Obsah

Úvod

Alica a Bob sú milionári a chcú zistiť, kto z nich je bohatší. Súčasne si ale navzájom nechcú prezradiť, kto vlastne aký veľký majetok vlastní. Vo všeobecnosti máme n hráčov, ktorí chcú vypočítať hodnotu danej funkcie $f(x_1, \ldots, x_n)$, pričom každý z hráčov vlastní jeden zo vstupov. Prirodzene, hráči si nechcú navzájom prezradiť svoje vstupy. Tento problém nazývame **problémom privátnych výpočtov**.

Úlohou tejto diplomovej práce je podať prehľad o riešení tohto problému pomocou informačno-teoretických metód. To znamená, že žiadny z hráčov sa nielenže nesmie priamo dozvedieť žiadnu informáciu o vstupe spoluhráča, ale takáto informácia nesmie byť z pre neho prístupných údajov ani len teoreticky vypočítateľná. Informačno-teoretický prístup k tomuto problému prvýkrát jasne definovali v roku 1988 (nezávisle) Chaum, Crépeau a Damgård v [13] a Ben-Or, Goldwasser a Wigderson v [6]. Dovtedy sa tieto problémy skúmali z **kryptografického hľadiska** použitím kryptografických metód, ako sú kódovanie verejným kľúčom, bit-commitment schémy a pod. (viď. napr. [32]).

Prácu sme rozdelili na niekoľko kapitol.

Kapitola 1. Kryptografia a privátne výpočty. V kapitole uvedieme problém privátnych výpočtov v kontexte kryptografie. Pokúsime sa načrtnúť motiváciu privátnych výpočtov, rozdeliť výskum privátnych výpočtov na niekoľko oblastí podľa zamerania a použitých modelov a na záver presne vymedziť oblasť, ktorej sa venuje táto diplomová práca.

Kapitola 2. Dvojúčastnícke privátne protokoly. Uvedieme model dvojúčastníckych bezpodmienečne privátnych výpočtov a pojem privátnosti funkcie. Zaoberáme sa charakterizáciou privátnych funkcií, komunikačnou a kolovou zložitosťou privátnych funkcií a úlohou randomizácie.

Kapitola 3. Mnohoúčastnícke privátne protokoly. Podobným spôsobom ako v kapitole 2 zavádzame model mnohoúčastníckych bezpodmienečne privátnych výpočtov a pojem t-privátnosti funkcie. Ďalej sa zaoberáme hierarchiami privátnosti funkcií.

Príloha A. Schémy pre zdieľanie tajomstva. Zavádzame tzv. schémy pre zdieľanie tajomstva, ktoré majú veľký význam hlavne pri konštrukcii protokolov v kapitole 3.

Aj keď ide o prácu z väčšej časti kompilačného charakteru, podarilo sa nám dosiahnuť niektoré čiastkové výsledky. Zvlášť si ceníme pôvodného konštrukčného dôkazu tvrdenia 2.11 v kapitole 2, ktorý nám dáva pre ľubovoľnú privátnu funkciu optimálny (vzhľadom na počet kôl komunikácie) protokol na jej privátny výpočet. Predchádzajúce dôkazy toto tvrdenie dokazovali sporom.

Označenia a štruktúra kapitol

V texte tejto práce používame niekoľko typografických označení, ktoré si považujeme za povinnosť vysvetliť.

> Niektoré časti textu sú vysádzané menším písmom v zúženom formáte strany (ako tento odstavec). Takéto časti textu predstavujú prípravu (pomocné tvrdenia a ich dôkazy) ku tvrdeniu, ktoré nasleduje bezprostredne po skončení tohoto úseku. V texte sme radšej volili uvedenie pomocných tvrdení a ich dôkazov pred hlavným tvrdením namiesto (v niektorých prácach obvyklého) viacúrovňového vnárania dôkazov (formulácia a dôkaz pomocného tvrdenia priamo vo vnútri dôkazu hlavného tvrdenia). Považovali sme za povinnosť čitateľa na takéto pasáže zvlášť upozorniť, keďže väčšinou je ich motivácia jasná až priamo z dôkazu hlavného tvrdenia.

U hlavných tvrdení uvádzame v zátvorke citáciu na prácu. Ak je dôkaz tvrdenia motivovaný inou prácou, je citácia uvedená aj v zátvorke za slovom dôkaz. Pre označenie pôvodných tvrdení používame značku [*].

Na konci niektorých kapitol môže čitateľ nájsť časť "Bibliografia a ďalšie smery", kde uvádzame práce, z ktorých sme čerpali pri písaní kapitoly a takisto uvádzame aj ďalšie smery výskumu a prípadné otvorené problémy.

