Základy složitosti a vyčíslitelnosti

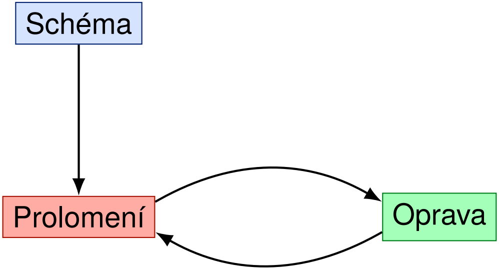
NTIN090

Petr Kučera

2021/22 (12. přednáška)

Kryptografie a složitost

Historický přístup k návrhu bezpečných systémů



Moderní kryptografie

> Věda vítězí v každém případě
>
> *Silvio Micali*

Bezpečnost založená na výpočetně obtížných problémech

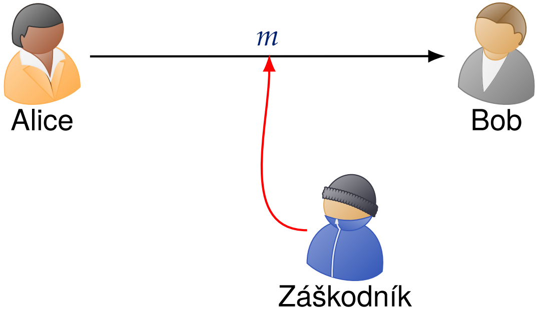
Máme bezpečný systém

nebo

máme lepší algoritmus pro obtížný problém

Bezpečná komunikace (symetrické šifrování)

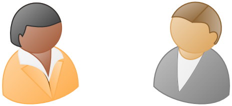
Alice chce Bobovi poslat tajnou zprávu $m \in \{0,1\}^n$



Perfektní schéma jednorázové tabulky

Alice se setká s Bobem na utajeném místě

Ahoj Alice, použij prosím tento klíč k zašifrování zprávy pro mne
$r = 01001101$

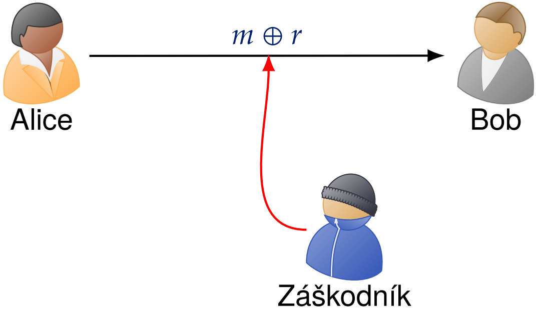


Alice Bob

Bob předá Alici náhodný klíč
$r \in \{0, 1\}^n$

Perfektní schéma jednorázové tabulky

Alice pošle zašifrovaný text $m \oplus r$



Záškodník nemůže rozlišit $m \oplus r$ od náhodného řetězce

Perfektní schéma jednorázové tabulky

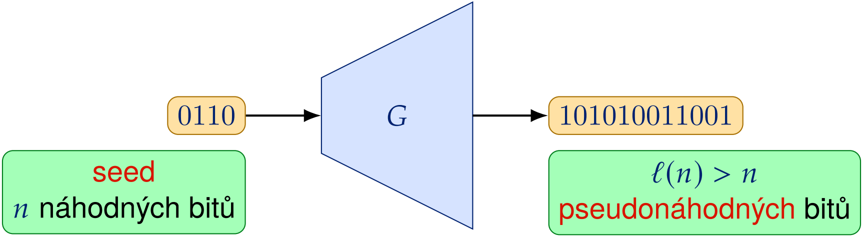
- $m \oplus r$ má stejné rozdělení jako r
- Záškodník nemůže zprávu přečíst
- Toto schéma je neprolomitelné (Claude Shannon, 1940s)
- Vernamova šifra
- Použito v 2. světové válce, studené válce, …

Nevýhody

- Klíč r lze použít jen jednou
- Klíč r má délku shodnou s délkou zprávy
- Klíč r musí být bezpečně předán od příjemce odesílateli

Záškodník s omezenou výpočetní silou

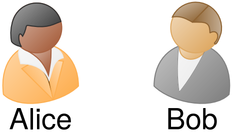
- Efektivní zabezpečená schémata založená na předpokladu omezené výpočetní síly záškodníka (80-tá léta)
- Více než jen symetrické šifrování
  - digitální podpis
  - šifrování s veřejným klíčem (RSA)
- Založeno na pseudonáhodných generátorech (PRG)



