International Journal of Bifurcation and Chaos, Vol. 13, No. 7 (2003) 1937–1948

APPROXIMATIONS OF DYNAMICAL SYSTEMS AND THEIR APPLICATIONS TO CRYPTOGRAPHY

J. M. AMIGÓ
Operations Research Center, Miguel Hernández University,
03202 Elche, Spain
jm.amigo@umh.es

J. SZCZEPAŃSKI
Institute of Fundamental Technological Research,
Polish Academy of Sciences, 00-049 Warsaw, Poland
Centre of Trust and Certification "Centrast" Co., Poland
jszczepa@ippt.gov.pl

Received February 18, 2001; Revised December 15, 2001

During the last years a new approach to construct safe block and stream ciphers has been developed using the theory of dynamical systems. Since a block cryptosystem is generally, from the mathematical point of view, a family (parametrized by the keys) of permutations of n-bit numbers, one of the main problems of this approach is to adapt the dynamics defined by a map f to the block structure of the cryptosystem. In this paper we propose a method based on the approximation of f by periodic maps T_n (v.g. some interval exchange transformations). The approximation of automorphisms of measure spaces by periodic automorphisms was introduced by Halmos and Rohlin. One important aspect studied in our paper is the relation between the dynamical properties of the map f (say, ergodicity or mixing) and the immunity of the resulting cipher to cryptolinear attacks, which is currently one of the standard benchmarks for cryptosystems to be considered secure. Linear cryptanalysis, first proposed by M. Matsui, exploits some statistical inhomogeneities of expressions called linear approximations for a given cipher. Our paper quantifies immunity to cryptolinear attacks in terms of the approximation speed of the map f by the periodic T_n. We show that the most resistant block ciphers are expected when the approximated dynamical system is mixing.

Keywords: Approximations of dynamical systems; block ciphers; immunity to linear cryptanalysis.

1. Introduction

Nowadays, secure communications play an important role in many fields of common life like telecommunications, industry, banking, commerce, etc. Traditionally, this issue has been handled with increasingly sophisticated algorithms like DES (private key block cipher) or RSA (public key encryption), which eventually have to be upgraded as computer power makes theoretical threads more practical. The construction of such algorithms is based on number theory, algebra, algebraic geometry (recently: elliptic curves over finite fields), combinatorics and complexity theory.

During the last decade, different alternatives to algorithmic encryption have been proposed. One of them makes use of the theory of both continuous and discrete dynamical systems to construct cryptosystems. This approach relies on dynamical properties such as ergodicity, mixing, chaos, ... to obtain safe ciphers. In the frame of the continuous theory, the method of synchronization of chaotic systems [Kapitaniak, 1996] and chaos control [Kapitaniak, 1996; Ott *et al.*, 1990] are applied. In the case of discrete systems, the method focuses on iterations of chaotic (ergodic, mixing, ...) maps and intelligent ways of introducing secret keys.

The earliest applications of continuous systems in cryptography were proposed by Pecora and Caroll [1990] as a possible application of the synchronization of chaotic dynamical systems. This idea has been further developed by Kocarev *et al.* [1992] and Parlitz *et al.* [1992], where they present an experimental test system based on a chaotic electronic circuit. In the first paper analog signals are used, while digital information is used in the second one. Other more recent applications of chaos synchronization to cryptography in the case of discrete maps can be found in [Millerioux & Mira, 1997, 1998]. For an overview of encryption methods based on the modulation of the trajectories of continuous dynamical systems, see [Kapitaniak, 1996]. On the other hand, application of discrete chaotic systems to cryptography was first proposed by Habutsu *et al.* [1991] and developed in [Kotulski, 1997, 1999; Fridrich, 1998; Kohda & Tsuneda, 1997].

In practical applications, the main problem of this approach consists of adapting the dynamics defined on a continuum to the n-bit block structure of the cryptosystems. While it is probably true that the typical behavior of finite approximations of chaotic systems should "converge" to that of their continuous counterparts, only very little is known so far. As a matter of fact, one expects that the better the ergodic properties of the approximated dynamical system, the better the cryptographic properties of the discrete maps obtained in the process of approximation. The subject of this paper is precisely the relation between the dynamical system used for encryption and the quality of the resulting cryptosystem. Traditionally, extensive statistical testing was used to assess this quality. Currently interest has shifted to immunity to linear and differential cryptanalysis and their modifications, which exploits certain statistical inhomogeneities of the block ciphers most commonly used. In the following pages, we will deal only with linear cryptanalysis.

Assuming that obtaining arbitrary numbers of known plaintext–ciphertext pairs is feasible, linear cryptanalysis (proposed by Matsui [1993]) provides the most powerful attack on DES to date [Menezes *et al.*, 1997]. The idea behind Matsui's method is to construct a linear approximation among the bits of the plaintext, the corresponding ciphertext and the key used for encryption such that the deviation $|p - \frac{1}{2}|$ is large, where p is the probability over all plaintexts (considered equiprobable) that the linear approximation constructed holds. It is known that the best block cipher occurs when the deviation of all linear approximations equals $2^{-(n+2)/2}$, n being the block length of the cipher. This raises the question of how to design such maps. We prove that the discrete approximations of appropriate dynamical systems provide a family of block permutations which implements such cryptosystems.

This paper is organized as follows. Sections 2 and 3 are devoted to introduce the concepts of dynamical systems and linear cryptanalysis, respectively, needed in Sec. 4 to study the cryptanalytical properties of the periodic approximations of dynamical systems, which build the core of the present paper. Section 5 contains the conclusions and final remarks.

2. Approximations of Dynamical Systems

Let $(X, \mathcal{A}, \mu)$ be a measure space and $(\mathcal{P}_n)_{n\geq 1}$ a sequence of increasingly finer partitions of $(X, \mathcal{A}, \mu)$. We say that $(\mathcal{P}_n)_{n\geq 1}$ is a *Lebesgue sequence* if, for every nested sequence $(P_n)_{n\geq 1}$ with $P_n \in \mathcal{P}_n$, the intersection $\bigcap_{n\geq 1} P_n$ contains exactly one point. The measure space $(X, \mathcal{A}, \mu)$ is a *Lebesgue space* if there exists $X_0 \in \mathcal{A}$ with $\mu(X\backslash X_0) = 0$ such that $(X_0, \mathcal{A} \cap X_0, \mu|\mathcal{A} \cap X_0)$ has a Lebesgue sequence of partitions.

The following statement [Cornfeld *et al.*, 1982] refers to the automorphisms of Lebesgue spaces.

Theorem 2.1. *If T is an aperiodic automorphism of the Lebesgue space $(X, \mathcal{A}, \mu)$, then for all $\varepsilon > 0$ and every $n \in \mathbb{N}$ there is a set $E \in \mathcal{A}$ such that*

(1) *the sets $E, TE, \ldots, T^{n-1}E$ are disjoint,*
(2) $\mu\Big(\bigcup_{i=0}^{n-1} T^i E\Big) > 1 - \varepsilon$.

