International Journal of Cryptology Research 1(2): 205-214 (2009)

The Beta-Transformation: A Case Study for Chaos Base Cryptography

[1]M.R.K.Ariffin and [2]M.S.M.Noorani

[1]Al-Kindi Cryptography Research Laboratory,
Laboratory of Theoretical Mathematics,
Institute for Mathematical Research and
Department of Mathematics, Faculty of Science,
Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[2]School of Mathematical Sciences,
Universiti Kebangsaan Malaysia,43600 UKM Bangi, Selangor, Malaysia
Email: [1]rezal@math.upm.edu.my, [2]msn@ukm.my

ABSTRACT

In this paper we study characteristics of the beta-transformation and its suitability as a candidate for implementation as a symmetric cryptosystem. For $\beta > 1$ the beta-transformation is given by $f_\beta(x) = \beta x(\mathrm{mod}\,1)$ and $x \in [0,1]$. It is well known that its Lyapunov exponent is $\lambda = \log \beta$. Since $\lambda > 0$, it ensures that the beta-transformation is a non-linear chaotic system. Finally, we will also attempt to build a discrete version of the beta-transformation.

INTRODUCTION

Chaotic dynamical systems dissipate information due to orbital instability with positive Lyapunov exponents and ergodicity. If these properties are appropriately utilized, chaotic cryptosystems are supposed to realize high security. Chaos theory deals with dynamical systems with loss of information along the orbits. Such chaotic properties as ergodicity and sensitive dependence on initial conditions and on system parameters, are quite advantageous to construct secure communication schemes. The idea of using chaos for data encryption can be traced to a paper by Shannon. Shannon suggested of using measure preserving transformations which depend on their arguments in a ‘sensitive’ way.

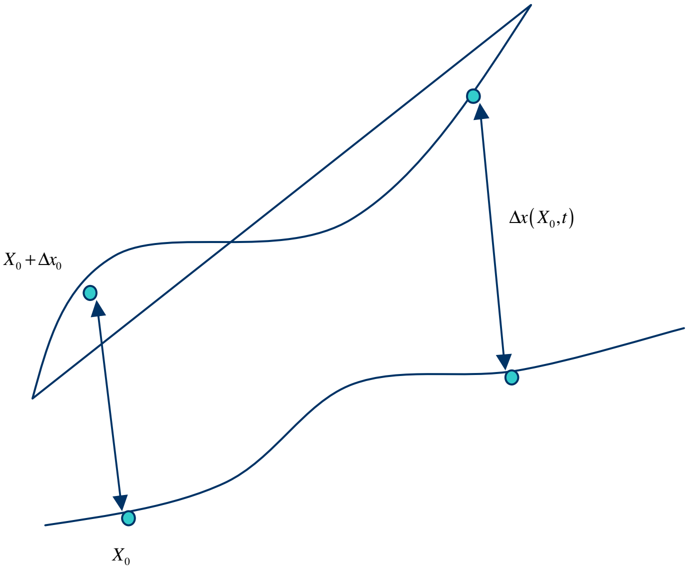
It is widely accepted that chaotic dynamical systems have good diffusion properties (spreading out the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical property of the plaintext.) and Confusion properties (use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext.)

BACKGROUND-CHAOTIC PROPERTY

A non-linear system is chaotic if it has a positive Lyapunov exponent. That is,

$$\lambda = \lim_{\substack{t\to\infty \\ |\Delta x_0 \to 0|}} \frac{1}{t} \ln \frac{\left|\Delta x\left(x_0, t\right)\right|}{\left|\Delta x_0\right|} > 0$$

Graphically,



Let us consider a one dimensional dynamical system $f : I \to I$. When $\lambda > 0$,

$$\forall \varepsilon > 0, \exists n_1, n_2, \exists x \in U_{n_1, n_2}, \forall n \in \left[n_1, n_2\right], \forall z_1, z_2 \in U_{n_1, n_2}$$
$$\exp\left\{\left(\lambda - \varepsilon\right)n\right\}\left|z_1 - z_2\right| < \left|f^n\left(z_1\right) - f^n\left(z_2\right)\right| < \exp\left\{\left(\lambda + \varepsilon\right)n\right\}\left|z_1 - z_2\right|$$

This means that the initial distance $\left|z_1 - z_2\right|$ between 2 arbitrary points z_1, z_2 (which are elements of the neighborhood U_{n_1, n_2} of point *x*) after *n* iterations will increase at least $\exp\left\{\left(\lambda - \varepsilon\right)n\right\}$ times.

