1}^{-1} \circ \cdots \circ f_{jn}^{-1}$ are generated as follows:

$$\begin{aligned} f_{ji}^{-1}(X) = f_{ji}^{-1}(M_1, M_2, M_3, M_4) = \\ [w_{ji}^{-1}(M_1, M_2, M_3, M_4)] \ggg 1, \end{aligned} \tag{6}$$

where f_{ji}^{-1} is the inverse function of f_{ji}, i.e., $f_{ji}^{-1}(f_{ji}(X)) = X$, and "$\ggg 1$" is the 1-bit circular right-shift operation.

- *The initialization procedure*: $C_0 = U_0, P_0 = U_1$.
- *The encryption procedure*:

$$C_j = f_{j-1}\left(P_j \oplus (C_{j-1} \boxplus U_{j+1})\right) \oplus \left(P_{j-1} \boxplus U_{j+1}\right), \tag{7}$$

where $\oplus$ denotes XOR and $a \boxplus b := (a + b) \bmod 2^{4n}$.

- *The decryption procedure*:

$$P_j = f_{j-1}^{-1}\left(C_j \oplus (P_{j-1} \boxplus U_{j+1})\right) \oplus \left(C_{j-1} \boxplus U_{j+1}\right). \tag{8}$$

III. Reduction of Key Space

This section discusses the reduction of the key space of the Yi-Tan-Siew cipher, i.e., its first two security defects.

A. The Differential Chosen-Plaintext Attack for Reducing K

To break the Yi-Tan-Siew cipher via a chosen-plaintext attack, the attacker has to make t fixed during the attack, i.e., to make the sub-key x_0 and the noise vector sequence $\{U_j\}$ fixed. This can be done by intentionally altering the local clock of the encryption machine, which is generally available since the attacker can access the encryption machine in chosen-plaintext attacks [3]. If t is generated from a public time service, the attacker can simply altering the time signal transmitted over the public channel to alter t. In the following, therefore, assume that t is fixed for all chosen plaintexts.

Assume $\{P_1, \cdots, P_{j-1}, P_j\}$ and $\{P_1, \cdots, P_{j-1}, P_j'\}$ are two plaintexts. The difference of the ciphertexts is as follows:

$$\begin{aligned} \Delta C_j = C_j \oplus C_j' &= f_{j-1}\left(P_j \oplus (C_{j-1} \boxplus U_{j+1})\right) \\ &\quad \oplus f_{j-1}\left(P_j' \oplus (C_{j-1} \boxplus U_{j+1})\right). \end{aligned} \tag{9}$$

Assume $CU_j = C_{j-1} \boxplus U_{j+1}$. Then, Eq. (9) is reduced to

$$\Delta C_j = f_{j-1}\left(P_j \oplus CU_j\right) \oplus f_{j-1}\left(P_j' \oplus CU_j\right). \tag{10}$$

Now, consider such a question: *what can one observe from ΔC_j, if P_j and P_j' have only one different bit?* Assume that

$$\begin{aligned} P_j &= \left(p_{4jn}, \cdots, p_{4jn+i}, \cdots, p_{4jn+(4n-1)}\right), \\ P_j' &= \left(p_{4jn}, \cdots, \overline{p_{4jn+i}}, \cdots, p_{4jn+(4n-1)}\right), \end{aligned}$$

and $CU_j = (cu_0, \cdots, cu_{4n-1})$. It is obvious that $P_j \oplus CU_j$ and $P_j' \oplus CU_j$ also have only one different bit at the same position i. Thus, further assuming that

$$\begin{aligned} P_j \oplus CU_j &= (p'_{4jn}, \cdots, p'_{4jn+i}, \cdots, p'_{4jn+(4n-1)}), \\ P_j' \oplus CU_j &= (p'_{4jn}, \cdots, \overline{p'_{4jn+i}}, \cdots, p'_{4jn+(4n-1)}), \end{aligned}$$

one has

$$\begin{aligned} \Delta C_j = f_{j-1}(p'_{4jn}, \cdots, p'_{4jn+i}, \cdots, p'_{4jn+(4n-1)}) \\ \oplus f_{j-1}(p'_{4jn}, \cdots, \overline{p'_{4jn+i}}, \cdots, p'_{4jn+(4n-1)}). \end{aligned}$$