Efektivní symetrické šifrování s PRG

Alice se setká s Bobem na utajeném místě

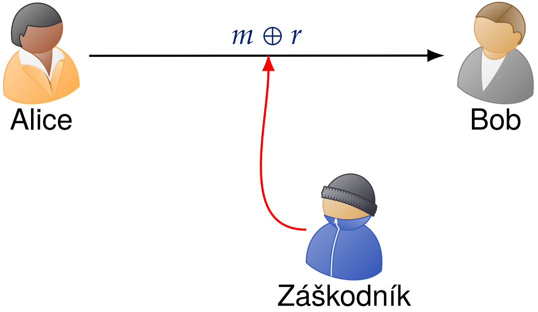
Ahoj Alice, použij prosím tento seed k vygenerování klíče pro PRG G:
$s = 01001101$



Bob předá Alici náhodný řetězec (seed) $s \in \{0, 1\}^n$

Efektivní symetrické šifrování s PRG

Alice použije PRG G k získání klíče $r = G(s)$



Záškodník s omezenou výpočetní silou nemůže rozlišit $m \oplus r$ od náhodného řetězce

Pseudonáhodný generátor

$$G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$$

je pseudonáhodný generátor, pokud

- G je vyčíslitelná deterministickým polynomiálním algoritmem
- $\ell(n) > n$ pro každé $n \in \mathbb{N}$ (stretch)
- Pro každý pravděpodobnostní polynomiální algoritmus $\mathcal{A}$ platí, že

$$\left| \Pr_{y \in \{0,1\}^{\ell(n)}} [\mathcal{A}(y) = 1] - \Pr_{y \in \{0,1\}^{n}} [\mathcal{A}(G(y)) = 1] \right| \leq \varepsilon(n)$$

  pro nějakou zanedbatelnou funkci $\varepsilon(n)$
- $\varepsilon(n)$ je zanedbatelná pokud pro každé $k \in \mathbb{N}$ existuje konstanta n_k taková, že pro každé $n > n_k$ platí $\varepsilon(n) < 1/n^k$
  - například 2^{-n}, $n^{-\log_2 n}$

Žádný PRG, pokud $\mathrm{P} = \mathrm{NP}$

Pokud $\mathrm{P} = \mathrm{NP}$, pak neexistuje žádný PRG

- Předpokládejme (sporem), že existuje PRG G
- Definujme obraz G jako

$$I_G = \{y \in \{0,1\}^{\ell(n)} \mid (\exists s \in \{0,1\}^n)[G(s) = y]\}$$

- I_G patří do $\mathrm{NP} = \mathrm{P}$
- Uvažme polynomiální algoritmus $\mathcal{A}$, pro který platí

$$\mathcal{A}(y) = 1 \iff y \in I_G$$

Žádný PRG, pokud $\mathrm{P} = \mathrm{NP}$

$$\left| \Pr_{y \in \{0,1\}^{\ell(n)}} [\mathcal{A}(y) = 1] - \Pr_{y \in \{0,1\}^n} [\mathcal{A}(G(y)) = 1] \right|$$

$$= \left| 2^{n-\ell(n)} - 1 \right| = 1 - 2^{n-\ell(n)} \geq 1 - \frac{1}{2} = \frac{1}{2}$$

- není zanedbatelná funkce
- Dostáváme spor s tím, že G je PRG

Co když $\mathrm{P} \neq \mathrm{NP}$?

- $\mathrm{P} \neq \mathrm{NP}$ ještě neznamená, že existují PRG
- Třídy P a NP jsou definované pomocí složitosti v nejhorším případě
  - V každém rozdělení instancí existují nějaké těžké instance
  - SAT může být těžký v nejhorším případě, ale heuristické SAT řešiče mohou i tak pracovat dobře v průměru
  - Bezpečnost pro nějaké zprávy
- Pro konstrukci PRG potřebujeme problém, který je těžký v průměrném případě
  - Vysoká složitost v průměrném případě
  - Obraz I_G pseudonáhodného generátoru G musí být těžký v průměrném případě
  - Bezpečnost pro většinu zpráv

Jednosměrné funkce

$$f\colon \{0,1\}^* \to \{0,1\}^*$$

je jednosměrná funkce (OWF), pokud je

snadno vyčíslitelná vyčíslitelná v polynomiálním čase

těžko invertovatelná pro každého záškodníka $\mathcal{A}$, který pracuje v pravděpodobnostním polynomiálním čase existuje zanedbatelná funkce $\varepsilon(n)$ taková, že pro každé $n \in \mathbb{N}$

$$\Pr_{x\in\{0,1\}^n}[\mathcal{A}(f(x)) \in f^{-1}(f(x))] \le \varepsilon(n)$$

Jednosměrné funkce a PRG

PRG existují, právě když existují OWF.

