Baptista-type chaotic cryptosystems: Problems and countermeasures

Shujun Li [a,*], Guanrong Chen [a], Kwok-Wo Wong [b],
Xuanqin Mou [c] and Yuanlong Cai [c]

[a] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China*

[b] *Department of Computer Engineering and Information Technology, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China*

[c] *School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, China*

Abstract

In 1998, M. S. Baptista proposed a chaotic cryptosystem, which has attracted much attention from the chaotic cryptography community: some of its modifications and also attacks have been reported in recent years. In [Phys. Lett. A 307 (2003) 22], we suggested a method to enhance the security of Baptista-type cryptosystem, which can successfully resist all proposed attacks. However, the enhanced Baptista-type cryptosystem has a nontrivial defect, which produces errors in the decrypted data with a generally small but nonzero probability, and the consequent error propagation exists. In this Letter, we analyze this defect and discuss how to rectify it. In addition, we point out some newly-found problems existing in all Baptista-type cryptosystems and consequently propose corresponding countermeasures.

Key words: chaos, encryption, cryptanalysis, Baptista-type chaotic cryptosystem
PACS: 05.45.Ac/Vx/Pq

1 Introduction

In [1], M. S. Baptista proposed a chaotic cryptosystem based on partitioning the visiting interval of chaotic orbits of the logistic map. After its publication,

---

several modified versions have been proposed [2–7]. On the other hand, some attacks have been reported as tools of breaking the original Baptista-type cryptosystem and some of its modified versions [8–11]. In this section, we give a brief survey on Baptista-type chaotic cryptosystems, including the original scheme and some modified versions, and on some proposed attacks. In the following sections, we will show some problems of this class of cryptosystems and then propose some countermeasures for enhancing its overall performance.

At first, we give a detailed introduction to the original Baptista-type cryptosystem, as a basis of the whole Letter. Note that different notations from those in [1] are used to make the description simpler and clearer.

Given a one-dimensional chaotic map $F : X \to X$ and an interval $X' = [x_{\min}, x_{\max}) \subseteq X$, divide X' into S ϵ-intervals: $\forall i = 1 \sim S$, $X_i' = [x_{\min} + (i-1)\varepsilon, x_{\min} + i\varepsilon)$, where $\varepsilon = \dfrac{x_{\max} - x_{\min}}{S}$. Assume that plain messages are composed by S different characters, $\alpha_1, \cdots, \alpha_S$, and use a bijective map,

$$f_S : \boldsymbol{X}_{\boldsymbol{\epsilon}} = \{X_1', \cdots, X_i', \cdots, X_S'\} \to \boldsymbol{A} = \{\alpha_1, \cdots, \alpha_i, \cdots, \alpha_S\}, \qquad (1)$$

to associate the S different ϵ-intervals with the S different characters. By introducing an extra character $\beta \notin \boldsymbol{A}$, we can define a new function $f_S' : X \to \boldsymbol{A} \cup \{\beta\}$ as follows:

$$f_S'(x) = \begin{cases} f_S(X_i'), & x \in X_i', \\ \beta, & x \notin X'. \end{cases} \qquad (2)$$

Based on the above notations, for a plain-message $M = \{m_1, m_2, \cdots, m_i, \cdots\}$ ($m_i \in \boldsymbol{A}$), the original Baptista-type cryptosystem can be described as follows.

