Odpornost praslike:

Za dan $y \in Y$ je težko najti $x \in X$, da je $h(x) = y$.

Odpornost druge praslike:

Za dan $x \in X$ je težko najti $x' \in X$, $x \neq x'$, da je $h(x) = h(x')$.

Odpornost na trke:

Težko je najti x, x', $x \neq x'$, da je $h(x) = h(x')$.

---

1) Naj bo $f: \{0,1\}^n \to \{0,1\}^n$ bijektivna enosmerna funkcija in $h: \{0,1\}^{2n} \to \{0,1\}^n$ zgoščevalna funkcija, definirana kot:

   - $\forall x \in \{0,1\}^{2n}: \; x = x_1 \| x_2, \; x_1, x_2 \in \{0,1\}^n$
   - $h(x) = f(x_1 \oplus x_2)$

   Preverite trditve.

a) Ali ima h odpornost praslik?

b) Ali ima h odpornost drugih praslik?

c) Ali ima h odpornost na trke?

a) Za poljuben $x = x_1 \| x_2$ bi morali dobiti prasliko $z = x_1 \oplus x_2$,
$f(z) = f(x_1 \oplus x_2) = h(x) = y$. Potem f ne bi mogla biti enosmerna.

Torej ima odpornost praslik.

b) $x = x_1 \| x_2$

$h(x) = f(x_1 \oplus x_2) = y$

Iščemo $x \neq x'$: $h(x') = f(x_1' \oplus x_2') = y$

$x' := x_2 \| x_1$

$\Rightarrow h(x') = f(x_2' \oplus x_1') = f(x_1 \oplus x_2) = y$

$\Rightarrow$ Nima odpornosti drugih praslik

c) Nima odpornosti drugih praslik, torej tudi nima odpornosti na trke.

---

2) Predpostavimo, da je $h_1 : \{0,1\}^{2n} \to \{0,1\}^n$ odporna na trke.
Definirajmo funkcijo $h_2 : \{0,1\}^{4n} \to \{0,1\}^n$ kot:

- $\forall x \in \{0,1\}^{4n}$: $x = x_1 \| x_2$, $x_1, x_2 \in \{0,1\}^{2n}$
- $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$

Dokažite, da je h_2 odporna na trke.

Predpostavimo, da lahko najdemo x, x', $x \neq x'$, da je $h_2(x) = h_2(x')$.

$\Rightarrow h_1(h_1(x_1) \| h_1(x_2)) = h_1(h_1(x_1') \| h_1(x_2'))$

Če je $h_1(x_1) \| h_1(x_2) \neq h_1(x_1') \| h_1(x_2')$ smo našli tirke za h_1, kar je v protislovju s tem, da je h_1 odporna na tirke.

Torej $h_1(x_1) \| h_1(x_2) = h_1(x_1') \| h_1(x_2')$.

$$\Rightarrow \begin{aligned} h_1(x_1) &= h_1(x_1') \\ h_1(x_2) &= h_1(x_2') \end{aligned}$$

Ker $x \neq y$, je $x_1 \neq x_1'$ ali $x_2 \neq x_2'$, torej smo spet našli tirke za h_1, kar je spet protislovje.

Torej h_2 nima tirkov.

---

3) Naj bo p varno praštevilo ($p = 2 \cdot q + 1$, q praštevilo). Naj bo α generator grupe $\mathbb{Z}_p^*$ in b naključno izbran element grupe $\mathbb{Z}_p^*$. Zgoščevalno funkcijo $h: \mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow \mathbb{Z}_p^*$ definiramo kot:

$$h: (x_1, x_2) \longmapsto \alpha^{x_1} b^{x_2} \bmod p$$

a) Pokažite, da je h odporna na tirke, če predpostavimo, da je problem diskretnega logaritma v $\mathbb{Z}_p^*$ težek.

b) Za $p = 23$, $q = 11$, $\alpha = 5$, $b = 4$ iz tirka $((4,9),(6,3))$ izračunajte diskretni logaritem elementa 4 z osnovo 5.