Considering f_{j-1} is a bit-permutation function, one has $f_{j-1}\left(P_j \oplus CU_j\right) = (p'_{4jn+I_0}, \cdots, p'_{4jn+I_l} = p'_{4jn+i}, \cdots, p'_{4jn+I_{4n-1}})$, and $f_{j-1}\left(P_j' \oplus CU_j\right) = (p'_{4jn+I_0}, \cdots, p'_{4jn+I_l} = \overline{p'_{4jn+i}}, \cdots, p'_{4jn+I_{4n-1}})$, where $I_0 \sim I_{4n-1} \in \{0, 1, \cdots, 4n-1\}$ denote the permuted positions of the $4n$ bits $p'_{4jn} \sim p'_{4jn+(4n-1)}$. As a result,

$$\Delta C_j = (\overbrace{0, \cdots, 0}^{4n-l}, 1, \overbrace{0, \cdots, 0}^{l-1}) = 2^{l-1}, \tag{11}$$

which means that the i-th bit of $\Delta P = P_j \oplus P_j'$ is permuted to the l-th bit of $\Delta C = C_j \oplus C_j'$ by f_{j-1}.

From the above discussion, one can immediately conclude that given the following $(4n+1)$ plaintexts containing j plain-blocks, the secret bit-permutation function f_{j-1} can be exactly reconstructed:

$$\begin{aligned} P^{(*)} &= (P^*, \cdots, P^*, P^*), \\ P^{(1)} &= (P^*, \cdots, P^*, P_1), \\ &\cdots \\ P^{(l)} &= (P^*, \cdots, P^*, P_l), \\ &\cdots \\ P^{(4n)} &= (P^*, \cdots, P^*, P_{4n}), \end{aligned}$$

where $P^* \oplus P_l = 2^{l-1}$. To get all r secret permutation functions $f_0 \sim f_{r-1}$ for the decryption of ciphertexts whose sizes are not larger than r, the number of required plaintexts is $(4n+1) \times r$.

Since the sub-key K is used only to determine $\{f_j\}$ (together with U_j), the reconstruction of $f_0 \sim f_{r-1}$ means the reduction of K from the whole secret key $(\alpha, \beta, \gamma, K)$.

Note that it is generally difficult to derive V_j from f_j, due to the strong mixing of v_{ji} and the bit-shifting operations. That is, it is generally difficult to derive K from f_j, even when U_j is known to the attacker.

B. The Differential Chosen-Ciphertext Attack for Reducing K

Due to the similarity of the encryption and decryption procedures, the above differential chosen-plaintext attack can be easily generalized to a differential chosen-ciphertext attack. Here, the attacker can make x_0 fixed during the attack by altering t transmitted over the public channel, which is possible since generally the attacker has a full control of the public channel. In the differential chosen-ciphertext attack, one can replace the $(4n+1) \times r$ chosen plaintexts in the above differential chosen-plaintext attack with $(4n+1) \times r$

chosen ciphertexts. As a result, one can get all r inverses permutation functions, $f_0^{-1} \sim f_{r-1}^{-1}$, which is equivalent to the r permutation functions, $f_0 \sim f_{r-1}$.

C. Reduction of β

In Sec. III-B of [1], it was said that "most likely, β does not act in the encryption and decryption processes", without any explanation. Here, we will theoretically verify this claim.

In the extended tent map $G_{\alpha,\beta}$, β will have to make influence on the cipher only after $x = 0$ or 1. However, the possibility that $x = 0$ or 1 is so tiny that the impact of β on the encryption/decryption procedures is computationally negligible from the Probabilistic point of view.

Without loss of generality, assume that the map $G_{\alpha,\beta}$ is realized in n-bit computing precision and that the digital chaotic orbit distributes uniformly in the discretized space, which is reasonable due to the uniform invariant density function of the skew tent map [4]. So, the Probability that $x = 0$ or 1 is $p = 2/2^n = 1/2^{n-1}$. As a result, from the mathematical expectation of the geometric distribution [5], the average position of the first occurrence of the above event ($x = 0$ or 1) is $1/p = 2^{n-1}$.