- PRG G implikuje existenci jednosměrné funkce
- Jednosměrnou funkci lze použít ke konstrukci pseudonáhodného generátoru
  - Hastad, Impagliazzo, Levin, and Luby, 1999

Existují jednosměrné funkce?

Záleží to na tom, ve kterém světě žijeme…

Pět světů Russela Impagliazza

Algorithmica

- $\mathrm{P} = \mathrm{NP}$
- NP je snadná v průměrném případě

- 🙂 Umíme řešit SAT v polynomiálním čase
- 🙂 Perfektní plánování, rozvrhování, strojové učení, optimalizace, …
- ☹ Žádné pseudonáhodné generátory ani jednosměrné funkce
- ☹ Žádné symetrické šifrování
- ☹ Žádný digitální podpis
- ☹ Žádné šifrování s veřejným klíčem

Heuristica

Heuristica

- $\mathrm{P} \neq \mathrm{NP}$
- NP je snadná v průměrném případě

- Heuristické SAT řešiče jsou velmi efektivní
- Téměř perfektní plánování, rozvrhování, strojové učení, optimalizace, …
- Žádné pseudonáhodné generátory ani jednosměrné funkce
- Žádné symetrické šifrování
- Žádný digitální podpis
- Žádné šifrování s veřejným klíčem

Pessiland

Pessiland

- $\mathrm{P} \neq \mathrm{NP}$
- NP je těžká v průměrném případě
- Žádné jednosměrné funkce

- Nejhorší ze všech světů
- Žádné dobré SAT řešiče
- Mnoho těžkých problémů
- Žádné pseudonáhodné generátory, žádná tajemství

Minicrypt

Minicrypt

- $\mathrm{P} \neq \mathrm{NP}$
- NP je těžká v průměrném případě
- Existují jednosměrné funkce
- Žádné šifrování s veřejným klíčem

- Pseudonáhodné generátory
- Symetrické šifrování
- Digitální podpis
- Žádné šifrování s veřejným klíčem

Cryptomania

Cryptomania

- $\mathrm{P} \neq \mathrm{NP}$
- NP je těžká v průměrném případě
- Existují jednosměrné funkce
- Šifrování s veřejným klíčem

- 🙂 Pseudonáhodné generátory
- 🙂 Symetrické šifrování
- 🙂 Digitální podpis
- 🙂 Šifrování s veřejným klíčem
- 🙂 Distribuovaná výměna klíčů

Kandidáti na jednosměrné funkce

Faktorizace celých čísel

$$f(p, q) = p \cdot q$$

- Předpokládá se, že f je v průměru těžké invertovat, pokud p a q jsou n-bitová prvočísla vybraná uniformně náhodně
  - $f(p, q)$ má $2n$ bitů
- Test prvočíselnosti lze provést v polynomiálním čase
- Souvisí s problémem RSA
- Umožňuje šifrování s veřejným klíčem, distribuovanou výměnu klíčů

Součet podmnožiny

$$f_{\text{ss}}(x_1, \ldots, x_n, J) = (x_1, \ldots, x_n, y = \sum_{j \in J} x_j \mod 2^n)$$

- $x_1, \ldots, x_n \in \{0, 1\}^n$
- $J \subseteq \{1, \ldots, n\}$
- Předpokládá se, že je v průměru těžké f_{ss} invertovat, pokud $x_1, \ldots, x_n, J$ jsou vybrány uniformně náhodně
- Souvisí s NP-problémem Součet podmnožiny

Součet podmnožiny (Subset Sum)

Instance: $x_1, \ldots, x_n, y \in \mathbb{N}$

Otázka: Platí $y = \sum_{j \in J} x_j$ pro nějakou množinu $J \subseteq \{1, \ldots, n\}$?