- *The employed chaotic system*: the logistic map, $F(x) = bx(1-x)$.
- *The secret key*: the association map f_S, the initial condition x_0 and the control parameter b of the logistic map.
- *The encryption procedure*: a) initialize $x_0^{(0)} = x_0$; b) encrypt the i-th plain-character m_i as follows: iterate the chaotic system from $x_0^{(i-1)}$ to find a chaotic state x satisfying $f_S'(x) = m_i$, record the iteration number C_i as the ith cipher-message unit and $x_0^{(i)} = F^{C_i}\left(x_0^{(i-1)}\right) = F^{C_1+C_2+\cdots+C_i}(x_0)$.
- *The decryption procedure*: for each cipher-message unit C_i, iterate the chaotic system for C_i times from $x_0^{(i-1)}$, and then use $x_0^{(i)} = F^{C_i}\left(x_0^{(i-1)}\right)$ to derive the current plain-character as follows: $m_i = f_S'\left(x_0^{(i)}\right)$.
- *Constraints on C_i*: each cipher-message unit C_i should satisfy $N_0 \leq C_i \leq N_{\max}$ ($N_0 = 250$ and $N_{\max} = 65532$ in [1]). Since there exist many options for each C_i in $[N_0, N_{\max}]$, an extra coefficient $\eta \in [0, 1]$ is used to choose the right number: if $\eta = 0$, C_i is chosen as the minimal number satisfying $f_S'(x) = m_i$; if $\eta \neq 0$, C_i is chosen as the minimal number satisfying $f_S'(x) = m_i$ and $\kappa \geq \eta$ simultaneously, where κ is a pseudo-random number with a normal

distribution within the interval $[0, 1]$.

The original Baptista-type chaotic cryptosystem has the following four defects.

(1) The distribution of the ciphertext is non-uniform, and the occurrence probability decays exponentially as C_i increases from N_0 to N_{max} (see Fig. 3 of [1] and also Fig. 1 of [2]).
(2) At least N_0 chaotic iterations are needed to encrypt a plain-character, which makes the encryption speed very slow as compared with most conventional ciphers.
(3) The ciphertext size is larger than the plaintext size.
(4) It is insecure against some different attacks proposed in [8,9], since some useful information about the chaotic system can be obtained from the ciphertext $\{C_i\}$, i.e., the iteration numbers of the chaotic system.

In recent years, some modifications have been proposed as possible remedies for the above defects [2–7]. Meanwhile, cryptanalysis works have also been developed to break some modifications [10–12].

In [2], the first modified version was proposed to overcome the first defect of the original Baptista-type cryptosystem. According to [10, 12], this modified version is still insecure against the keystream attack proposed in [9].

In [3, 4], to overcome the second defect, the original Baptista-type cryptosystem was enhanced by dynamically updating the association map f_S. However, following the cryptanalysis given in [11], the two modified versions are still insecure, since the essential security defect (i.e., the existence of C_i in the ciphertext) remains. In [5], utilizing the technique proposed in [3, 4], another modified version was further proposed to achieve shorter ciphertext. This modification has not been cryptanalyzed, but the attacks proposed in [11] may be generalized to break it.

In [6], as a new idea of increasing the security, cycling chaos generated by multiple different chaotic attractors is used instead of chaos generated from one single chaotic map. Though the use of multiple chaotic maps can effectively increase the complexity of some attacks, it seems that the keystream attack proposed in [9] may still work to its advantage.

In [7], we proposed a new modification to essentially enhance the security of the original Baptista-type cryptosystem. In this scheme, the original ciphertext stream $\{C_i\}$ is masked by a pseudo-random number stream and then be output as the final ciphertext stream. In this case, it is impossible for an attacker to get the number of chaotic iterations from the ciphertext, so that all proposed attacks will fail. Unfortunately, later we noticed that this modified scheme has a nontrivial defect, which produces errors in the decrypted data with a generally small but nonzero probability. In the next section, we give more

details on this defect and discuss how to rectify it.

In all the above Baptista-type cryptosystems, there exist some general problems that have not been reported before, which can influence the overall performance of the cryptosystems to some extent. In Sec. 3 of this Letter, we will further discuss these problems and provide some corresponding countermeasures.

2 Rectifying our early-proposed remedy of Baptista-type chaotic cryptosystem that can resist all proposed attacks

2.1 A brief introduction of the enhanced Baptista-type cryptosystem

Since the occurrence of C_i in the ciphertext stream is the prerequisite of all proposed attacks, we can bypass it by concealing C_i in the ciphertext stream. A natural idea is to secretly mask C_i with a pseudo-random number stream. It is easy to generate the pseudo-random number stream from the chaotic system itself. Given a pseudo-random number generation function $f_{be}(\cdot)$, using $\oplus$ to denote the masking operation, the enhanced Baptista-type cryptosystem proposed in [7] can be described as follows (without changing other details of the original cryptosystem, such as the constraints on C_i):

