TKKPFMF2026-02-24

Def.: naj bo G PRG in A (napadalec) odločitveni algoritem:

$A: \{0,1\}^s \to \{0,1\}$, ki se odloči, ali je input string povsem naključen ali generiran s PRG G.

Prednost A je $Adv(A,G) = \left| P_{k \leftarrow K}\left(A(G(k))=1\right) - P_{r \leftarrow \{0,1\}^s}\left(A(r)=1\right) \right|.$

Primer: $A(x)=1 \quad Adv(A,G)=|1-1|=0$

$A(x) = \begin{cases} 0 ; & \text{z verjetnostjo } 1/2 \\ 1 ; & \text{z verjetnostjo } 1/2 \end{cases} \quad Adv(A,G) = |\tfrac{1}{2}-\tfrac{1}{2}| = 0.$

Def.: Fja $\varepsilon: \mathbb{N} \to \mathbb{R}^+$ je zanemarljiva, če

$\forall d\, \exists \lambda_0\, \forall \lambda > \lambda_0: \varepsilon(\lambda) \le \frac{1}{\lambda^d}.$

Primer: $\varepsilon(\lambda) = 2^{-\lambda}$ je zanemarljiva.

$\varepsilon'(\lambda) = \frac{1}{\lambda^{1000}}$ ni zanemarljiva.

Def.: Naj bo λ varnostni parameter. Preslikava $G: \{0,1\}^\lambda \to \{0,1\}^s$ je varen PRG, če za vsak polinomski odločitveni algoritem A obstaja zanemarljiva ε_A, da velja

$Adv(A,G) \le \varepsilon_A(\lambda).$

KONSTRUKCIJE PRG

LFSR – linear feedback shift register
linearna rekurzivna šifra.

parametri: $k \in \mathbb{Z}_2^m$ (skrivnost), $c_1, \dots, c_m \in \mathbb{Z}_2$

Trditev: Perioda je lahko največ $2^m - 1$.

Dokaz: 2^m je možnih kombinacij m bitov.
Odštejemo $000\dots0$.

Def.: karakteristični polinom LFSR je
$c(x) = \sum_{i=0}^{m} c_i x^i \quad c_0 = 1 \quad \in \mathbb{Z}_2[x].$

Red $c(x)$ je najmanjši t, za katerega velja $c(x) \mid (1 - x^t)$ (deli).

NTS: naredi histogram period LFSRja za vse ključe in dan polinom. lahko še dodaš dimenzijo polinom in dobiš 2D sliko.

Izrek: naj ima LFSR karpol $c(x)$, ki je nerazcepen. Potem ima LFSR periodo enako $c(x)$.

Posledica: če je $c(x)$ primitiven, je perioda $2^m - 1$.

Primeri PRG (šifer) z LFSR: stari: CSS šifra (DVD) glej deCSS haiku

A5/1 šifra (GSM)

4LFSR E0 šifra (bluetooth)

sodobne: salsa20

Opomba:

ne obstaja dokazano varen PRNG.

varen PRNG $\rightarrow$ $P \neq NP$

[semantična (računska) varnost kriptosistema]

izzivalec — napadalec

napadalec: izbere dve sporočili m_0, m_1

m_0, m_1 → izzivalec

$k \leftarrow K$

$b \leftarrow \{0,1\}$

$c = E_k(m_b)$

c → napadalec

napadalec: izbere bit 0/1 (ugiba bit b)

Def.: prednost

$$Adv(A,E) = \left| P(A \text{ vrne } 1 \mid b=1) - P(A \text{ vrne } 1 \mid b=0) \right|$$

Kriptosistem je semantično varen, če za $|K| = 2^\lambda$ je

$$Adv(A,E) < \varepsilon_A \leftarrow \text{zanemarljiva}$$

za vsakega polinomskega napadalca A.

Trditev:

če ima kriptosistem (E,D) lastnost popolne tajnosti, je $Adv(A,E) = 0$.