For single-precision floating-point arithmetic, $n = 30$ (two sign bits are excluded), averagely $2^{29} = 512$M iterations are needed to activate the influence of β on the encryption/decryption procedures. This means averagely $2^{29}/8 = 64$M leading bytes of the ciphertext can be successfully decrypted without any knowledge of β. Similarly, when the double-precision floating-point arithmetic ($n = 62$) is used, the condition will become much worse: averagely $2^{61}/8 = 2$GG leading cipher-bytes can be decrypted without knowing β.

Therefore, in most (if not all) cases, β is not meaningful in the key. In fact, it is just a trivial parameter (not part of the secret key) to avoid the digital chaotic orbit of the normal skew tent map F_α to fall into the fixed point $x = 0$.

As a summary, under the above differential chosen-plaintext attack, the original key $(\alpha, \beta, \gamma, K)$ collapses to be (α, γ). When the differential chosen-plaintext attack is impossible, the original key $(\alpha, \beta, \gamma, K)$ collapses to be (α, γ, K).

IV. NON-UNIFORMITY OF NOISE VECTOR U_j

In the encryption procedure of the Yi-Tan-Siew cipher, the noise vector U_{j+1} is used to mask the plaintext P_j together with the previous plaintext P_{j-1} and the previous ciphertext C_{j-1}. To enhance the potential capability of resisting statistics-based attacks [3], it is desirable that U_j distributes uniformly in the discrete space $\{0, \cdots, 2^{4n} - 1\}$. However, as mentioned in Sec. III-B of [1], U_j does not distributes uniformly when α is close to 0 or 1. As a suggestion, $0.49 < \alpha < 0.5$ was suggested in [1]. However, neither theoretical nor experimental analysis is given in [1] to support this claim.

In this section, we investigate the theory underlying the non-uniformity of U_j over $\{0, \cdots, 2^{4n} - 1\}$. In addition, it is pointed out that the non-uniformity of U_j is also very significant when $\alpha = 0.5$, which was not noticed in [1].

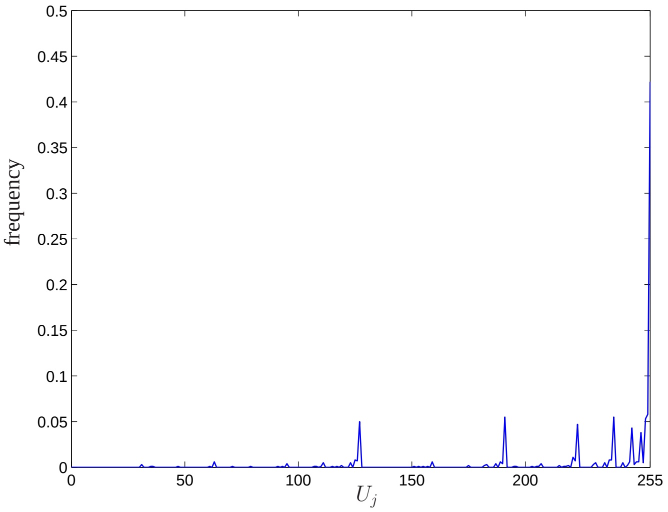

Fig. 1. The occurrence frequency of $U_j = a \in \{0, \cdots, 255\}$, when $(\alpha, \beta, x_0) = (0.1, 0.7, 0.3)$ (1000 samples).

A. Non-Uniformity of U_j when $\alpha \neq 0.5$

In this subsection, it is shown that when $\alpha \neq 0.5$, the closer the α is to 0 or 1, the more severe the non-uniformity of U_j will become. Strictly speaking, $\alpha \neq 0.5$ can never lead to a uniform distribution.