THE BETA-TRANSFORMATION

The one-dimensional beta-transformation is given by

$$f_\beta(x)=\begin{cases}\beta x \text{ if } 0\le x<\dfrac{1}{\beta}\\ \vdots\\ \beta x-k \text{ if } \dfrac{k}{\beta}\le x<\dfrac{k+1}{\beta}\\ \vdots\\ \beta x-(\beta-1) \text{ if } \dfrac{\beta-1}{\beta}\le x\le 1\end{cases}$$

or simply $f_\beta(x)=\beta x(\mathrm{mod}\,1)$ for $\beta>1$.

The Lyapunov exponent is given by $\lambda=\log\beta>0$. It is also known that the beta-transformation is ergodic. Hence, the beta-transformation is a 'good' candidate for chaos based cryptography.

However, the beta-transformation is defined on a continuum (i.e.[0,1]). Real-time application (such as on the computer) is discrete and finite in nature. Hence, we would have to 'discretize' the beta-transformation.

However, setbacks while discretizing the beta-transformation be observed from the following definition:

Definition 1

Let X be a finite (generally large) set and *F* be a map of *X* onto itself. The sequence defined by

$$x_{n+1}=F\left(x_n\right),\ n=0,1,2,\ldots,\ x_0\in X$$

is called a discrete iteration.

Discrete iterations either end at fixed points or in cycles of certain length. Thus, for our system we will not depend on the number of cycles as our key security feature while building this SYMMETRIC encryption system.

THE DISCRETE BETA-TRANSFORMATION

The discrete beta-transformation will be defined by:

$$Y = F_B\left(X\right) = BX\left(\operatorname{mod} N\right) = \begin{cases} BX & BX < N \\ 0 & BX = N \\ BX - N & BX > N \end{cases}$$

The k- th iteration is $F_B^k\left(X\right) = F_B\left(F_B^{k-1}\left(X\right)\right)$

It is invertible when N and B are co-prime.

THE INVERSE

$$X = F^{-1}(Y) = \begin{cases} \dfrac{Y+N}{B} & ,\dfrac{Y+N}{B} \in Z \\ 0 & ,Y = 0 \\ \dfrac{Y}{B} & ,\dfrac{Y+N}{B} \notin Z \end{cases}$$

THE SYMMETRIC CRYPTOSYSTEM

We will proceed in building this symmetric system by defining the keys involved:

- The pair (B,N)
- The set $\{k_j\}_{j=1}^{M}$ which should be used in an orderly manner as the number of iteration of the transformation. It could be either a collection of pseudo-random numbers or not, as long as it remains secret.

SENSITIVE DEPENDENCE ON PLAINTEXT

We will now investigate the sensitivity of our discrete beta-transformation on two adjacent initial conditions (i.e. the plaintext).

Let n_1 be the number of iterations either for $F_B(X_0) < N$ to eventually become $F_B^k(X_0) > N$ or vice-versa.

<u>Lemma 1</u>

If $BX_0 < N$ after the *k₁-th* iteration where k_1 is given by

$$k_1 = \left\lceil \log\left(\frac{N}{X_0}\right)\frac{1}{\log B} \right\rceil$$

(i.e. the ceiling function) we will have $F_B^{k_1}(X_0) > N$.

<u>Lemma 2</u>

If $BX_0 > N$ after the k_2-th iteration where k_2 is given by

$$k_2 = \left\lfloor \log\left(\frac{N}{N - X_0(B-1)}\right)\frac{1}{\log B} \right\rfloor$$

(i.e. the floor function) we will have $F_B^{k_2}(X_0) < N$.

Suppose $X_2 = X_1 + 1$ (i.e. distance of unity).

<u>Case 1</u>

Let $F_B(X_1) < N$ and $F_B(X_2) < N$
After (m_1-1) iterations, $F_B^{m_1}(X_1) > N$
After (m_2-1) iterations, $F_B^{m_2}(X_2) > N$
Let n_1=min{m_1-1,m_2-1}. After n_1 iterations distance of unity becomes B^{n_1} .

Case 2

Let $F_B(X_1) > N$ and $F_B(X_2) > N$

After (m$_1$-1) iterations, $F_B^{m_1}(X_1) < N$

After (m2-1) iterations, $F_B^{m_2}(X_2) < N$

Let n_1=min{m$_1$-1,m$_2$-1}. After $n_1$iterations distance of unity becomes B^{n_1}.

