Finite Dimensional Generalized Baker Dynamical Systems for Cryptographic Applications

Franz Pichler and Josef Scharinger
Institute of Systems Science
Chair of Systems Theory and Information Engineering
Johannes Kepler University Linz, Austria
A - 4040 Linz

1 Introduction

In the past there have been several attempts to apply the field of deterministic chaos to cryptography. In this paper we propose for cryptographic applications to use maps as state transition function of a discrete dynamical system which leads to deterministic chaos. More specifically, we make use of generalized versions of the well-known baker transform, which are discrete and finite. Since they relate by group-theoretic representation to Bernoulli-shifts, we call them Bernoulli permutations.

The iteration of Bernoulli permutations on a set of data realizes a repeated "stretching" and "compressing" which has been compared by the "rolling" and "folding" in the work of a baker by mixing a dough. The knowledge of the importance of such operations for cryptography goes back to the fundamental paper of Claude Shannon ([8]), a fact which has been pointed out earlier in a paper by N.J.A. Sloane ([9]).

The results reported in this paper are based mainly on the PhD-thesis of the second author ([6]). A Technical Report of the first author formed the starting basis for it. This paper extends the results which have been reported in earlier papers ([10],[11]).

2 Baker Transform and its Generalization

2.1 Baker Transform $T$

The baker transform $T : [0,1)^2 \rightarrow [0,1)^2$ can be defined by

$$T(x,y) := \begin{cases} (2x, \frac{1}{2} y) & : 0 \leq x < \frac{1}{2} \\ (2x - 1, \frac{1}{2} (y + 1)) & : \frac{1}{2} \leq x < 1 \end{cases} \quad (1)$$

By $T$ the left part $[0, \frac{1}{2}) \times [0,1)$ of $[0,1)^2$ is mapped by "stretching" and "folding" to the part $[0,1) \times [0,\frac{1}{2})$. The right part $[\frac{1}{2},1) \times [0,1)$ of $[0,1)^2$ is similar mapped to $[0,1) \times [\frac{1}{2}, 1)$. The following properties of $T$ are well-known in mathematics ([1],[2]).
1. $T$ is invertible

2. If $(x, y) \in [0, 1)^2$ is represented as a both-side infinite sequence

\[ s = \ldots, x_3, x_2, x_1, y_1, y_2, y_3, \ldots \]

where

\[ x = x_1 2^{-1} + x_2 2^{-2} + x_3 2^{-3} + \ldots \]
\[ y = y_1 2^{-1} + y_2 2^{-2} + y_3 2^{-3} + \ldots \]

(chose for dyadic rational $x, y$ the finite expansion) then $T$ as defined by (1) has on $s$ the effect of a left-shift that is:

\[ T(x, y) \text{ corresponds to the one-step-shift of } s \text{ to the left } \]

\[ s \rightarrow 1 = \ldots x_2, x_1, y_1, y_2, y_3, y_4, \ldots \]

3. the dynamical system $T^*$ generated by $T$ is mixing and ergodic.

2.2 Generalized baker transform $T_\pi$

For $\pi = (p_1, p_2, \ldots, p_k)$ with $0 < p_i < 1$ for $i = 1, 2, \ldots, k$ and $p_1 + p_2 + \ldots + p_k = 1$ the generalized baker transform $T_\pi : [0, 1)^2 \rightarrow [0, 1)^2$ is defined by

\[ T_\pi(x, y) = \left( \frac{1}{p_s}(x - F_s), psy + F_s \right) \]  

for $(x, y) \in [F_s, F_s + p_s)$ where $F_1 := 0$ and $F_s := p_1 + p_2 + \ldots + p_{s-1}$ for $s = 2, \ldots, k$.

The "probabilities" $p_1, p_2, \ldots, p_k$ of $\pi$ partition the unit square $[0, 1)^2$ into $k$ vertical strips; the numbers $F_1, F_2, \ldots, F_k$ represent the initial $x$-coordinates of these strips (compare with figure 1).

Application of $T_\pi$ on $[0, 1)^2$ maps the vertical strip $[F_s, F_s + p_s)$ of $[0, 1)^2 \rightarrow [F_s, F_s + p_s)$ into the horizontal strip $[0, 1) \times [F_s, F_s + p_s)$. $x$-values of the strip are stretched by the factor $\frac{1}{p_s}$; $y$-values of the strip are compressed by $p_s$ (compare with figure 2).

It can be proven, that $T_\pi$ has similar mathematical properties as the baker transform $T$. As a specific property, it should be mentioned that $T_\pi$ can also be realized by Bernoulli-shift operations.

3 Bernoulli Permutations

3.1 Definition

By $\mathbb{N}_0^n$ we denote the subset $\mathbb{N}_0^n := \{0, 1, 2, \ldots, n - 1\}$ of integers. With $\delta$ we denote a list of non-negative integers $\delta = (n_1, n_2, \ldots, n_k)$ with the following properties