Similar to Sec. III-C, assume again that the digital chaotic orbit of the map $G_{\alpha,\beta}$ distributes uniformly in the discretized space. It is then easy to deduce the following two Probabilities:

$$\mathrm{Prob}\{u_i = 0\} = \alpha, \mathrm{Prob}\{u_i = 1\} = 1 - \alpha. \qquad (12)$$

The above equations mean that U_j will contain more 0-bits than 1-bits when $\alpha > 0.5$, and more 1-bits than 0-bits when $\alpha < 0.5$. That is, U_j does not have a uniform distribution over $\{0, \cdots, 2^{4n} - 1\}$ if $\alpha \neq 0.5$. When $(\alpha, \beta, x_0) = (0.1, 0.7, 0.3)$ and $n = 2$, for example, under double-precision floating-point arithmetic, Figure 1 gives an experimental curve of the occurrence frequency of U_j with different values between 0 and $2^{4n} - 1 = 2^8 - 1 = 255$. It can be seen that the frequency of $U_j = 255 = (11111111)_2$ is close to 0.5 but many others are almost 0.

Under the assumption that all bits in U_j are independent each other, $\forall a \in \{0, \cdots, 2^{4n} - 1\}$, one can theoretically deduce the Probability of $U_j = a$: $\mathrm{Prob}\{U_j = a\} = \alpha^{N_0(a)}(1 - \alpha)^{4n - N_0(a)}$, where $N_0(a) \in \{0, \cdots, 4n\}$ denotes the number of 0-bits in a. In total there are $(4n + 1)$ *different* values in all 2^{4n} Probabilities: $\mathrm{Prob}(0) = \alpha^{4n}$, $\mathrm{Prob}(1) = \alpha^{4n}(1 - \alpha)$, $\cdots$, $\mathrm{Prob}(i) = \alpha^{4n-i}(1 - \alpha)^i$, $\cdots$, $\mathrm{Prob}(4n) = (1 - \alpha)^{4n}$.

The non-uniformity of each U_j is useful for an attacker to get its value more quickly via a specially-designed guess order. Since the secret bit-permutation functions $\{f_{j-1}\}$ can be reconstructed under chosen-plaintext attack (recall Sec. III-A), the attacker can successfully decrypt any ciphertext once $\{U_j\}$ are obtained. That is, $(\{U_j\}, \{f_j\})$ can be considered as an equivalent of the original secret key $(\alpha, \beta, \gamma, K)$.

To find the right value of each U_j, the following guess order of $U_j = a$ is suggested: $\forall a \in A_0 \cup A_{4n}$, $\cdots$, $\forall a \in A_i \cup A_{4n-i}$, $\cdots$, $\forall a \in A_{2n}$, where A_i ($i = 0 \sim 2n$) denotes the set of all

$$
\begin{aligned}
Com(\alpha) &= \sum\nolimits_{i=0}^{2n-1}\left(\mathrm{Prob}(i)\cdot\left(H(i)+\sum\nolimits_{m=0}^{\binom{4n}{i}} m\right)+\mathrm{Prob}(4n-i)\cdot\left(H(i)+\binom{4n}{i}+\sum\nolimits_{m=0}^{\binom{4n}{4n-i}} m\right)\right)\\
&\quad+\mathrm{Prob}(2n)\cdot\left(H(2n)+\sum\nolimits_{m=0}^{\binom{4n}{2n}} m\right)\\
&= \sum\nolimits_{i=0}^{2n-1}\left((\mathrm{Prob}(i)+\mathrm{Prob}(4n-i))\cdot\left(H(i)+\frac{\binom{4n}{i}\left(\binom{4n}{i}+1\right)}{2}\right)+\mathrm{Prob}(4n-i)\cdot\binom{4n}{i}\right) \qquad (13)\\
&\quad+\mathrm{Prob}(2n)\cdot\left(H(2n)+\frac{\binom{4n}{2n}\left(\binom{4n}{2n}+1\right)}{2}\right)
\end{aligned}
$$

