21. 12. 2017

Zero knowledge

Co když Alice nevěří Bobovi?
Alice chce dokázat Bobovi, že $x \in L$ tak, aby Bob uvěřil, ale nebyl schopen důkaz replikovat.
Alice má $N = pq$ a chce dokázat, že je složené, tak, aby Bob nevěděl p a q (crypto aplikace)
Kde je Waldo (Wally)?

Položíme knížku na stůl a překryjeme dostatečně velkým papírem s okénkem. Buď v okénku najdeme Wallyho, nebo pod papírem knížku, ale nemáme informaci o tom, kde se Wally na stránce nachází.

Interaktivní protokoly

Alice, Bob, interaktivní TS
mají společný vstup x a sdílejí komunikační pásky
interakce probíhá po kolech
Exekuce je dvojice

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

kde x je vstup, z anxiliary input, r mince a M_A zprávy od Boba (podobně M_B). Platí:

$$M_a = \{m_A^1, m_A^2, \dots\},\ M_B = \{m_B^1, m_B^2, \dots\},\ x, r_i, z_i \in \{0,1\}^*.$$

Interakci mezi $\mathrm{TM}(A, B)$ značíme $A(r_1, z_1) \leftrightarrow B(r_2, z_2)$ a mějme odpovídající náhodné proměnné (pokud $r_1, r_2 \in \{0,1\}^k$): V_A je view A, podobně V_B je view B, $\mathrm{out}_x(e),\ x \in \{A, B\}$ výstup příslušného stroje a m_A^i je $i$tá zpráva od Boba

Interactive proof

P prover, V verifier
Dvojice interaktivních TS A a B je interaktivní důkaz pro jazyk L, pokud V je PPT a platí:

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

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

2. **Soundness** $\dots \exists \mathrm{reg!}\, z$ t.ž. $\forall x \notin L,\ \forall \mathrm{PPT}\ P^*$ a $\forall z \in \{0,1\}^*$ $(|x| = n)$:

$$\Pr[\mathrm{out}_V[P^*(x) \leftrightarrow V(x,z)] = 1] \leq \epsilon(n)$$

(Tady může mít prover informaci y v sobě zakódovanou)

Buď IP třída jazyků, které mají interaktivní důkaz ($\mathrm{NP} \subseteq \mathrm{IP}$)
Shamir: IP=PSPACE

Interaktivní důkaz pro neizomorfismus grafů

$G_0 = (V_0, E_0), G_1 = (V_1, E_1)$ (oba na n vrcholech), definuji izomorfismus $\exists \sigma \in S_n$ t.ž. $\sigma(G_0) = G_1$.
Izomorfismus grafů $L_{\mathrm{ISO}} \subset \mathrm{NP}$, neizomorfismus grafů $L_{\mathrm{NISO}} \subset \mathrm{coNP}$.

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 $b = b'$

Opakuj $n$krát.

Tvrzení: (P, V) je interaktivní důkaz pro L_{NISO}.
Důkaz: Completeness: $x \in L_{\text{NISO}} \Rightarrow P$ vždy najde $b' = b$
Soundness: $x \in L_{\text{ISO}} \Rightarrow$ pst. úspěchu v jednom pokusu je právě $1/2$ □

Najít si: zero cash, měny s anonymitou, prakticky použitelné aplikace pro kryptografické problémy

Pro přirozené jazyky v NP program dává nějakou hodnotu na vstupu

Exektivní interaktivní důkaz pro G.ISOMORFISMUS

Společný vstup $X = (G_0, G_1)$, $|V_0| = |V_1|$
svědkem pro P je σ t.ž. $\sigma(G_1) = G_0$.
Prover zvolí $\pi \leftarrow S_n$, $H = \pi(G_0)$ a pošle V graf H.
V zvolí bit b a pošle proverovi
Pokud $b = 0$, P pošle π, jinak pošle $\pi' = \pi \circ \sigma$ (tedy $H = \pi'(G_1)$)
Verifier ověří, že dostal správný izomorfismus.
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 nejvýš s pravděpodobností $1/2$, neboť H může být izomorfní jen jednomu grafu.
Zero knowledge: V se z protokolu nedozví vůbec nic. □

Definice: (Honest verifier zero knowledge)
Nechť P_V je interaktivní důkaz pro jazyk $L \in NP$ se svědeckou relací R_L. Bere svědecké relace a vrací 0 nebo 1.

Řekneme, že (P, V) je Honest verifier zero knowledge, pokud existuje PPT simulátor t.ž. $\forall$ PPT distinguishery D $\exists$ negligible $\varepsilon : \forall x \in L, y \in R_L(x)$ a $z \in \{0,1\}^*$ D rozliší následující distribuce s pravděpodobností nejvýše $\varepsilon(|x|)$:
$\{\text{view}_V[P(x,y) \leftrightarrow V(x,z)]\}$ vs. $\{S(x,z)\}$

Definice: (Zero knowledge)
$\forall$PPT P^* $\exists$ expected PPT (očekávaný polynomiální čas) simulátor

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

Tvrzení: (P, V) je zero knowledge důkaz pro L_{ISO}
Důkaz: simulátor $S(x,z)$ $\forall V^*$ pro jednu iteraci

1. vyber bit b', π in S_n: $H = \pi(G_b)$
2. emuluj V_r^* se vstupem x, z pro $r \leftarrow \{0,1\}^k$ na vstupu H pro k
   dostaneme $b = V_r^*(x, z, H)$
3. pokud $b = b'$, vrať $\text{view}_{V^*}(x, z, r, H, b, \pi)$, jinak se vrať do 2. a opakuj

a) S pracuje v očekávaném poly čase, distribuce jsou stejné
b) při exekuci $S(x,z)$ má H stejnou distribuci jako $\pi(G_0)$ a $\Pr[b' = b] = \frac{1}{2}$
když g_0, G_1 jsou izomorfní, pak $\{\pi(G_0\}$ a $\{\pi(G_1)\}$ jsou stejné $\Rightarrow$ distribuce $H, \pi(G_0)$ jsou stejné.
distribuce H, b' jsou nezávislé $\Rightarrow$ V^* má na vstupu pouze H, které nezávisí na b', protože b' je rovnoměrně rozdělené
a) z lemmatu, protože očekávaný počet iterací jsou 2 a jednotlivé iterace jsou PPT
b) H nezávisí na b', π nezávisí na $b' \Rightarrow$ distribuce π se nezmění