Random Number Generators Based on Permutations Can Pass the Collision Test

Alexey Urivskiy

InfoTeCS

urivskiy@infotecs.ru, alexey.urivskiy@mail.ru

CTCrypt'2019

Pseudo Random Number Generators

G: $\{0,1\}^m \rightarrow \{0,1\}^s$ for $s \gg m$

Typical assumptions for a PRNG:

- **G** is efficiently computable
- the seed is uniformly distributed on $\{0,1\}^m$
- '**random-like**'

Theorem [Yao'82] : if for **G** the next bit cannot be predicted with probability better than ½ given any prefix by any polynomial predictor (the next-bit test) it will pass any polynomial statistical test.

(Random) Permutations

V_n – vector space of n-bit vectors

σ – permutation on V_n

0	1	2	…	2^n-2	2^n-1
$\sigma(0)$	$\sigma(1)$	$\sigma(2)$	…	$\sigma(2^n\text{-}2)$	$\sigma(2^n\text{-}1)$

PRNG on a Random Permutation

$IV \in V_n$ – initializing variable

σ – random permutation on V_n

G1I:

for *i* = 0 to *s* do

$$T := (IV + i) \bmod 2^n$$

$$x_i := \sigma(T)$$

Consider the case $\boldsymbol{s < N = 2^n}$.

Properties of G1I

G1I, in which is σ is modeled as an n-bit block cipher with a random key, is highly appreciated and widely used – ISO/IEC 18031 **`CTR_DRBG`.**

However, if **G1I** has output a symbol, it will never output it again →

For $s \sim \sqrt{N}$ due to the **birthday paradox** becomes **distinguishable** from a truly RNG.

PRNGs on 2 Random Permutations

σ_1, σ_2 – random permutation on V_n

G2I:

for i = 0 to s do

$$T := i \; mod \; 2^n$$

$$x_i := \sigma_1(T) \oplus \sigma_2(T)$$

Conditional probability

Conditional probability

$P(x_s|x_{s-1}, x_{s-2}, \ldots, x_0)$ is the probability for a generator to output x_s provided $x_{s-1}, x_{s-2}, \ldots, x_0$ were output before.

Equivalent representation for G2I

$$\mathbf{M} = \begin{array}{c|c} \oplus & \begin{array}{cccccc} 0 & 1 & 2 & 3 & \dots & N-1 \end{array} \\ \hline \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ \vdots \\ N-1 \end{array} & \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix} \end{array}$$

Equivalent representation for G2I

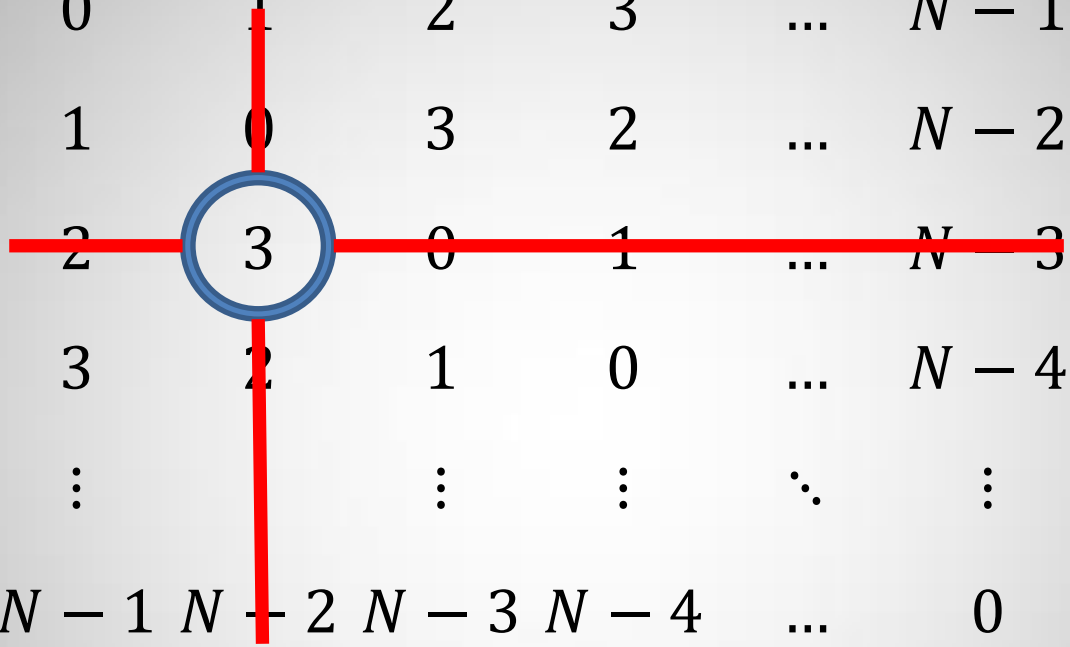
$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix}$$