a) Predpostavimo, da h ni odporna na tirke in pokažimo, da potem lahko računamo diskretne logaritme v $\mathbb{Z}_p^*$.

$$(x_1, x_2) \neq (y_1, y_2), \quad h(x_1, x_2) = h(y_1, y_2)$$

$$\alpha^{x_1} b^{x_2} = \alpha^{y_1} b^{y_2} \bmod p$$

$$\alpha^{x_1-y_1} = b^{y_2-x_2} \mod p$$

$$\alpha^{x_1-y_1} = \alpha^{(y_2-x_2)\ell} \mod p$$

$$x_1-y_1 = (y_2-x_2)\ell \mod p-1 = 2q$$

Preverimo obstoj $(y_2-x_2)^{-1}$ v $\mathbb{Z}_{2q}$:

$$\gcd(y_2-x_2, 2q) \stackrel{?}{=} 1$$

- Če je y_2-x_2 liho, je $\gcd(y_2-x_2, 2q) = 1$.

  $\Rightarrow \ell = (x_1-y_1)(y_2-x_2)^{-1} \mod 2q$

  $\Rightarrow \log_\alpha b = (x_1-y_1)(y_2-x_2)^{-1} \mod p$

- Če je y_2-x_2 sodo, je $\gcd(y_2-x_2, 2q) = 2$.

  $\Rightarrow \gcd(y_2-x_2, q) = 1$

  $\Rightarrow \exists k, k' : (y_2-x_2)k + qk' = 1$

  $k'' = -k'$

  $$\alpha^{(x_1-y_1)k} = b^{(y_2-x_2)k} = b^{1+qk''} = b \cdot b^{q \cdot k''} \mod p$$

  $$(b^{qk''})^2 = 1 \mod p$$

  $$\Rightarrow b^{qk''} = \begin{cases} 1 \\ -1 = \alpha^q \end{cases}$$

  Če je $b^{qk''} = 1$, je $\log_\alpha b = (x_1-y_1)k$.

Če je $b^{2k''} = -1$, je $\log_a b = (x_1 - y_1)k + q$.

To je v protislovju s tem, da je DL težek.

Torej je h odporna na trke.

b) Trk: $((4,9),(6,3))$

$a^4 b^9 = a^6 b^3$

$a^2 = b^6$

$\gcd(y_2 - x_2, 2q) = \gcd(6, 22) = 2$

$\Rightarrow \exists k, k' : 6k + 11k' = 1$

$k = 2, \; k' = -1$ ✓

Imamo 2 možnosti:

- $\log_5 4 = 2 \cdot 2 = 4$

  Preizkus: $5^4 = 4 \bmod 23$ ✓

- $\log_5 4 = 2 \cdot 2 + 11 = 15$

  Preizkus: $5^{15} \neq 4 \bmod 23$ //

---

4) Naj bo $n \geq 2$ naravno število. Zgoščevalno funkcijo $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ definiramo kot:

$h(x,y) = ax + by \mod n$

Poiščite trk za poljubna $a, b \in \mathbb{Z}$, ne oba 0.

Iščemo $(x_1, y_1) \neq (x_2, y_2)$, da $h(x_1, y_1) = h(x_2, y_2)$.

$ax_1 + by_1 = ax_2 + by_2 \mod n$

$a\underbrace{(x_1 - x_2)}_{b} = b\underbrace{(y_2 - y_1)}_{a} \mod n$

$x_2 := x_1 - b$
$y_2 := y_1 + a$

Trk: $((x_1, y_1), (x_1 - b, y_1 + a))$

---

5) Naj bo $n \geq 2$. Dana je zgoščevalna funkcija $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^n$. Zgoščevalno funkcijo $H_i : \mathbb{Z}_2^{2^i n} \to \mathbb{Z}_2^n$ definiramo kot:

- $H_1 = f$
- $H_i(x_1 \| x_2) = f(H_{i-1}(x_1) \| H_{i-1}(x_2))$

Pokažite, da če je f odporna na trke, so tudi H_i odporne na trke za $i \geq 1$.

DN