Some applications of IFS based on square symmetries

Gintautas Bareikis, Algirdas Mačiulis

Faculty of Mathematics and Informatics, Vilnius University
Naugarduko str. 24, LT-03225 Vilnius, Lithuania
gintautas.bareikis@mif.vu.lt; algirdas.maciulis@mif.vu.lt

Received: 8 July 2011 / **Revised:** 15 February 2012 / **Published online:** 24 February 2012

Abstract. This paper describes a fractal based method for generating the pseudorandom permutations. We construct an Iterated Function System (IFS) belonging to the class of square symmetries and simulate the pseudorandom walk on a square. In this way some families of key based permutations are generated. The cardinalities of generated families are analysed.

Keywords: key based permutation, iterated function system, square symmetries.

1 Introduction

Let S be a finite set. A p-permutation is a sequence of p distinct elements in S. If $p = |S|$, then p-permutation of S is simply called a permutation. Algorithms for generating and numbering permutations have been developed over the years (see, e.g. [1–3]). Since permutation is widely used in cryptography, it is of special interest algorithms and methods which compute a unique permutation for a specific key [1, 4].

Recently, following Hutchinson, Barnsley and others [5–8], iterated function systems (IFS) as well as other fractal theory tools were employed in various encryption schemes (see, e.g. [9–11]).

In this paper we introduce a new method based on the properties of a special class of contraction mappings which allows us to generate invertible key based pseudorandom permutations. Namely, we will construct an IFS belonging to the class of square symmetries and simulate the pseudorandom walk on a square. Sensitive dependence on the parameters of IFS ensure chaotic nature of dynamical system, based on a corresponding Hutchinson map. So small changes of parameters can result in significant changes of permutation generated.

Our paper is organized as follows. The second section following introduction contains definitions and notations. In the third section we investigate the properties of defined contractions maps. Section 4 provides the iterative algorithms for evaluating of superposition of contraction maps and its inverse. In the last section we construct key based pseudorandom permutations and discuss some unsolved problems.

2 Preliminaries

We will consider maps based on symmetry transformations of the square $T := (0,\Delta)\times(0,\Delta),\ \Delta>0$. Eight symmetry transformations of T are defined by

$$\begin{aligned}
&\omega_0(x,y;\Delta) := (x,y), && \omega_1(x,y;\Delta) := (\Delta-y,x),\\
&\omega_2(x,y;\Delta) := (\Delta-x,\Delta-y), && \omega_3(x,y;\Delta) := (y,\Delta-x),\\
&\omega_4(x,y;\Delta) := (\Delta-y,\Delta-x), && \omega_5(x,y;\Delta) := (x,\Delta-y),\\
&\omega_6(x,y;\Delta) := (y,x), && \omega_7(x,y;\Delta) := (\Delta-x,y)
\end{aligned}$$

for each point $X=(x,y)\in T$.

Let c be a positive integer. Splitting $\overline{T} := [0,\Delta]\times[0,\Delta]$ into $l := 2^{2c}$ equal squares $\overline{V}_0,\overline{V}_1,\dots,\overline{V}_{l-1}$ we denote by P_k their bottom left vertices, namely:

$$P_k := \left(\left(k-\left[\frac{k}{2^c}\right]\cdot 2^c\right)\frac{\Delta}{2^c},\ \left[\frac{k}{2^c}\right]\frac{\Delta}{2^c}\right),\quad k\in\mathbb{N}(l) := \{0,1,\dots,l-1\}.$$

Then the interior of the square $\overline{V}_k$ is

$$V_k = V_0 + P_k,\quad \text{where } V_0 = 2^{-c}\cdot T.$$

Here and subsequently we follow usual notations:

$$\begin{aligned}
\phi(B) &:= \big\{\phi(X)\ \big|\ X\in B\big\},\\
X_0+\alpha B &:= \big\{(x_0+\alpha x, y_0+\alpha y)\ \big|\ (x,y)\in B\big\}
\end{aligned}$$

for each $B\subset\mathbb{R}^2$, $X_0=(x_0,y_0)\in\mathbb{R}^2$, $\alpha\in\mathbb{R}$ and transformation $\phi:\mathbb{R}^2\to\mathbb{R}^2$.