An ergodic automorphism $T : X \to X$ is said to be *uniquely ergodic* if (up to normalization) there exists only one T-invariant measure. For uniquely ergodic automorphism, the Birkhoff–Khinchin ergodic theorem can be sharpened in the following way [Cornfeld *et al.*, 1982]:

Theorem 2.2. *Let T be an automorphism of the probability space $(X, \mathcal{A}, \mu)$. The following conditions are equivalent*:

1. *T is uniquely ergodic.*
2. *For every f continuous on X, the sequence $\left(\frac{1}{n}\sum_{i=0}^{n-1} f(T^i(x))\right)_{n\geq 1}$ uniformly converges to a constant $\kappa(f)$.*
3. *Every $x \in X$ is typical for the dynamical system $(X, \mathcal{A}, \mu, T)$.*

Moreover, given $\varepsilon > 0$ the estimate

$$\begin{aligned}\left\|\frac{1}{n}\sum_{i=0}^{n-1} f\circ T^i - \kappa(f)\right\| &= \sup_{x\in X}\left|\frac{1}{n}\sum_{i=0}^{n-1} f(T^i(x)) - \kappa(f)\right| \\ &\leq \frac{2\|g\|}{n} + \varepsilon \qquad (1)\end{aligned}$$

holds for every $n \in \mathbb{N}$, where

$$\kappa(f) = \int_X f d\mu \qquad (2)$$

and g is a continuous function in X such that

$$\|f - \kappa(f) - (g\circ T - g)\| < \varepsilon \qquad (3)$$

Observe that the parameters n and ε appearing in (1) can be chosen independently.

Suppose T is an automorphism of the Lebesgue space $(X, \mathcal{A}, \mu)$. We shall consider sequences of finite partitions $(\mathcal{P}_n)_{n\geq 1}$ of the space X and sequences of automorphisms $(T_n)_{n\geq 1}$ such that T_n preserves the partition $\mathcal{P}_n = \{P_i^{(n)} : 1 \leq i \leq q_n\}$, i.e. T_n sends every element of $\mathcal{P}_n$ into an element of the same partition. By $\mathcal{A}(\mathcal{P}_n)$ we denote the σ-algebra of subsets of X generated $(\text{mod}\, 0)$ by the elements of $\mathcal{P}_n$, i.e. $\mathcal{A}(\mathcal{P}_n)$ is generated by $P_i^{(n)} \cup N$, $1 \leq i \leq q_n$, for any $N \subset X$ with $\mu(N) = 0$. The notation $\mathcal{P}_n \to \mathcal{E}$ when $n \to \infty$, where $\mathcal{E}$ is the partition of X into separate points, means that for each $A \in \mathcal{A}$ there is a sequence of sets $A_n \in \mathcal{A}(\mathcal{P}_n)$ such that $\mu(A_n \Delta A) \to 0$ when $n \to \infty$. Since the number of elements of the partition $\mathcal{P}_n$ is finite, the trajectory of each $P_i^{(n)}$ under T_n is finite, i.e. for some $r_i \in \mathbb{N}$, $1 \leq i \leq q_n$, we will have $T_n^{r_i} P_i^{(n)} = P_i^{(n)}$.

One important example of partition-preserving maps are the interval exchange transformations. Without loss of generality, we say that a map $T : [0, 1] \to [0, 1]$ is an *interval exchange transformation* if it is injective and there exist numbers $0 = t_0 < t_1 < \cdots < t_m = 1$ and $a_i \in \mathbb{R}$, $1 \leq i \leq m$, such that for every i and every $t_{i-1} < x < t_i$ we have

$$T(x) = \sigma_i x + a_i$$

where $\sigma_i = +1$ or -1. Obviously T preserves Lebesgue measure. If $\sigma_i = +1$ for every i we say that the interval exchange transformation preserves orientation.

Partition preserving transformations can be used to approximate measure preserving automorphisms [Cornfeld *et al.*, 1982].

Definition 2.3. Suppose $f(n) \downarrow 0$.

1. Let T be an automorphism of the Lebesgue space $(X, \mathcal{A}, \mu)$, $\mathcal{P}_n \to \mathcal{E}$ a sequence of partitions of X and T_n a sequence of automorphisms of $(X, \mathcal{A}, \mu)$ preserving $\mathcal{P}_n$. Then, $(T_n, \mathcal{P}_n)$ is said to be a *periodic approximation of the first type* of T *with speed* $f(n)$ if
$$\sum_{i=1}^{q_n} \mu(TP_i^{(n)} \Delta T_n P_i^{(n)}) < f(q_n)\,,$$
$n = 1, 2, \ldots$
2. If for the sequences $(\mathcal{P}_n)$, (T_n), where T_n is a periodic automorphism of order p_n, we have the inequality
$$\sum_{i=1}^{q_n} \mu(TP_i^{(n)} \Delta T_n P_i^{(n)}) < f(p_n)\,,$$
$n = 1, 2, \ldots$, and the linear operators $U_{T_n} : L^2(X, \mathcal{A}, \mu) \to L^2(X, \mathcal{A}, \mu)$ defined by
$$U_{T_n}(f) := f \circ T_n$$
converge to $U_T : f \mapsto f \circ T$ in the strong topology of operators in $L^2(X, \mathcal{A}, \mu)$, then $(T_n, \mathcal{P}_n)$ is said to be a *periodic approximation of the second type* of T *with speed* $f(n)$.
3. If $(T_n, \mathcal{P}_n)$ is a periodic approximation of the first type of T and T_n cyclically permutes the elements of $\mathcal{P}_n$, then $(T_n, \mathcal{P}_n)$ is said to be a *cyclic approximation* of T *with speed* $f(n)$.

If nothing else is stated, periodic approximations are meant to be of the first kind. It follows from Theorem 2.1 (known as the Rohlin–Halmos Lemma) that any automorphism can be approximated by periodic ones. Clearly, the faster the automorphism T is approximated by periodic ones, the worse are its statistical properties, v.g. ergodicity and mixing. In fact, the following result can be proved [Cornfeld *et al.*, 1982]:

Theorem 2.4

(1) *If the automorphism T possesses an approximation of the first type by a periodic transitive transformation with speed θ/n and $\theta < 4$, then T is ergodic.*

(2) *If the automorphism T possesses an approximation of the second type with speed θ/n and $\theta < 2$, then T is not mixing.*

3. Linear Cryptanalysis

We start this section by defining some basics of block ciphers. Let $\mathbb{Z}_2 = \{0, 1\}$ be the two-element field provided with the binary sum ($0\oplus 0 = 1\oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$) and the product, and denote by

$$\begin{aligned}\mathbb{Z}_2^n &= \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \\ &= \{\xi = (\xi_1, \ldots, \xi_n) : \xi_i = 0,\, 1 \text{ for } 1 \le i \le n\}\end{aligned}$$

the set of *n-bit blocks* (or *words*). The set of k-bit (secret) *keys* will be denoted by $\mathcal{K}$.

Definition 3.1. An *n-bit block cipher* is a function $E_K : \mathbb{Z}_2^n \times \mathcal{K} \to \mathbb{Z}_2^n$ such that for each key $K \in \mathcal{K}$, $E(P, K)$ is an invertible map (the *encryption function* for K) from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ written $E_K(P)$. The inverse mapping is the *decryption function*, denoted $D_K(C)$.

$$\begin{aligned}E_K :\quad &\mathbb{Z}_2^n \quad\to\quad \mathbb{Z}_2^n \\ &P = (p_1, \ldots, p_n) \mapsto C = (c_1, \ldots, c_n)\,.\end{aligned}$$

Each P is called a *plaintext* and $C = E_k(P)$, the corresponding *ciphertext*.

Among the most frequently used ciphers, the Data Encryption Standard (DES) is the most well-known block cipher. It is defined by the American standard FIPS 46-2.

