Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91

Eli Biham

Abstract

In this conference, Habutsu[1] suggested a cryptosystem based on iterating a chaotic map. In this paper several properties of this cryptosystem are studied and two cryptanalytic attacks are described.

1 Introduction

The cryptosystem based on iterating chaotic maps encrypts 64-bit plaintexts using a key α into a random 147-bit ciphertext out of the 2^{75} ciphertexts corresponding to the plaintext. The plaintexts and the ciphertexts are viewed as numbers between zero and one whose least significant bits are 2^{-64} and 2^{-147} respectively and the key α is between 0.4 and 0.6. The encryption process which contains 75 iterations using 75 random bits r_i is formulated by

$$\begin{aligned} a_{75} &= P \\ a_{i-1} &= \begin{cases} \alpha a_i, & \text{if } r_i = 0; \\ (\alpha - 1)a_i + 1, & \text{if } r_i = 1 \end{cases} \\ T &= a_0 \end{aligned}$$

where P is the plaintext and T is the ciphertext. The decryption process is

$$\begin{aligned} a_0 &= T \\ a_{i+1} &= \begin{cases} a_i/\alpha, & \text{if } a_i \le \alpha; \\ (a_i - 1)/(\alpha - 1), & \text{if } a_i > \alpha \end{cases} \\ P &= a_{75}. \end{aligned}$$

2 Properties

The ciphertext size is much larger than the plaintext size. In the decryption process we find the plaintext along with the 75 random bits r_i used in the choice of a_{i-1}'s. In order to make the ciphertext size closer to the plaintext size we can change the encryption function to have 139-bit plaintexts, from which 64 bits enter as the plaintext of the original function and 75 bits enter in place of the random bits r_i.

This modification has several disadvantages which lead to several possible attacks. One of the chosen plaintext attacks fixes all the 75 "random" bits to zero. In this case the ciphertext is just $T = \alpha^{75}P$ and α is easily derivable from $\alpha^{75} = T/P$. A simple ciphertext only attack can easily predict r_1 which is now one bit of the plaintext. If $T \leq 0.4$ then $r_1 = 0$. If $T \geq 0.6$ then $r_1 = 1$. If $T \leq 0.4^2$ then the last two random bits can be predicted and if $T \leq 0.4^k$ then k random bits can be predicted.

Another observation is that for each fixed choice of the random bits r_i there is a linear relationship between the plaintexts and the ciphertexts. All the ciphertexts received using a fixed choice of the random bits are in a small range. Therefore, if we only find two ciphertext in such a range and their corresponding plaintexts we can find the linear relationship $T = c_r P + d_r$. The limits of the range are just $T_0 = c_r \cdot 0 + d_r = d_r$ and $T_1 = c_r + d_r$. We can easily decrypt any ciphertext in this range by this relationship and can encrypt any plaintext into this range.

In contrast to the remark in [1] that about 147 ciphertext bits (44 decimal digits) always suffice for a successful decryption, we observed that more than 164 ciphertext bits (about 50 decimal digits) are needed. For example, in the range near the zero ciphertext, where all the random bits are chosen as $r_i = 0$ and the key is taken as $\alpha = 0.4$, the 2^{64} possible plaintexts are encrypted into a range of size about $\alpha^{75} = 0.4^{75} \approx 2^{-100}$. Therefore, the difference between two consecutive ciphertexts in this range is about $2^{-100} \cdot 2^{-64} = 2^{-164}$. In the analysis in this paper we ignore this technical difficulty and assume that the ciphertext size suffices.

3 A Chosen Ciphertext Attack

The ciphertext range corresponding to the choice of all the 75 random bits to be zero ($r_i = 0$) is $[0, \alpha^{75}]$ ($2^{-100} < \alpha^{75} < 2^{-55}$). In this range every ciphertext corresponds to the plaintext $P = T/\alpha^{75}$. In particular, for any key α any ciphertext $T \leq 2^{-100}$ is in this range. Therefore, the following chosen ciphertext attack finds α:

1. Choose a ciphertext $T \leq 2^{-100}$.
2. Request the decrypted plaintext P of T.
3. Calculate $\alpha^{75} = T/P$ and derive α.

The attack uses only one chosen ciphertext and its corresponding plaintext.

4 A Known Plaintext Attack

We observed that each choice of the random bits r_i leads to a ciphertext range for which there is a linear correlation between the plaintexts and the ciphertexts $T = c_r P + d_r$, where c_r and d_r depend on the choice of the r_i's and the key α. The values of c_r and d_r are

$$\begin{aligned} c_r &= \prod_{i=1}^{75} \alpha - r_i \\ d_r &= \sum_{i=1}^{75} r_i \prod_{j=1}^{i-1} \alpha - r_j. \end{aligned}$$

We can see that the value of c_r depends only on the number n_0 of the r_i's with values zero rather than on the actual values of the r_i's. Therefore, for a given α, there are only 76 possible values of c_r which are $c_r = \alpha^{n_0} \cdot (\alpha - 1)^{75-n_0}$, $n_0 \in \{0, \ldots, 75\}$. The 38 even values of n_0 cause negative values of c_r and the 38 odd values of n_0 cause positive values of c_r.

Given about 2^{38} known plaintexts and their corresponding ciphertexts, there is a high probability to have two plaintexts which are encrypted by the same choice of random bits. In such a pair the difference between the ciphertexts should be smaller than c_r, and in particular, smaller than 2^{-50} (since $c_r < 2^{-50}$). The average difference between two adjacent ciphertexts is much larger (about 2^{-38}).

In the attack, we search for the pairs of adjacent ciphertexts whose difference is sufficiently small, find the value of c_r they suggest by $c_r = \frac{T_2 - T_1}{P_2 - P_1}$ and solve the polynoms $c_r = \alpha^{n_0} \cdot (\alpha - 1)^{75-n_0}$ numerically for all the 38 choices of n_0 for which c_r has the calculated sign. Each such polynom has at most two solutions in the range $0.4 \leq \alpha \leq 0.6$ and every solution is verified by decrypting ciphertexts and comparing the result to the known plaintexts.

This attack needs about 2^{38} known plaintexts and has complexity about 2^{38}.

References

[1] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, Shinsaku Mori, *A Secret Key Cryptosystem by Iterating Chaotic Map*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'91, pp. 127–140, 1991.