- *The encryption procedure*: for the i-th plain-character m_i, iterate the chaotic system starting from $x_0^{(i-1)}$ to find a suitable chaotic state x satisfying $f'_S(x) = m_i$, record the number of chaotic iterations starting from $x_0^{(i-1)}$ to x as $\widetilde{C}_i$ and $x_0^{(i)} = x = F^{\widetilde{C}_i}\left(x_0^{(i-1)}\right)$. Then, the i-th cipher-message unit of m_i is $C_i = \widetilde{C}_i \oplus f_{be}\left(x_0^{(i)}\right)$.
- *The decryption procedure*: for each ciphertext unit C_i, firstly iterate the chaotic system for N_0 times and set $\widetilde{C}_i = N_0$, then perform the following operations: if $\widetilde{C}_i \oplus f_{be}(x) = C_i$ then use the current chaotic state x to derive the plain-character m_i and goto the next ciphertext unit C_{i+1}; otherwise, iterate the chaotic system once and $\widetilde{C}_i + +$, until the above condition is satisfied.
- *The selection of $f_{be}(\cdot)$*: due to the non-uniformity of the ciphertext, it has been known that $f_{be}(\cdot)$ cannot be freely selected to avoid information leaking. For example, the simplest function $f_{be}(x) = x$ is not secure. Two classes of such functions are suggested, and both can make information leaking impossible. If the distribution of C_i is modified to be uniform with some techniques [1], then $f_{be}(\cdot)$ can freely selected.

---

[1] As mentioned in [7], two methods are available: the modification proposed in [2] and the entropy-based lossless compression technique [13].

2.2 A defect in the above modified Baptista-type cryptosystem

Although the above modified Baptista-type cryptosystem can resist the attacks proposed in [8, 9], considering $\widetilde{C}_i \oplus f_{be}(x) = \widetilde{C}'_i \oplus f_{be}(x')$ is possible for $\widetilde{C}_i \neq \widetilde{C}'_i$, erroneous plain-characters may be "decrypted" with a generally small but nonzero probability: at the decipher side, when $\widetilde{C}_i \oplus f_{be}(x) = C_i$, the restored "$\widetilde{C}_i$" may not be the real $\widetilde{C}_i$ at the encipher side, so that the restored chaotic state x is wrong and, as a result, the decrypted plain-character is also wrong.

At first, let us see how serious this defect is. We can estimate the error probability at the encipher side as follows. Apparently, the decryption is correct if and only if the real $\widetilde{C}_i$ never occur before the first x satisfying $f'_S(x) = m'$ is found. That is, for a specific $\widetilde{C}_i$, the probability to successfully restore $\widetilde{C}_i$ (i.e. the probability to get the correct decryption) via the above decryption procedure is

$$P_c\left(\widetilde{C}_i\right) = P\left\{\bigcap_{k=N_0}^{\widetilde{C}_i-1} \left(k \oplus f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right) \neq C_i\right)\right\}$$
$$= P\left\{\bigcap_{k=N_0}^{\widetilde{C}_i-1} \left(f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right) \neq k \oplus C_i\right)\right\}. \tag{3}$$

Generally, assume the bit size of C_i is n (for the original Baptista-type cryptosystem $n = 16$) and the chaotic orbit $\left\{F^k\left(x_0^{(i-1)}\right)\right\}$ has a uniform distribution, we have: $\forall C_i, P\left\{f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right) = C_i\right\} = 2^{-n}$, i.e.,

$$P\left\{f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right) \neq k \oplus C_i\right\} = 1 - 2^{-n}. \tag{4}$$

Assume $f_{be}\left(F^k\left(x_0^{(i-1)}\right)\right) = k \oplus C_i (k = N_0 \sim \widetilde{C}_i - 1)$ are independent events. Then, we can deduce $P_c\left(\widetilde{C}_i\right) = (1 - 2^{-n})^{\widetilde{C}_i - N_0}$. It is obvious that $P_c\left(\widetilde{C}_i\right) \to 0$ as $\widetilde{C}_i \to \infty$, which means any decryption behaves like a random guess after a sufficiently long period of time.

