Generátory pseudonáhodných čísel a jejich aplikace v kryptografii (proudové šifry)

Hana Srbová

Fakulta jaderná a fyzikálně inženýrská, ČVUT Praha

11. 3. 2013

Obsah

Generátory náhodných čísel (RNG)

- Využívání náhodnosti fyzikálních jevů
- Příklady fyzikálních jevů:
  - čas mezi vyzařovaním částic při radioaktivním rozpadu
  - tepelný šum polovodičové diody nebo rezistoru
  - nestabilita frekvence volného oscilátoru
  - fluktuace v přístupové době čtení na disku způsobené proudění vzduchu tímto diskem
- Vygenerovaná posloupnost nelze zrekonstruovat
- Neefektivní

Generátory preudonáhodných čísel (PRNG)

- Generování pomocí předpisu $X_i = f(X_{i-1}, \ldots, X_{i-j})$
- Procesy, ze kterých získáváme počáteční hodnotu, tzv. „Seed“:
  - systémový čas
  - prodleva mezi stisknutím klávesy či pohyb myši
  - obsah input/output paměti
  - vstup od uživatele
- Zrekonstruovatelnost
- Efektivita
- Existence periody

Využití generátorů

- Kryptografie
- Testování softwaru
- Simulace
- GPS
- Ranging-systems
- Code-division systems
- Širokospektrální komunikační systémy
- Počítačové hry
- Teorie náhodných matic
- Teorie rozhodování

Generátory pseudonáhodných čísel

- Kongruenční generátory:
  - lineární
  - kvadratické
  - kubické
  - inverzní
- Blum-Blum-Shub generátor
- Mersenne-Twister generátor
- Zpožděný Fibonacciho generátor
- Lineární posuvný registr se zpětnou vazbou
- RSA a Micali-Schnorrův generátor

Blum-Blum-Shub generátor

- Zaveden rekurentním vztahem

$$X_{n+1} = X_n^2 \mod m, \quad n \geq 0,$$

kde m je produkt dvou velkých prvočísel t a u kongruentních s 3 mod 4

- Možnost vypočítat každý člen přímo podle vzorce

$$X_n = X_0^{2^n \mod \lambda(m)} \mod m,$$

přičemž $\lambda(m) = \lambda(t \cdot u) = \mathrm{lcm}(t-1, u-1)$

- Nevhodný pro simulace metodou Monte Carlo (pomalý)
- Kryptograficky bezpečný

Mersenne-Twister

- Maximální délka periody $2^{19\,937} - 1$
- Efektivně využívá paměť
- Vysoká rychlost
- K získání semínka se často využívá LCG nebo zpožděný Fibonacciho generátor
- Není kryptograficky bezpečný – při znalosti 624 po sobě jdoucích čísel lze předpovědět ostatní
- Uplatnění v simulacích metodou Monte Carlo
- V MATLABu implementováno pod příkazem rand(n)

Zpožděný Fibonacciho generátor

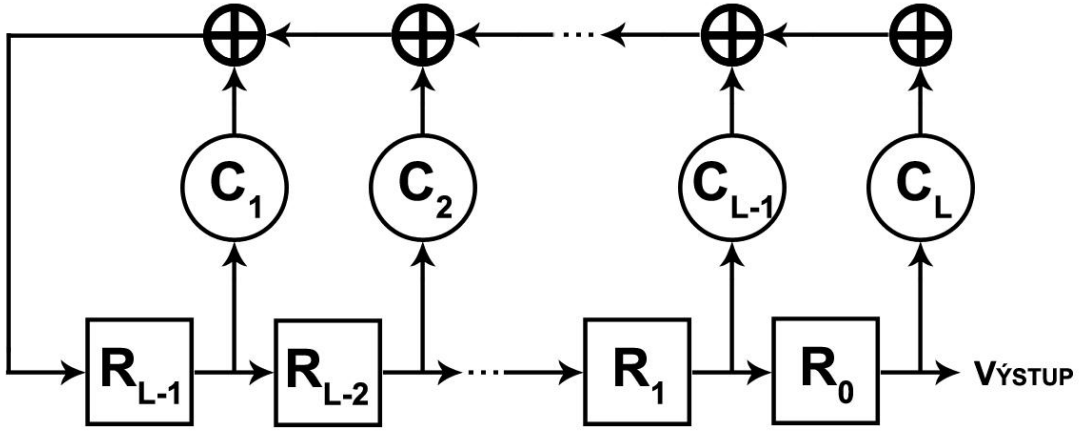
- Dán rekurentním vztahem

$$X_n = X_{n-p} \bigoplus X_{n-q} \mod m,$$

  kde p, q jsou koeficienty zpoždění, $p > q$; $\bigoplus$ binární operace sčítání, odečítaní, násobení, XOR
- Operace XOR vyžaduje uchování předchozích p hodnot posloupnosti
- Dlouhá perioda
- Velmi rychlé

Lineární posuvný registr se zpětnou vazbou

- Skládá se z L vnitřních registrů $R_0, \ldots, R_{L-1}$, časovacího signálu a charakteristického polynomu
- Obsah registru R_i je přesunut do R_{i-1} a R_0 se předá na výstup, a poté se vypočte obsah registru R_{L-1} (registr zpětné vazby)