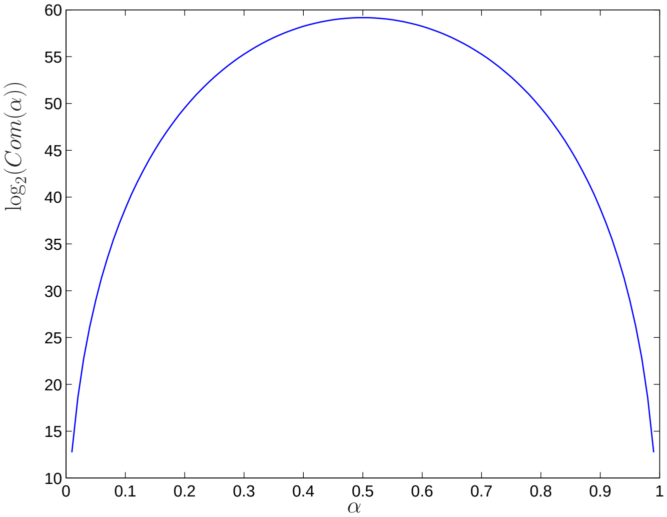

Fig. 2. $\log_2(Com(\alpha))$ vs. $\alpha \in \{0.01, \cdots, 0.01\times i, \cdots, 0.99\}$.

$4n$-bit binary integers that contain i 0-bits. With such a guess order, the average number of searched integers (i.e., the guess complexity) $Com(\alpha)$ can be calculated with Eq. (13), where $H(i)$ denotes the number of previous searched integers:

$$
H(i)=\sum_{l=0}^{i-1}\binom{4n}{l}+\sum_{l=0}^{i-1}\binom{4n}{4n-l}=2\sum_{l=0}^{i-1}\binom{4n}{l}. \qquad (14)
$$

When $n=16$, for instance, the relationship between the calculated complexity and the value of α is shown in Fig. 2. Note that there exist calculation errors[2] that make each $\log_2(Com(\alpha))$ a little less than the real value, but this fact does not influence the following qualitative analysis. From the experimental data given in Fig. 2, one can see that the complexity is much less than $2^{4n-1}=2^{63}$ (the complexity of the brute-force guess of a uniformly-distributed $4n$-bit integer) when α is close to 0 or 1. Apparently, the closer the α is to 0 or 1, the weaker the sub-key α will be. As a result, to ensure the security of the Yi-Tan-Siew cipher, the sub-key α has to be constrained in $[\alpha_0, 1-\alpha_0]\subset(0,1)$, where $Com(\alpha_0)$ should be cryptographically large. This, however, will further reduce the key space to some extent.

In [1], $0.49<\alpha<0.5$ is suggested to avoid this security defect. In this case, 1-bit will always occur with a higher Probability than 0-bit, since $\mathrm{Prob}\{u_i=1\}=1-\alpha>\mathrm{Prob}\{u_i=0\}=\alpha$. So, one can guess the value of each U_j with a different order: $A_0\rightarrow\cdots\rightarrow A_{4n}$. Although $\mathrm{Prob}\{u_i=1\}-\mathrm{Prob}\{u_i=0\}=1-2\alpha\in(0,0.02)$ is not so much, the guess complexity will still be less than the simple brute-force search. From such a point of view, $0.49<\alpha<0.5$ should be replaced by its balanced version: $|\alpha-0.5|<0.01$.

B. Non-Uniformity of U_j when $\alpha=0.5$

From the discussion given above, $\alpha=0.5$ seems to be the best parameter to generate uniformly distributed $\{U_j\}$ that should maximize the value of $Com(\alpha)$. Unfortunately, according to our previous studies on the digital dynamics of piecewise-linear chaotic maps (PWLCM) realized in fixed-point arithmetic [2, Chap. 3], $\alpha=0.5$ is the worst parameter from the viewpoint of dynamical degradation occurring in the discretized space, which destroys the uniform distribution of the generated pseudo-random numbers.

Actually, as a special case of the digital PWLCM, the digital chaotic orbit of $G_{0.5,\beta}$ can be theoretically analyzed, which is similar to but a little more complex than the orbit of $F_{0.5}$. Without loss of generality, assume that the least significant bit of x_0 is the n_{x_0}-th bit after the dot, i.e., $x_0=(0.a_1a_2\cdots a_{n_{x_0}})_2$, where $a_{n_{x_0}}=1$. To facilitate the following discussion, n_{x_0} is called the *binary precision* of x_0. Substituting $\alpha=0.5$ into the equation of $F_{0.5}$, one can get

$$
F_{0.5}: x_i=\begin{cases}2\cdot x_{i-1}, & 0\le x_{i-1}\le 0.5,\\ 2\cdot(1-x_{i-1}), & 0.5<x_{i-1}\le 1.\end{cases} \qquad (15)
$$