Diskrétní logaritmus

$$f_{g,p}(x) = g^x \mod p$$

- p je n-bitové prvočíslo
- g je generátor multiplikativní grupy $\mathbb{Z}_p^*$
- Předpokládá se, že $f_{g,p}$ je v průměru těžké invertovat pro vhodně zvolené grupy
- Umožňuje šifrování s veřejným klíčem, distribuovanou výměnu klíčů

Goldreichův kandidát na jednosměrnou funkci

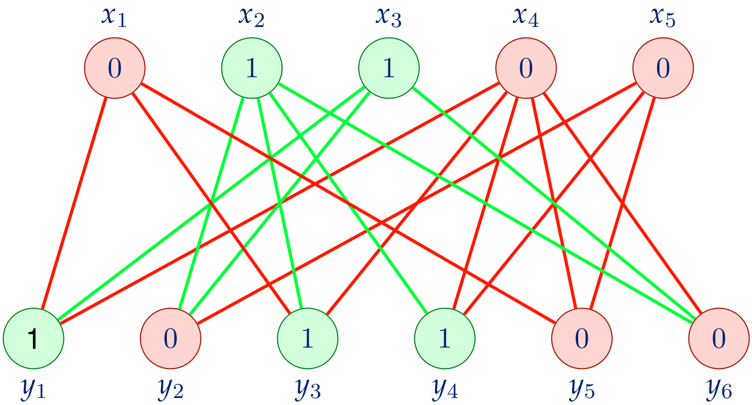
- Vstupní bity $x_1, \ldots, x_n$
- Výstupní bity $y_1, \ldots, y_m$
- Zvolíme náhodný bipartitní graf $G = (V, E)$ s partitami $\{x_1, \ldots, x_n\}$ a $\{y_1, \ldots, y_m\}$, kde y_i má stupeň d pro $i = 1, \ldots, m$
- Vybereme náhodný predikát $P : \{0, 1\}^d \to \{0, 1\}$
- $y_j = P(x_i \mid \{x_i, y_j\} \in E)$
- Definujeme funkci

$$f_{G,P}(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$$

- Předpokládá se, že s vhodnou volbou parametrů je v průměru těžké tuto funkci invertovat

Goldreichův kandidát na OWF (příklad)

$d = 3$ $\quad$ $P(a, b, c) = a \oplus b \oplus c$



$f(01101) = 101100$

Bitový závazek
a
zvětšení stretch

Bitový závazek (Bit Commitment)

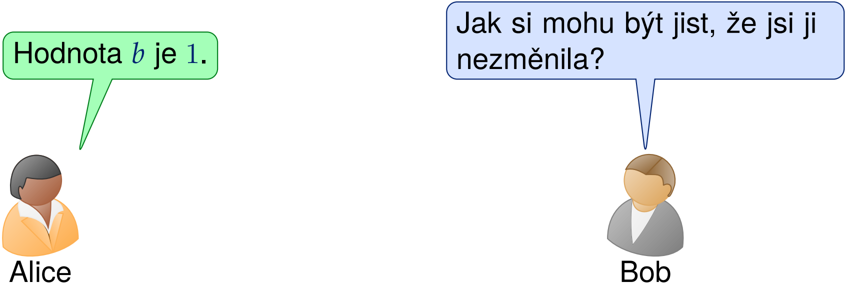
Fáze závazku

Alice se zaváže k bitu $b \in \{0, 1\}$, ale nesdělí Bobovi jeho hodnotu.

