21. 12. 2017

Zero knowledge

Alice chce dokázat Bobovi, že $x \in L$ tak, aby Bob uvěřil, ale nebyl schopen důkaz replikovat. Zero knowledge má mnoho aplikací v kryptografii.
Příklady:

Alice má číslo $N = pq$ a chce dokázat Bobovi, že N je složené. Navíc Bob se z důkazu nesmí dozvědět žádnou další informaci. Tedy chce to udělat tak aby nakonec Bob neznal p ani q.
Kde je Waldo (Wally)? Kde je Waldo (Wally)? Úkolem je najít na velkém obrázku přeplněném postavičkami najít Wallyho (konkrétní postavička). Představte si, že chcete přesvědčit kamaráda, že na obrázku Waldo skutečně je, ale nechat jej ho najít. Uděláme to tak, že položíme obrázek na stůl a překryjeme jej dostatečně velkým papírem s okénkem, ve kterém je vidět pouze Waldo. Kamarád může v okénku najít Walda. Tím bychom jej ale nepřesvědčili – mohli jsme podstrčit jiný obrázek. Proto okénko zakryjeme a povolíme udělat právě jednu z těchto dvou akcí

1. odkrýt okénko – najít Walda a přesvědčit se, že na obrázku je.
2. odkrýt celý obrázek – přesvědčit se, že není podstrčen jiný obrázek

Kamarád se nechá přesvědčit pokud při náhodně zvolené akci dostane správnou odpověď (na obrázku je Waldo nebo na stole je obrázek). Pokud na vybraném obrázku Waldo není může být kamarád podveden s pravděpodobností 1/2 (musel si špatně zvolit akci). Pokud Waldo na obrázku je bude kamarád přesvědčen vždy.

Interaktivní protokoly

Alice a Bob jsou interaktivní Turingovy stroje se společnám vstupem x , které sdílejí komunikační pásku. Interakce probíhá v kolech.

Exekuce těchto Turingových strojů je dvojice

$$(V_A, V_B) = ((x, z_1, r_1, M_a), (x, z_2, r_2, M_B)),$$

kde x je společný vstup, z_1 (resp. z_2) případný soukromý vstup Alice (Boba), r_1, r_2 náhodné řetězce a M_A zprávy od Boba (podobně M_B zprávy od Alice). Tedy

$$M_A = \{m_A^1, m_A^2, \dots\},\ M_B = \{m_B^1, m_B^2, \dots\}$$

$$m_A^i, m_B^i,\ x, r_i, z_i \in \{0,1\}^*.$$

Interakci mezi Turingovými stroji (A, B) je náhodná proměnná, kterou značíme $A_{r_1}(x, z_1) \leftrightarrow B_{r_2}(x, z_2)$, kde $r_1, r_2 \leftarrow \{0,1\}^k$.

$V_A = (x, z_1, r_1, M_A)$ je view A, podobně $V_B = (x, z_2, r_2, M_B)$ je view B. Dále $out_x(e)$, kde $x \in \{A, B\}$, značí výstup stroje x a m_A^i je i-tá zpráva od Boba.

Interactive proof

Dvojice interaktivních Turingových strojů P a V je interaktivní důkaz pro jazyk L, pokud V je PPT a platí:

1. **Completeness:** $\forall x \in L\ \exists y \in \{0,1\}^*$ t.ž. $\forall z \in \{0,1\}^*$:

$$\Pr[\text{out}_V[P(x, y) \leftrightarrow V(x, z)] = 1] = 1\ ^1$$

[1]Poznamenejme, že můžeme požadovat pouze, že pravděpodobnost přijetí je alespoň c .

2. **Soundness:** $\exists$ negligible ε t.ž. $\forall x \notin L,\ \forall$ Turingovy stroje P^* a $\forall z \in \{0,1\}^*$:

$$\Pr[\text{out}_V[P^*(x) \leftrightarrow V(x,z)] = 1] \leq \varepsilon(n),$$ [2][3]

kde $|x| = n$.

Definujeme IP jako třídu jazyků, které mají interaktivní důkaz.
Pozorování: NP$\subseteq$IP.
Věta (Shamir): IP=PSPACE

Interaktivní důkaz pro neizomorfismus grafů

Vstupem jsou dva grafy $G_0 = (V_0, E_0), G_1 = (V_1, E_1)$ (oba na n vrcholech), chceme rozhodnout, jestli jsou izomorfní (tj. $\exists \sigma \in S_n$ t.ž. $(u,v) \in E_0 \leftrightarrow (\sigma(u), \sigma(v)) \in E_1$ a značíme $\sigma(G_0) = G_1$).

Izomorfismus grafů budeme značit $L_{\text{ISO}} \in$ NP a neizomorfismus grafů $L_{\text{NISO}} \in$ coNP.

Protokol pro L_{NISO}

Společný vstup je $X = (G_0, G_1)$

1. Verifier $V(X)$ zvolí náhodně bit b a permutaci σ.
2. Pošle proverovi $H = \sigma(G_b)$.
3. Prover najde b' t.ž. $H \sim G_{b'}$.
4. Pošle b' verifierovi.
5. Verifier vrátí 1, pokud $b = b'$

Celý postup opakuj n-krát.