It is obvious that $F_{0.5}(x_0)$ must be in the form of $(0.a_1'a_2'\cdots a_{n_{x_0}-1}'0)_2$, where $a_{n_{x_0}-1}'=1$. This means that the *binary precision* of x_0 is decreased by 1 after one iteration. Thus, the digital chaotic orbit of $F_{0.5}$ will always trend to the same fixed point $x=0$ after n_{x_0} iterations.

For $G_{0.5,\beta}$, the introduction of β makes things a little complicated: assuming that the *binary precision* of β is n_β, the orbit of $G_{0.5,\beta}$ will be in the following form:

$$
x_0 \xrightarrow{n_{x_0}\ \text{iterations}} 0\rightarrow\beta \xrightarrow{n_\beta\ \text{iterations}} 0\rightarrow\beta\cdots
$$

$$
0\rightarrow\beta \xrightarrow{n_\beta\ \text{iterations}} 0\rightarrow\beta\cdots
$$

That is, the digital chaotic orbit of $G_{0.5,\beta}$ enters a periodic cycle determined by β after a transient stage determined by x_0. The period of the final cycle is $n_\beta+1$.

[2] The errors are natural results of the unavoidable accumulation of the intermediate quantization errors.

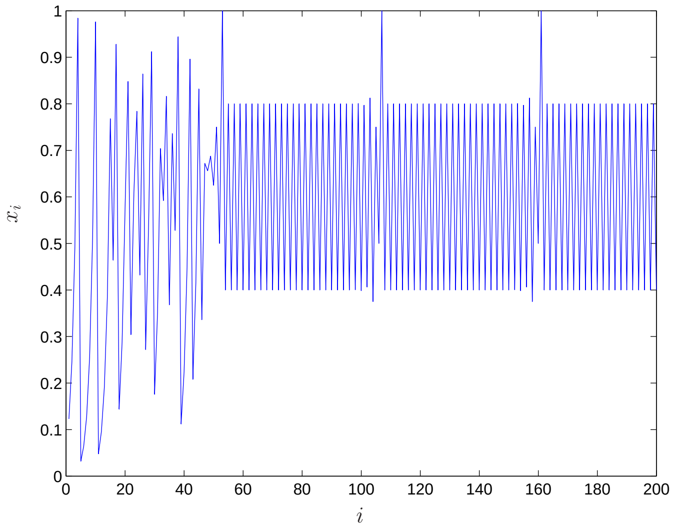

Fig. 3. The digital chaotic orbit of $G_{0.5,0.4}$ when $x_0 = 0.123$.

As an example, when $x_0 = 0.123$, the digital chaotic orbit of $G_{0.5,0.4}$ is shown in Fig. 3. Apparently, such a degraded chaotic orbit will generate badly non-uniform $\{U_j\}$. When $n = 2$, experiments show that the frequency of $U_j = 170$ is about 0.993, which means that the non-uniformity is even worse than the one given in Fig. 1. One more example is also tested by changing the value of α in Fig. 1 from 0.1 to 0.5 (but the values of β and x_0 are kept unchanged), and it is found that the distribution of U_j has two prominent peaks at $U_j = 85$ and 170 (the frequencies are 0.412 and 0.418), respectively.

The above analysis shows that $\alpha = 0.5$ is also a rather bad parameter for the generation of $\{U_j\}$ toward a uniform distribution. So, 0.5 should be excluded from the range of α. For example, the range $|\alpha - 0.5| < 0.01$ should be replaced by $0 < |\alpha - 0.5| < 0.01$.