Bitový závazek

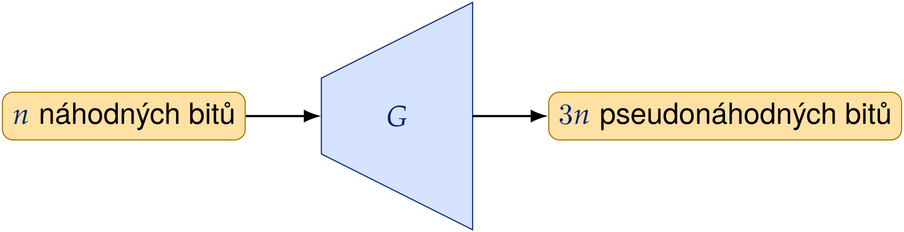
Fáze odhalení

Alice odhalí hodnotu b Bobovi

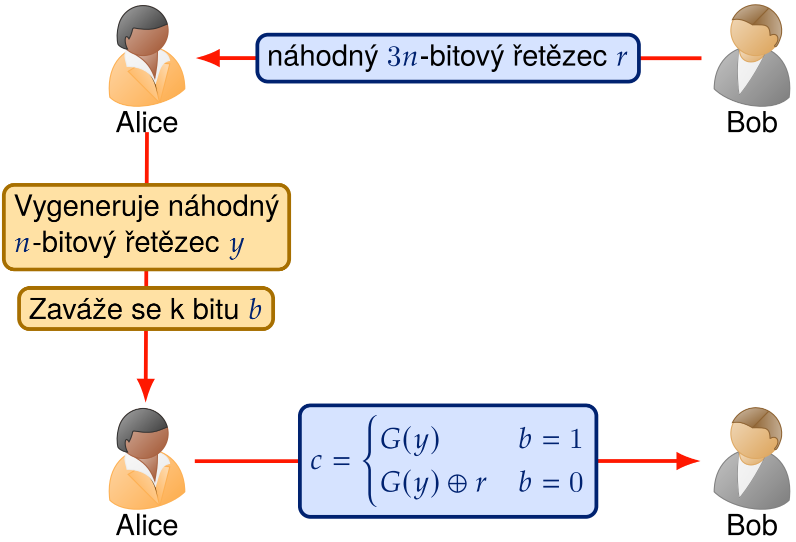


Bitový závazek s PRG

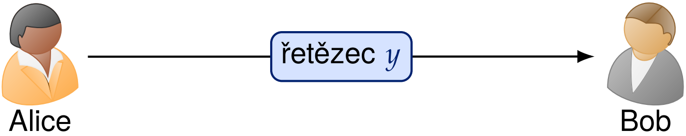
Předpokládáme PRG G se stretch $\ell(n) = 3n$.



Fáze závazku s PRG



Fáze odhalení s PRG



Bob určí $b = \begin{cases} 1 & c = G(y) \\ 0 & c = G(y) \oplus r \end{cases}$

Zvětšení stretch

- Předpokládejme, že G_1 je PRG se stretch $\ell_1(n) = n + 1$
- Nechť $\ell(n)$ je funkce stretch, která je omezená polynomem a vyčíslitelná v polynomiálním čase
- Uvažme seed s délky n
- Definujme $x_0 = s$
- Pro $i = 1, \ldots, \ell(n)$, položíme
  - $x_i =$ prvních n bitů $G_1(x_{i-1})$
  - $\sigma_i = n + 1$-ní bit $G_1(x_{i-1})$
- Definujme

$$G(s) = \sigma_1 \sigma_2 \ldots \sigma_n$$

Proposition (Bez důkazu)

G je pseudonáhodný generátor se stretch $\ell(n)$.

Reklama

NTIN104 — Foundations of theoretical cryptography

Vyčíslitelnost (NTIN064, doc. Antonín Kučera)

- Základy vyčíslitelnosti
  - Algoritmicky vyčíslitelné funkce, numerace, s-m-n věta
  - Základní vlastnosti rekurzivních a rekurzivně spočetných množin — shrnutí
  - Věty o rekurzi a jejich aplikace
  - Produktivní a kreativní množiny a jejich vlastnosti
  - Efektivně neoddělitelné dvojice množin, Gödelovy věty o neúplnosti
- Relativní vyčíslitelnost
  - Relativní vyčíslitelnost, částečně rekurzivní funkcionály, Turingovská převeditelnost
  - Stupně nerozhodnutelnosti, operace skoku, relativizovaný halting problém
  - Limitní vyčíslitelnost
  - Aritmetická hierarchie, věta o hierarchii
  - Aplikace teorie vyčíslitelnosti

Složitost (NTIN063, doc. Ondřej Čepek)

- Turingovy stroje s orákulem
- Polynomiální hierarchie (definice pomocí orákulí a pomocí alternujicích kvantifikátorů, důkaz ekvivalence)
- Kvantifikované booleovské formule QBF a jejich úplnost pro PSPACE a Σ_i
- Nedeterministická hierarchie
- Log-space převoditelnost, P-úplnost a její důsledky
- Věta Szelepcsenyi-Immermana a $\mathrm{NL} = \text{co-NL}$
- Neuniformní výpočetní modely — radící funkce, booleovské obvody, třídy NC a $\mathrm{P/poly}$, funkce s maximální velikostí obvodu.
- Pravděpodobnostní algoritmy — třídy RP, co-RP, ZPP a BPP
- Redukce chyby pro BPP, BPP je v $\mathrm{P/poly}$, BPP je v Σ_2
- NP-úplnost UNIQUE-SAT (pravděpodobnostní redukce)
- PCP věta (bez důkazu) a její využití pro neaproximovatelnost.

Rozhodovací procedury a SAT/SMT řešiče (NAIL094)

Pokud vás zajímá, jak řešit SAT prakticky …

Zkoušky

- Sledujte aktuální informace v Moodle
- On-line zkoušky
  - Nejsou rozvrženy
  - Pokud potřebujete zkoušku složit on-line, napište mi, abychom se dohodli na termínu