Consider the family of contraction transformations

$$\mathcal{F}_T := \big\{f_{ij}: T\to T\ \big|\ i\in\mathbb{N}(8),\ j\in\mathbb{N}(l)\big\}$$

defined by

$$f_{ij}(x,y) := \frac{1}{2^c}\omega_i(x,y;\Delta)+P_j,\quad (x,y)\in T.$$

Note that $f_{ij}(T)=V_j$ for each $i\in\mathbb{N}(8)$, $j\in\mathbb{N}(l)$.

For any $\tau=(\tau_0,\tau_1,\dots,\tau_{l-1})\in\mathbb{N}^l(8)$ and permutation $\sigma:\mathbb{N}(l)\to\mathbb{N}(l)$ we introduce the notations $\lambda := \langle\tau,\sigma\rangle$, $\lambda(i) := (\tau_i,\sigma(i))$ and

$$f_{\lambda(i)} := f_{\tau_i\sigma(i)}\in\mathcal{F}_T,\quad i\in\mathbb{N}(l). \tag{1}$$

The set of parameters λ

$$\Lambda := \big\{\lambda=\langle\tau,\sigma\rangle\ \big|\ \tau\in\mathbb{N}^l(8),\ \sigma\in\mathbb{S}_l\big\}$$

contains $|\Lambda| = l!8^l$ elements. Here $\mathbb{S}_l$ is symmetric group on $\mathbb{N}(l)$.

Let $n \in \mathbb{N}(l^s)$ be given by the s-digits representation to the base l

$$n = (\overline{n_{s-1} \dots n_0})_l = \sum_{k=0}^{s-1} n_k l^k, \quad n_k \in \mathbb{N}(l).$$

Then

$$f_n(\lambda, X) := f_{\lambda(n_{s-1})} \circ f_{\lambda(n_{s-2})} \circ \dots \circ f_{\lambda(n_0)}(X). \tag{2}$$

Note, that function $f_n(\lambda, \cdot) : T \to T$ is injective since $f_{\lambda(i)}$ are injective.

3 Designing IFS on square symmetries

We are interested in an IFS related to the family $\mathcal{F}_T$. Using above defined maps we will construct a family of key based pseudorandom permutations. In this section we investigate the properties of the superposition (2).

Theorem 1. *Let s be a positive integer and $n \neq m$, $n, m \in \mathbb{N}(l^s)$. Then for each $\lambda \in \Lambda$ we have*

$$f_n(\lambda, T) \cap f_m(\lambda, T) = \emptyset.$$

Proof. We will prove the theorem by induction on s. The definition of the functions $f_{\lambda(i)} : T \to T$ implies that

$$f_{\lambda(i)}(T) \cap f_{\lambda(j)}(T) = \emptyset, \quad \text{if } i \neq j, \ \ i, j \in \mathbb{N}(l). \tag{3}$$

Assume the assertion holds for $s-1$, that is

$$f_n(\lambda, T) \cap f_m(\lambda, T) = \emptyset \tag{4}$$

for

$$n = (\overline{n_{s-2} \dots n_0})_l, \quad m = (\overline{m_{s-2} \dots m_0})_l, \quad n_i, m_i \in \mathbb{N}(l).$$

Suppose, that $n' = (\overline{n_{s-1} n_{s-2} \dots n_0})_l \neq n'' = (\overline{m_{s-1} m_{s-2} \dots m_0})_l$.

Consider two cases.

Case 1. Let $n' = (\overline{n_{s-1} n_{s-2} \dots n_0})_l \neq n'' = (\overline{m_{s-1} n_{s-2} \dots n_0})_l$, here $n_{s-1} \neq m_{s-1}$. We have

$$f_{n'}(\lambda, T) = f_{\lambda(n_{s-1})}\big(f_{\lambda(n_{s-2})} \circ \dots \circ f_{\lambda(n_0)}(T)\big)$$

and

$$f_{n''}(\lambda, T) = f_{\lambda(m_{s-1})}\big(f_{\lambda(n_{s-2})} \circ \dots \circ f_{\lambda(n_0)}(T)\big).$$

Applying (3) we deduce that

$$f_{n'}(\lambda, T) \cap f_{n''}(\lambda, T) = \emptyset.$$

Case 2. Assume $n' = (\overline{n_{s-1} n_{s-2} \dots n_0})_l \neq n'' = (\overline{n_{s-1} m_{s-2} \dots m_0})_l$.