Considering the non-uniform distribution of $\widetilde{C}_i$, for the first plain-character m_1, from the total probability rule we can calculate[2] the final probability $P_{c,1}$:

$$P_{c,1} = \sum_{k=N_0}^{N_{max}} P\left\{\widetilde{C}_i = k\right\} \cdot P_c(k)$$
$$= \sum_{k=N_0}^{N_{max}} P\left\{\widetilde{C}_i = k\right\} \cdot \left(1 - 2^{-n}\right)^{k-N_0}. \tag{5}$$

---

[2] Here, assume $P\{C_i > N_{max}\} = 0$ (see Sec. 3.4 for an explanation).
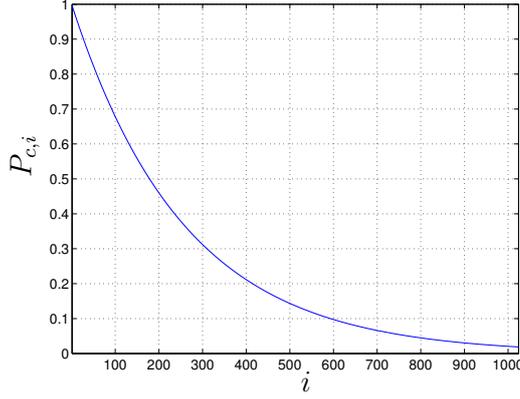
Fig. 1. $P_{c,i}$ with respect to the position of the plain-character i.

To simplify the calculation, without loss of generality, assume $F(x)$ visits each ϵ-interval with the same probability [3] $p = 1/S$. Then, we have $P\{\tilde{C}_i = k\} = p(1-p)^{k-N_0}$, so that

$$
\begin{aligned}
P_{c,1} &= \sum_{k=N_0}^{N_{max}} p(1-p)^{k-N_0} \cdot (1 - 2^{-n})^{k-N_0} \\
&= \sum_{k'=0}^{N_{max}-N_0} p \cdot q^{k'} = p \cdot \frac{1 - q^{N_{max}-N_0}}{1 - q},
\end{aligned}
\tag{6}
$$

where $q = (1-p) \cdot (1 - 2^{-n})$. When $S = 256, n = 16, N_0 = 250, N_{max} = 65532$ (values in the original Baptista-type cryptosystem), $P_{c,1} \approx 0.9961240899211138$. Considering $1/(1 - P_{c,1}) \approx 258$, we expect that one plaintext with wrong leading plain-character will occur averagely in 258 plain-characters. Here, note that all plain-characters after a wrong plain-character will be wrong with a high probability close to 1, i.e., there exists error propagation. It is obvious that the error propagation makes things worse for $i > 1$:

$$
P_{c,i} = \left(\prod_{j=1}^{i-1} P_{c,j} \right) \cdot \frac{p \left(1 - q^{N_{max}-N_0} \right)}{1 - q} = \left(\prod_{j=1}^{i-1} P_{c,j} \right) \cdot P_{c,1} = P_{c,1}^i.
\tag{7}
$$

For the above calculated $P_{c,1}$, $P_{c,i}$ with respect to i is shown in Fig. 1. As i increases, the probability decreases exponentially. Once $P_{c,i}$ goes below $1/S$, a random guess process will replace the role of the designed decipher.

---

[3] logistic map does not satisfy this requirement, so we suggest using PWLCM to replace the logistic map in Sec. 3.1.

2.3   Rectification to the existing defect

Now, we try to rectify the above-discussed encryption/decryption scheme to avoid the existing defect. The goal is to ensure that $\forall i$, $P_{c,i} \equiv 1$.

