PRNG vs. CSPRNG

Romana Linkeová

November 21, 2014

Random number generators

- random numbers, sequence of random numbers
- gambling (lotteries, slot machines), computer simulations, data sampling, cryptography
- random (physical phenomena) vs. pseudorandom (computer programme)

TRNG

- true random number generator, hardware random number generator
- mouse movement, background noise
- radioactive source, atmospheric noise, photoelectric effects

PRNG

- pseudorandom number generator
- deterministic computer program - seed
- faster
- statistical tests

Statistical tests

- measure randomness
- frequency test, serial test, gap test etc.
- Diehard tests, Monobit test, Kolmogorov–Smirnov test etc.

CSPRNG

- cryptographically secure pseudorandom number generator
- key generation, nonce
- satisfy: statistical tests, k-bit test, "state revelation test"

Reciprocal polynomials

Definition

Let F be an arbitrary field. For a polynomial $p(x) = a_0 + a_1x + \ldots + a_nx^n$ with coefficients from F, the reciprocal polynomial is $p^*(x) = a_n + a_{n-1}x + \ldots + a_0x^n = x^n p(x^{-1})$.

Example

$p(x) = x^3 + x + 2$
$p^*(x) = 2x^3 + x^2 + 1$

Reciprocal polynomials

Lemma

Polynomial $p(x)$ is primitive iff $p^*(x)$ is primitive.

Proof.

- $p(x)$ is irreducible iff $p^*(x)$ is irreducible
- $\text{ord}(\alpha) = \text{ord}(\alpha^{-1})$

LFSR

- linear feedback shift register
- length n, feedback function, seed
- pseudorandom sequence $X = (x_0, x_2, \ldots)$
- $x_k = \sum_{i=1}^{n} a_i x_{k-i} \Rightarrow \sum_{i=0}^{n} a_i x_{k-i} = 0,\ a_0 = 1$
- linear reccurent sequence (LRS)

Characteristic and connection polynomial

Definition

The connection polynomial is $p(x) = \sum_{i=0}^{n} a_i x^i$.

Definition

The characteristic polynomial is $p^*(x)$.

Shift operator, shift equivalence

Definition

Let A be a finite set. $\mathrm{V}(A) = \{\{a_i\}_{i\geq 0}, a_i \in A\}$.

Definition

Map $L : \mathrm{V}(\mathbb{F}_q) \to \mathrm{V}(\mathbb{F}_q) : L(\{a_i\}_{i\geq 0}) = \{a_{i+1}\}_{i\geq 0}$ is called the shift operator.

$p^*(L)(X) = 0$

Definition

Let $\overrightarrow{a} \in \mathrm{V}(\mathbb{F}_q)$ and $p(L) \in \mathbb{F}_q[L]$.

- $G(p) := \{\overrightarrow{a} \in V(\mathbb{F}_q) \mid p(L)(\overrightarrow{a}) = 0\}$.
- $A(\overrightarrow{a}) := \{p(L) \in \mathbb{F}_q[L] \mid p(L)(\overrightarrow{a}) = 0\}$.

Shift operator, shift equivalence

Definition

Let $\overrightarrow{a}, \overrightarrow{b} \in V(\mathbb{F}_q)$ periodic sequences. Then $\overrightarrow{a}, \overrightarrow{b}$ are shift equivalent if $\exists k \in \mathbb{N} : L^k(\overrightarrow{a}) = \overrightarrow{b}$.

Definition

Let $p(x) \in \mathbb{F}_q[x]$. The period $per(p) = \min\{n \in \mathbb{N}, p|x^n - 1\}$.

Lemma

The shift equivalence on $G(p)$ has for a LFSR with irreducible characteristic polynomial $p^* \in \mathbb{F}_q[x]$ of degree n $\frac{q^n - 1}{per(p^*)}$ cycles of length $per(p^*)$ and one cycle of length 1.

Minimal polynomial, primitive polynomial

Definition

Monic polynomial of minimal degree in $A(\overrightarrow{a})$ is called the minimal polynomial $m_{\overrightarrow{a}}$.

Lemma

Let $\overrightarrow{a} \in V(\mathbb{F}_q)$ *be a LRS,* $m_{\overrightarrow{a}}$, $\deg(m_{\overrightarrow{a}}) = n$. *For* $\alpha \in \mathbb{F}_{q^n} : m_{\overrightarrow{a}}(\alpha) = 0$ *we get*

$$per(\overrightarrow{a}) = per(m_{\overrightarrow{a}}) = ord(\alpha).$$

Lemma

For p primitive $per(p^*) = ord(\alpha) = q^n - 1 \Rightarrow G(p)$ *has one equivalence class of* $q^n - 1$ *elements.*

Xorshift

- generator based on a repeated use of the xor operation of a word with a shifted version of itself
- PRNG, LFSR
- fast, low memory costs

Example

Input: 64-bit x
$x = x\hat{}(x >> 12);$
$x = x\hat{}(x << 25);$
$x = x\hat{}(x >> 27);$
Return x.