Kapitola 1

Kryptografia a privátne výpočty

Kryptografiu od nepamäti spájame s dvoma používateľmi, Alicou a Bobom, ktorí si navzájom neustále telefonujú a snažia sa týmto spôsobom vyriešiť všetky svoje problémy, ako je podpisovanie kontraktov, autentická komunikácia, privátna komunikácia, dôkazy s nulovou vedomosťou a pod. Aby to nemali také jednoduché, v telefónnej ústredni pracuje Eva, ktorá ich telefónnu linku neustále odpočúva a robí im množstvo ďalších zlých vecí.

Dnes sú Alica, Bob a dokonca aj Eva používateľmi internetu a sú súčasťou skupiny n používateľov, ktorí sa prostredníctvom tejto počítačovej siete snažia počítať hodnoty rôznych funkcií. Pritom každý z nich chce utajiť svoje vlastné údaje. Problémy, ktoré našich n používateľov obvykle rieši, sú napríklad:

Voľby prostredníctvom internetu. Voliči chcú mať možnosť overiť, že ich hlasy boli správne spočítané, a to bez toho, aby prezradili, ako vlastne volili. Chcú hlasovať nezávisle, chcú vylúčiť akúkoľvek možnosť vzájomného donucovania. A organizátori volieb chcú mať istotu, že sa volieb zúčastnia iba oprávnení voliči.

Elektronické verejné súťaže. Niekoľko uchádzačov sa uchádza o kontrakt prostredníctvom siete, najnižšia ponuka kontrakt získava. Ponuky majú zostať utajené a opäť má byť vylúčená možnosť ovplyvňovania.

Spoločné databázové výpočty. Niekoľko databáz by malo počítať dotazy týkajúce sa dát uložených v týchto databázach, a to bez toho, aby si databázy navzájom prezrádzali svoje dáta.

Privátny a bezpečný prístup k databáze. Používateľ chce vyhodnocovať dotazy bez toho, aby databázový operátor mohol zistiť, na čo sa vlastne používateľ pýtal. A databázový operátor nechce, aby sa používateľ dozvedel viac, ako odpoveď na dotaz, ktorý položil.

Spoločné podpisy. Skupina používateľov chce digitálne podpisovať dokumenty, ale iba v prípade, že všetci používatelia (resp. väčšina, alebo podmnožina danej veľkosti) súhlasia.

Spoločné zdieľanie dát. Skupina používateľov chce uložiť dáta takým spôsobom, aby mohli tieto dáta rozkódovať iba v prípade, že s tým všetci (resp. väčšina, alebo podmnožina danej veľkosti) súhlasia.

Uvedené problémy sú špeciálnym prípadom problému **mnohoúčastníckych výpočtov**: n účastníkov v distribuovanej sieti chce vypočítať funkciu n argumentov, pričom každý z účastníkov vlastní jeden zo vstupov. Popri tom chceme, aby vypočítaný výsledok bol korektný a aby komunikácia neposkytovala účastníkom (resp. skupine účastníkov) ďalšie informácie, ktoré nemôžu vypočítať zo svojich vstupov a z výstupov.

V ideálnom prípade všetci účastníci postupujú podľa daného protokolu, nesnažia sa zistiť informácie o vstupoch ostatných účastníkov a nesnažia sa ovplyvniť voľbu ich vstupov. Keď sa účastník začne správať iným spôsobom, považujeme jeho správanie za nepriateľské. Literatúra sa zaoberá niekoľkými druhmi takéhoto nepriateľského správania, pričom sa snaží nájsť protokoly, ktoré budú voči takémuto správaniu odolné.

Pasívne nepriateľské správanie je správanie skupiny niekoľkých používateľov siete, ktorí sa zúčastňujú na komunikácii, pričom sa riadia predpísaným protokolom. Okrem toho si však navzájom môžu prezrádzať svoje vstupy a informácie získané počas komunikácie, navyše pred začatím komunikácie môžu voliť svoje vstupy spoločne (nie nezávisle). Cieľom takejto skupiny je získať informácie o vstupoch ostatných hráčov.

Byzantínske nepriateľské správanie je správanie skupiny niekoľkých používateľov, ktorí sa zúčastňujú na komunikácii, ale nepostupujú podľa predpísaného protokolu. Cieľom takejto skupiny môže byť získanie informácie o vstupoch ostatných účastníkov, prípadne zamedzenie správneho dokončenia priebehu protokolu.

Mobilné nepriateľské správanie je pasívne alebo byzantínske správanie, pričom v každom kroku komunikácie (predpokladáme synchrónny model komunikácie) sa takto správa iná skupina nanajvýš t hráčov.

Donucovacie nepriateľské správanie je správanie, kde sa jeden alebo niekoľko hráčov snaží prinútiť ostatných hráčov, aby svoje vstupy zvolili nejakým konkrétnym spôsobom. Toto správanie sa uvažuje obvykle v kontexte elektronických volieb.

