Záväzkové schémy (Commitment schemes)

Martin Stanek

2025

KI FMFI UK Bratislava

Úvod

- Aplikácie záväzkových schém
  - bezznalostné dôkazy
  - bezpečné výpočty viacerých účastníkov
- pôvodná motivácia: hádzanie mincou po telefóne
  - prevencia pred zmenou „názoru“ účastníka
  - prevencia pred predčasným odhalením hodu

Cieľ: Predstaviť základné vlastnosti a konštrukcie záväzkových schém.

Záväzkové schémy (neformálne)

Kryptografická konštrukcia (protokol), ktorá umožňuje odosielateľovi zaviazať sa vopred k nejakej hodnote $m \in \{0,1\}^*$ a neskôr túto hodnotu odkryť.

Záväznosť (binding)
Odosielateľ nevie po zverejnení záväzku zmeniť hodnotu m, teda odkryť inú hodnotu ako m.

Utajenie (hiding)
Príjemca nevie zo samotného záväzku zistiť hodnotu m.

- analógia s uzamykateľnou krabicou
  - záväzok: hodnota v zamknutej krabici
  - odkrytie: odovzdanie kľúča
- záväzkové schémy pre bity, reťazce, vektory, polynómy
  - niekedy len čiastkové odkrytie
- obvykle neinteraktívne schémy (len odosielateľ niečo posiela)
- schémy sa líšia predpokladmi bezpečnosti, zložitosťou (čas a dĺžka), či potrebujú dôveryhodnú inicializáciu (trusted setup)

Záväzkové schémy (formálnejšie)

- neinteraktívna záväzková schéma je trojica algoritmov:
  - Setup(1^k) – vygeneruje verejné parametre schémy (nebudeme explicitne uvádzať)
  - $c, d \leftarrow \text{Commit}(m, r)$ – vypočíta záväzok c pre hodnotu m a náhodný reťazec r; hodnota d slúži na otvorenie záväzku; častokrát $d = r$ a $c = \text{Commit}(m, r)$
  - $\text{Verify}(c, m, d) \in \{\text{true}, \text{false}\}$ – overí, či c je platný záväzok pre m
- korektnosť: $\forall m, r \; \forall (c, d) \leftarrow \text{Commit}(m, r) : \text{Verify}(c, m, d) = \text{true}$
- záväznosť: ľubovoľný odosielateľ nevie s nezanedbateľnou pravdepodobnosťou nájsť (c, m_0, m_1, d_0, d_1) také, že $m_0 \neq m_1$ a $\text{Verify}(c, m_0, d_0) = \text{Verify}(c, m_1, d_1) = \text{true}$
- utajenie: ľubovoľný príjemca nevie zistiť o m nič
  - presnejšie, môže si zvoliť dve správy m_0 a m_1 a po získaní záväzku c_b jednej z nich nie je schopný určiť správnu m_b s pravdepodobnosťou nezanedbateľne lepšou ako $1/2$

Perfektná/nepodmienená vs. výpočtová bezpečnosť

- perfektná záväznosť – výpočtovo neobmedzený odosielateľ; neexistujú „kolidujúce“ záväzky
- perfektné utajenie – pravdepodobnostné distribúcie záväzkov pre ľubovoľné m sú identické; prijemca môže byť výpočtovo neobmedzene silný
- výpočtovo obmedzený príjemca/odosielateľ – pravdepodobnostný polynomiálny algoritmus (vzhľadom na k)
- záväzková schéma s perfektnou záväznosťou aj perfektným utajením **neexistuje**
  - pre schému s perfektnou záväznosťou neexistujú d_0, d_1 a c také, že $\text{Verify}(c, 0, d_0) = \text{Verify}(c, 1, d_1) = \text{true}$
  - neobmedzený útočník pre c dokáže prebrať všetky d a otestovať, ktorý bit je hodnotou záväzku, teda schéma nemá vlastnosť perfektného utajenia

Ad-hoc konštrukcia z hašovacej funkcie

– nech H je kryptografická hašovacia funkcia

Záväzok pre m: $c = H(m, r)$,
kde r je náhodný reťazec podstatne dlhší ako $|c|$

– odkrytie záväzku: prezradenie m a r

– korektnosť/Verify – očividné

Záväznosť (výpočtovo)

– odolnosť voči kolíziám

– ťažké nájsť $m \neq m'$, r a r' také, že $H(m, r) = H(m', r')$

Utajenie

– (výpočtovo) špecializovaná verzia odolnosti vzoru (čiastočný vzor)

– (štatisticky) H ako náhodné orákulum, vtedy pre každé c a m existuje veľa hodnôt r takých, že $c = H(m, r)$

Pedersenova schéma

- $(G, \cdot)$ je grupa prvočíselného rádu q
- nech g, h sú generátory G;
  napr. volené náhodne
  $\log_g h$ nie je známe
  voľba parametrov je dôležitá!