Linear cryptanalysis was first envisaged as a known-plaintext attack to DES, although it is also well fitted to mount an attack on other kinds of block ciphers. A *known-plaintext attack* is one where the adversary has a quantity of plaintext and corresponding ciphertext.

The purpose of linear cryptanalysis is to find the following "effective" linear expression (also called linear approximation) of a given cipher algorithm:

$$\begin{aligned}P[i_1, i_2, \ldots, i_a] &\oplus C[j_1, j_2, \ldots, j_b] \\ &= K[k_1, k_2, \ldots, k_c] \qquad (4)\end{aligned}$$

where $P[i_1]$ denotes the ith bit of P (and analogously for C and K),

$$P[i_1, i_2, \ldots, i_a] := P[i_1] \oplus \cdots \oplus P[i_a]$$

(and analogously for C and K), $i_1, \ldots, j_b$ and $k_1, \ldots, k_c$ denote fixed bit locations and Eq. (4) holds with probability $p \neq 1/2$ for randomly given plaintext P and the corresponding ciphertext C. The magnitude of $|p - 1/2|$ represents the *effectiveness* of Eq. (4). The actual value of p can be determined by a detailed analysis of the encrypting algorithm for all (eventually, "almost" all) key numbers. In doing this, one typically derives relations of the form (4) for one or several rounds (taking into account that the output of a round is the input of the next one) and then applies the following lemma:

Lemma 3.2 (Piling-up Lemma). *Let X_i $(1\le i\le n)$ be independent random variables whose values are 0 with probability p_i or 1 with probability $1-p_i$. Then the probability that $X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0$ is*

$$\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2}\right).$$

Once one succeeds in reaching an effective linear expression, it is possible to determine one key bit $K[k_1, k_2, \ldots, k_c]$ by the following two-step algorithm based on the maximum likelihood method [Matsui, 1993]:

Algorithm. *Let N be the number of plaintexts.*

1. (***Step 1***) *Determine the number N_0 of plaintexts such that the left side of Eq. (4) is equal to zero.*
2. (***Step 2***) *If $N_0 > N/2$, then guess*

$$K[k_1, k_2, \ldots, k_c] = \begin{cases} 0 & \text{when } p > 1/2 \\ 1 & \text{when } p < 1/2 \end{cases}$$

If $N_0 < N/2$, then guess

$$K[k_1, k_2, \ldots, k_c] = \begin{cases} 1 & \text{when } p > 1/2 \\ 0 & \text{when } p < 1/2 \end{cases}.$$

The most effective linear expression (i.e. $|p - 1/2|$ is maximal) is called the *best expression* and the corresponding probability p, the *best probability*.

The following lemma describes the success rate of this method:

Lemma 3.3. *Let N be the number of given random plaintexts and p be the probability that Eq.* (4) *holds,* *and assume* $|p-1/2|$ *is sufficiently small. Then the success rate of the foregoing* Algorithm *is*

$$\int_{-2\sqrt{N}|p-1/2|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx\,. \tag{5}$$

According to (5), the bigger $|p-1/2|$ is, the smaller number N of plaintexts one needs to achieve a given success rate. Numerical integration yields the success rate of Algorithm 1:

$N = \frac{1}{2}\lvert p-1/2\rvert^{-2}$	$\lvert p-1/2\rvert^{-2}$	$2\lvert p-1/2\rvert^{-2}$
92.1%	97.7%	99.8%

4. Cryptanalytical Properties of the Approximations of Dynamical Systems

For simplicity we will discuss two-dimensional dynamical systems defined, without loss of generality, in the unit interval $[0,\,1]\times[0,\,1] \equiv [0,\,1]^2$ and establish the connection between them and the structure of n-bit block ciphers. Higher dimensional dynamical systems are treated analogously. For the reader's convenience, we keep (essentially) the notation of Matsui [1996].

Given any pair of binary sequences $\Gamma_P = (\pi_1, \ldots, \pi_n) \neq 0$, $\Gamma_C = (\gamma_1, \ldots, \gamma_n) \neq 0$ and a map $S_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, define $f_{\Gamma_P,\Gamma_C} : \mathbb{Z}_2^n \to \mathbb{Z}_2$ as

$$\xi = (\xi_1, \ldots, \xi_n) \mapsto 1 \oplus \xi \circ \Gamma_P \oplus S_n(\xi) \circ \Gamma_C$$

where $\alpha\circ\beta$ denotes the parity (0 or 1) of the bitwise product of α and β, i.e.

$$\xi \circ \Gamma_P := \xi_1\pi_1 \oplus \cdots \oplus \xi_n\pi_n \in \{0,\,1\}$$

and, analogously,

$$S_n(\xi) \circ \Gamma_C = S(\xi)_1\gamma_1 \oplus \cdots \oplus S(\xi)_n\gamma_n \in \{0,\,1\}$$

Observe that the products $\xi \circ \Gamma_P$ and $S_n(\xi) \circ \Gamma_C$ "pick up" those bits of ξ and $S_n(\xi)$ which positions are given by the entries 1 in Γ_P and Γ_C, respectively. Indeed, if

$$\pi_i = \begin{cases} 1 & \text{for } i = i_1,\, i_2, \ldots,\, i_a \\ 0 & \text{otherwise} \end{cases}$$

and

$$\gamma_j = \begin{cases} 1 & \text{for } j = j_1,\, j_2, \ldots,\, j_b \\ 0 & \text{otherwise} \end{cases}$$

then, for all $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{Z}_2^n$,

$$\xi \circ \Gamma_P = \xi_{i_1} \oplus \cdots \oplus \xi_{i_a}\,,$$

$$S_n(\xi) \circ \Gamma_C = S_n(\xi)_{j_1} \oplus \cdots \oplus S_n(\xi)_{j_b}$$

and

$$\begin{aligned} &f_{\Gamma_P,\Gamma_C}(\xi) \\ &\quad = 1 \oplus \xi_{i_1} \oplus \cdots \oplus \xi_{i_a} \oplus S_n(\xi)_{j_1} \oplus \cdots \oplus S_n(\xi)_{j_b} \end{aligned}$$

Sometimes one says that the bits of ξ and $S_n(\xi)$ are masked by Γ_P and Γ_C, respectively.

Let $S : [0,\,1]^2 \to [0,\,1]^2$ be a map and $\mathcal{P}_n = \{P(\xi) : \xi \in \mathbb{Z}_2^n\}$ a partition of $[0,\,1]^2$. Then, given $x \in [0,\,1]^2$, we have $x \in P(\xi)$ for some $\xi \in \mathbb{Z}_2^n$ and $S(x) \in P(\eta)$ for some $\eta \in \mathbb{Z}_2^n$. This being the case, set

$$x \circ \Gamma_P := \xi \circ \Gamma_P\,, \quad S(x) \circ \Gamma_C := \eta \circ \Gamma_C \tag{6}$$

As a matter of fact, the function $f_{\Gamma_P,\Gamma_C} : \mathbb{Z}_2^n \to \mathbb{Z}_2$ induces a map $\overline{f}_{\Gamma_P,\Gamma_C} : [0,\,1]^2 \to \mathbb{Z}_2$ in the obvious way:

$$\begin{aligned} &\overline{f}_{\Gamma_P,\Gamma_C}(x) \\ &\quad = 1 \oplus \xi \circ \Gamma_P \oplus \eta \circ \Gamma_C \\ &\quad = 1 \oplus \xi_1\pi_1 \oplus \cdots \oplus \xi_n\pi_n \oplus \eta_1\gamma_1 \oplus \cdots \oplus \eta_n\gamma_n \end{aligned} \tag{7}$$

