Pseudorandom Permutations of a Prescribed Type [NR00]

Orr Paradise* and Neil Vexler†

March 3, 2019

An interpretation of [NR00], mistakes are likely ours.

`Part one of two in a talk on pseudorandom objects of a prescribed type (notes for the second part are unavailable, unfortunately.`

1 Introduction

1.1 Cycle notation

Let S_n be the set of bijections from $[n]$ to itself. Endowed with the composition operation $(\circ)$ it forms a group. Further, each $\sigma \in S_n$ can be decomposed into its *cycles*:

1. Initialize $N \coloneqq [n]$ and an empty cycle set. While $N \neq \emptyset$:
   (a) Choose $i \in N$, and initialize $\gamma = (i)$. Let $j \coloneqq \sigma(i)$. While $j \neq i$:
      i. Append j to γ and let $j \coloneqq \sigma(j)$.
   (b) Add c to the cycle set and update $N \coloneqq N \setminus \gamma$.

We know of Cauchy's *two-line* notation for permutations, in which we represent $\sigma \equiv \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$. We can now represent σ by listing its cycles, $\sigma \equiv (1, \sigma(1), \dots)(i, \sigma(i), \dots), \dots$. Notice that this representation is unique only up to the order of cycles, and the starting element of each cycle[1]. Also, single-element cycles are usually omitted.

We associate with each permutation σ its *cycle type* $\mathrm{CT}(\sigma)$, which is simply a list of the lengths of each cycle of σ. Again this property is determined only up to the order of cycles. Three examples:

Two-line notation	Cycle notation	Cycle Type
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	$(1,2,3,4) \equiv (4,1,2,3)$	(4)
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$	$(1,2)(3,4)$	$(2,2)$
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$	$(1,3)(1)(4) \equiv (1,3)$	$(1,1,2) \equiv (2,1,1)$

For any cycle type C, let $S_n(C) \coloneqq \{\sigma \in S_n | \mathrm{CT}(\sigma) = C\}$ be the set of all permutations on $[n]$ elements with cycle type C. Elements of $S_n(C)$ will be known as C-permutations (on n elements).[2] A final important notion is the *conjugation of* $\sigma \in S_n$ *by* $\pi \in S_n$, defined by $\sigma^\pi \coloneqq \pi \circ \sigma \circ \pi^{-1}$. An elementary result in group theory is that $\mathrm{CT}(\sigma) = \mathrm{CT}(\sigma^\pi)$ and that $S_n(C)$ is the set of all conjugations of σ, hence $S_n(C)$ is known as σ's *conjugacy class*. We will in fact show a stronger result in lemma 2.

*orr.paradise@weizmann.ac.il
†neil.vexler@weizmann.ac.il

[1] This depends on the choice of i in 1a and can be canonicalized by always choosing $i = \min N$.

[2] These two definitions are nonstandard.

1.2 Pseudo-random Permutations

Definition 1. A family of permutations $\mathcal{P}_n = \left\{P_k \in S_n | k \in \{0,1\}^l\right\}$ is called *pseudo-random* if it satisfies the following:

1. *Succinct Representation*: The key length l is polynomial in the input/output length n.
2. *Efficient Computation*: For any k, P_k,P_k^{-1} can be computed efficiently, i.e in time polynomial in l.
3. *Indistinguishability*: No efficient distinguisher, given oracle access to $\pi, \pi^{-1} \in S_n$ can distinguish whether τ is a random member of $\mathcal{P}_n$ or a truly random permutation with non-negligible probability. That is, for any efficient distinguisher D there exists a negligible $\mathrm{negl}(\cdot)$ such that

$$\left|\mathbb{P}_{k\sim U\left(\{0,1\}^l\right),D}\left[D^{P_k,P_k^{-1}}\left(1^n\right)=1\right]-\mathbb{P}_{\pi\sim U(S_n),D}\left[D^{\pi,\pi^{-1}}\left(1^n\right)=1\right]\right|\le \mathrm{negl}\left(n\right)$$

For any cycle type C we could replace S_n with $S_n(C)$ in the above definition to obtain a definition for *pseudo-random* C*-permutations*. Notice that the adversary would then be required to distinguish between a random member of $\mathcal{P}_n$ and a random C-permutation. Also notice that we require $\mathcal{P}_n$ to truly be a family of C-permutations and not just computationally indistinguishable from one—more on this later.