In this case we apply assumption (4) and get

$$f_{\lambda(n_{s-1})}\big(f_{\lambda(n_{s-2})} \circ \dots \circ f_{\lambda(n_0)}(T)\big) \cap f_{\lambda(n_{s-1})}\big(f_{\lambda(m_{s-2})} \circ \dots \circ f_{\lambda(m_0)}(T)\big) = \emptyset,$$

since $f_{\lambda(i)}$ are injective. □

The images of superpositions describes the following theorem.

Theorem 2. *For given $(x,y) \in T$ and $f_{i_t j_t} \in \mathcal{F}_T$, $t = 1,2,\ldots$ define the sequence of points $(x_k, y_k) := f_{i_k j_k} \circ \cdots \circ f_{i_1 j_1}(x,y)$, $k = 1,2,\ldots$. Then*

$$(x_k, y_k) = \frac{1}{2^{kc}}\big(\Delta \cdot Q_k + \omega_{r_k}(x,y;\Delta)\big), \tag{5}$$

where

$$Q_k = (q_{1,k}, q_{2,k}) \in \mathbb{N}\big(2^{kc}\big) \times \mathbb{N}\big(2^{kc}\big), \quad r_k \in \mathbb{N}(8) \quad \textit{and} \quad \omega_{r_k} = \omega_{i_k} \circ \cdots \circ \omega_{i_1}.$$

Proof. By the definition

$$P_{j_t} = \frac{\Delta}{2^c}\big(j_{0t}, j_{1t}\big), \quad \text{if } j_t = 2^c j_{1t} + j_{0t}, \;\; j_{0t}, j_{1t} \in \mathbb{N}\big(2^c\big).$$

This gives

$$(x_1, y_1) = f_{i_1 j_1}(x,y) = \frac{1}{2^c}\omega i_1(x,y;\Delta) + P_{j_1} = \frac{1}{2^c}\big(\omega_{i_1}(x,y;\Delta) + \Delta \cdot (j_{01}, j_{11})\big).$$

Assuming (5) to hold for $k-1$, we will prove it for k. Letting $(a,b) := \omega_{r_{k-1}}(x,y;\Delta)$ for short, we have

$$\begin{aligned}(x_{k-1}, y_{k-1}) &= \frac{1}{2^{(k-1)c}}\big(\Delta \cdot Q_{k-1} + (a,b)\big) \\ &= \frac{1}{2^{(k-1)c}}\big(\Delta \cdot q_{1,k-1} + a, \Delta \cdot q_{2,k-1} + b\big).\end{aligned} \tag{6}$$

We consider only the case $i_k = 3$, for example. The other 7 cases can be proved in the same way. Since

$$\omega_{i_k}(x_{k-1}, y_{k-1}; \Delta) = \omega_3(x_{k-1}, y_{k-1}; \Delta) = (y_{k-1}, \Delta - x_{k-1}),$$

we have

$$\begin{aligned}(x_k, y_k) = f_{i_k j_k}(x_{k-1}, y_{k-1}) &= \frac{1}{2^c}\omega_{i_k}(x_{k-1}, y_{k-1}; \Delta) + P_{j_k} \\ &= \frac{1}{2^c}\big(y_{k-1} + \Delta \cdot j_{0k},\ \Delta - x_{k-1} + \Delta \cdot j_{1k}\big).\end{aligned}$$

From this and (6) it follows, that

$$\begin{aligned}x_k &= \frac{1}{2^{kc}}(\Delta \cdot q_{2,k-1} + b) + \frac{\Delta}{2^c} j_{0k} \\ &= \frac{1}{2^{kc}}\big(\Delta \cdot \big(2^{(k-1)c} j_{0k} + q_{2,k-1}\big) + b\big) = \frac{1}{2^{kc}}(\Delta \cdot q_{1,k} + b),\end{aligned}$$

where

$$q_{1,k} = 2^{(k-1)c} j_{0k} + q_{2,k-1} \in \mathbb{N}\big(2^{kc}\big).$$

Analogously

$$y_k = \frac{1}{2^c}\left(\Delta - \frac{1}{2^{(k-1)c}}(\Delta \cdot q_{1,k-1} + a) + \Delta \cdot j_{1k}\right)$$
$$= \frac{1}{2^{kc}}(\Delta \cdot q_{2,k} + \Delta - a),$$

where

$$q_{2,k} = 2^{(k-1)c} j_{1k} + 2^{(k-1)c} - q_{1,k-1} - 1 \in \mathbb{N}\big(2^{kc}\big).$$