Lemma 4.1. *Let* $\Gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_2^n$, $\Gamma \neq 0$, *and define*

$$A_\Gamma = \{x \in [0,\,1]^2 : x \circ \Gamma = 0\}$$

$$B_\Gamma = \{x \in [0,\,1]^2 : x \circ \Gamma = 1\} = [0,\,1]^2 \sim A_\Gamma$$

Then, $P(\xi) \subset A_\Gamma$ *or* $P(\xi) \subset B_\Gamma$ *for any* $\xi \in \mathbb{Z}_2^n$ *and*

$$\#\{P(\xi) \subset A_\Gamma\} = \#\{P(\xi) \subset B_\Gamma\}\,.$$

Proof. For any $x \in P(\xi)$, $x \circ \Gamma = \xi \circ \Gamma = 0$ or 1 and, therefore, $P(\xi) \subset A_\Gamma$ or $P(\xi) \subset B_\Gamma$, respectively. On the other hand, suppose $\gamma_{i_0} = 1$ (remember that $\Gamma = (\gamma_1, \ldots, \gamma_n) \neq 0$) and call, as usual, $e_k = (0, \ldots, 1, \ldots, 0)$ the kth unit vector of $\mathbb{Z}_2^n$. Then

$$P(\xi) \subset A_\Gamma \Rightarrow P(\xi \oplus e_{i_0}) \subset B_\Gamma$$

and

$$P(\xi) \subset B_\Gamma \Rightarrow P(\xi \oplus e_{i_0}) \subset A_\Gamma$$

where here

$$\begin{aligned} \xi \oplus e_{i_0} &= (\xi_1, \ldots, \xi_n) \oplus (0, \ldots, 1, \ldots, 0) \\ &= (\xi_1, \ldots, \xi_{i_0} \oplus 1, \ldots, \xi_n) \end{aligned}$$

Since $e_{i_0} \oplus e_{i_0} = 0$, it follows that the pairing $P(\xi) \leftrightarrow P(\xi \oplus e_{i_0})$ is well defined, with each element being in a different set of the partition $A_\Gamma \cup B_\Gamma = [0,\,1]^2$. ■

For notational convenience, we use eventually the labeling

$$\mathcal{P}_n = \{P_k : 1 \leq k \leq 2^n\}$$

instead of $\mathcal{P}_n = \{P(\xi) : \xi \in \mathbb{Z}_2^n\}$. Choose, for example, $k = \xi_1 \cdot 2^n + \cdots + \xi_{n-1} \cdot 2 + \xi_n$.

Corollary 4.2. *Let $S : [0, 1]^2 \to [0, 1]^2$ be a μ-preserving ergodic map and $\mathcal{P}_n = \{P_k : 1 \leq k \leq 2^n\}$, a partition of $[0, 1]^2$. If $\mu(P_k) = 1/2^n$ for all k, then*

$$\mu(\overline{f}_{\Gamma_P,\Gamma_C}) := \int_{[0,1]^2} \overline{f}_{\Gamma_P,\Gamma_C}(x) d\mu(x) = \frac{1}{2} \tag{8}$$

for every Γ_P, $\Gamma_C \in \mathbb{Z}_2^n$.

Proof. From the definitions (6) and (7) one has

$$\begin{aligned}
&S^i(x) \circ \Gamma_P \in A_{\Gamma_P} \ \&\ S^{i+1}(x) \circ \Gamma_C \in A_{\Gamma_C} \\
&\qquad \Rightarrow \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) = 0 \\
&S^i(x) \circ \Gamma_P \in A_{\Gamma_P} \ \&\ S^{i+1}(x) \circ \Gamma_C \in B_{\Gamma_C} \\
&\qquad \Rightarrow \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) = 1 \\
&S^i(x) \circ \Gamma_P \in B_{\Gamma_P} \ \&\ S^{i+1}(x) \circ \Gamma_C \in A_{\Gamma_C} \\
&\qquad \Rightarrow \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) = 1 \\
&S^i(x) \circ \Gamma_P \in B_{\Gamma_P} \ \&\ S^{i+1}(x) \circ \Gamma_C \in B_{\Gamma_C} \\
&\qquad \Rightarrow \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) = 0
\end{aligned}$$

for $i = 0, 1, \ldots$.

On the other hand, owing to Lemma 4.1 and to the hypothesis $\mu(P_k) = 1/2^n$ for $1 \leq k \leq 2^n$,

$$[0, 1]^2 = A_{\Gamma_P} \cup B_{\Gamma_P} = A_{\Gamma_C} \cup B_{\Gamma_C}$$

with $\mu(A_{\Gamma_P}) = \mu(B_{\Gamma_P}) = \mu(A_{\Gamma_C}) = \mu(B_{\Gamma_C}) = 1/2$ for all $\Gamma_P, \Gamma_C \in \mathbb{Z}_2^n$. Since S preserves the measure μ of $[0, 1]^2$ and is ergodic, the orbit of x under the action of S is uniformly dense in $[0, 1]^2$, for almost every $x \in [0, 1]^2$. It follows

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\nu=0}^{N-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^\nu(x)) = \frac{1}{2}$$

Apply now the ergodic theorem. ■

From the mathematical point of view, any bijection of n-bit numbers, $S_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, can be considered an n-bit block cipher. Set as before

$$\begin{aligned}
N_0 &= \#\{\xi \in \mathbb{Z}_2^n : \xi \circ \Gamma_P \oplus S_n(\xi) \circ \Gamma_C = 0\} \\
&= \#\{\xi \in \mathbb{Z}_2^n : f_{\Gamma_P,\Gamma_C}(\xi) = 1\}
\end{aligned}$$

where Γ_P, $\Gamma_C \in \mathbb{Z}_2^n$, and define

$$LP^{S_n}(\Gamma_P, \Gamma_C) := \left(2\,\frac{N_0}{2^n} - 1\right)^2 \tag{9}$$

By definition, $0 \leq LP^{S_n}(\Gamma_P, \Gamma_C) \leq 1$.

Let p be the probability for the linear approximation

$$\xi \circ \Gamma_P \oplus S_n(\xi) \circ \Gamma_C = K \circ \Gamma_K$$

to hold. Then,

(i) if $K \circ \Gamma_K = 0$,

$$\left(p - \frac{1}{2}\right)^2 = \left(\frac{N_0}{2^n} - \frac{1}{2}\right)^2 = \frac{1}{4} LP^{S_n}(\Gamma_P, \Gamma_C)$$

(ii) if $K \circ \Gamma_K = 1$,

$$\begin{aligned}
\left(p - \frac{1}{2}\right)^2 &= \left(\frac{2^n - N_0}{2^n} - \frac{1}{2}\right)^2 \\
&= \left(\frac{1}{2} - \frac{N_0}{2^n}\right)^2 \\
&= \frac{1}{4}\, LP^{S_n}(\Gamma_P, \Gamma_C)
\end{aligned}$$

In any of both cases,

$$\left|p - \frac{1}{2}\right| = \frac{1}{2}\sqrt{LP^{S_n}(\Gamma_P, \Gamma_C)}$$

or

$$LP^{S_n}(\Gamma_P, \Gamma_C) = 4\left(p - \frac{1}{2}\right)^2$$

Furthermore, it can be proved [Matsui, 1996] that

$$\sum_{\Gamma_P \in \mathbb{Z}_2^n} LP^{S_n}(\Gamma_P, \Gamma_C) = 1 \quad \forall\, \Gamma_C \in \mathbb{Z}_2^n$$

The natural quantity measuring the *immunity* of the cipher S_n to linear cryptanalysis is [Matsui, 1996]

$$LP^{S_n}_{\max} := \max_{\Gamma_P,\Gamma_C \neq 0} LP^{S_n}(\Gamma_P, \Gamma_C)$$

the immunity being higher the smaller $LP^{S_n}_{max}$ is. One also speaks of *resistance* against linear cryptanalysis with the same meaning.

