TKKPFMF 2026-04-07

odločitveni LWE

$A \leftarrow \mathbb{Z}_p^{m \times n}$ $\quad x \leftarrow \mathbb{Z}_p^n$ $\quad r \leftarrow \mathbb{Z}_p^m$ $\quad e \leftarrow \chi$ $\quad |e_i| < \delta_r p$

razlikuj $(A, Ax+e)$ in (A, r).

Predpostavka (nedotazana): za prav izbrane parametre ne obstaja polinomski napadalec, ki reši LWE.

LWE kriptosistem z javnim ključem:

$G(1^\lambda)$: $n = \lambda$, p praštevilo med n^2 in $2n^2$, $m = \lceil n \cdot \log(p) \rceil$,

$$\delta_r = \frac{1}{n \cdot (\log n)^2}.$$

$A \leftarrow \mathbb{Z}_p^{m \times n}$ $\quad x \leftarrow \mathbb{Z}_p^n$ $\quad e \leftarrow$ vektor šuma, da je $|e_i|_{\mathbb{Z}_p} \leq \delta_r \cdot p$

$y = Ax + e$. $\quad pubkey = (A, y)$

$seckey = x$

$E(pk, M)$: $\quad w \leftarrow \{0,1\}^m$ (št. vrstic v A)

$M \in \{0,1\}$

$c_0 = w^T A$

$c_1 = w^T y + M \cdot \lfloor \frac{p}{2} \rfloor$

$c = (c_0, c_1)$

$D(sk, c)$: $\quad M' = c_0^T x - c_1$.

če je $|M'|_{\mathbb{Z}_p} < \frac{p}{4}$ vrni $M = 0$

sicer $M = 1$.

PRAVILNOST:

$$M' = c_0^T x - c_1 = (w^T A)^T x - w^T (Ax + e) + M \cdot \lfloor \frac{p}{2} \rfloor \overset{\text{za } M=0}{=} w^T e + M \cdot \lfloor \frac{p}{2} \rfloor$$

$$\|w^T e\| \leq m \cdot \delta_r \cdot p = \frac{n \log(p) \cdot p}{n (\log p)^2} = \frac{p}{\log p} < \frac{p}{4} \text{ za dovolj velik } p$$

za $M = 1$ pa če $\lfloor \frac{p}{2} \rfloor$ večji kot približno $\frac{p}{4}$.

VARNOST: če velja LWE predpostavka za izbrane parametre, je kriptosistem CPA-varen.

Skica dokaza: CPA varen (chosen plaintext attack): napadalec ne more razlikovati med zašifriranima chosen plaintextoma — v tem primeru ne more razlikovati med $M=0/M=1$

napadalec vidi $y = Ax + e$, $c_0 = w^T A$, $c_1 = w^T y + M \lfloor \frac{p}{2} \rfloor$.

Podmena: napadalec zna ločiti $M=0$ in $M=1$. Napadalcu zamenjamo y z $r \in \mathbb{Z}_p^m$. Sedaj več ne more ločiti $M=0/M=1$, trdimo:

$c_1 = w^T r + M \cdot \lfloor \frac{p}{2} \rfloor$

enakom. natlj. — enakom. natlj. (ne bomo dokazali) — enakom. natlj.

torej napadalec zna ločiti med $(A, Ax+e)$ in (A, r), torej se ne sklada z LWE predpostavko ⨯.

opomba: namesto z matrikami lahko delamo s kolobarjem polinomov:

$a \in \mathbb{Z}_p[x] / f(x)$ $a \cdot x = e$ RLWE (ring)

[CELOVITOST PODATKOV]

kodi za overjanje (MAC - message authentication codes):

$A \leftarrow k \rightarrow B$ (deljen)

$\rightarrow$ | m | $MAC_k(m)$ | $\rightarrow$

$MAC_k(m) = SHA256(concat(m, k))$ (večino en primer)

Def.: Varen MAC: Imejmo družino f. $MAC = \{MAC_k : B \to \{0,1\}^\lambda ; k \in K\}$ in igro:

izzivalec — nasprotnik

$m_1, \dots, m_\ell$ (nasprotnik → izzivalec)

$k \leftarrow K$

$\forall i \in [\ell]: t_i := MAC_k(m_i)$

$t_1, \dots, t_\ell$ (izzivalec → nasprotnik)

VRNE PAR (m, t).

A je uspešen, če $(m, t) = (m, MAC_k(m))$ in $(m, t) \notin \{(m_i, t_i) ; i = 1, \dots, \ell\}$

Kod za overjanje je varen, če za vsakega polinomskega

napadalca A velja $Adv_{MAC}(A) := P(A \text{ uspešen}) \le \varepsilon(\lambda)$ ← zanemarljivo.

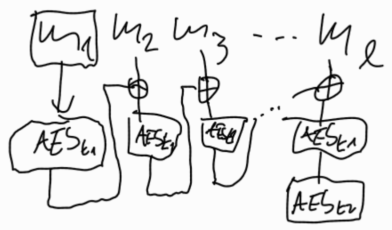
Izrek: vsaka varna PRF (pseudorandom function) $F = \{f_k : B \to \{0,1\}^\lambda\}$ je varen MAC.