$$x_0 = 3$$

$$(2,1),$$

Equivalent representation for G2I

$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix}$$

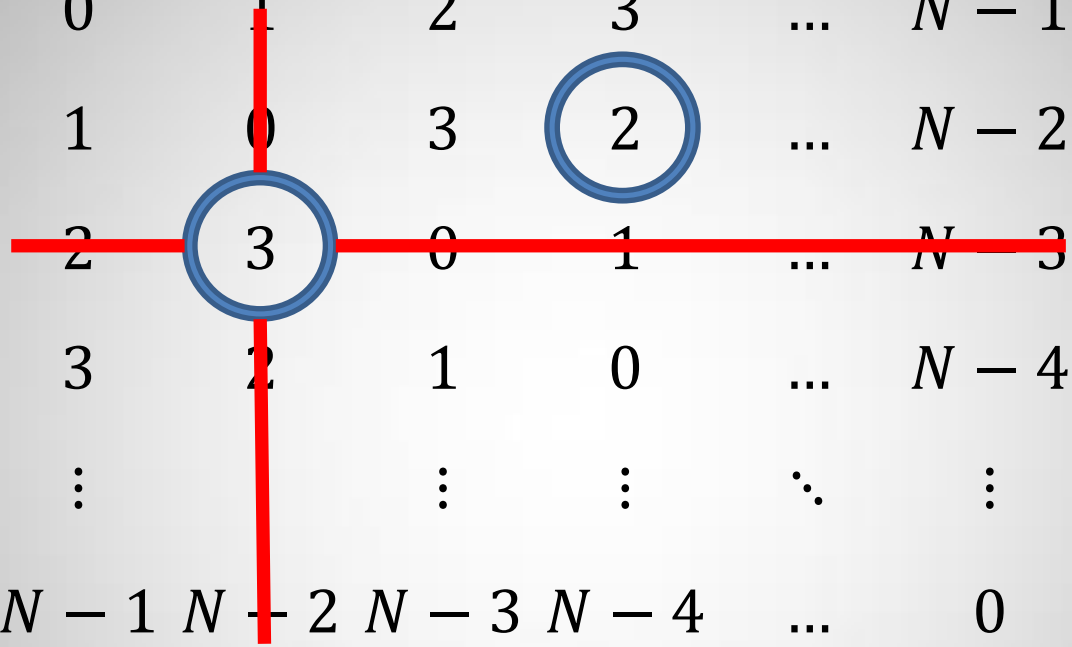


$$x_0 = 3$$

$$(2,1),$$

Equivalent representation for G2I

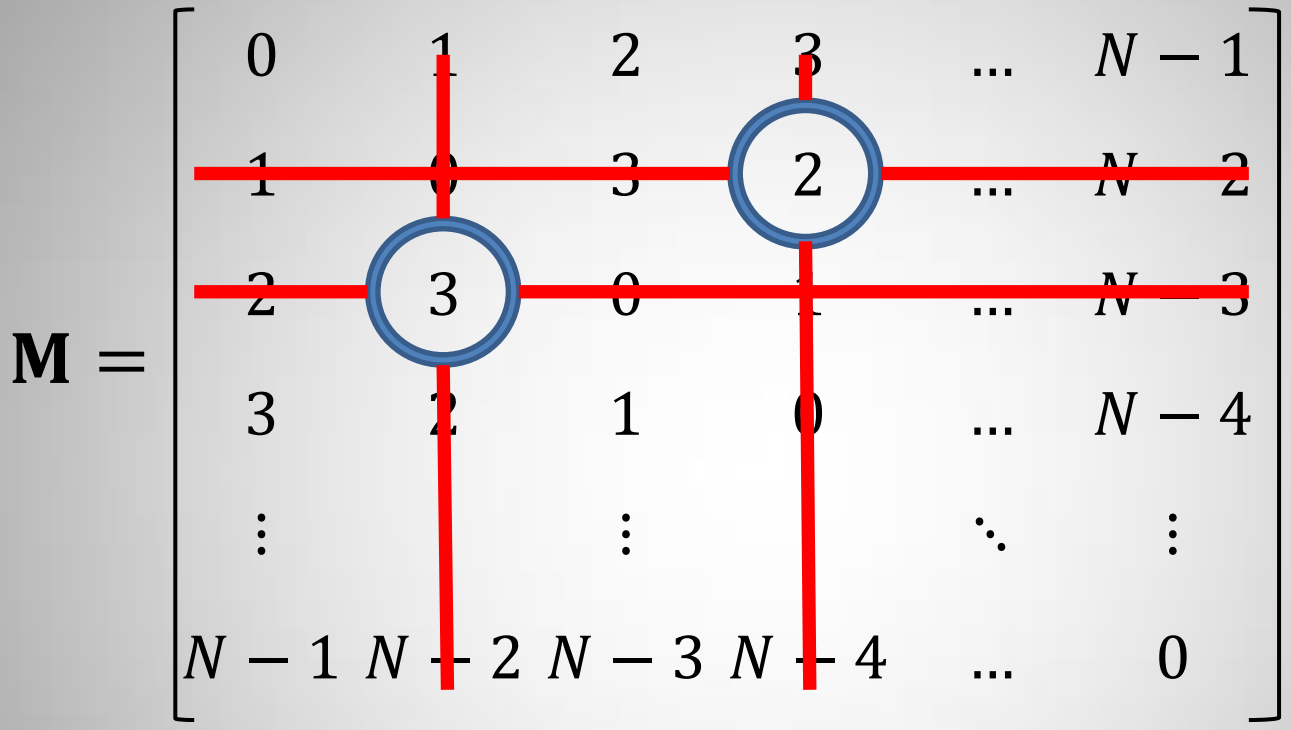
$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix}$$