With a memory unit allocated to store $N_{max} - N_0 + 1$ variables $B[N_0] \sim B[N_{max}]$ representing $C_i = N_0 \sim C_i = N_{max}$ respectively, we propose to change the encryption/decryption procedure as follows:

- *The encryption procedure*: for the i-th plain-character m_i, firstly set $B[N_0] = \cdots = B[N_{max}] = 0$, iterate the chaotic system starting from $x_0^{(i-1)}$ for N_0 times, set $\widetilde{C}_i = N_0$, and then perform the following operations: $C_i = \widetilde{C}_i \oplus f_{be}(x)$, $B[C_i] + +$, if the current chaotic state x satisfying $f_S(x) = m_i$, then a 2-tuple ciphertext $(C_i, B[C_i])$ is generated and set $x_0^{(i)} = x$ and then goto the next plain-character m_{i+1}; otherwise, repeat this procedure until a ciphertext is generated.
- *The decryption procedure*: for each ciphertext unit (C_i, B_i), firstly iterate the chaotic system for N_0 times and set $\widetilde{C}_i = N_0$, then perform the following operations: if $\widetilde{C}_i \oplus f_{be}(x) = C_i$ for the B_j-th times then use the current chaotic state x to derive the plain-character m_i and goto the next ciphertext unit (C_{i+1}, B_{i+1}); otherwise iterate the chaotic system and $\widetilde{C}_i + +$ for 1 iteration, until the above condition is satisfied.

In Fig. 2, we show flow charts for the above rectified encryption and decryption procedures, in which $B[j] = 0$ means setting all $B[j]$ ($j = N_0 \sim N_{max}$) to zeros, $\widetilde{C}'_i = N_0$ denotes N_0 chaotic iterations and setting $\widetilde{C}'_i$ to N_0, and $\widetilde{C}'_i + +$ indicates one chaotic iteration and increasing $\widetilde{C}'_i$ by one.

Compared with the original Baptista-type cryptosystem, this rectified cryptosystem manages to solve the aforementioned defect with a cost of adding more implementation complexity:

(1) Extra memory is needed to store $N_{max} - N_0 + 1$ variables $B[j]$. When each $B[j]$ is stored as a 2-byte integer, the memory size is $2 \times (N_{max} - N_0 + 1)$ bytes. When $N_{max} = 65532$ and $N_0 = 250$, it is not greater than 128 KB.
(2) The encryption speed becomes lower since $N_{max} - N_0 + 1$ variables $B[j]$ should be set to zero for each plain-character.
(3) The ciphertext size becomes even longer: $B[C_i]$ is added into each ciphertext unit.

Fortunately, the requirement on extra memory is acceptable in all digital computers nowadays (128 KB is not so much for a computer with over tens or hundreds of MB in memory), and the encryption speed will not be influenced much when this rectified cipher is implemented in hardware with parallel sup-

a) Encryption procedure b) Decryption procedure
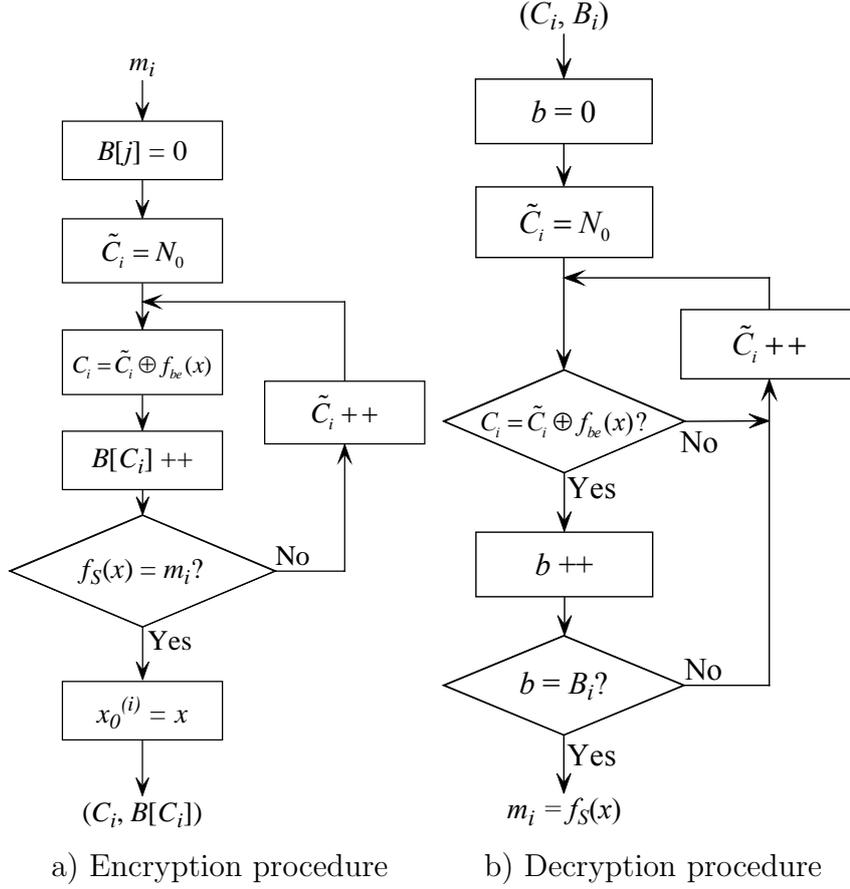
Fig. 2. The encryption and decryption procedures of the rectified Baptista-type cryptosystem.