Hence

$$(x_k, y_k) = \frac{1}{2^{kc}}\big(\Delta \cdot Q_k + (b, \Delta - a)\big).$$

The group properties of the square symmetries yield

$$(b, \Delta - a) = \omega_3(a, b; \Delta) = \omega_3 \circ \omega_{r_{k-1}}(x, y; \Delta) = \omega_{r_k}(x, y; \Delta)$$

for some $r_k \in \mathbb{N}(8)$. □

Dividing each side of the square T into 2^{cs} equal intervals, we get open squares

$$T_k := \left\{ \left(x + \left(k - \left[\frac{k}{2^{cs}} \right] \cdot 2^{cs} \right) \frac{\Delta}{2^{cs}},\ y + \left[\frac{k}{2^{cs}} \right] \frac{\Delta}{2^{cs}} \right) \,\Big|\, x, y \in \left(0, \frac{\Delta}{2^{cs}}\right) \right\},$$

for $k \in \mathbb{N}(l^s)$. If $k = k_2 2^{cs} + k_1$, then

$$T_k = \left\{ \left(x + k_1 \frac{\Delta}{2^{cs}},\ y + k_2 \frac{\Delta}{2^{cs}} \right) \,\Big|\, x, y \in \left(0, \frac{\Delta}{2^{cs}}\right) \right\} = T_0 + \frac{\Delta}{2^{cs}}(k_1, k_2).$$

Theorem 3. *For any $n \in \mathbb{N}(l^s)$ and $\lambda \in \Lambda$ we have*

$$f_n(\lambda, T) = T_k$$

for some $k = k(n, \lambda)$.

Proof. For each $X = (x, y) \in T$ and $n \in \mathbb{N}(l^s)$ Theorem 2 implies

$$f_n(\lambda, X) = \frac{1}{2^{cs}}\big(\Delta \cdot Q_s + \omega_{r_s}(x, y; \Delta)\big),$$

where

$$Q_s = (q_{1,s}, q_{2,s}) \in \mathbb{N}\big(2^{cs}\big) \times \mathbb{N}\big(2^{cs}\big), \quad r_s \in \mathbb{N}(8).$$

Let us define

$$k = 2^{cs} q_{2,s} + q_{1,s} \in \mathbb{N}\big(l^s\big).$$

Having in mind, that $\omega_r(T; \Delta) = T$ for any $r \in \mathbb{N}(8)$, we get

$$f_n(\lambda, T) = \frac{1}{2^{cs}}\big(\Delta \cdot (q_{1,s}, q_{2,s}) + \omega_{r_s}(T; \Delta)\big) = T_k.$$ □

We define the key K to be a pair $K := \langle \lambda, X \rangle$, where $\lambda \in \Lambda$, $X \in T$. The key K based function $f_K : \mathbb{N}(l^s) \to T$ is given by

$$f_K(n) := f_n(\lambda, X), \quad n \in \mathbb{N}\big(l^s\big).$$

It follows from Theorem 1 that the function f_K is injection. This enables us to construct the bijection $g_K : \mathbb{N}(l^s) \to \mathbb{N}(l^s)$ as follows:

$$g_K(n) = k, \quad \text{if } f_n(\lambda, X) \in T_k, \ \ n, k \in \mathbb{N}\big(l^s\big).$$

Now let us fix an integer $m \geq 2$. From now on we assume that $\Delta = m2^{cs}$ and consider points of the square $\overline{T}$ with integer coordinates. These points are contained in the grid

$$\widetilde{G} := \big\{(i, j) \bigm| i, j = 0, 1, 2, \ldots, m2^{cs}\big\}.$$

In addition we define the subsets of $\widetilde{G}$:

$$E = \big\{\big(m_1 2^{cs}, m_2 2^{cs}\big) \bigm| m_1, m_2 = 1, 2, \ldots, m-1\big\},$$