$$x_0 = 3, x_1 = 2$$

$$(2,1), \quad (1,3)$$

Equivalent representation for G2I

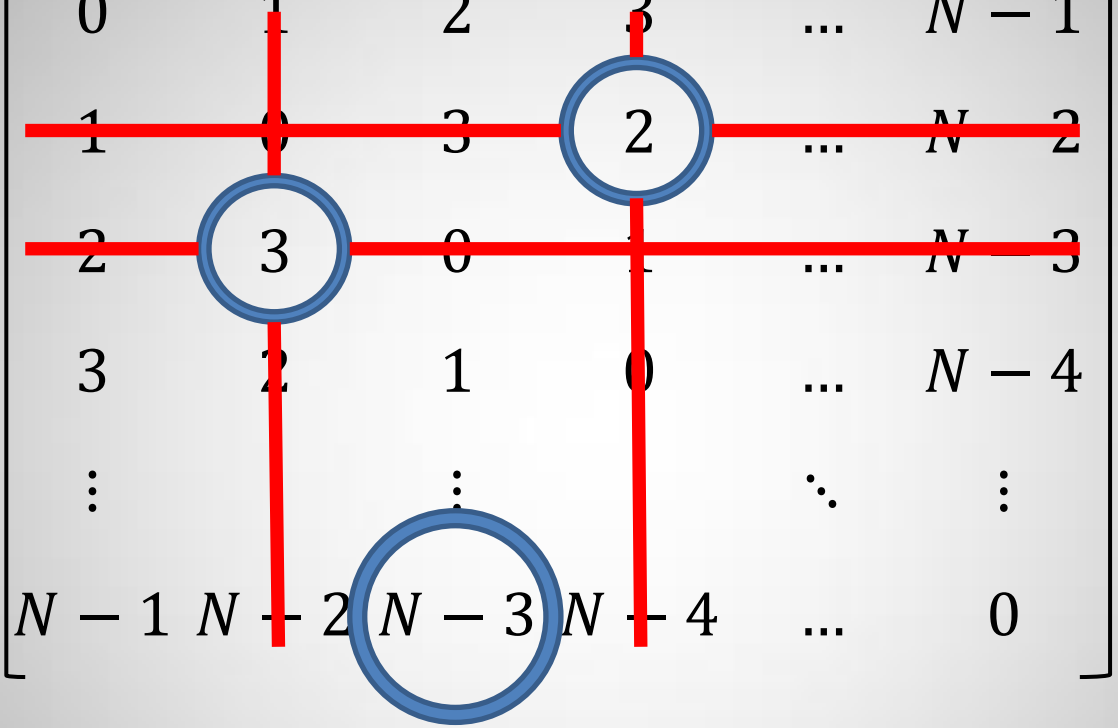


$a_0 = 3, a_1 = 2$

$(2,1)$, $(1,3)$

Equivalent representation for G2I

$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix}$$



$$x_0 = 3, x_1 = 2, x_2 = N-3$$

(2,1), (1,3), (*N*-1,2)

Equivalent representation for G2I

$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & \dots & N-1 \\ 1 & 0 & 3 & 2 & \dots & N-2 \\ 2 & 3 & 0 & 1 & \dots & N-3 \\ 3 & 2 & 1 & 0 & \dots & N-4 \\ \vdots & & & & \ddots & \vdots \\ N-1 & N-2 & N-3 & N-4 & \dots & 0 \end{bmatrix}$$

$$a_0 = 3, a_1 = 2, a_2 = N-3$$

(2,1), (1,3), (*N*-1,2)

Conditional probability for G2I

$$P_1 = \frac{N-2s}{(N-s)^2} \leq P(x_s | x_{s-1}, x_{s-2}, \ldots, x_0) \leq \frac{N-s}{(N-s)^2} = P_2$$

$$P_1 < \frac{1}{N} < P_2$$

Collision Test

Collision – the occurrence of two or more identical symbols in the output sequence.

Collision probability for a true RNG:

$$P_I(s) \simeq 1 - \exp\left(-\frac{s(s-1)}{2N}\right)$$

An RNG fails the **collision test** if the collision probability falls far from $P_I(s)$.

Collision Probability for G2I – 1