port: all $N_{max} - N_0 + 1$ variables $B[j]$ can be set to zeros within a clock cycle simultaneously, which eliminates the negative effect on the encryption speed. In addition, chaotic iteration can be run in parallel with $C_i = \widetilde{C}_i \oplus f_{be}(x)$, $B[C_i] + +$ and $f_S(x) = m_i$? with pre-calculation and delay design. Therefore, the above rectification is quite practical in enhancing the performance of Baptista-type cryptosystem. Moreover, the enlargement of the ciphertext size can be effectively minimized by some other methods, which will be discussed in the next subsection.

2.4 Minimizing the enlargement of the ciphertext size

In the rectified cryptosystem, the ciphertext size is prolonged. Some methods can be used to overcome this problem. Here, we introduce two of them.

The first method is to use variable-length ciphertext. For example, we can change the ciphertext as follows:

- When $B[C_i] = 1$ and $N_0 \leq C_i < N_{max}$, output C_i as the ciphertext.
- When $B[C_i] = 1$ and $C_i = N_{max}$, output $(N_{max}, 0)$ as the ciphertext.
- When $B[C_i] > 1$, output $(N_{max}, B[C_i], C_i)$ as the ciphertext.

Assume the size of C_i is n. We can calculate the mathematical expectation of the ciphertext size, corresponding to one plain-character, as follows:

$$(1 - P_{c,1}) \cdot \left(P\left\{ N_0 \leq \widetilde{C}_i < N_{max} \right\} \cdot n + P\left\{ \widetilde{C}_i = N_{max} \right\} \cdot 2n \right) + P_{c,1} \cdot 3n. \quad (8)$$

Since $P\left\{ \widetilde{C}_i = N_{max} \right\} \ll P\left\{ N_0 \leq \widetilde{C}_i < N_{max} \right\}$, it can be approximately reduced to

$$(1 - P_{c,1}) \cdot n + P_{c,1} \cdot 3n = (1 + 2P_{c,2}) \cdot n. \quad (9)$$

Generally, $0 \approx P_{c,1} \ll 1$, so it is only a little bit greater than n, which is the ciphertext size of the original Baptista-type cryptosystem.

Another method is to use the compression algorithm suggested in [7,14]. Since both C_i and $B[C_i]$ have exponentially decreasing distributions, it is natural to use lossless entropy-based compression algorithms to make the ciphertext size shorter. Following the deduction given in [14], assuming that the bit size of C_i is n, the average size of the compressed C_i will be $n/2$. Since generally $0 \approx P_{c,1} \ll 1$, it is obvious that the average size of a compressed $B[C_i]$ will be close to 1 from a probabilistic point of view. That is, the average ciphertext size corresponding to one plaintext will be close to $n + 1$.

Actually, we can also combine the above two methods to obtain a better solution. Using a compressed C_i in the first method can successfully reduce the average ciphertext size to about $n/2$.