Takisto bolo v literatúre uvažovaných mnoho parametrov siete, použitej pre komunikáciu hráčov, ako sú napríklad topológia siete, časovanie siete (synchrónny resp. asynchrónny model), bezpečnostná úroveň jednotlivých kanálov (bezpečné, neodpočúvateľné kanály alebo verejné kanály), existencia broadcast kanálov. Dôležitú úlohu hrajú aj výpočtové možnosti jednotlivých hráčov — sú tieto obmedzené (napr. na triedu BPP výpočtov[1]) alebo sa predpokladá neobmedzená výpočtová sila. Vo všeobecnosti výsledky možno rozdeliť do dvoch tried:

[1] Pravdepodobnostné polynomiálne výpočty s ohraničenou chybou (menšou ako $\frac{1}{2}$).

1. Výsledky, ktoré kladú výpočtové ohraničenia na jednotlivých hráčov (predpokladá sa existencia jednosmerných funkcií, resp. problémov, ktoré nemožno riešiť v danom výpočtovom ohraničení) a vo všeobecnosti nepredpokladajú bezpečnosť kanálov. Takýto prístup budeme nazývať **kryptografický** a navrhnuté protokoly budú **výpočtovo privátne**.

2. Výsledky, ktoré kladú fyzické obmedzenia, ako napr. požiadavka bezpečnosti kanálov, na druhej strane však nekladú žiadne výpočtové ohraničenia. To znamená, že komunikácia nesmie v konečnom dôsledku niesť **žiadnu** (ani kódovanú) informáciu o vstupoch jednotlivých hráčov okrem tej, ktorú možno odvodiť aj z hodnoty samotnej funkcie. Tento prístup budeme nazývať **informačno-teoretický** a navrhnuté protokoly budú **bezpodmienečne privátne**.

Príklad: Uvažujme nasledujúci problém. Alica a Bob sú dvaja milionári a chcú vedieť, kto z nich je bohatší. Alica má i miliónov, Bob má j miliónov $1 \leq i, j \leq 10$. Potrebujeme teda protokol, ktorý rozhodne, či $i < j$. Navyše sa hráči z priebehu protokolu nesmú dozvedieť žiadnu (ani čiastočnú) informáciu o vstupe druhého hráča (samozrejme okrem samotného výsledku).

Kryptografický prístup. Predpokladajme, že Alica a Bob môžu počítať iba funkcie z BPP. Nech N je nejaké veľké celé číslo, nech ďalej M je množina všetkých nezáporných N-bitových celých čísel a Q_N je množina všetkých bijekcií z množiny M na množinu M. Nech ďalej Alica vybrala z Q_N dvojicu funkcií E_a a D_a takých, že $E_a = D_a^{-1}$. Funkciu E_a Alica zverejní (nazveme ju verejný kľúč), funkciu D_a však bude poznať iba Alica. Protokol bude vyzerať takto (podrobnejší popis viď. [32]):

1. Bob zvolí náhodné N-bitové celé číslo x a vypočíta $k = E_a(x)$.
2. Bob pošle Alici číslo $k - j + 1$.
3. Alica vypočíta hodnoty $y_u = D_a(k - j + u)$ pre $u = 1, 2, \ldots, 10$.
4. Alica vyberie náhodné $\frac{N}{2}$-bitové prvočíslo p a vypočíta $z_u = y_u \pmod p$ pre $u = 1, 2, \ldots, 10$. Tento krok opakuje, až kým neplatí pre ľubovoľné i, j $(z_i - z_j) \bmod p \geq 2$.
5. Alica pošle Bobovi prvočíslo p a nasledujúcu postupnosť čísel:

$$z_1, z_2, \ldots, z_i, (z_{i+1} + 1) \bmod p, \ldots, (z_{10} + 1) \bmod p$$

6. Bob sa pozrie na j-te číslo. Ak sa toto číslo rovná $x \bmod p$, potom $i \geq j$, inak $i < j$.
7. Bob oznámi výsledok Alici.

Je jasné, že tento protokol korektne odpovie na otázku, kto je bohatší. Kryptografickú privátnosť tohto protokolu rozoberá Yao v [32] (hlavným problémom je ukázať, že Bob nemôže vypočítať žiadnu informáciu o Alicinom vstupe v danom výpočtovom ohraničení).

Informačno-teoretický prístup. V tomto prípade nemôžeme použiť techniky kódovania verejným kľúčom, ani ďalšie podobné kryptografické techniky. Komunikácia v tomto prípade nesmie niesť žiadnu ďalšiu informáciu, okrem tej, ktorú možno odvodiť z výstupu protokolu. V kapitole 1 dokážeme, že protokol s požadovanými vlastnosťami pre milionársky problém v dvojúčastníckom modeli neexistuje. V kapitole 2 uvedieme riešenie milionárskeho problému vo viacúčastníckom modeli.

