TKEPFMF2026-02-17 Meta: uvod: PDF slajdi

Ta predmet se navezuje na znanje
- Algebre: grupe, kolobarji, polja, evklidov algoritem, CRT
- Verjetnosti: končni verjetnostni prostori
- Algoritmov: nedeterministični (vsebujejo RAN#), O notacija

snov:

[šifriranje]

Def: kriptosistem/šifra je petorka $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

$\mathcal{B}$ je končna množica besedil
$\mathcal{C}$ je končna množica kriptogramov (ciphertext)
$\mathcal{K}$ je končna množica ključev
$\mathcal{E} = \{E_k ; E_k : \mathcal{B} \to \mathcal{C} ; \forall k \in \mathcal{K}\}$ so učinkovito polinomsko izračunljive šifrirne funkcije
$\mathcal{D} = \{D_k ; D_k : \mathcal{C} \to \mathcal{B} ; \forall k \in \mathcal{K}\}$ so učinkovito polinomsko izračunljive dešifrirne funkcije

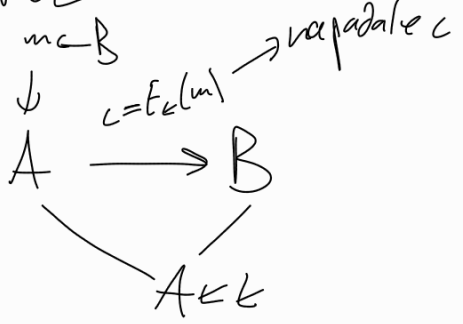
in veljati mora PRAVILNOST: $\forall k \in \mathcal{K} \exists k' \in \mathcal{K} \forall m \in \mathcal{B}: D_{k'}(E_k(m)) = m$

Opomba: sledi, da je $\mathcal{E}$ množica injektivnih funkcij $\Rightarrow |\mathcal{B}| \leq |\mathcal{C}|$

Opomba: ker so $\mathcal{B}, \mathcal{C}, \mathcal{K}$ implicitno v $\mathcal{E}$ in $\mathcal{D}$, običajno kriptosistem označimo kar s parom $(\mathcal{E}, \mathcal{D})$.

in veljati mora VARNOST:
- Kerckhoffovo načelo: kriptosistem naj bo varen, četudi napadalec pozna sistem (šifrirne in dešifrirne f-je.), ne pa uporabljenega ključa.
- kriptosistem je varen. Kaj to sploh pomeni? ni definirano.

POPOLNA TAJNOST



označimo z $X_{\mathcal{B}}$ slučajno spremenljivko izbire besedila.
označimo z $X_{\mathcal{C}}$ slučajno spremenljivko izbire kriptograma.

$P(X_{\mathcal{C}} = c) > 0 \quad \forall c \in \mathcal{C}$. LPT

Def: kriptosistem ima lastnost popolne tajnosti, če za vsaka $m \in \mathcal{B}$ in $c \in \mathcal{C}$ velja $P(X_{\mathcal{B}} = m \mid X_{\mathcal{C}} = c) = P(X_{\mathcal{B}} = m)$. ZPB

četudi vemo kriptogram, se verjetnosti o besedilu ne spremenijo, tj. nam to nič ne pove o besedilu.

Lema: LPT $\Leftrightarrow P(X_{\mathcal{C}} = c \mid X_{\mathcal{B}} = m) = P(X_{\mathcal{C}} = c)$ ZOB četudi vemo kaj bomo šifrirali, so verjetnosti za vse kriptograme enake.

Dokaz: $(\Rightarrow) P(X_{\mathcal{C}} = c \mid X_{\mathcal{B}} = m) \overset{\text{Bayes}}{=} \frac{P(X_{\mathcal{B}} = m \mid X_{\mathcal{C}} = c) \cdot P(X_{\mathcal{C}} = c)}{P(X_{\mathcal{B}} = m)} = P(X_{\mathcal{C}} = c)$ PREDPOSTAVKA

$(\Leftarrow)$ podobno (pet bayesa). □

Pripomba: $\forall m_1, m_2 \in \mathcal{B}$ in $c \in \mathcal{C}$ velja $P_{k \in \mathcal{K}}(E_k(m_1) = c) = P_{k \in \mathcal{K}}(E_k(m_2) = c)$

VERNAMOVA ŠIFRA (ONE-TIME PAD)

$B = C = K = \{0,1\}^\lambda \qquad \lambda \in \mathbb{N}$

$k \leftarrow \{0,1\}^\lambda$ enakovredno naključno izberemo

$E_k(m) = m \oplus k \qquad D_k(c) = c \oplus k$

Dokažimo: Pravilnost: $D_k(E_k(m)) = m \oplus k \oplus k = m \oplus 0 = m$ ✓

Popolna tajnost: Fiksirajmo m in c. $P(X_c = c \mid X_b = m) =$

$= \underset{k \leftarrow K}{P}(E_k(m) = c) = \underset{k \leftarrow K}{P}(m \oplus k = c) = \underset{k \leftarrow K}{P}(k = m \oplus c) = 2^{-\lambda}.$

to velja $\forall m, c$. $P(X_c = c) = 2^{-\lambda}$ (očitno) $\Rightarrow P(X_c = c) = P(X_c = c \mid X_b = m)$.

Izziv: Ključi so enako dolgi kot besedila.
Ključa istega ključa dvakrat izdaja $m_1 \oplus m_2$.

Trditev: Če ima kriptosistem CPT, potem $|B| \leq |C| \leq |K|$.

Dokaz: • $|B| \leq |C|$ vedno, ker E_k injektivna.

• izberimo poljubna $m \in B$. $c \in C$. Velja (po CPT):

$P(X_c = c \mid X_B = m) = P(X_c = c) > 0.$

$= \sum_{\substack{k \in K \\ E_k(m) = c}} P(X_k = k)$ → množica sprememljivk izbire ključa

$\Downarrow$

$\exists k \in K : P(X_k = k) > 0 \Rightarrow \exists k \in K : E_k(m) = c$

FIKSIRAJMO m, oglejmo si $f_m : K \to C$; $f_m : k \mapsto E_k(m)$ in f_m je surjektivna $\Rightarrow |C| \leq |K|$.

[fotovne šifre] Ideja: zamenjaj naključnost OTP ključem s pseudonaključnostjo.

Def: Generator pseudonaključnosti (pseudorandom generator / PRG) je preslikava $G : \{0,1\}^\lambda \to \{0,1\}^s$; $\lambda >> s$. G mora biti: deterministična, učinkovito izračunljiva. Želimo, da $G(k)$ izgleda naključno.

Če imamo dober PRG, λ-bitek ključ razteguemo z G in lahko z dobljenim s-dolgim ključem OTP-jamo s-dolga sporočila.

Varnost PRG definiramo tasnejše.