Thus, immunity of S_n to linear cryptanalysis means that $LP^{S_n}(\Gamma_P, \Gamma_C)$ should be uniformly distributed in Γ_P (resp. Γ_C) for fixed Γ_C (resp. Γ_P) so that

$$LP^{S_n}(\Gamma_P, \Gamma_C) \simeq \frac{1}{2^n} \quad \forall\, \Gamma_P, \Gamma_C \in \mathbb{Z}_2^n$$

We show below that the permutations obtained by means of periodic approximations of appropriate dynamical systems have this property.

A permutation $S_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ is called *cyclic* if the orbit of $\xi \in \mathbb{Z}_2^n$, $\{\xi, S\xi, S^2\xi, \dots, S^{2^n-1}\xi\}$, is $\mathbb{Z}_2^n$ for all ξ. If S_n is a cyclic permutation on $\mathbb{Z}_2^n$, formula (9) can be written as

$$LP^{S_n}(\Gamma_P, \Gamma_C) = 4\left(\frac{1}{2^n}\sum_{i=0}^{2^n-1} f_{\Gamma_P,\Gamma_C}(S_n^i(\xi)) - \frac{1}{2}\right)^2 \tag{10}$$

where, according to (7),

$$f_{\Gamma_P,\Gamma_C}(S_n^i(\xi)) = 1 \oplus S_n^i(\xi)\circ\Gamma_P \oplus S_n^{i+1}(\xi)\circ\Gamma_C \in \mathbb{Z}_2$$

Given a transitive map $S : [0, 1]^2 \to [0,1]^2$, set

$$LP^{S}(\Gamma_P, \Gamma_C) = 4\left(\frac{1}{2^n}\sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) - \frac{1}{2}\right)^2$$

where $\overline{f}_{\Gamma_P,\Gamma_C} : [0, 1]^2 \to \mathbb{Z}_2$ is the map induced by f_{Γ_P,Γ_C} as in (7) via a partition $\mathcal{P}_n = \{P(\xi) : \xi \in \mathbb{Z}_2^n\}$. In particular, if $(S_n, \mathcal{P}_n)$ is a cyclic approximation of S, then

$$LP^{S_n}(\Gamma_P, \Gamma_C) = 4\left(\frac{1}{2^n}\sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) - \frac{1}{2}\right)^2 \tag{11}$$

Suppose S_n sends $P(\xi)$ to $P(\eta)$ and define the permutation $S_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ by $\eta = S_n(\xi)$. Observe that, although we use the same letter for the periodic approximation and the corresponding permutation, there is no confusion since the first is defined on points or intervals of $[0, 1]^2$, whereas the latter only makes sense on n-bit blocks. Hence, if $S_n^i(x) \in P(\xi)$ and $S_n^{i+1}(x) \in P(\eta)$, then

$$\begin{aligned}\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) &= 1 \oplus \xi\circ\Gamma_P \oplus \eta\circ\Gamma_C \\ &= f_{\Gamma_P,\Gamma_C}(S_n^i(\xi))\end{aligned}$$

$0 \le i \le 2^n - 1$, which shows that (10) and (11) are actually the same.

The expression (11) relates a cryptanalytical quantity (a measure of immunity to linear cryptanalysis) to a dynamical quantity (average of $\overline{f}_{\Gamma_P,\Gamma_C}$ along orbits), allowing to study the first one with the help of the second.

Lemma 4.3. *Let* $\overline{f}_{\Gamma_P,\Gamma_C} : [0, 1]^2 \to \{0, 1\}$ *be as in (7)* $S : [0, 1]^2 \to [0, 1]^2$ *an automorphism with invariant measure* μ *and* $g : [0, 1]^2 \to \mathbb{R}$ *a continuous map such that*

$$\|\overline{f}_{\Gamma_P,\Gamma_C} - \kappa - (g\circ S - g)\| < \frac{\varepsilon}{4} \tag{12}$$

where $\kappa \in \mathbb{R}$, $\varepsilon > 0$ *and* $\|\cdot\|$ *denotes the supremum norm in* $C([0, 1]^2)$, *the space of the continuous functions defined in* $[0, 1]^2$. *Then* g *can be chosen such that*

$$K_\varepsilon := \|g\| > 1 - \varepsilon\,.$$

Proof. First of all notice that the condition (12), which says that $\overline{f}_{\Gamma_P,\Gamma_C} - \kappa$ is "almost" a cocycle, does not fix $\|g\|$. Indeed, if g fulfills (12), so does $g_\alpha := g + \alpha$ for every $\alpha \in \mathbb{R}$ since $g_\alpha \circ S - g_\alpha = g\circ S - g$. This being the case, α can be chosen in such a way that $\|g_\alpha\|$ is minimal, namely

$$\begin{aligned}g_\alpha(x) &= g(x) - \frac{g(x^*) + g(x_*)}{2} \\ &= \frac{2g(x) - g(x^*) - g(x_*)}{2}\end{aligned}$$

where x^*, $x_* \in [0, 1]^2$ are points where g reaches its maximum and minimum, respectively. Then

$$\begin{aligned}\|g_\alpha\| &= g_\alpha(x^*) = -g_\alpha(x_*) \\ &= \frac{g(x^*) - g(x_*)}{2}\end{aligned} \tag{13}$$

Therefore, we may suppose in the following without loss of generality that g is "centered" so that it fulfills (13).

For all $x \in X_{\Gamma_P,\Gamma_C} := \{x \in [0, 1]^2 : \overline{f}_{\Gamma_P,\Gamma_C}(x) = 0\}$ one has the bound

$$|-\kappa - g(S(x)) + g(x)| < \frac{\varepsilon}{4}$$

and, for all $y \in Y_{\Gamma_P,\Gamma_C} := \{y \in [0, 1]^2 : \overline{f}_{\Gamma_P,\Gamma_C}(y) = 1\} = [0, 1]^2 \sim X_{\Gamma_P,\Gamma_C}$, the bound

$$|1 - \kappa - g(S(y)) + g(y)| < \frac{\varepsilon}{4}$$

hence

$$\begin{aligned}\frac{\varepsilon}{2} &> |\kappa + g(S(x)) - g(x)| \\ &\quad + |1 - \kappa - g(S(y)) + g(y)| \\ &\ge |1 + g(S(x)) - g(S(y)) + g(y) - g(x)| \\ &\ge |1 + g(S(x)) - g(S(y))| - |g(x) - g(y)|\end{aligned} \tag{14}$$