Let in the prefix $x_{s-1}, x_{s-2}, \dots, x_0$
all symbols be different.

No collision for x_s happens with probability
$P_d(s+1) = P(x_s \notin \{x_{s-1}, \dots, x_0\} | x_{s-1} \neq \dots \neq x_0)$

Proposition.

$$\boldsymbol{1 - sP_2 \leq P_d(s+1) \leq 1 - sP_1}$$

Collision Probability for G2I – 2

From the chain rule for the probability of joint events through conditional probabilities: the probability to found no collision in the prefix of length $s + 1$

$$\boldsymbol{P_D(s+1) = P(x_s \neq \cdots \neq x_0) = \prod_{i=0}^{s} P_d(i+1)}$$

where $P_d(1) = 1$.

Collision Probability for G2I – 3

$P_C(s+1)$ - the probability for the collision to occur in the prefix of length $s+1$ for **G2I** :

$$1 - \prod_{i=0}^{s}\left(1 - \frac{i(N-2i)}{(N-i)^2}\right) \leq$$

$$P_C(s+1)$$

$$\leq 1 - \prod_{i=0}^{s}\left(1 - \frac{i(N-i)}{(N-i)^2}\right)$$

Technical details – 1

For $z \ll 1$, the Taylor series

$$\exp(z) = 1 + z + \frac{z^2}{2} + o(z^2) \ .$$

Thus, for $s \ll N/2$:

$$\boldsymbol{1 - \frac{i(N-2i)}{(N-i)^2} \approx exp\left(-\frac{i(N-2i)}{(N-i)^2}\right)}$$

$$\boldsymbol{1 - \frac{i(N-i)}{(N-i)^2} \approx exp\left(-\frac{i(N-i)}{(N-i)^2}\right)}$$