Nie je v našich možnostiach zaoberať sa v tejto práci problémom privátnych výpočtov v celej jeho šírke. Predmetom tejto práce je nasledujúci model:

- Informačno-teoretický prístup k privátnym výpočtom, t.j. bezpodmienečne privátne výpočty.
- Synchrónny model komunikácie. Každá dvojica účastníkov je spojená bezpečným komunikačným kanálom.
- Pripúšťame iba pasívne nepriateľské správanie.

Kapitola 2

Dvojúčastnícke privátne protokoly

Táto kapitola sa venuje dvojúčastníckemu modelu privátnych výpočtov tak, ako sme ho vymedzili v kapitole 1. Najskôr zavedieme komunikačný model, pojem protokolu a zložitostné charakteristiky protokolov. Ďalej zavedieme pojem privátnosti protokolu a funkcie.

V ďalšej časti sa budeme zaoberať kombinatorickou charakterizáciou privátnych funkcií. Mimo iné navrhneme konštrukciu, ktorou k ľubovoľnej privátnej funkcii zostrojíme príslušný deterministický privátny protokol. Neskôr ukážeme, že takto zostrojený protokol je aj optimálny vzhľadom na kolovú zložitosť.

V poslednej časti kapitoly ukážeme, že prípadné použitie randomizovaných protokolov neprináša v dvojúčastníckom modeli nič nové a ukážeme, že naša definícia (slabá privátnosť) a definícia vyskytujúca sa v niektorých iných prácach (silná privátnosť) určuje rovnakú triedu funkcií.

Na záver prinášame bibliografiu uvedených výsledkov a prehľad ďalších smerov výskumu.

2.1 Definície a model

2.1.1 Komunikačný model

Nech je daná funkcia $f : D_X \times D_Y \to H$, pričom D_X, D_Y a H sú konečné množiny. Uvažujme dvoch hráčov X a Y, ktorí chcú vypočítať hodnotu funkcie $f(x,y)$ pre $x \in D_X$ a $y \in D_Y$. Problém je v tom, že hráč X pozná iba hodnotu x a hráč Y iba hodnotu y. Hráči preto musia medzi sebou komunikovať. Pre zvýšenie prehľadnosti popíšeme model komunikácie najskôr neformálne a potom tento prístup zformalizujeme.

V tejto kapitole budeme uvažovať deterministické a randomizované protokoly. **Deterministický protokol** je algoritmus, podľa ktorého hráči navzájom komunikujú pri výpočte funkcie. Výpočet prebieha v kolách. V každom kole práve jeden z hráčov pošle druhému správu (t.j. binárny reťazec). Nech t_l je postupnosť správ poslaných hráčmi v prvých l kolách (pre nejaký vstup (x,y)). Protokol musí na základe t_l jednoznačne určiť:

- či výpočet končí;
- ak výpočet končí, musí určovať hodnotu vypočítanú protokolom;
- ak výpočet nekončí, musí určovať
  - ktorý hráč je v kole $l+1$ na ťahu,
  - správu, ktorú pošle hráč, ktorý je v kole $l+1$ na ťahu; táto správa je jednoznačne určená vstupom hráča, ktorý je na ťahu, a postupnosťou t_l.

Navyše budeme pre každé kolo l požadovať, aby správy, ktoré môžu byť zaslané v l-tom kole, boli bezprefixové; presnejšie, ak t_l (resp. t'_l) je postupnosť správ zaslaných v prvých l kolách výpočtu na vstupe (x, y) (resp. na vstupe (x', y')) a t_l a t'_l sa zhodujú v prvých $l-1$ členoch, potom l-tá správa v t_l nie je vlastným prefixom l-tej správy v t'_l. Týmto spôsobom docielime, že ak napíšeme správy za seba tak, ako boli postupne vysielané v prvom, druhom, treťom, atď. kole, dostaneme reťazec, ktorý možno jednoznačne rozložiť na jednotlivé správy. Takýto reťazec budeme nazývať *transkript*.

Randomizované protokoly sú vlastne deterministické protokoly, v ktorých povolíme obom hráčom navyše pri rozhodnutiach hádzať mincou. Formálnejšie povedané, každý hráč má okrem svojho vstupu pri rozhodovaní k dispozícii aj (potenciálne nekonečnú) postupnosť náhodných bitov a správa, ktorú posiela hráč v $(l+1)$-vom kole je jednoznačne určená jeho vstupom, jeho postupnosťou náhodných bitov a postupnosťou t_l.