Choose $x \in X_{\Gamma_P,\Gamma_C}$ and $y \in Y_{\Gamma_P,\Gamma_C}$ such that $|g(x) - g(y)| < \varepsilon$. Then

$$|1 + g(S(x)) - g(S(y))| < \frac{3\varepsilon}{2}$$

so that

$$1 - \frac{3\varepsilon}{2} < g(S(y)) - g(S(x)) < 1 + \frac{3\varepsilon}{2} \tag{15}$$

Consider now the images $S(X_{\Gamma_P,\Gamma_C})$ and $S(Y_{\Gamma_P,\Gamma_C})$. Because of ergodicity these sets have nonempty intersections with X_{Γ_P,Γ_C} and Y_{Γ_P,Γ_C}. This means that there exists a point z such that every neighborhood U of z has a nonempty intersection with X_{Γ_P,Γ_C}, Y_{Γ_P,Γ_C}, $S(X_{\Gamma_P,\Gamma_C})$ and $S(Y_{\Gamma_P,\Gamma_C})$. In $S^{-1}(U)$ there are points $x \in X_{\Gamma_P,\Gamma_C}$, $y \in Y_{\Gamma_P,\Gamma_C}$ such that $|g(x) - g(y)| < \varepsilon$ and $S(x) \in X_{\Gamma_P,\Gamma_C}$, $S(y) \in Y_{\Gamma_P,\Gamma_C}$. Hence, applying the inequality (14) with $S(x)$ and $S(y)$ instead of x and y, respectively, one obtains

$$\frac{\varepsilon}{2} > |1 + g(S(y)) - g(S(x))| - |g(S^2(y)) - g(S^2(x))|$$

Thus

$$\begin{aligned} &|g(S^2(y)) - g(S^2(x))| \\ &\qquad \geq |1 + g(S(y)) - g(S(x))| - \frac{\varepsilon}{2} \\ &\qquad > 2 - \frac{3\varepsilon}{2} - \frac{\varepsilon}{2} \\ &\qquad = 2 - 2\varepsilon \end{aligned}$$

where (15) was used. Finally,

$$\begin{aligned} \|g\| &= \frac{g(x^*) - g(x_*)}{2} \\ &\geq \frac{g(S^2(y)) - g(S^2(x))}{2} > 1 - \varepsilon \quad \blacksquare \end{aligned}$$

Observe that $\|g\|$ does not depend on Γ_P, Γ_C, but only on ε.

Lemma 4.4. *Let $S : [0, 1]^2 \to [0, 1]^2$ be a uniquely ergodic automorphism with invariant measure μ such that*

$$\mu(\overline{f}_{\Gamma_P,\Gamma_C}) = \int_{[0,1]^2} \overline{f}_{\Gamma_P,\Gamma_C}(x) d\mu(x) = \frac{1}{2}$$

and suppose $(S_n, \mathcal{P}_n)$, $\mathcal{P}_n = \{P_k : 1 \leq k \leq 2^n\}$, is a cyclic approximation of S. Then the following estimate holds for every $\varepsilon > 0$:

$$\begin{aligned} &\left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} (\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) + \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x))) - 1 \right| \\ &\qquad \leq \frac{1}{2}(LP^{S_n}(\Gamma_P, \Gamma_C))^{1/2} + \varepsilon + \frac{2K_\varepsilon}{2^n} \end{aligned}$$

where $K_\varepsilon > 1 - \varepsilon$.

Corollary 4.2 guarantees that if $\mathcal{P}_n$ is *uniform* in the sense that $\mu(P_k) = 1/2^n$ for all k, then the hypothesis $\mu(\overline{f}_{\Gamma_P,\Gamma_C}) = 1/2$ is fulfilled.

Proof. We have

$$\begin{aligned} &\left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} (\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) + \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x))) - 1 \right| \\ &\qquad \leq \left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) - \frac{1}{2} \right| \\ &\qquad\quad + \left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) - \frac{1}{2} \right| \\ &\qquad = \frac{1}{2}\,(LP^{S_n}(\Gamma_P, \Gamma_C))^{1/2} \\ &\qquad\quad + \left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) - \frac{1}{2} \right| \end{aligned}$$

after using (11). The estimate

$$\left| \frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) - \frac{1}{2} \right| < \varepsilon + \frac{2K_\varepsilon}{2^n}$$

follows from (1)–(3) applied to S, together with Lemma 4.3 with $\kappa = \mu(\overline{f}_{\Gamma_P,\Gamma_C})$. Observe that, although $\overline{f}_{\Gamma_P,\Gamma_C}$ is not continuous, it can be approximated arbitrarily well in the supremum norm by continuous functions (Urysohn's Lemma) so that (1) still holds. $\blacksquare$

Observe for later reference that

$$\begin{aligned} LP^S(\Gamma_P, \Gamma_C) &= 4 \left(\frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C} \circ S^i(x) - \frac{1}{2} \right)^2 \\ &\leq 4 \left\| \frac{1}{2^n} \sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C} \circ S^i - \frac{1}{2} \right\|^2 \\ &\leq 4 \left(\varepsilon + \frac{2K_\varepsilon}{2^n} \right)^2 \end{aligned} \tag{16}$$

Theorem 4.5. *Let $S : [0, 1]^2 \to [0, 1]^2$ be a uniquely ergodic automorphism with invariant measure μ such that $\mu(\overline{f}_{\Gamma_P,\Gamma_C}) = 1/2$. Furthermore, suppose $(S_n, \mathcal{P}_n)$, $\mathcal{P}_n = \{P_k : 1 \leq k \leq 2^n\}$, is a cyclic approximation of S with speed $\theta/2^n$ $(0 < \theta < 4)$ such that*

$$\max_{1\leq i\leq 2^n-1} \sum_{k=1}^{2^n} \mu(S^{-i}P_k \Delta S_n^{-i}P_k) < \frac{\theta}{2^n} \tag{17}$$

Then

$$LP^{S_n}(\Gamma_P, \Gamma_C) \approx \frac{1}{2^n} + \frac{8}{2^{3n/2}} \pm \frac{4\theta}{2^{3n/2}}$$

where "≈" means "up to higher order" in n.

The condition (17) amounts to $(S_n^{-i}, \mathcal{P}_n)$ being a periodic approximation of S^{-i} for $1 \leq i \leq 2^n - 1$.

Proof. From

$$\frac{1}{4}\,|LP^{S_n}(\Gamma_P, \Gamma_C) - LP^{S}(\Gamma_P, \Gamma_C)|$$

$$= \left|\left(\frac{1}{2^n}\sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) - \frac{1}{2}\right)^2 - \left(\frac{1}{2^n}\sum_{i=0}^{2^n-1} \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)) - \frac{1}{2}\right)^2\right|$$

$$= \left|\frac{1}{2^n}\sum_{i=0}^{2^n-1}(\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) + \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x))) - 1\right| \times \left|\frac{1}{2^n}\sum_{i=0}^{2^n-1}(\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) - \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x)))\right|$$

one derives

$$|LP^{S_n}(\Gamma_P, \Gamma_C) - LP^{S}(\Gamma_P, \Gamma_C)| \leq \frac{4M}{2^n}\sum_{i=0}^{2^n-1} |\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) - \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x))| \tag{18}$$

where, according to Lemma 4.4,

$$M := \left|\frac{1}{2^n}\sum_{i=0}^{2^n-1}(\overline{f}_{\Gamma_P,\Gamma_C}(S_n^i(x)) + \overline{f}_{\Gamma_P,\Gamma_C}(S^i(x))) - 1\right| \leq \frac{1}{2}\,(LP^{S_n}(\Gamma_P, \Gamma_C))^{1/2} + \varepsilon + \frac{2K_\varepsilon}{2^n}$$

for arbitrary $\varepsilon > 0$, $K_\varepsilon > 1 - \varepsilon$.