Tvrzení: (P, V) je interaktivní důkaz pro L_{NISO}.
Důkaz: Completeness: $x \in L_{\text{NISO}} \Rightarrow$ Prover P spočítá, který z grafů mu byl poslán (poznamenejme, že P je unbounded) a tedy vždy určí $b' = b$.
Soundness: $x \in L_{\text{ISO}} \Rightarrow$ Prover není schopen určit jestli dostal G_0 nebo G_1 a tedy pravděpodobnost úspěchu při jednom opakování je právě $\frac{1}{2}$. Při n opakování dostaneme pravděpodobnost úspěchu nejvýš $\frac{1}{2}^n$. □

Zero cash, měny s anonymitou, existují prakticky použitelné implementace pro kryptografické problémy a pro přirozené jazyky v NP.

Efektivní interaktivní důkaz pro grafový isomorfismus

Společný vstup $X = (G_0, G_1)$ takové, že $|V_0| = |V_1| = n$, svědkem pro P je σ t.ž. $\sigma(G_1) = G_0$.

1. Prover zvolí $\pi \leftarrow S_n$ a pošle verifierovi graf $H = \pi(G_0)$.
2. Verifier zvolí bit b a pošle jej proverovi
3. Pokud $b = 0$, prover pošle π, jinak pošle $\pi' = \pi \circ \sigma$ (tedy $H = \pi'(G_1)$)
4. Verifier ověří, že dostal správnou permutaci.

[2] P^* nemá vstup y, protože prover ji v sobě může mít zadrátovánu.
[3] Poznamenejme, že můžeme požadovat, že pravděpodobnost přijetí je nejvýše nějaké s

Opakujeme n-krát.

Tvrzení: (P, V) je interaktivní důkaz pro L_{ISO}.
Důkaz: Completeness: Jsou-li grafy izomorfní, prover umí pro oba případy odpovědět.

Soundness: Nejsou-li izomorfní, v jednom pokusu umí prover odpovědět nejvýše s pravděpodobností $1/2$, neboť H může být isomorfní jen jednomu grafu. □

Poznamenejme, že verifier se nedozvěděl σ. Tedy protokol bude i zero-knowledge. Viz důkaz dále.

Definice: (Honest verifier zero knowledge)

Nechť P_V je interaktivní důkaz pro jazyk $L \in NP$ se svědeckou relací R_L.

Řekneme, že (P, V) je *Honest verifier zero knowledge*, pokud existuje PPT simulátor takový, že pro každého PPT distinguishera D existuje negligible ε takové, že $\forall x \in L, y \in R_L(x)$ a $z \in \{0,1\}^*$: D rozliší následující distribuce s pravděpodobností nejvýše $\varepsilon(|x|)$

$$\{\text{view}_V[P(x,y) \leftrightarrow V(x,z)]\} \text{ vs. } \{S(x,z)\}.$$

Definice: (Zero knowledge)

$\forall$ PPT V^* existuje expected PPT[4] simulátor S takový, že pro každého PPT distinguishera D existuje negligible ε takové, že $\forall x \in L, y \in R_L(x)$ a $z \in \{0,1\}^*$: D rozliší následující distribuce s pravděpodobností nejvýše $\varepsilon(|x|)$

$$\{\text{view}_{V^*}[P(x,y) \leftrightarrow V^*(x,z)]\} \text{ vs. } \{S(x,z)\}.$$

Tvrzení: (P, V) je zero knowledge interaktivní důkaz pro L_{ISO}
Důkaz: Potřebujeme sestrojit simulátor $S(x, z)$ pro každého verifiera V^*, pro jednu iteraci protokolu bude dělat následující:

1. Vyber bit $b' \leftarrow \{0,1\}$ a permutaci $\pi \leftarrow S_n$ nechť $H = \pi(G_b)$.
2. Emuluj V_r^* na vstupu x, z s náhodnými bity $r \leftarrow \{0,1\}^k$ se zprávou H od Provera.
   Z emulace dostaneme $b = V_r^*(x, z, H)$.
3. Pokud $b = b'$, vrať $\text{view}_{V^*}(x, z, r, H, b, \pi)$, jinak se vrať na začátek a postup opakuj.

Potřebujeme ukázat: a) S pracuje v očekávaném polynomiálním čase.
b) Distribuce ze simulátoru S a view verifiera V^* jsou nerozlišitelné.
Add b) Nejprve dokážeme pomocné lemma:

Lemma: Při exekuci $S(x, z)$ má H stejnou distribuci jako $\pi(G_0)$ a $\Pr[b' = b] = \frac{1}{2}$

Pokud G_0, G_1 jsou izomorfní, pak $\{\pi(G_0\}$ a $\{\pi(G_1)\}$ jsou stejné distribuce $\Rightarrow$ Distribuce $H, \pi(G_0)$ jsou stejné.

Distribuce H, b' jsou nezávislé (protože G_0, G_1 jsou isomorfní) $\Rightarrow V^*$ má na vstupu pouze H, to nezávisí na b' a navíc b' je rovnoměrně rozdělené, tedy $\Pr[b' = b] = \frac{1}{2}$. Tedy distribuce H nezávisí na b', stejně tak distribuce π nezávisí na b' a tedy jsou distribuce H a $\pi(G_0)$ stejné.

Add a) Protože očekávaný počet iterací algoritmu, než vrátí view jsou 2 (v každé iteraci má pravděpodobnost $\frac{1}{2}$ na skončení dle lemmatu) a jednotlivé iterace jsou v polynomiálním čase.

[4] očekávaný polynomiální čas