S použitím randomizovaných protokolov však vyvstáva otázka, čo vlastne je výsledkom protokolu. Kým u deterministických protokolov bol výsledok určený iba vstupmi x a y jednotlivých hráčov, u randomizovaných protokolov sa môže stať, že protokol určuje pre konkrétne x a y viacero možných rôznych výstupov. V takomto prípade bude výstupom protokolu hodnota, pre ktorú je pravdepodobnosť (počítaná cez všetky možné kombinácie náhodných bitov) väčšia ako $\frac{1}{2}$. Ak taká neexistuje, potom výstup bude nedefinovaný.

Formálny model

Uvedenú predstavu môžeme zhrnúť do definícií, ktoré presnejším spôsobom vyjadrujú vyššie uvedené myšlienky:

Definícia 2.1 Protokol Π *je usporiadaná štvorica funkcií* (u, m_X, m_Y, v)*, pričom:*

$u(t)$ *je funkcia s oborom hodnôt* $\{\emptyset, X, Y\}$*, pričom* $t \in \{0,1\}^*$

$m_X(t, x, r_X)$ *je funkcia definovaná práve ak* $u(t) = X$*, pričom* $t \in \{0,1\}^*$*,* x *je vstup hráča* X *a* r_X *je postupnosť náhodných bitov pre hráča* X*. Hodnota funkcie určuje správu, ktorú má poslať hráč* X*, ak* t *je zreťazenie správ vyslaných v predchádzajúcich kolách. Navyše musí platiť:*

- *Oborom hodnôt funkcie je* $\{0,1\}^+$*.*

- *Ak $M_X(t)$ označíme množinu všetkých možných hodnôt m_X pre dané t a všetky možné x a r_X, potom $M_X(t)$ musí byť bezprefixová (t.j. v $M_X(t)$ sa nevyskytujú také dve správy, že jedna je vlastným prefixom druhej).*
- *Pre každé konkrétne t a x je m_X závislá iba od konečného počtu bitov z r_X.*

$m_Y(t, y, r_Y)$ je definovaná práve ak $u(t) = Y$, jej hodnota je definovaná obdobne ako m_X.

$v(t)$ je definovaná práve ak $u(t) = \emptyset$, pričom $t \in \{0,1\}^*$ je zreťazenie správ vyslaných v predchádzajúcich kolách. Hodnota funkcie určuje výsledok protokolu.

Definícia 2.2 *Nech $\vdash_{(r_X,r_Y)}$ je relácia definovaná nasledujúcim predpisom:*

$$(t, x, y) \vdash_{(r_X,r_Y)} (t \cdot m, x, y),$$

práve ak:

- *$u(t) = X$ a súčasne $m_X(t, x, r_X) = m$,*
- *alebo $u(t) = Y$ a súčasne $m_Y(t, y, r_Y) = m$.*

Tranzitívny uzáver relácie $\vdash_{(r_X,r_Y)}$ označme $\vdash^*_{(r_X,r_Y)}$.

Označenie 2.3 *Prázdny reťazec budeme označovať znakom ϵ. V ďalšom texte, ak nepovieme inak, budeme t_l označovať reťazec, ktorý vznikol zreťazením l správ. Ak navyše pre dané $x \in D_X$ a $y \in D_Y$ bude existovať r_X a r_Y také, že $(\epsilon, x, y) \vdash^*_{(r_X,r_Y)} (t_l, x, y)$, potom tento reťazec budeme nazývať* **transkriptom prvých** l **správ**.

Ak pre dané $x \in D_X$ a $y \in D_Y$ a reťazec t bude existovať r_X a r_Y, pre ktoré $(\epsilon, x, y) \vdash^*_{(r_X,r_Y)} (t, x, y)$ a súčasne $u(t) = \emptyset$, potom t budeme nazývať **transkriptom protokolu pre** x, y.

Definícia 2.4 *Ak $\Pi = (u, m_X, m_Y, v)$ je protokol, pričom funkcie m_X resp. m_Y nezávisia od parametra r_X resp. r_Y, potom protokol Π je* **deterministický**. *V opačnom prípade je protokol* **randomizovaný**.

U deterministických protokolov budeme zjednodušene písať $\vdash$ namiesto $\vdash_{(r_X,r_Y)}$ a takisto $\vdash^*$ namiesto $\vdash^*_{(r_x,r_Y)}$.

Poznámka: Na základe vyššie uvedených definícií možno pre deterministické protokoly ľahko zadefinovať pojmy ako "výsledok protokolu pre dané x, y", alebo jednoznačne určiť transkript protokolu pre dané x a y. V prípade randomizovaných protokolov však pri pokuse o priamočiaru definíciu narážame na nutnosť definovať výsledok protokolu, ako aj transkript protokolu pre x a y ako náhodnú premennú. Ako špeciálny prípad dostávame potom definície pre deterministické protokoly.