C. How to Mend This Defect?

Since the non-uniformity of $\{U_j\}$ is mainly caused by the fact that $\mathrm{Prob}\{u_i = 0\} \neq \mathrm{Prob}\{u_i = 1\}$, it is easy to mend it by changing Eq. (4) to the following one:

$$u_i = \begin{cases} 0, & 0 \leq x_i \leq 0.5, \\ 1, & 0.5 < x_i \leq 1. \end{cases} \tag{16}$$

It has been pointed out that dynamical degradation of $G_{0.5,\beta}$ in the digital domain will influence the uniformity of $\{U_j\}$. In fact, this Problem also exists for any $\alpha \neq 0.5$, which has been clarified in [2, Sec. 2.5.1]. Following previous studies, the average length of all digital orbit of the tent map is $O(2^{L/2})$, when L is the bit number of the employed finite-precision arithmetic. For double-finite floating-point arithmetic, $L = 62$, so the average length is about 2^{31}, which is not sufficiently large from the cryptographical point of view. To overcome this Problem and also the non-uniformity caused by the digital dynamical degradation, a small pseudo-random signal is suggested to be used to perturb the digital chaotic orbit timely, as discussed in Secs. 2.5.2 and 3.4.1 of [2].

V. Incapability of Chaos for Security

In Sec. IV-A above, it was mentioned that $(\{U_j\}, \{f_j\})$ is an equivalent of the original key. By studying the possibility of solving for $\{U_j\}$ from chosen plaintext-ciphertext pairs, it can be shown that the security of the Yi-Tan-Siew cipher is independent of the use of the chaotic map $G_{\alpha,\beta}$.

Given a plaintext P_j and the corresponding ciphertext C_j, one can get Eq. (7) for U_{j+1}. Under the condition that f_{j-1} has been reconstructed, it is possible to solve for U_{j+1} with a number of such equations. Apparently, the solvability of U_{j+1} is independent of the chaotic map $G_{\alpha,\beta}$. That is, the security of the cipher is independent of $G_{\alpha,\beta}$. In fact, one can replace the chaotic map with any other PRNG to generate U_j, without influencing the security of the cipher. Therefore, from this point of view, the Yi-Tan-Siew cipher cannot be considered as a typical chaotic cipher.

Next, the solvability of Eq. (7) is discussed. Basically, the mixture of three different operations, XOR, modulo 2^{4n} addition, and f_{j-1}, makes it rather difficult to get U_{j+1} from Eq. (7). Rewrite Eq. (7) as follows:

$$C_j \oplus (P_{j-1} \boxplus U_{j+1}) = f_{j-1} \left(P_j \oplus (C_{j-1} \boxplus U_{j+1}) \right), \tag{17}$$

which can be simplified as

$$a \oplus (b \boxplus x) = f_{j-1}(c \oplus (d \boxplus x)). \tag{18}$$

The task is to find a $4n$-bit integer solution of x from a number of such equations. Considering that f_{j-1} contains n circular left-shift operations, it should have at least 2^n separate branches. This implies that at least 2^n points of intersection between the graph of $a \oplus (b \boxplus x)$ and that of $f_{j-1}(c \oplus (d \boxplus x))$ have to be checked to find the only right integer solution of x. That is, a lower bound of the complexity is $O(2^n)$.

VI. Conclusion

This paper has studied the security of the recently-proposed Yi-Tan-Siew chaotic cipher [1]. Some defects of this cipher have been pointed out and analyzed in detail. The security analyses given in this paper should provide some useful references for better design of various chaotic ciphers in the future.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] X. Yi, C. H. Tan, and C. K. Siew, "A new block cipher based on chaotic tent maps," *IEEE Trans. Circuits Syst. I*, vol. 49, no. 12, pp. 1826–1829, December 2002.

[2] S. Li, "Analyses and new designs of digital chaotic ciphers," Ph.D. dissertation, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, China, June 2003, fulltext is available online at http://www.hooklee.com/pub.html.

[3] B. Schneier, *Applied Cryptography – Protocols, Algorithms, and Souce Code in C*, 2nd ed. New York: John Wiley & Sons, Inc., 1996.

[4] A. Baranovsky and D. Daems, "Design of one-dimensional chaotic maps with prescribed statistical properties," *Int. J. Bifurcation Chaos*, vol. 5, no. 6, pp. 1585–1598, 1995.

[5] E. W. Weisstein, "Geometric distribution," From MathWorld: http://mathworld.wolfram.com/GeometricDistribution.html, 2004.