Definition

Definition

Let x be a binary vector of length n and let L be $n \times n$ matrix, which has ones on its subdiagonal and zeroes elsewhere. Then the *left xorshift operation* $x\hat{}(x \ll a), 0 < a < n$ can be written as $x(\mathrm{Id} + L^a)$.
And $n \times n$ matrix R which has ones on its superdiagonal and zeroes elsewhere corresponds to the *right xorshift operation* and $x\hat{}(x \gg a) = x(\mathrm{Id} + R^a)$.

$$L = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & 0 \end{pmatrix}.$$

Definition

Definition

Let S be a seed set made up of m-tuples $(x_1, \ldots, x_m)$, where x_i are binary vectors of length n. A nonsingular $nm \times nm$ matrix T over $\mathbb{F}_2$ is called the *companinon matrix*.
Pseudorandom sequence $(y_0, y_1, \ldots)$ can then be produced for seed $s \in S$ as

$$y_0 = s$$
$$y_j = sT^j.$$

Example

Example

Input: 64-bit x

$x = x\hat{}(x >> 12); \rightsquigarrow (\mathrm{Id} + R^{12})$

$x = x\hat{}(x << 25); \rightsquigarrow (\mathrm{Id} + L^{25})$

$x = x\hat{}(x >> 27); \rightsquigarrow (\mathrm{Id} + R^{27})$

Return x.

$$T_{64\times 64} = ((\mathrm{Id} + R^{12})(\mathrm{Id} + L^{25})(\mathrm{Id} + R^{27}))$$

Example

- Marsaglia, G.: **Xorshift RNGs**, *Journal of Statistical Software*, 2003.
- $T = ((\mathrm{Id} + L^a)(\mathrm{Id} + R^b)(\mathrm{Id} + L^c))$
- 81 triples for 32-bit, 275 triples for 64-bit

Xorshift is LFSR

Definition

The minimal polynomial m_T of $n \times n$ matrix T over field $\mathbb{F}$ is monic polynomial of least degree in $\mathbb{F}[x]$ such that $m_T(T) = 0$.

Lemma

TFSAE

- α *is root of* m_T
- α *is root of the characteristic polynomial of* T
- α *is an eigenvalue of* T

Xorshift is LFSR

- matrix T, $(y_k) : y_k = sT^k$
- $m_T = \sum_{i=0}^{n} c_i x^{n-i}$ the minimal polynomial
  $\Rightarrow \sum_{i=0}^{n} c_i T^{n-i} = 0$
- multiplying on the left by sT^{k-n}
- $\sum_{i=0}^{n} c_i sT^{k-i}$
- $\sum_{i=0}^{n} c_i y_{k-i}$

Xorshift is not CSPRNG

- Pannetof, F. - L'Ecuyer, P.: **On the Xorshift Random Number Generators**, *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 2005.
- SmallCrush, Crush (software package TestU01)
- combining Xorshift generators with some non linear functions

Example

Example

Given four 32-bit nonzero seeds x, y, z, w we can construct a xorshift generator as follows:

$t = x \hat{} (x \ll 11);$

$x = y;\ y = z;\ z = w;$

$w = w \hat{} (w \gg 19) \hat{} t \hat{} (t \gg 8);$

Return (x, y, z, w).

Example

Example

The companion matrix T will be

$$\begin{pmatrix} 0 & 0 & 0 & (1+L^{11})(1+R^8) \\ \mathrm{Id} & 0 & 0 & 0 \\ 0 & \mathrm{Id} & 0 & 0 \\ 0 & 0 & \mathrm{Id} & (1+R^{19}) \end{pmatrix}$$

and then for given seed (x, y, z, w) we have

$$(x, y, z, w)T = (y, z, w, x(1+L^{11})(1+R^8) + w(1+R^{19})).$$

Period

Lemma

This xorshift generator has maximum period $2^{128} - 1$.

Period

Lemma

A xorshift generator with 128×128 *companion matrix* T *over* $\mathbb{F}_2$ *has maximum period* $2^{128} - 1$ *if and only if the characteristic polynomial of matrix* T *is primitive.*

Proof.

- Xoshift is LFSR (minimal polynomial, connection polynomial)
- LFSR has maximal period iff it's characteristic polynomial is primitive

□

Period

Definition

Polynomial $f \in \mathbb{F}_q[x]$ of degree n is primitive over $\mathbb{F}_q$ if f is irreducible over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}, f(\alpha) = 0$ is a primitive element of $\mathbb{F}_{q^n}$ (i.e. generates $\mathbb{F}^*_{q^n}$).

- $F = \mathbb{F}_2 = \mathbb{Z}_2$
- characteristic polynomial p, $n = \deg(p) = 128$, $\alpha : p(\alpha) = 0$
- $\alpha, \alpha^2, \ldots, \alpha^{2^n-2} \neq 1, \alpha^{2^n-1} = 1$
- Lagrange theorem $\Rightarrow \alpha^q$, $q | 2^n - 1$
- $K = F[\alpha]$, $K' = F[x]/(f(x)K[x])$
- $K \simeq K'$, $\alpha \mapsto x$
- $x^i \bmod p \neq 1$, $i | 2^n - 1$

Attack

- seed $s = (x_0, y_0, z_0, w_0)$
- $y_j = sT^j$
- 128-bit y_j
- $s_x = y_j$
- $y_{j+1} = s_x T$, $y_{j+2} = s_x T^2$, ...
- $b = (b_0, b_1, \ldots, b_{127})$, $b_i = [s_x T^i]_0$

Conclusion

- fast, simple, low memory costs
- not CSPRNG
- carefully chosen parameters in order to achieve a long period

Thank you for your attention!