$$G := \bigcup_{k=0}^{l^s-1} G_k,$$

where $G_k := \widetilde{G} \cap T_k$, $k \in \mathbb{N}(l^s)$. So we have that

$$G_k = \big\{(mk_1 + x, mk_2 + y) \bigm| x, y = 1, 2, \ldots, m-1\big\},$$

provided $k = k_2 2^{cs} + k_1$. The number of elements in G_k equals to $(m-1)^2$. The sets G_k are pairwise disjoint and therefore $|G| = l^s(m-1)^2$. Moreover the definition of square symmetries implies $\omega_r(E; \Delta) = E$ and

$$\frac{1}{2^{cs}} \omega_r(E; \Delta) = G_0$$

for each $r \in \mathbb{N}(8)$.

Consider the discrete versions of the functions f_n and f_K.

Theorem 4. *For any $n \in \mathbb{N}(l^s)$ and $\lambda \in \Lambda$ there exists $k = k(n, \lambda) \in \mathbb{N}(l^s)$ such that*

$$f_n(\lambda, \cdot) : E \to G_k$$

is bijection. Moreover, $k(n', \lambda) \neq k(n'', \lambda)$ if $n' \neq n''$.

Proof. Theorem 3 yields, that $f_n(\lambda, T) = T_k$ for some $k = k_2 2^{cs} + k_1 \in \mathbb{N}(l^s)$. Choose $X = (m_1 2^{cs}, m_2 2^{cs}) \in E$ and $\Delta = m2^{cs}$. Applying Theorem 2 we obtain

$$\begin{aligned} f_n(\lambda, X) &= \frac{\Delta}{2^{cs}}(k_1, k_2) + \frac{\Delta}{2^{cs}} \omega_{r_s}(X; \Delta) \\ &= (mk_1, mk_2) + \omega_{r_s}(m_1, m_2; m), \quad r_s \in \mathbb{N}(8). \end{aligned}$$

We see that $f_n(\lambda, X) \in G_k$ for any $X \in E$. The function $f_n(\lambda, \cdot) : E \to G_k$ is bijection, since $|G_k| = |E|$. The rest part of the proof follows from Theorem 1. □

Corollary 1. *Let $K = \langle \lambda, X \rangle$ be a key, where $\lambda \in \Lambda$, $X \in E$. Then*

$$f_K : \mathbb{N}\big(l^s\big) \to G$$

is injective. It becomes bijection if $m = 2$.

Let us consider an example showing how can be evaluated the function f_K for the given key K.

Example. Assume $c = 1$, $s = 3$, $m = 3$. Using definitions above we obtain, that $l = 2^{2c} = 4$ and $\Delta = m2^{cs} = 24$. Let us take a key $K = \langle \lambda, X \rangle$ with $\lambda = \langle \tau, \sigma \rangle$ by choosing $X = (8, 8) \in E$, $\tau = (0, 3, 4, 7) \in \mathbb{N}^4(8)$ and

$$\sigma = \begin{pmatrix} 0\,1\,2\,3 \\ 1\,0\,2\,3 \end{pmatrix} \in \mathbb{S}_4.$$

Let us evaluate $f_K(54)$ for example. We have $54 = 3 \cdot 4^2 + 1 \cdot 4 + 2 \cdot 4^0 \in \mathbb{N}(64)$. Therefore

$$f_K(54) = f_{\lambda(3)} \circ f_{\lambda(1)} \circ f_{\lambda(2)}(X) = f_{73}\big(f_{30}\big(f_{42}(8, 8)\big)\big).$$

Direct computations yield

$$f_{42}(8, 8) = \frac{1}{2}\omega_4(8, 8; 24) + P_2 = \frac{1}{2}(16, 16) + (0, 12) = (8, 20).$$

Analogously $f_{30}(8, 20) = (10, 8)$ and finally $f_{73}(10, 8) = (19, 16)$. Thus

$$f_K(54) = (19, 16) = (3 \cdot 6 + 1, 3 \cdot 5 + 1) \in G_{46},$$

since $5 \cdot 2^{1 \cdot 3} + 6 = 46$.

It is natural to try to relate the set of mappings f_K to the set of keys K.

