

Odpornost praslke:

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

Odpornosti druge praslke:

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

$$\bullet \forall x \in \{0,1\}^{2n}: x = x_1 \parallel x_2, \quad x_1, x_2 \in \{0,1\}^n$$

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

Preverite trditve.

a) Ali ima h odpornosti praslke?

b) Ali ima h odpornosti drugih praslke?

c) Ali ima h odpornost na trke?

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

Torej ima odpornost preslik.

b) $x = x_1 \parallel x_2$

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

$$\text{Iščemo } x \neq x' : h(x') = f(x'_1 \oplus x'_2) = y$$

$$x' = x_2 \parallel x_1$$

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

\Rightarrow Nima odpornosti drugih preslik

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

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

$$\bullet \forall x \in \{0,1\}^{4n}: x = x_1 \parallel x_2, x_1, x_2 \in \{0,1\}^{2n}$$

$$\bullet h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2))$$

Dokažite, da je h_2 odporna na trke.

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

$$\Rightarrow h_1(h_1(x_1) \parallel h_1(x_2)) = h_1(h_1(x'_1) \parallel h_1(x'_2))$$

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

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

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

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

Torej h_2 nima trkov.

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

$$h: (x_1, x_2) \mapsto \alpha^{x_1} b^{x_2} \pmod{p}$$

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

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

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

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

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

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

$$\alpha^{x_1 - y_1} = \alpha^{(y_2 - x_2)l} \pmod{p}$$

$$x_1 - y_1 = (y_2 - x_2)l \pmod{p-1 = 2g}$$

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

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

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

$$\Rightarrow l = (x_1 - y_1)(y_2 - x_2)^{-1} \pmod{2g}$$

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

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

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

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

$$k'' = -k'$$

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

$$(b^{gk''})^2 = 1 \pmod{p}$$

$$\Rightarrow b^{gk''} = \begin{cases} 1 \\ -1 = \alpha^g \end{cases}$$

Če je $b^{gk''} = 1$, 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 tezek.

Torej je h odporna na trke.

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

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

$$a^2 = b^6$$

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

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

$$k = 2, k' = -1 \quad \checkmark$$

Imamo 2 možnosti:

$$\bullet \log_5 4 = 2 \cdot 2 = 4$$

$$\text{Preizkus: } 5^4 = 4 \pmod{23} \quad \checkmark$$

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

$$\text{Preizkus: } 5^{15} \neq 4 \pmod{23} \quad //$$

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

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

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

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

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

$$a \underbrace{(x_1 - x_2)}_b = b \underbrace{(y_2 - y_1)}_a \pmod n$$

$$x_2 := x_1 - b$$

$$y_2 := y_1 + a$$

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

5) Naj bo $n \geq 2$. Dana je zgosčevalna funkcija $f: \mathbb{Z}_2^{2n} \rightarrow \mathbb{Z}_2^n$.
Zgosčevalno funkcijo $H_i: \mathbb{Z}_2^{2in} \rightarrow \mathbb{Z}_2^n$ 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