Technical details – 2

For $z \ll 1$, the Taylor series

$$(1+z)^{\alpha} = 1 + \alpha z + \frac{\alpha(\alpha-1)}{2} z^2 + o(z^2) \ :$$

$$\sum_{i=0}^{s} \frac{i(N-i)}{(N-i)^2} = \sum_{i=0}^{s} \frac{i}{N}\left(1 + \frac{i}{N} + \left(\frac{i}{N}\right)^2 + o\left(\frac{i}{N}\right)^2\right)$$

$$\sum_{i=0}^{s} \frac{i(N-2i)}{(N-i)^2} = \sum_{i=0}^{s} \frac{i}{N}\left(1 - \left(\frac{i}{N}\right)^2 + o\left(\frac{i}{N}\right)^2\right)$$

Technical details – 3

Table sums

$$\sum_{i=0}^{s} i = \frac{s(s+1)}{2}$$

$$\sum_{i=0}^{s} i^2 = \frac{s(s+1)(2s+1)}{6}$$

$$\sum_{i=0}^{s} i^3 = \frac{s^2(s+1)^2}{4}$$

Collision Probability for G2I – 4

Lemma. For **G2I**:

$$1 - exp\left(-\frac{s(s+1)}{2N} + \frac{s^4}{4N^3}\right) \leq$$

$$P_C(s+1)$$

$$\leq 1 - exp\left(-\frac{s(s+1)}{2N} - \frac{s^3}{3N^2} - \frac{s^4}{4N^3}\right)$$

PRNGs on Random Permutations

G1LI: $MSB_n(\sigma_1(T))$ – truncation of a $2n$-bit permutation to n bits

GXHI: – XOR of two halves of $2n$-bit permutation

$$MSB_n(\sigma_1(T)) \oplus LSB_n(\sigma_1(T))$$

GXTrI: – XOR of an n-bit and a $2n$-bit permutations

$$\sigma_2(T) \oplus MSB_n(\sigma_1(T))$$

Conditional probabilities

G2I:

$$P_1 = \frac{N-2s}{(N-s)^2} \leq P(x_s|S) \leq \frac{N-s}{(N-s)^2} = P_2$$

GTrI:

$$\frac{N-s}{N^2-s} \leq P(x_s|S) \leq \frac{N}{N^2-s}$$

GXHI:

$$\frac{N-s}{N^2-s} \leq P(x_s|S) \leq \frac{N}{N^2-s}$$

GXTrI:

$$\frac{N^2-Ns-s}{(N-s)(N^2-s)} \leq P(x_s|S) \leq \frac{N^2-Ns}{(N-s)(N^2-s)}$$

Collision Probability for G1LI

Lemma. For **G1LI**:

$$1 - exp\left(-\frac{s(s+1)}{2N} + \frac{s^3}{2N^2}\right) \leq$$

$$P_C(s+1)$$

$$\leq 1 - exp\left(-\frac{s(s+1)}{2N} - \frac{s^3}{3N^3}\right)$$

Examples

Let $s^2 > 2N$, but $s \ll \frac{N}{2}$

Fix $\delta(s) = |P_C(s+1) - P_I(s+1)|$

Compare possible prefix lengths $\boldsymbol{s}$ for **G1I** and $\boldsymbol{t}$ for **G2I.**

$$\boldsymbol{\delta \approx \frac{s^2}{2N} \approx \left(\frac{t^3}{3N^2} + \frac{t^4}{4N^3}\right) exp\left(-\frac{t^2}{2N}\right)}$$

Examples

$$N = 2^{64}, \delta = 2^{-34}$$

G1I: $s = 2^{15,5}$

G2I: $t > 2^{32}$

$$N = 2^{128}, \delta = 2^{-68}$$

G1I: $s = 2^{30,5}$

G2I: $t > 2^{63}$

Thank you!
Questions?