Theorem 5. *Let $K = \langle \lambda, X \rangle$ and $K' = \langle \lambda', X' \rangle$ be the keys. If $s \geq 2$ and $K \neq K'$, then there exists $n \in \mathbb{N}(l^s)$ such that*

$$f_K(n) \neq f_{K'}(n).$$

Proof. Setting $\lambda = \langle \tau, \sigma \rangle \in \Lambda$ and $\lambda' = \langle \tau', \sigma' \rangle \in \Lambda$ we conduct the proof in three steps.

Step 1. Suppose that $\lambda = \lambda'$. Then $f_n(\lambda, X) \neq f_n(\lambda, X')$ since $f_n(\lambda, \cdot)$ is injective and $X \neq X'$.

Step 2. Assume that $\sigma \neq \sigma'$. Then there exists $k \in \mathbb{N}(l)$ such that $\sigma(k) \neq \sigma'(k)$. Choosing $n = (\overline{k n_{s-2} \dots n_0})_l$ we have

$$f_K(n) = f_{\lambda(k)}\big(f_{\lambda(n_{s-2})} \circ \dots \circ f_{\lambda(n_0)}(X)\big) \in V_{\sigma(k)},$$
$$f_{K'}(n) = f_{\lambda'(k)}\big(f_{\lambda'(n_{s-2})} \circ \dots \circ f_{\lambda'(n_0)}(X')\big) \in V_{\sigma'(k)}.$$

Hence $f_K(n) \neq f_{K'}(n)$ since $V_{\sigma(k)}$ and $V_{\sigma'(k)}$ are disjoint.

Step 3. Suppose that $\sigma = \sigma'$ and $\tau \neq \tau'$. Without loss of generality we can assume that $\tau_0 \neq \tau_0'$. One can easily show that for each $\tau_0 \neq \tau_0'$ there exist at least two squares $V_r,\ V_{r'}$ such that

$$\omega_{\tau_0}(V_r;\Delta) \cap \omega_{\tau_0'}(V_r;\Delta) = \emptyset, \quad \omega_{\tau_0}(V_{r'};\Delta) \cap \omega_{\tau_0'}(V_{r'};\Delta) = \emptyset.$$

Set $i = r$, if $\sigma(0) \neq r$, otherwise $i = r'$.

Let us choose $n = (\overline{0kn_{s-3}\dots n_0})_l$, where $k = \sigma^{-1}(i)$. Then

$$\begin{aligned} f_K(n) &= f_{\lambda(0)}\big(f_{\lambda(k)} \circ f_{\lambda(n_{s-3})} \circ \cdots \circ f_{\lambda(n_0)}(X)\big) \\ &= f_{\lambda(0)}(X_i) = \frac{1}{2^c}\omega_{\tau_0}(X_i;\Delta) + P_{\sigma(0)} \end{aligned}$$

and analogously

$$f_{K'}(n) = f_{\lambda'(0)}(X_i') = \frac{1}{2^c}\omega_{\tau_0'}\big(X_i';\Delta\big) + P_{\sigma(0)},$$

where $X_i, X_i' \in V_i$. This implies

$$\omega_{\tau_0}(X_i;\Delta) \neq \omega_{\tau_0'}\big(X_i';\Delta\big)$$

and consequently $f_K(n) \neq f_{K'}(n)$. □

4 Computation

Given key K the function $f_K(n)$ and its inverse can be evaluated efficiently.

At first let us fix integer parameters $s \geq 2$, $c \geq 1$, $m \geq 2$ and recall that $l = 4^c$, $\Delta = m2^{cs}$. Choose a key $K = \langle \lambda,\ X\rangle$, which consists of a subkey $\lambda = \langle \tau, \sigma\rangle \in \Lambda$ and an initial point $X \in E$.

Computation of f_K. Given key K and $n = (\overline{n_{s-1}\dots n_0})_l \in \mathbb{N}(l^s)$, computing $X_s = f_K(n) \in G$ is straightforward by performing s iterations

$$X_i = f_{\lambda(n_{i-1})}(X_{i-1}), \quad i = 1, 2, \dots, s, \tag{7}$$

with $X_0 = X$. Here $f_{\lambda(n_{i-1})}$ is defined in (1).