2 Pseudo-random C-permutations

The first main result we will see is due to Moni Naor and Omer Reingold [NR00], and asserts that if there are pseudo-random permutations then there are pseudo-random C-permutations for any cycle type C. Also, these pseudo-random C-permutations have the *fast-forward property*, meaning that they can be iterated at 'zero' cost.

2.1 The construction

Let $\mathcal{P}_n$ be a family of pseudo-random permutations, and let C be a cycle type. The construction is straightforward. Fix $\sigma \in S_n(C)$. The family is

$$\mathcal{F}_n := \left\{F_k := \sigma^{P_k} := P_k \circ \sigma \circ P_k^{-1} | k \in \{0,1\}^l\right\}$$

2.2 Correctness

We turn to to prove that $\mathcal{F}_n$ is a family of pseudo-random C-permutations.

2.2.1 Truthfulness

We first need to prove that indeed $F_k \in S_n(C)$ for all k. We prove a stronger result.

Lemma 2. *If π is a random permutation then σ^π is a random C-permutation. That is, if $\pi \sim U(S_n)$ then $\sigma^\pi \sim U(S_n(C))$.*

Proof. Let $\tau, \tau' \in S_n(C)$. We need to show that

$$\mathbb{P}_\pi\left[\sigma^\pi = \tau\right] = \mathbb{P}_\pi\left[\sigma^\pi = \tau'\right]$$

Since π is uniformly chosen from S_n, letting $\Pi = \{\pi \in S_n | \sigma^\pi = \tau\}$ and $\Pi' = \{\pi \in S_n | \sigma^\pi = \tau'\}$ it suffices to prove that $|\Pi| = |\Pi'|$. This is shown by constructing a bijection between the sets. Assume there exists $P \in S_n$ such that $\tau' = \tau^P$. The bijection from Π to Π' is then $\pi \mapsto P \circ \pi$.

- It is well defined: If $\pi \in \Pi$ then $\sigma^{P\circ\pi} = \left(\sigma^\pi\right)^P = \tau^P = \tau'$, so $P \circ \pi \in \Pi'$.

- It is invertible: Its inverse is clearly $\pi' \mapsto P^{-1} \circ \pi'$, and is well defined since if $\pi' \in \Pi'$ then $\sigma^{P^{-1} \circ \pi'} = \left(\sigma^{\pi'}\right)^{P^{-1}} = (\tau')^{P^{-1}} = \left(\tau^{P}\right)^{P^{-1}} = \tau$.

What's left is to construct such P. Since $\mathrm{CT}(\tau) = \mathrm{CT}(\tau')$ we can uniquely associate each cycle γ in τ with a cycle of same length γ' in τ'. For any such cycles $\gamma = (i_0, \ldots, i_g)$ and $\gamma' = \left(i'_0, \ldots, i'_g\right)$, let $P\left(i'_j\right) \coloneqq i_j$. This defines a permutation $P \in S_n$ for which $\tau' = \tau^P$. Indeed

- P is a well defined permutation because each $i \in [n]$ appears exactly once in the cycles of τ and of τ', and the correspondence of those cycles is 1-to-1 and onto.
- For any $i \in [n]$, assume that $i = i_j$ in cycle γ of τ. with corresponging i'_j in cycle γ' of τ,

$$\tau'\left(P\left(i_j\right)\right) = \tau'\left(i'_j\right) = i'_{j+1 \mod g} = P\left(i_{j+1 \mod g}\right) = P\left(\tau\left(i_j\right)\right)$$

  therefore $\tau' \circ P = P \circ \tau$ and so $\tau' = \tau^P$.

$\square$

Proving the first two axioms of pseudo-randomness is easy, so we turn to prove indistinguishability.