3 Some general problems of Baptista-type chaotic cryptosystems and some corresponding countermeasures

3.1 Problems of the logistic map for encryption

In the original Baptista-type chaotic cryptosystem and all its modifications proposed thus far, the logistic map is used as the chaotic system. But the logistic map is not a good chaotic system for encryption due to the following reasons.

a) Non-uniform visiting probability on each ϵ-interval. It is well-known that the logistic map has a non-uniform invariant density function, which cause the visiting probability of each ϵ-interval to be different. Experimental data given in Fig. 2 of [1] have shown such a disadvantage, but Baptista [1] did not

consider it as a negative factor to security. From a cryptographical point of view, this issue indeed is not desirable and may be vulnerable to some subtle statistics-based attacks. In fact, such a disadvantage has been successfully utilized to design an entropy-based attack by Alvarez et al. in [9].

b) Limits on the control parameter b. It is also well-known that the logistic map becomes chaotic when $b > 3.5699\cdots$ and is completely chaotic (with the Lyapunov exponent being maximal) only when $b = 4$. To ensure that the generated orbit is sufficiently chaotic, b has to be sufficiently close to 4, which limits the key space to be a small set near 4. In addition, dynamics of the logistic map with different values of the control parameter b are different, which may be utilized to develop some new attacks. In [14], we have shown a similar defect in the chaotic cryptosystem developed in [15].

To avoid the above problems of the logistic map, we suggest using the following piecewise linear chaotic maps (PWLCM) with the *onto* property [16, §3.2.1] to replace the logistic map. An *onto* PWLCM is generally chaotic and has the following good dynamical properties on its defining interval X [16–19]: 1) its Lyapunov exponent $\lambda = -\sum_{i=1}^{m} \|C_i\| \cdot \ln \|C_i\|$ satisfying $0 < \lambda < \ln m$; 2) it is exact, mixing and ergodic; 3) it has a uniform invariant density function, $f(x) = 1/\|X\| = 1/(\beta - \alpha)$; 4) its auto-correlation function $\tau(n) = \frac{1}{\sigma^2} \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{x})(x_{i+n} - \bar{x})$ approaches zero as $n \to \infty$, where $\bar{x}, \sigma$ are the mean value and the variance of x, respectively. A typical example is the well-known skew tent map with a single control parameter $p \in (0, 1)$:

$$F(x) = \begin{cases} x/p, & x \in [0, p], \\ (1-x)/(1-p), & x \in (p, 1]. \end{cases} \tag{10}$$

Besides the above properties, PWLCM are also the simplest chaotic maps from the digital implementation point of view. In addition, some theoretical results on a direct digital realization of such maps has been rigorously established [17], which are useful for optimizing the implementation of Baptista-type chaotic cryptosystems.

3.2 Problems of the secret key

In the original Baptista-type cryptosystem, the association map f_S also serves as part of the whole secret key. But we believe that f_S should not be included in the secret key from an implementation consideration: it is too long for most users to remember. If a secret algorithm is used to generate f_S, then the secret key will be changed from f_S to the key of the secret algorithm, which is easier to implement.

In [9], the correlation between b and x_0 has been used to develop some theoretical attacks. To avoid potential dangers, it is advisable to use only control parameter(s) as the secret key.

3.3   Dynamical degradation of digital chaotic systems

In all versions of Baptista-type chaotic cryptosystems, dynamical degradation of digital chaotic systems is neglected. However, it has been found that dynamics of chaotic systems can easily collapse in the digital world, and the dynamical degradation may make some negative influences on the performance of digital chaos-based applications [16, 17]. Also, dynamical degradation may enlarge differences among different visiting probabilities of different ϵ-intervals of a chaotic map.

Therefore, some methods should be used to improve such dynamical degradation of the employed chaotic system in all Baptista-type chaotic cryptosystems, which will ensure the visiting probability of each ϵ-interval to be close enough to the theoretical value. As we discussed in [16, 17], a pseudo-random perturbation algorithm is desirable and hence is recommended: use a simple pseudo-random number generator (PRNG) to generate a small signal, to perturb the concerned chaotic orbit every $\Delta \geq 1$ iterations.