Označme $Pr(t_l|x, y, s_X, s_Y)$ pravdepodobnosť transkriptu t_l prvých l správ v protokole, pričom hráči majú vstupy $x \in D_X$, $y \in D_Y$ a $s_X \in \{0,1\}^*$, $s_Y \in \{0,1\}^*$ sú začiatky postupností náhodných bitov r_X a r_Y. Potom ľahko nahliadneme, že platí:

$$Pr(t_l|x,y,s_X,s_Y) = \begin{cases} 0, & \text{ak } \textbf{neexistuje } r_X, r_Y \in \{0,1\}^\infty \text{ také, že } s_X \text{ je prefix } r_X,\ s_Y \text{ je prefix } r_Y \text{ a súčasne } (\epsilon,x,y) \vdash^*_{(r_X,r_Y)} (t_l,x,y) \\ 1, & \text{ak } \textbf{pre všetky } r_X, r_Y \in \{0,1\}^\infty \text{ také, že } s_X \text{ je prefix } r_X,\ s_Y \text{ je prefix } r_Y \text{ platí } (\epsilon,x,y) \vdash^*_{(r_X,r_Y)} (t_l,x,y) \\ \frac{1}{4}\sum_{u_X\in\{0,1\},u_Y\in\{0,1\}} Pr(t_l|x,y,s_X\cdot u_X,s_Y\cdot u_Y), & \text{inak.} \end{cases}$$

Uvedomme si, že vyššie uvedeným vzťahom je $Pr(t_l|x,y,s_X,s_Y)$ jednoznačne určená. Pre ľubovoľný transkript t_l a pre dané x,y možno zhora odhadnúť konštantou, ktorý posledný bit sa v r_X resp. v r_Y protokol využíva pre rozhodovanie (keďže v každom kole sa využije iba konečný počet bitov). Z toho ale vyplýva, že pre dostatočne dlhé s_X a s_Y bude $Pr(t_l|x,y,s_X,s_Y) \in \{0,1\}$.

Označenie 2.5 ([*]) *Pre ľubovoľný transkript prvých l správ t_l a dané $x \in D_X$, $y \in$ $\in D_Y$, označme pravdepodobnosť priebehu protokolu podľa t_l pri vstupoch x a y takto*[1]*:*

$$Pr(t_l|x,y) = Pr(t_l|x,y,\epsilon,\epsilon)$$

Poznámka: Možno sa zdá, že horeuvedená definícia je príliš zložitá pre naše potreby. Skutočne, pre veľkú časť protokolov (hlavne konečných) by bolo možné rozdelenie pravdepodobnosti definovať podstatne jednoduchším spôsobom.

Našim cieľom však bolo podchytiť aj niektoré ďalšie typy protokolov. Uveďme (v neformálnom zápise) protokol pre funkciu XOR nad jednoduchými bitmi:

1. Hráč X hodí mincou a pošle výsledok hodu (0 alebo 1) hráčovi Y.

2. Ak hráč Y dostane správu 0, pošle hráčovi X správu 0 a protokol pokračuje opäť od bodu 1.

3. V opačnom prípade hráč Y pošle hodnotu svojho vstupu (0 alebo 1) hráčovi X, tento spočíta výsledok a oznámi ho (opäť správa 0 alebo 1) hráčovi Y.

Tento protokol má niekoľko nepríjemných vlastností:

- Napriek tomu, že protokol nemusí v niektorých prípadoch skončiť, pravdepodobnosť jeho skončenia je 1.

- Počet náhodných bitov použitých protokolom nemožno ohraničiť.

[1]Ak by sme ďalej určili rozdelenie pravdepodobnosti na $D_X \times D_Y$, mohli by sme pomocou vzťahu pre podmienenú pravdepodobnosť vypočítať pravdepodobnosť, že si hráč X vyberie vstup x, hráč Y vstup y a že komunikácia bude prebiehať podľa transkriptu t_l takto: $Pr(t_l,x,y) =$ $= Pr(t_l|x,y)Pr(x,y)$. Výsledky uvedené v ďalšom texte však nie sú závislé od konkrétneho rozdelenia pravdepodobnosti na $D_X \times D_Y$.

- Pre ľubovoľné $\epsilon > 0$ existuje transkript, ktorý má v našom protokole nižšiu pravdepodobnosť.

Odteraz budeme ku protokolom pristupovať výhradne cez pravdepodobnostnú charakterizáciu zavedenú v predchádzajúcej definícii. K dobudovaniu tohoto pohľadu je však potrebné zaviesť niekoľko ďalších označení.