Záväzok pre $m \in \mathbb{Z}_q$: $c = g^r h^m$,
kde $r \in_R \mathbb{Z}_q$

- odkrytie záväzku: prezradenie m a r
- korektnosť/Verify – očividné

Záväznosť (výpočtovo, opiera sa o problém DL)

- nech vieme nájsť r, r' a $m \neq m'$:
  $g^r h^m = g^{r'} h^{m'} \implies g^{r-r'} = h^{m'-m}$
- teda vieme vypočítať $\log_g h$: $g^{(r-r')/(m'-m)^{-1}} = h$

Utajenie (perfektne)

- každé $c \in G$ môže byť záväzkom ľubovoľného
  $m \in \mathbb{Z}_q$: $g^r = c \cdot h^{-m}$
- také r existuje, lebo g je generátor

ElGamalova schéma

- $(G, \cdot)$ je grupa prvočíselného rádu q
- nech g, h sú generátory G;
  napr. volené náhodne
  $\log_g h$ nie je známe
  voľba parametrov je dôležitá!

Záväzok pre $m \in G$: $c = (g^r, mh^r)$,
kde $r \in_R \mathbb{Z}_q$

- variant pre $m \in \mathbb{Z}_q$: $c = (g^r, h^{m+r})$
- odkrytie záväzku: prezradenie m a r
- korektnosť/Verify – očividné

Záväznosť (perfektne)
- komponent g^r jednoznačne určuje hodnotu r
- tým je jednoznačne dané h^r a teda aj m
- výpočtovo neobmedzený odosielateľ nevie nájsť kolidujúce záväzky (napriek tomu, že vie napr. počítať DL)

Utajenie (výpočtovo, DDH predpoklad)
- záväzky pre rôzne m sú disjunktné množiny
- schopnosť počítať DL umožní zistiť m
- presnejšie: DDH predpoklad (ElGamalova asymetrická šifrovacia schéma vyžaduje)

Aplikačne užitočné vlastnosti záväzkových schém (niektorých)

Neinteraktívne
- všetky správy posiela odosielateľ
  - záväzok aj jeho odkrytie
- nie je potrebná žiadna správa od príjemcu

Nejednoznačné (equivocable)
- schéma je simulovateľná (iný Setup, s *trapdoor* parametrom) tak, že simulátor vie nájsť záväzok odkryteľný ako ľubovoľná hodnota

Extrahovateľné (extractable)
- schéma je simulovateľná tak, že simulátor vie odkryť ľubovoľný záväzok

Homomorfné
- možnosť počítať so záväzkami bez odkrytia
- užitočné pre bezpečné výpočty s viacerými účastníkmi
  - napr. elektronické voľby a spočítanie hlasov ako záväzkov
- Pedersenova schéma:

$$c_1 \cdot c_2 = g^{r_1} h^{m_1} \cdot g^{r_2} h^{m_2} = g^{r_1+r_2} h^{m_1+m_2}$$

  - na odkrytie záväzku hodnoty $m_1 + m_2$ postačuje $r_1 + r_2$

Vektorové záväzkové schémy

- záväzková schéma pre vektor hodnôt $(m_1, \ldots, m_n)$
  - pozičná záväznosť: na pozícii i nie je možné odkryť inú hodnotu ako m_i
  - pozičné utajenie: záväzok a odkryté hodnoty neprezradia nič o neodkrytých hodnotách
  - čiastočné odkrytie: hodnotu m_i je možné odkryť samostatne, bez ostatných hodnôt
- intuitívna konštrukcia – Merkleho stromy
  - záväzok je hodnota v koreni Merkleho stromu
  - odkrytie záväzku pre m_i je táto hodnota a autentizačná cesta zodpovedajúca pozícii
- Pedersenova vektorová záväzková schéma (bez čiastočného odkrytia)
  - Setup: $(G, \cdot)$ – grupa prvočíselného rádu q; náhodné generátory $g, h_1, \ldots, h_n \in G$
  - Commit$\left((m_1, \ldots, m_n), r\right) = g^r \cdot \prod_{i=1}^{n} h_i^{m_i}$, kde $m_i \in \mathbb{Z}_q$, $r \in_R \mathbb{Z}_q$
  - odkrytie záväzku pre celý vektor: overenie výpočtu s $(m_1, \ldots, m_n)$ a r

Úlohy

1. Ukážte, že ak odosielateľ v Pedersenovej záväzkovej schéme pozná $\log_g h$, dokáže odkryť záväzok c hodnoty m ako záväzok ľubovoľnej hodnoty m'.
2. Ukážte, že oba varianty ElGamalovej záväzkovej schémy sú homomorfné.