- Použití v telekomunikaci (GPS, přenos v rozprostřeném spektru) a v kryptografii (proudové šifry)

Testování náhodnosti

- Testování hypotéz H_0 oproti alternativě H_1
- H_0 – testovaná posloupnost je náhodná
- Možnost výskytu dvou druhů chyb, chyb I. a II. druhu
- Chyba I. druhu – posloupnost je náhodná, avšak hypotéza H_1 nebyla zamítnuta
- Pravděpodobnost výskytu chyby I. druhu se nazývá hladina významnosti a je určována předem
- Chyba II. druhu – H_1 zamítnuta (tj. zamítnuta nenáhodnost), přestože posloupnost nenáhodná je

Statistické testy

- NITS
  - Frekvenční test
  - Frekvenční blokový test
  - Sériový test
  - Test runů
  - Test kumulativních součtů
  - ...
- DIEHARD
  - Birthday spacing test
  - Parking lot test
  - The 3DSpheres Test
  - ...
- χ^2 test
- Kolmogorovov-Smirnův test
- a další

Frekvenční (blokový) test a sériový test

- Frekvenční test:
  - Zkoumá počet 0 a 1 v posloupnosti s
  - Zjišťuje zda jsou tyto dva počty přibližně stejné
- Frekvenční blokový test:
  - Frekvenční test aplikovaný na bloky délky m v sekvenci s
- Sériový test:
  - Zkoumá počet výskytu (překrývajících) se bloků délky m v posloupnosti s
  - Porovnává s očekávanými hodnotami pro náhodné generátory
  - Náhodné posloupnosti mají rovnoměrně rozdělené překrývání

Test runů a test kumulativních součtů

- Test runů
  - Zkoumá sady 0 (resp. 1) různých délek (sada je zepředu i zezadu ohraničena opačným bitem)
  - Porovnává s očekávým počtem pro náhodnou posloupnost
  - Očekáváný počet sad 0 (resp. 1) délky i v posloupnosti délky n je

$$e_i = \frac{n - i + 3}{2^{i+2}}$$

- Test kumulativních součtů
  - Testuje, zda kumulativní součet částečných posloupností testované posloupnosti s je příliš velký či příliš malý vzhledem k očekávanému chování kumulativních součtů pro náhodné posloupnosti
  - Kumulativní součet může být považován za náhodnou procházku
  - Pro náhodné posloupnosti by se hodnota náhodné procházky měla blížit nule

Proudové šifry

- Zašifrovávají každý znak zvlášť užitím pokaždé jiné transformace
- Dělí se na synchronní a asynchronní
- Synchronní – proudový klíč je generován bez závislosti na OT a na ŠT
- Asynchronní – proudový klíč je funkcí klíče a několika předchozích znaku ŠT
- Rychlejší a méně náročné na vybavení než blokové šifry
- Žádná nebo omezená chyba přenosu
- Používané hlavně v telekomunikacích

Vernamova šifra (one-time pad)

- Posun každého znaku o náhodně zvolený počet míst v abecedě
- Pokud pracujeme s binární abecedou, je dána vztahem

$$c_i = m_i \oplus k_i, \quad \text{pro } i = 1, 2, 3, \ldots$$

kde m_i jsou znaky OT, k_i znaky klíče, c_i znaky ŠT a $\oplus$ operace XOR

- Neprolomitelná (klíč je stejně dlouhý jako OT)
- K vygenerování klíče se použije PRNG

RC4

- Synchronní proudová šifra navržená v roce 1987
- Popis nebyl nikdy oficiálně publikován, ale byl zveřejněn neznámým hackerem v roce 1994
- Binární aditivní šifra (používá binární operaci XOR)
- Variabilní délka klíče
- Pomocí klíče generuje pseudonáhodný proudový klíč až do velikosti OT, který poté i s OT kombinuje užitím operace XOR
- Určená na rychlé šifrování velkého objemu dat
- Používá se v SSL a TLS, v zabezpečovacím standardu bezdrátových sítích, v šifrování emailů

Závěr

- Generátory pseudonáhodných čísel
- Testy náhodnosti
- Proudové šifry

Zdroje

- R. Ganian: **Testování rychlosti proudových šifer**, Bc. práce, Masarykova univerzita, 2006
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone:**Handbook of applied cryptography**,CRC Press, 1997
- O. Málek: **Generování pseudonáhodných dat založené na použité LFSR**, Bc. práce, Masarykova univerzita, 2007
- Z. Mikulka: **Generátory náhodných čísel**, Bc. práce, VUT v Brně, 2008
- K. Břinda: **Generátory pseudonáhodných čísel**, [online], Dostupné z: http://tigr.fjfi.cvut.cz/cow-workshops/11/ PrezentaceFrysava/KarelBrinda.pdf
- A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo: **A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications**, 2010.
- M. Čečunda: **Analýza bezpečnosti prúdovej šifry RC4**, Bc. práce, Masarykova univerzita, 2013
- R. Wash: **Lecture Notes on Stream Ciphers and RC4**
- V. Klíma: **Základy moderní kryptografie – Symetrická kryptografie II.**, verze 1.3, 2005

Děkuji za pozornost.