Nech $t_l = t_{l-1} \cdot m_l$, pričom m_l je posledná správa vyslaná v t_l, nech $Pr(t_{l-1}|x,y) \neq$ $\neq 0$; potom:

$$Pr(m_l|x,y,t_{l-1}) = \frac{Pr(t_l|x,y)}{Pr(t_{l-1}|x,y)}.$$

Ak teraz:

správa m_l **bola posielaná hráčom** X, potom (vzhľadom k tomu, že funkcia m_X nezávisí od y), môžeme písať:

$$Pr(t_l|x,y) = Pr(m_l|x,t_{l-1})Pr(t_{l-1}|x,y)$$

správa m_l **bola posielaná hráčom** Y, potom podobne:

$$Pr(t_l|x,y) = Pr(m_l|y,t_{l-1})Pr(t_{l-1}|x,y)$$

Zadefinujme teraz pravdepodobnostné rozdelenie výsledkov protokolu Π.

Definícia 2.6 ([*]) *Nech je daný protokol* $\Pi = (u, m_X, m_Y, v)$. *Označme* $\mu_a(x,y)$ *pre* $x \in D_X$, $y \in D_Y$ *a* $a \in H$ *množinu transkriptov, pre ktoré je výsledkom protokolu* a, *t.j.*

$$\mu_a(x,y) = \{t | (\exists r_X, r_Y)((\epsilon,x,y) \vdash^*_{(r_X,r_Y)} (t,x,y) \wedge \\ \wedge\, u(t) = \emptyset \wedge v(t) = a)$$

Potom $\mathcal{A}_\Pi(x,y)$ *bude označovať distribúciu pravdepodobnosti takto:*

$$Pr(\mathcal{A}_\Pi(x,y) = a) = \sum_{t \in \mu_a(x,y)} Pr(t|x,y)$$

a zapisujeme tiež $Pr(\mathcal{A}_\Pi = a|x,y)$. *Uvedenú distribúciu budeme považovať za* **výsledok protokolu** Π *pre dané* x, y.

Definícia 2.7 ([*]) *Protokol* Π *počíta funkciu* $f : D_X \times D_Y \to H$, *ak pre každé* $x \in D_X$, $y \in D_Y$ *platí:*

$$Pr(\mathcal{A}_\Pi = f(x,y)|x,y) > \frac{1}{2}$$

Poznámka: U deterministických protokolov možno zápisy zjednodušiť. Stačí si uvedomiť, že

$$Pr(t_l|x,y) = \begin{cases} 0, & ak(\epsilon,x,y) \not\vdash^* (t_l,x,y) \\ 1, & ak(\epsilon,x,y) \vdash^* (t_l,x,y) \end{cases}$$

a ďalej, ak protokol počíta funkciu f, potom $Pr(\mathcal{A}_\Pi = f(x,y)|x,y) = 1$ a budeme tiež písať $A_\Pi(x,y) = f(x,y)$.

Protokoly ako stromy

V niektorých prípadoch budeme potrebovať zapisovať protokoly o niečo názornejšie, ako pomocou pravdepodobnostných charakteristík. V takom prípade môžeme protokol zapísať pomocou stromu. Nasledujúce označenie si nekladie za úlohu navrhnúť zápis, pomocou ktorého možno zapísať prehľadne všetky protokoly. Napriek tomu nám poskytne možnosť prehľadného zápisu dostatočne širokého okruhu protokolov, aby sme mohli v tomto formáte uvádzať potrebné príklady (stromy vlastne zodpovedajú protokolom, v ktorých sú posielané iba jednobitové správy).

Označenie 2.8 *Binárny strom predstavuje nejaký protokol* $\Pi = (u, m_X, m_Y, v)$, *ak*

1. *V každom liste stromu sa nachádza hodnota,*
2. *V každom vnútornom vrchole stromu sa nachádza podmienka, ktorej pravdivosť závisí:*
   - *buď iba od hodnôt vstupu* x *a vektora* r_X,
   - *alebo iba od hodnôt vstupu* y *a vektora* r_Y.
3. *Každá hrana je označená 0 alebo 1.*

Ak t *je cesta od koreňa tohoto stromu k ľubovoľnému vrcholu* w, *potom*

- *ak* w *je list, potom* $u(t) = \emptyset$ *a* $v(t)$ *je hodnota v tomto liste*
- *ak* w *je vrchol s podmienkou* P *závisiacou od* x *a* r_X, *potom* $u(t) = X$ *a* $m_X(t, x, r_X) = 1$, *ak je* $P(x, r_X)$ *splnená, inak* $m_X(t, x, r_X) = 0$.
- *ak* w *je vrchol s podmienkou* P *závisiacou od* y *a* r_Y, *potom* $u(t) = Y$ *a* $m_Y(t, y, r_Y) = 1$, *ak je* $P(y, r_Y)$ *splnená, inak* $m_Y(t, y, r_Y) = 0$.

Príklad: Uvažujme protokol pre výpočet funkcie XOR . Hráč X pošle hráčovi Y v prvom kole hodnotu svojho vstupu a hráč Y pošle hráčovi X v druhom kole výsledok. Na obrázku 2.1 vidíme tento protokol zakreslený pomocou stromu.