Case 3

Let $F_B(X_1) < N$ and $F_B(X_2) > N.$

After (m$_1$-1) iterations $F_B^{m_1}(X_1) > N$

After (m2-1) iterations, $F_B^{m_2}(X_2) < N$

Let n_1=min{m$_1$-1,m$_2$-1}. After n_1 iterations distance of unity becomes $B^{n_1} - \sum_{i=0}^{n_1-1} B^i N$.

For all possible cases, any adjacent plaintexts diverge the corresponding ciphertexts from each other exponentially. This will ensure independent behavior of 2 ciphertexts from 2 close plaintexts.

Coupled with the fact that we use the set $\{k_j\}_{j=1}^{M}$(i.e. iteration value) 2 close plaintext will in fact diverge from each other independently. In fact even if we were to encrypt the same plaintext again the possibility the result would be the same will be s/M where s is the number of times a particular k_j emerges.

SENSITIVE DEPENDENCE ON KEYS

Case 1

Let $B_2 = B_1 + 1$, $N_2 = N_1 + 1$, $F_{B_2}(X_0) < N_1$ and $F_{B1}(X_0) < N_1$.

Then , $\left| F_{B_2}^k(X_0) - F_{B_1}^k(X_0) \right| = \left| \left(\sum_{i=1}^{k} \binom{k}{i} B_1^{k-i} \right) X_0 \right|$.

Case 2

Let $B_2 = B_1 + 1$, $N_2 = N_1 + 1$, $F_{B_2}(X_0) > N_2$ and $N_2 = N_1 + 1$.

Then,

$$\left|F_{B_2}^k(X_0) - F_{B_1}^k(X_0)\right| = \left|\left(\sum_{i=1}^{k}\binom{k}{i}B_1^{k-i}X_0\right) - \left(N\left(\sum_{u=0}^{k-1}\left(\sum_{u=0}^{v}\binom{v}{u}B_1^{v-u}\right) + \sum_{j=1}^{k-1}B_1^j\right)\right)\right|$$

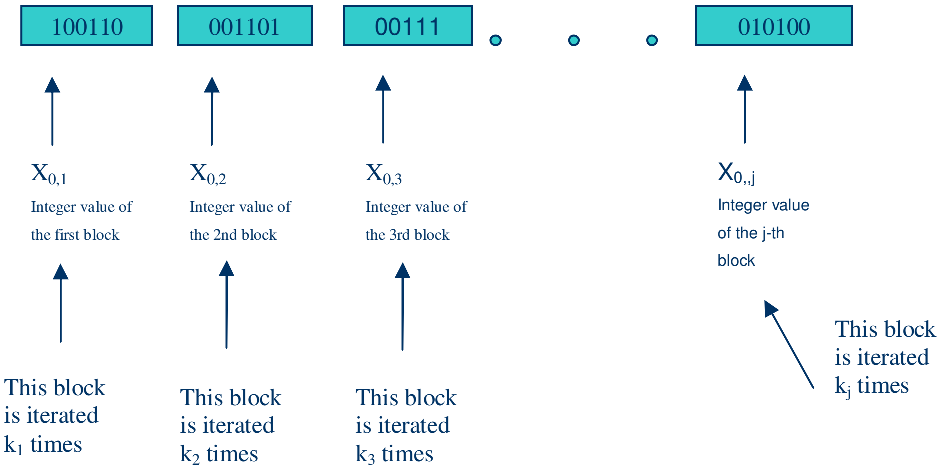
Case 3

Let $B_2 = B_1 + 1$, $N_2 = N_1 + 1$, $F_{B_2}(X_0) > N_2$ and $F_{B2}(X_0) > N_1$.

Then, $\left|F_{B_2}^k(X_0) - F_{B_2}^k(X_0)\right| = \left|(2N_1 + 1)\sum_{i=0}^{k-1}B_2^i\right|$.

For all possible cases, any adjacent keys will diverge the corresponding ciphertexts from each other exponentially. This will ensure independent behavior of 2 ciphertexts from 2 close keys.

SYMMETRIC BLOCK CIPHERS


100110
001101
00111
010100
X0,1
Integer value of the first block
X0,2
Integer value of the 2nd block
X0,3
Integer value of the 3rd block
X0,,j
Integer value of the j-th block
This block is iterated k1 times
This block is iterated k2 times
This block is iterated k3 times
This block is iterated kj times

STRENGTH-BRUTE FORCE ATTACK

Definition 2

A cryptosystem is ε - secure against brute-force attacks when, for almost all pairs of initial conditions $x_0^{'}$ and x_0 such that $\left|x_0 - x_0^{'}\right| \geq \varepsilon$, the corresponding orbits get apart from each other by 0.9x10^k after k-iterations needed to encrypt/decrypt the message.