2.2.2 Indistinguishability

Suppose that we have an efficient distinguisher D for which

$$\left|\mathbb{P}_{k \sim U\left(\{0,1\}^l\right), D}\left[D^{F_k, F_k^{-1}}\left(1^n\right) = 1\right] - \mathbb{P}_{\tau \sim U(S_n(C)), D}\left[D^{\tau, \tau^{-1}}\left(1^n\right) = 1\right]\right| > \frac{1}{p(n)}$$

for some polynomial p. Let $t(n), q(n)$ denote the polynomial time, query complexities (resp.) of D on inputs of length n. We construct a distinguisher E that will contradict $\mathcal{P}_n$ being a pseudo-random permutation family.

Algorithm 1 The distinguisher E

The run $E^{\pi, \pi^{-1}}\left(1^n\right)$ simulates D in the following way:

1. Let $\tau = \sigma^{\pi} = \pi \circ \tau \circ \pi^{-1}$. E simulates $D^{\tau, \tau^{-1}}\left(1^n\right)$ as follows:
   (a) When D makes the query $\tau(x)$, E queries its oracle twice: Once for $z \coloneqq \pi^{-1}(x)$ and again for $y \coloneqq \pi(\sigma(z))$. E answers D's query with y.
   (b) When D makes the query $\tau^{-1}(x)$, E queries its oracle twice: Once for $z \coloneqq \pi(x)$ and gain for $y \coloneqq \pi^{-1}(\sigma(z))$. E answers D's query with y.
2. E answers the same as D.

Denoting σ's runtime with s—which is fixed in the context of this analysis. Then E's query and runtime complexities are

$$q_E(n) = 2q_D(n)$$
$$t_E(n) \leq \underbrace{q(n)(2+s)}_{\text{queries of } D} \underbrace{p(n)}_{\text{other operations of } D} \leq p(n)(3+s) = O(p(n))$$

so E is efficient, and it holds that

$$\mathbb{P}_{k \sim U\left(\{0,1\}^l\right), D}\left[D^{F_k, F_k^{-1}}\left(1^n\right) = 1\right] = \mathbb{P}_{k \sim U\left(\{0,1\}^l\right), E}\left[E^{P_k, P_k^{-1}}\left(1^n\right) = 1\right]$$

$$\mathbb{P}_{\tau \sim U(S_n(C)), D}\left[D^{\tau, \tau^{-1}}\left(1^n\right) = 1\right] \underset{\text{Lemma}}{=} \mathbb{P}_{\pi \sim U(S_n), D}\left[D^{\sigma^{\pi}, \left(\sigma^{\pi}\right)^{-1}}\left(1^n\right) = 1\right] = \mathbb{P}_{\pi \sim U(S_n), E}\left[E^{\pi, \pi^{-1}}\left(1^n\right) = 1\right]$$

2.2.3 Fast Forward Property

An appealing property of this construction is that it enables fast-forwarding. Denote the runtime of computing $\sigma^{(m)} = \sigma \circ \cdots \circ \sigma$ by $s(m)$. Notice that

$$F_k^{(m)} = \left(P_k \circ \sigma \circ P_k^{-1}\right)^{(m)} = \left(P_k \circ \sigma \circ P_k^{-1}\right) \circ \left(P_k \circ \sigma \circ P_k^{-1}\right) \circ \cdots \circ \left(P_k \circ \sigma \circ P_k^{-1}\right) = P_k \circ \sigma^{(m)} \circ P_k^{-1}$$

so iterating m times over F_k adds only $s(m)$ to the evaluation runtime complexity. Therefore if we assume that σ also has the fast forward property[3], that is that $s(m) = s(m')$ for all m, m', then we could have provided the distinguisher D with more power, namely issuing queries to $\tau^{(m)}$, while maintaining security. If we assume σ^{-1} has the fast forward property as well, this holds also for negative m.

References

[NR00] Naor, Moni and Omer Reingold. "Constructing Pseudo-Random Permutations with a Prescribed Structure." Journal of Cryptology 15 (2000): 97-102.

[3] For example when σ is the cyclic permutation $\sigma = (1, \ldots, 2^n)$, then $\sigma^{(m)}(x) = x + m \mod 2^n$.