3.4   A trivial problem when $C_i > N_{max}$

The original Baptista-type cryptosystem did not consider what one should do if $C_i > N_{\max}$. It seems to presume that C_i will never be greater than $N_{\max}$. However, this is obviously not true. Here, assume $F(x)$ visits each ϵ-interval with the same probability, $p = 1/S$. We can deduce that

$$P\{C_i > N_{\max}\} = P\{C_i - N_0 > N_{\max} - N_0\} = (1-p)^{N_{\max}-N_0}. \tag{11}$$

Although this probability is very small when $N_{\max}$ is large enough, it is nevertheless non-zero. To make the cryptosystem rigorously complete, we propose to use the following $(n+1)$-tuple data to replace C_i when $C_i \geq N_{\max}$: $(\overbrace{N_{\max}, \cdots, N_{\max}}^{n}, c_i)$, where the number of total chaotic iterations is equal to $C_i = N_{\max} \times n + c_i$. Apparently, $(\overbrace{N_{\max}, \cdots, N_{\max}}^{n}, c_i)$ can be represented in a more brief format: $(N_{\max}, n, c_i)$. When $C_i = N_{\max}$, the 3-tuple ciphertext $(N_{\max}, n, c_i)$ can be further reduced to $(N_{\max}, 0)$.

In fact, it is also acceptable to modify the original cryptosystem as follows: once $C_i = N_{\max}$ occurs, immediately output a 2-tuple data $(N_{\max}, m_i)$ instead

of C_i. Considering $P\{C_i > N_{\max}\}$ is very small, such a tiny chance of information leaking does no harm on the security of the cryptosystem in practice.

Acknowledgements

References

[1] M. S. Baptista, Cryptography with chaos, Physics Letters A 240 (1-2) (1998) 50–54.

[2] W.-K. Wong, L.-P. Lee, K.-W. Wong, A modified chaotic cryptographic method, Computer Physics Communications 138 (3) (2001) 234–236.

[3] K.-W. Wong, A fast chaotic cryptographic scheme with dynamic look-up table, Physics Letters A 298 (4) (2002) 238–242.

[4] K.-W. Wong, A combined chaotic cryptographic and hashing scheme, Physics Letters A 307 (5-6) (2003) 292–298.

[5] K.-W. Wong, S.-W. Ho, C.-K. Yung, A chaotic cryptography scheme for generating short ciphertext, Physics Letters A 310 (1) (2003) 67–73.

[6] A. Palacios, H. Juarez, Cryptography with cycling chaos, Physics Letters A 303 (5-6) (2002) 345–351.

[7] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems, Physics Letters A 307 (1) (2003) 22–28.

[8] G. Jakimoski, L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, Physics Letters A 291 (6) (2001) 381–384.

[9] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of an ergodic chaotic cipher, Physics Letters A 311 (2-3) (2003) 172–179.

[10] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Keystream cryptanalysis of a chaotic cryptographic method, Computer Physics Communications 156 (2) (2003) 205–207.

[11] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of dynamic look-up table based chaotic cryptosystems, Physics Letters A 326 (3-4) (2004) 211–218.

[12] W. Wong, L. Lee, K. Wong, Reply to the comment "Keystream cryptanalysis of a chaotic cryptographic method", Computer Physics Communications 156 (2) (2003) 208.

[13] K. R. Castleman, Digital Image Processing, Prentice Hall Inc., New York, 1996.

[14] S. Li, X. Mou, Y. Cai, Improving security of a chaotic encryption approach, Physics Letters A 290 (3-4) (2001) 127–133.

[15] E. Alvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, New approach to chaotic encryption, Physics Letters A 263 (1999) 373–375.

[16] S. Li, Analyses and new designs of digital chaotic ciphers, Ph.D. thesis, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, China, available online at `http://www.hooklee.com/pub.html` (2003).

[17] S. Li, G. Chen, X. Mou, On the dynamical degradation of digital piecewise linear chaotic maps, accepted by Int. J. Bifurcation and Chaos, preprint available online at `http://www.hooklee.com/pub.html` (August 2004).

[18] A. Baranovsky, D. Daems, Design of one-dimensional chaotic maps with prescribed statistical properties, Int. J. Bifurcation and Chaos 5 (6) (1995) 1585–1598.

[19] A. Lasota, M. C. Mackey, Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics, 2nd Edition, Springer-Verlag, New York, 1997.