Therefore, if $\varepsilon = 1$ is the distance between 2 adjacent keys, the maximal security is attained after an initial transient $T > T_0$, when the distance $\left|x_{T_0} - x_{T_0}^{'}\right| \geq \varepsilon$ is of the order 10^m.

An estimation of T$_0$ comes from $B^m = (1) B^{\lambda T_0}$, which gives $T_0 = \dfrac{m}{\lambda}$

Say the eavesdropper tries a pair of key (B*, N*) such that |B-B*|=1 and |N-N*|=1. Let $\varepsilon \to 0$.

One will have either $\left|\dfrac{Y}{B} - \dfrac{Y}{B^*}\right| \geq \dfrac{Y}{BB^*} > 0$ or $\left|\dfrac{Y+N}{B} - \dfrac{Y+N^*}{B^*}\right| \geq \dfrac{Y + NB^* - BN^*}{BB^*} > 0$ or $\left|\dfrac{Y}{B} - \dfrac{Y+N^*}{B^*}\right| \geq \dfrac{Y - N^*B}{BB^*} > 0$ or $\left|\dfrac{Y+N}{B} - \dfrac{Y}{B^*}\right| \geq \dfrac{Y + NB^*}{BB^*} > 0$.

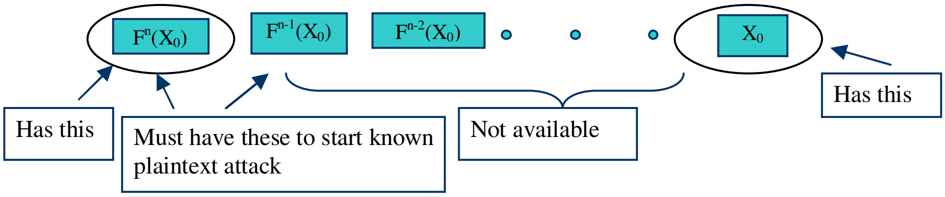
STRENGTH-KNOWN CIPHERTEXT ATTACK

Eavesdropper has Y, tries to get B&N from $\dfrac{Y+N}{B} \in Z$. Infinitely many possibilities.

Eavesdropper has Y, tries to get B&N from $\dfrac{Y+N}{B} \notin Z$. Infinitely many possibilities.

STRENGTH-KNOWN PLAINTEXT ATTACK

Eavesdropper has X_0 and $Y = F_B^n(X_0)$ tries to get B&N. Since no information on the values of $F_B^{n-1}(X_0), F_B^{n-2}(X_0), \ldots$, this type of attack is infeasible.



REFERENCES

Fridrich, J. 1998. Symmetric Ciphers Based on 2-dimensional Chaotic Maps. *Int. Journal of Bifurcations and Chaos.* **8**(6): 1259-1284.

Kocarev, L. 2001. Chaos Based Cryptography: A Brief Overview. *Circuits and Systems.* **1**(3): 6-21.

Kotulski, Z., Szczepanski, J. 1999. On the Application of Discrete Chaotic Dynamical Systems to Cryptography. DCC Method. *Biuletyn Wat. ROK XLVIII.* **NR 10**(566):111-123.

Kotulski, Z., Szczepanski, J. 1997. Discrete Chaotic Cryptography. *Ann. Physik,* **6**:381-394.

Masuda, N., Aihara, K. 2002. Cryptosystems with Discretized Chaotic Maps. *IEEE Transactions on Circuits and Systems-I. Fundamental Theory and Applications.* **49**(1): 28-40.

Olivera, L.P.L., Sobottka, M. 2006. Cryptography with Chaotic Mixing. *Chaos, Solitons and Fractals,* doi:10.1016. 2006.05.049.

Schmitz, R. 2001. Use of Chaotic Dynamical Systems in Cryptography. *Journal of the Franklin Institute,* **338:** 429-441.

Shannon, C.E. October 1949. Communication Theory of Secrecy Systems. T*he Bell SystemTechnical Journal.* **28**(4): 656-715.

S.Li, X. Mou, Y. Cai. 2003. Chaotic Cryptography in Digital World: State of the Art, Problems and Solutions. *Comuter Science Preprint Archive,* **2003**(1): 65-79

Yoshioka, D., Tsuneda, A., Inoue, T. October 2005. On Transformation between Discretized Bernoulli and Tent Maps. *IEICE Trans. Fundamentals*. **E88-A**.(10):2678-2683.