Let μ be the S-invariant measure on $[0, 1]^2$ and

$$H := \{x \in [0, 1]^2 : \overline{f}_{\Gamma_P,\Gamma_C}(x) = 1\}$$

so that $\overline{f}_{\Gamma_P,\Gamma_C} = \chi_H$, the characteristic function of H. On integrating (18) over $[0, 1]^2$, we obtain

$$|LP^{S_n}(\Gamma_P, \Gamma_C) - LP^{S}(\Gamma_P, \Gamma_C)|$$

$$\leq \frac{4M}{2^n}\sum_{i=0}^{2^n-1}\int_{[0,1]^2} |\chi_H(S_n^i(x)) - \chi_H(S^i(x))|d\mu(x)$$

$$= \frac{4M}{2^n}\sum_{i=0}^{2^n-1}\int_{[0,1]^2} |\chi_{S_n^{-i}H}(x) - \chi_{S^{-i}H}(x)|d\mu(x)$$

$$= \frac{4M}{2^n}\sum_{i=0}^{2^n-1}\int_{[0,1]^2} \chi_{S_n^{-i}H\Delta S^{-i}H}d\mu$$

$$= \frac{4M}{2^n}\sum_{i=0}^{2^n-1} \mu(S_n^{-i}H\Delta S^{-i}H)$$

Now, by the assumption (17),

$$\sum_{i=0}^{2^n-1} \mu(S_n^{-i}H\Delta S^{-i}H) = \sum_{i=0}^{2^n-1}\sum_{k=1}^{2^n} \mu(S_n^{-i}(H\cap P_k)\Delta S^{-i}(H\cap P_k)) \leq \sum_{i=0}^{2^n-1}\sum_{k=1}^{2^n} \mu(S_n^{-i}P_k\Delta S^{-i}P_k) < 2^n\,\frac{\theta}{2^n} = \theta$$

Hence,

$$\left|LP^{S_n}(\Gamma_P, \Gamma_C) - \int LP^{S}(\Gamma_P, \Gamma_C)d\mu\right| \leq \frac{4}{2^n}\left(\frac{1}{2}\,(LP^{S_n}(\Gamma_P, \Gamma_C))^{1/2} + \varepsilon + \frac{2K_\varepsilon}{2^n}\right)\theta = \frac{2\theta}{2^n}\,(LP^{S_n}(\Gamma_P, \Gamma_C))^{1/2} + \frac{4\theta\varepsilon}{2^n} + \frac{8\theta K_\varepsilon}{2^{2n}} \tag{19}$$

Set

$$t = \sqrt{LP^{S_n}(\Gamma_P, \Gamma_C)}$$

1. Let us suppose first that $LP^{S_n}(\Gamma_P, \Gamma_C) \geq \int LP^{S}(\Gamma_P, \Gamma_C)d\mu$. From (19) we get

$$t^2 - 2\,\frac{\theta}{2^n}\,t - A \leq 0$$

where

$$A := \int LP^S(\Gamma_P, \Gamma_C)d\mu + \frac{4\theta}{2^n}\,\varepsilon + \frac{8\theta K_\varepsilon}{2^{2n}}$$

The roots of $t^2 - 2\frac{\theta}{2^n}t - A = 0$ are

$$\alpha_\pm = \frac{\theta}{2^n}\left(1 \pm \sqrt{1 + \frac{2^{2n}A}{\theta^2}}\right) \tag{20}$$

2. Let us suppose now that $\int LP^S(\Gamma_P, \Gamma_C)d\mu \geq LP^{S_n}(\Gamma_P, \Gamma_C)$. From (19) we get

$$t^2 + 2\,\frac{\theta}{2^n}\,t - B \geq 0$$

where

$$B := \int LP^S(\Gamma_P, \Gamma_C)d\mu - \frac{4\theta}{2^n}\,\varepsilon - \frac{8\theta K_\varepsilon}{2^{2n}}$$

The roots of $t^2 + 2\frac{\theta}{2^n}t - B = 0$ are

$$\beta_\pm = -\frac{\theta}{2^n}\left(1 \mp \sqrt{1 + \frac{2^{2n}B}{\theta^2}}\right) \tag{21}$$

Since $t = \sqrt{LP^{S_n}(\Gamma_P, \Gamma_C)} \geq 0$, (19) boils down to the restriction

$$\beta_+ \leq \sqrt{LP^{S_n}(\Gamma_P, \Gamma_C)} \leq \alpha_+$$

Choose now

$$\varepsilon = \frac{1/2}{2^{n/2}}$$

Then, using (16), we get

$$A \leq 4\left(\varepsilon + \frac{2K_\varepsilon}{2^n}\right)^2 + \frac{4\theta}{2^n}\varepsilon + \frac{8\theta K_\varepsilon}{2^{2n}} \approx \frac{1}{2^n} + 2\frac{4K_\varepsilon + \theta}{2^{3n/2}}$$

and

$$B \leq 4\left(\varepsilon + \frac{2K_\varepsilon}{2^n}\right)^2 - \frac{4\theta}{2^n}\varepsilon - \frac{8\theta K_\varepsilon}{2^{2n}} \approx \frac{1}{2^n} + 2\frac{4K_\varepsilon - \theta}{2^{3n/2}}$$

Substitution in (20) and (21) yields

$$\begin{aligned}\alpha_+ &\approx \frac{\theta}{2^n}\left(1 + \frac{2^n}{\theta}\sqrt{A}\right)\\ &\lessapprox \frac{\theta}{2^n}\left(1 + \frac{2^{n/2}}{\theta}\sqrt{1 + 2\,\frac{4K_\varepsilon + \theta}{2^{n/2}}}\right)\\ &\approx \frac{1}{2^{n/2}} + 2\frac{2K_\varepsilon + \theta}{2^n}\end{aligned}$$

and, analogously,

$$\beta_+ \lessapprox \frac{1}{2^{n/2}} + 2\,\frac{2K_\varepsilon - \theta}{2^n}$$

respectively. Therefore,

$$LP^{S_n}(\Gamma_P, \Gamma_C) \in [\beta_+^2, \alpha_+^2] =: I_n \tag{22}$$

where

$$\alpha_+^2 \approx \left(\frac{1}{2^{n/2}} + 2\,\frac{2K_\varepsilon + \theta}{2^n}\right)^2 \approx \frac{1}{2^n} + 4\,\frac{2K_\varepsilon + \theta}{2^{3n/2}}$$

and

$$\beta_+^2 \approx \left(\frac{1}{2^{n/2}} + 2\,\frac{2K_\varepsilon - \theta}{2^n}\right)^2 \approx \frac{1}{2^n} + 4\,\frac{2K_\varepsilon - \theta}{2^{3n/2}} \tag{23}$$

The middle point of I_n is

$$\bar{t} = \frac{\alpha_+^2 + \beta_+^2}{2} \approx \frac{1}{2^n} + \frac{8K_\varepsilon}{2^{3n/2}}$$

and the width of I_n is

$$\Delta = \frac{\alpha_+^2 - \beta_+^2}{2} \approx \frac{4\theta}{2^{3n/2}} \quad ■$$