(obratno očitno ne velja; rezultat MAC se lahko začne z 111111)

Konkretno: s pomočjo AES (CBC-MAC)

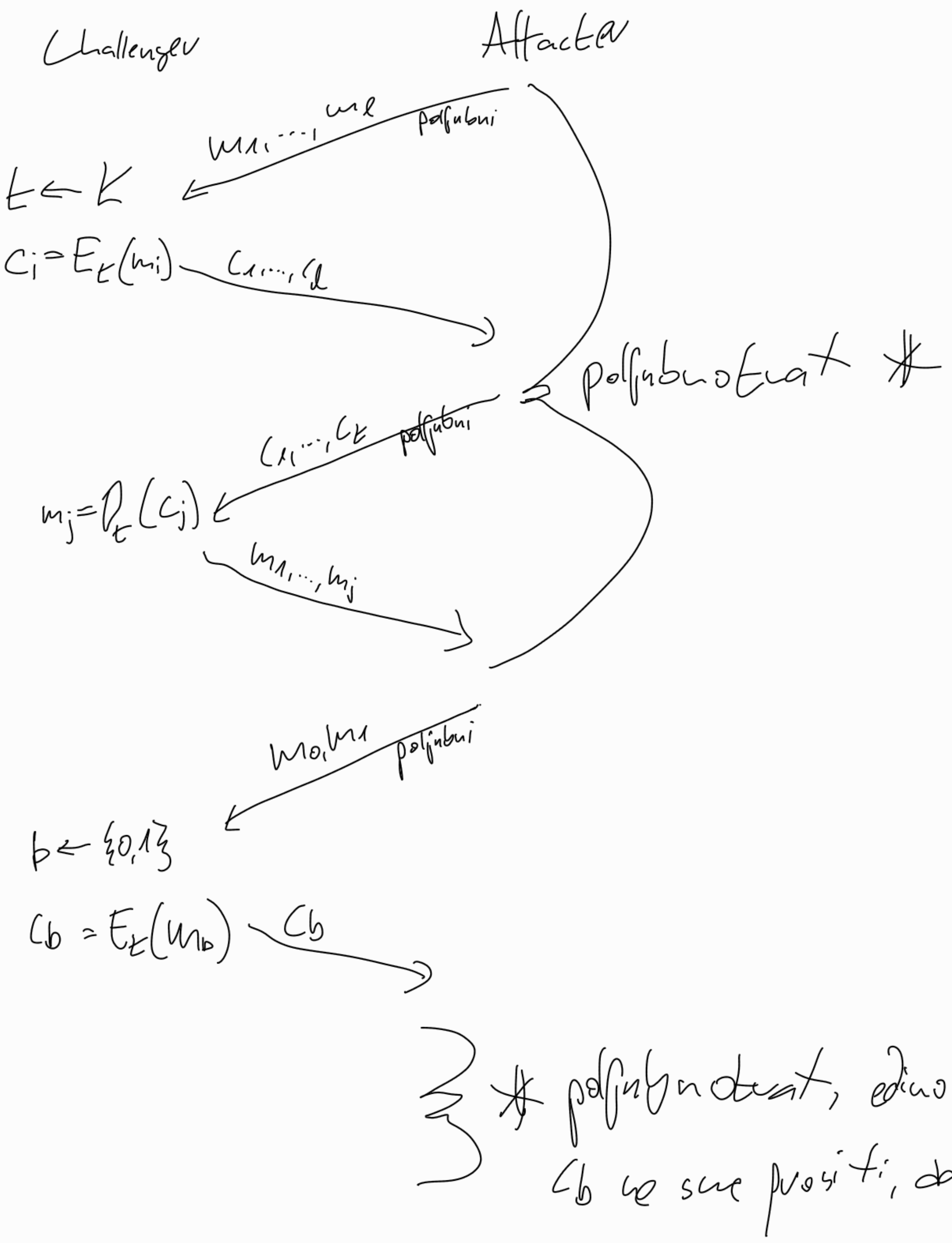
$k = (k_1, k_2)$ (2 ključa za AES).

f_k:



OVERJENO ŠIFRIRANJE:

Def: imejmo kriptosistem, $|K| = 2^\lambda$, in sledečo CCA igro (CCA):
(chosen cyphertext attack)



vrne 0/1

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

kriptosistem ______ je CCA varen, če je $Adv_{CCA}(A,E) \le \varepsilon_A(\lambda)$

za usat polinomsti A.

A JE ELGAMAL CCA varen?

ElGamal: $E(pk, m)$: $r \leftarrow \mathbb{Z}_q$

$c_0 = g^r$

$c_1 = m \cdot pk^r$

ni, $c_1' := 2 \cdot c_1$. $(c_0, c_1) \xrightarrow{\text{diffr.}} 2m \xrightarrow{:2} m$