Computation of f_K^{-1}. Given key K and $X_s \in f_K(\mathbb{N}(l^s)) \subset G$, to evaluate $n = (\overline{n_{s-1}\dots n_0})_l = f_K^{-1}(X_s)$ we perform reverse iterations as follows. Suppose that $X_{s-1}, \dots, X_i$ and $n_{s-1}, \dots, n_i$ are computed. Let us find n_{i-1} and X_{i-1}. Since $X_i = (x_i, y_i) \in V_{k_{i-1}}$ with

$$k_{i-1} = \left[\frac{y_i}{\Delta}2^c\right]2^c + \left[\frac{x_i}{\Delta}2^c\right],$$

it follows that $n_{i-1} = \sigma^{-1}(k_{i-1})$ and consequently

$$X_{i-1} = f^{-1}_{\lambda(n_{i-1})}(X_i)$$

for $i = s, s-1, \ldots, 1$.

If K is unknown, the task of computing f_K^{-1} seems to become computationally infeasible by increasing l, since the set of keys has cardinality

$$|\Lambda| \cdot |E| = 8^l l!(m-1)^2$$

and by Theorem 5 $f_K \neq f_{K'}$, if $K \neq K'$.

5 Applications and final remarks

Let us consider some special cases of mappings f_K which enable us to construct key based pseudorandom permutations.

Permutations I. According to Corollary 1 of Theorem 4 we have constructed the injective function

$$f_K : \mathbb{N}(l^s) \to G$$

for each key $K = \langle \lambda, X \rangle$, where $\lambda \in \Lambda,\ X \in E$. Having numbered points in the grid $G = \{Y_i \mid i = 0, 1, \ldots, (m-1)^2 l^s - 1\}$ one can define the family of l^s-permutations in $\mathbb{N}((m-1)^2 l^s)$

$$\mathcal{A}(s,l,m) := \big\{\varphi_K : \mathbb{N}\big(l^s\big) \to \mathbb{N}\big((m-1)^2 l^s\big) \ \big|\ K = \langle \lambda, X \rangle,\ \lambda \in \Lambda,\ X \in E\big\},$$

where $\varphi_K(n) = k$, if $f_K(n) = Y_k \in G$. Theorem 5 yields, that for $s \geq 2$ this family has cardinality

$$\big|\mathcal{A}(s,l,m)\big| = 8^l l!(m-1)^2.$$

Permutations II. Let us define the bijection $\pi_K : \mathbb{N}(l^s) \to \mathbb{N}(l^s)$ iteratively. If $j = (\overline{j_{s-1} \ldots j_0})_l$, then $\pi_K(j) := (\overline{n_{s-1} \ldots n_0})_l$, where

$$n_i = \big(j_i + (l+1)\big(y_i \bmod (l+1)\big) + x_i \bmod (l+1)\big) \bmod l, \quad i = 0, \ldots, s-1,$$

and $X_i = (x_i, y_i)$ are defined by iterations (7). The inverse permutation π_K^{-1} can be evaluated analogously provided key K is known. Therefore, having in mind the applications in cryptography, instead of $\mathcal{A}(s,l,m)$ we may consider the family of l^s-permutations in $\mathbb{N}((m-1)^2 l^s)$

$$\mathcal{B}(s,l,m) := \big\{\beta \ \big|\ \exists \text{ key } K\colon\ \beta = \varphi_K \circ \pi_K,\ \varphi_K \in \mathcal{A}(s,l,m)\big\}.$$

Permutations III. If $m = 2$, then $|E| = 1$ and $|G| = l^s$. Taking into account the binary representations of integers we may assume, that $\varphi_K(n) = \varphi_\lambda(n) = k$, where $n, k \in \{0,1\}^N$, $N = s \log_2 l = 2cs$. Therefore $\mathcal{A}(s,l,2)$ can be thought of as family of key based pseudorandom permutations

$$\mathcal{A}(s,l,2) = \big\{\varphi_\lambda : \{0,1\}^N \to \{0,1\}^N \ \big|\ \lambda \in \Lambda\big\}.$$

Similar considerations apply to the family of permutations $\mathcal{B}(s,l,2)$.