Corollary 4.6. *If $LP^{S_n}(\Gamma_P, \Gamma_C)$ is asymptotically uniformly distributed with respect to Γ_P and Γ_C, then the approximation speed of $(S_n, \mathcal{P}_n)$ to the ergodic automorphism S is $\theta/2^n$ with $2 \leq \theta < 4$.*

Proof. If $LP^{S_n}(\Gamma_P, \Gamma_C)$ is asymptotically uniformly distributed with respect to Γ_P and Γ_C, then $LP^{S_n}(\Gamma_P, \Gamma_C) = 1/2^n$ for all $\Gamma_P, \Gamma_C \in \mathbb{Z}_2^n$. From $1/2^n \geq \beta_+^2$ [see (22)] and (23) we obtain

$$\theta \geq 2K_\varepsilon$$

Thus, from Lemma 4.3 it follows

$$\theta \geq 2\left(1 - \frac{\varepsilon}{2}\right) = 2 - \varepsilon$$

for all $\varepsilon > 0$. ■

Remark 4.7. According to *Theorem* 2.4, if $(S_n, \mathcal{P}_n)$ is a periodic approximation of S of the second type with $\theta < 2$, then S is not mixing. Therefore, *Corollary* 4.6 suggests that to get by this method a cryptosystem immune to linear cryptanalysis, ergodicity and approximation of the first type might not be enough, rather one should use a mixing automorphism and approximations of the second type.

5. Conclusions and Final Remarks

We presented in this paper a theoretical construction of n-bit block permutations based on approximations S_n of an ergodic map S which, under certain assumptions on the speed of approximation, can be used as a cryptosystem immune to linear cryptanalysis. We showed that the deviation for the resulting ciphers from the most efficient linear approximations is of the order $1/2^{3n/2}$, i.e.

$$\left| LP^{S_n}(\Gamma_P, \Gamma_C) - \frac{1}{2^n} \right| \lessapprox \frac{1}{2^{3n/2}} \quad \forall \Gamma_P, \Gamma_C$$

where n is the length of the bitblocks. Moreover our results indicate that one should approximate mixing maps rather than only ergodic ones to ensure optimal cryptanalytical performance of S_n. We described this new approach in the case of two-dimensional maps defined in $[0, 1]^2$ in order to show its feasibility, but it can be easily generalized to higher dimensional systems, which are even more interesting for applications [Brown & Chua, 1996; Fridrich, 1998].

In fact, let X be a subset of $\mathbb{R}^n$ endowed with the Lebesgue measure λ (v.g. $X = [0, 1]^n$ or $\mathbb{T}^n$, the n-dimensional torus), let $S : X \to X$ be an automorphism and suppose that $S_n : X \to X$ is an approximation of S in the sense of Halmos–Rohlin, i.e. there exists a partition $\mathcal{P}_n = \{P_i : i = 1, \ldots, 2^n\}$ of X such that S_n preserves $\mathcal{P}_n$. Associate to each $P_i \in \mathcal{P}_n$ an n-bit number so that S_n can also be interpreted as a permutation of such n-bit blocks. Thus, the situation is formally the same as the one discussed in the previous section and, hence, the techniques used above are also applicable with the same conclusions.

Also notice that some of the mathematical tools used above can be weakened. For example, the L_p-ergodic theorem for uniquely ergodic maps can be used instead of the C^0-ergodic theorem.

In this paper our main concern was the immunity of the cryptosystem to linear cryptanalysis. It seems that attacks using differential cryptanalysis [Menezes *et al.*, 1997], nonlinear cryptanalysis [Knudsen & Robshaw, 1996] or any variant or combination of them can be also formulated in the language of dynamical systems and will be the subject of further analysis.

Acknowledgments

This paper was written during the stay of one of the authors (J. Szczepański) at the Operations Research Center of the Miguel Hernández University. The financial support of the Generalitat Valenciana, grant INV00-01-19, is grateful acknowledged. J. Szczepański thanks the Operations Research Center for its kind hospitality. This work has been also partially supported by a DGESIC grant PB97-0342 (J. M. Amigó) and a Polish Scientific Committee grant 8T11D02019 (J. Szczepański).

References

Brown, R. & Chua, L. O. [1996] "Clarifying chaos: Examples and counterexamples," *Int. J. Bifurcation and Chaos* **6**, 219–249.

Cornfeld, I. P., Fomin, S. V. & Sinai, Ya. G. [1982] *Ergodic Theory* (Springer-Verlag).

Fridrich, J. [1998] "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos* **8**, 1259–1284.

Habutsu, T., Nishio, Y., Sasase, I. & Mori, S. [1991] "A secret key cryptosystem by iterating a chaotic map," in *Eurocrypt'91* (Springer-Verlag), pp. 127–136.

Kapitaniak, T. [1996] "Controlling chaos," in *Theoretical and Practical Methods in Non-Linear Dynamics* (Academic Press, London).

Knudsen, L. R. & Robshaw, M. J. B. [1996] "Nonlinear approximations in linear cryptanalysis," in *Eurocrypt'96* (LNCS, Springer-Verlag), Vol. 1070, pp. 224–236.

Kocarev, L. J., Halle, K. S., Eckert, K., Chua, L. O. & Parlitz, U. [1992] "Experimental demostration of secure communications via chaos synchronization," *Int. J. Bifurcation and Chaos* **2**, 709–716.

Kohda, T. & Tsuneda, A. [1997] "Statistics of chaotic binary sequences," *IEEE Tran. Inf. Th.* **43**, 104–112.

Kotulski, Z. & Szczepański, J. [1997] "Discrete chaotic cryptography," *Ann. Physik* **6**, 381–394.

Kotulski, Z., Szczepański, J., Górski, K., Paszkiewicz, A. & Zugaj, A. [1999] "Application of discrete chaotic dynamical systems in cryptography–DCC method," *Int. J. Bifurcation and Chaos* **9**, 1121–1135.

Matsui, M. [1993] "Linear cryptanalysis methods for DES cipher," in *Eurocrypt'93* (Springer-Verlag).

Matsui, M. [1996] "New structure of block ciphers with provable security against differential and linear cryptanalysis," in *Fast Software Encryption*, ed. Gollmann, D. (Springer-Verlag, LNCS, 1039), pp. 205–218.

Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. [1997] *Handbook of Applied Cryptography* (CRC Press).

Millerioux, G. & Mira, C. [1997] "Noninvertible piecewise linear maps applied to chaos synchronization and secure communications," *Int. J. Bifurcation and Chaos* **7**, 1617–1634.

Millerioux, G. & Mira, C. [1998] "Coding schemes based on chaos synchronization from noninvertible maps," *Int. J. Bifurcation and Chaos* **8**, 2019–2029.

Nyberg, K. [1995] "Linear approximation of block ciphers," in *Eurocrypt'94* (Springer-Verlag), LCNS, Vol. 950, pp. 439–444.

Ott, E., Grebogi, C. & Yorke, J. A. [1990] "Controlling chaos," *Phys. Rev. Lett.* **64**, 1196–1199.

Oxtoby, J. C. [1952] "Ergodic sets," *Bull. Amer. Math. Soc.* **58**, 116–136.

Parlitz, U., Chua, L. O., Kocarev, L. J., Halle, K. S. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation and Chaos* **2**, 973–977.

Pecora, L. M. & Caroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.