Permutations IV. If $m = 2^c + 1$, then $|E| = l$ and say $E = \{Z_0, Z_1, \ldots, Z_{l-1}\}$. We write $h(\lambda)$ for the value of hash function $h : \Lambda \to \mathbb{Z}$. For example, we can take a prime number $p > l$ and set

$$h(\lambda) = h(\langle \tau, \sigma \rangle) = \sum_{k=0}^{l-1} \big(p \cdot \tau_k + \sigma(k)\big) p^{2k} \bmod l.$$

Each integer $n \in \mathbb{N}(l^{s+1})$ can be written in the form

$$n = n' \cdot l + n_0, \quad n' \in \mathbb{N}(l^s), \;\; n_0 \in \mathbb{N}(l).$$

Taking

$$n_\lambda := \sigma\big(\big(h(\lambda) + n_0\big) \bmod l\big)$$

we define $\psi_\lambda : \mathbb{N}(l^{s+1}) \to \mathbb{N}(l^{s+1})$ by

$$\psi_\lambda(n) := f_{n'}(\lambda, Z_{n_\lambda}).$$

Slight modifications in the proofs of Theorems 4 and 5 show, that ψ_λ is bijection and the family

$$\mathcal{C}(s, l, h) := \big\{\psi_\lambda : \{0,1\}^M \to \{0,1\}^M \;\big|\; \lambda \in \Lambda\big\}$$

consists of $|\mathcal{C}(s, l, h)| = 8^l l!$ distinct permutations. Here $M = (s+1)\log_2 l = 2c(s+1)$ and $c \geq 1$, $s \geq 2$.

Final remarks. Based on IFS we have constructed families of key based pseudorandom permutations. Actually each family consists of virtual permutations which do not need to store. Any permutation of size $l^s = 4^{cs}$ is defined as injective function on $\mathbb{N}(l^s)$. Given key $K = \langle \lambda, X \rangle$ this function and its inverse can be evaluated efficiently for any $n \in \mathbb{N}(l^s)$. The length of the key does not exceed $l(3 + \log_2 l) + 2\log_2 m$ bits and may become much less then the size of permutation by increasing number of iterations s. However to prove rigorously how hard is the problem of computing the inverse function with unknown key (or maybe to find some fast algorithm) remains still open question.

We have proved that the cardinalities of the families $\mathcal{A}(s, l, m)$ and $\mathcal{C}(s, l, h)$ equal to the number of possible keys. In view of data encryption applications, permutations $\beta \in \mathcal{B}(s, l, m)$ are likely to perform better than those of $A(s, l, m)$. The question is: how many members contains the family $\mathcal{B}(s, l, m)$? One may conjecture that $|\mathcal{B}(s, l, 2)| = l!8^l$. Direct computation shows that this is true when $l = 4$ and $s = 2, 3, 4, 5$. However, in general case this question is still unanswered.

References

1. A. De Matteis, S. Pagnutti, Pseudorandom permutation, *J. Comput. Appl. Math.*, **142**, pp. 367–375, 2002.

2. M. Naor, O. Reingold, Constructing pseudo-random permutations with a prescribed structure, *J. Cryptology*, **15**, pp. 97–102, 2002.

3. R. Sedgewick, Permutation generation methods, *Comput. Surv.*, **9**, pp. 137–164, 1977.

4. S.M. Hussain, N.M. Ajlouni, Key based random permutation (KBRP), *Journal of Computer Science*, **2**(5), pp. 419–421, 2006.

5. M.F. Barnsley, *Fractals Everywhere*, Academic Press, New York, 1988.

6. M.F. Barnsley, J.E. Hutchinson, O. Stenflo, V-variable fractals: Fractals with partial self similarity, *Adv. Math.*, **218**, pp. 2051–2088, 2008.

7. J. Hutchinson, Fractals and self-similarity, *Indiana Univ. Math. J.*, **30**, pp. 713–747, 1981.

8. A.E. Jacquin, Image coding based on a fractal theory of iterated contractive image transformations, *IEEE Trans. Image Process.*, **1**(1), pp. 18–31, 1992.

9. M.A. Alia, A.B. Samsudin, A new digital signature scheme based on Mandelbrot and Julia fractal sets, *American Journal of Applied Sciences*, **4**(11), pp. 848–856, 2007.

10. L. Kocarev, M. Sterjev, A. Fekete, G. Vattay, Public key encryption with chaos, *Chaos*, **14**(4), pp. 1078–1082, 2004.

11. N.M.G. AL-Saidi, M.R.Md. Said, A new public key cryptosystem based on IFS, *International Journal of Cryptology Research*, **2**(1), pp. 1–13, 2010.