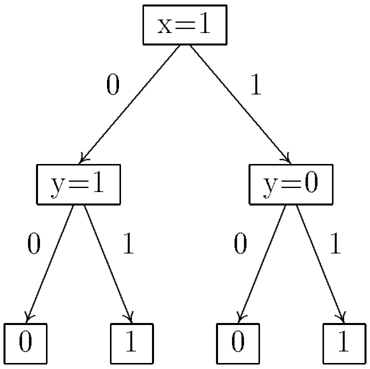
Špeciálne druhy protokolov

Definícia 2.9 *Protokol je* **explicitne oznamujúci**, *ak posledná správa, vyslaná protokolom je kód vypočítanej hodnoty.*

Je ľahké ukázať, že pre ľubovoľný protokol existuje explicitne oznamujúci protokol, ktorý počíta tú istú funkciu. Do protokolu stačí pridať jedinú správu o veľkosti $\lceil \log(|H|) \rceil$ oznamujúcu výslednú hodnotu.

Definícia 2.10 *Protokol je* **striktne striedavý**, *ak ten istý hráč nikdy neposiela dve po sebe nasledujúce správy.*

Opäť vidíme, že nie je problémom túto podmienku zabezpečiť. Triviálne možno zostrojiť taký protokol, že správy, ktoré v pôvodnom protokole jeden hráč vysiela bezprostredne po sebe, budeme v novom protokole vysielať ako jednu správu.



Obrázok 2.1: Strom, predstavujúci protokol pre výpočet funkcie XOR

2.1.2 Privátne protokoly a funkcie

Protokol je privátny, ak žiadny hráč nemôže po skončení výpočtu na základe transkriptu protokolu, svojho vstupu a výsledku výpočtu zistiť žiadnu informáciu o vstupe druhého hráča. Neuvažujeme pri tom informáciu, ktorú hráč môže zistiť iba na základe svojho vstupu a výsledku výpočtu (teda bez toho, aby uvažoval transkript). Formálne zapísané:

Definícia 2.11 *Protokol* Π *je* **privátny**, *ak platia nasledujúce podmienky:*

1. *Protokol skončí s pravdepodobnosťou 1.*[2]

2. **(Podmienka pre hráča** X**)** *Pre ľubovoľné* $y, y' \in D_Y$ *a* $x \in D_X$, *pre ktoré* $f(x,y) = f(x,y')$, *a pre ľubovoľný transkript protokolu* t*:*

$$Pr(t|x,y) = Pr(t|x,y').$$

3. **(Podmienka pre hráča** Y**)** *Pre ľubovoľné* $x, x' \in D_X$ *a* $y \in D_Y$, *pre ktoré* $f(x,y) = f(x',y)$, *a pre ľubovoľný transkript protokolu* t*:*

$$Pr(t|x,y) = Pr(t|x',y).$$

Poznámka: V podmienke 1 bude pre nás v budúcnosti podstatné, že pri jej splnení pre ľubovoľný transkript t_l prvých l ťahov a pre ľubovoľnú dvojicu vstupov $x \in D_X$ a $y \in D_Y$ existuje transkript protokolu t taký, že $Pr(t|x,y) > 0$ a súčasne t_l je prefixom t. Podmienka nám teda zaručuje, že sa v našom protokole nevyskytujú "slepé" vetvy, t.j. také, ktoré nemôžu viesť k výsledku.

[2] Touto podmienkou sa naša definícia líši od bežných definícií privátnosti protokolov. Literatúra totiž obvykle uvažuje výhradne konečné protokoly. Našim cieľom bolo rozšíriť príslušné výsledky aj na potenciálne nekonečné protokoly.

Poznámka: Uvedomme si, že ak uvažujeme deterministický protokol, podmienka privátnosti žiada, aby sa v prípade $f(x, y) = f(x, y')$ (resp. $f(x, y) = f(x', y)$) transkripty zhodovali.

Aj keď predchádzajúca definícia je pomerne jasná, môže sa zdať, že celkom nevystihuje pôvodný zámer. Definícia totiž vyžaduje od protokolu, aby v určitých prípadoch bola distribúcia pravdepodobnosti medzi jednotlivé transkripty rovnaká. V horeuvedenom kontexte sa však zdá byť logickejšia iná podmienka (sformulujeme iba pre hráča X): ak $f(x, y) = f(x, y')$, potom pre ľubovoľný transkript protokolu t:

$$Pr(y|t, x) = Pr(y'|t, x).$$

Ukážeme, že tieto dve podmienky sú za určitých podmienok ekvivalentné.

Lema 2.1 ([*]) *Predpokladajme rovnomernú distribúciu pravdepodobnosti na množinách D_X a D_Y. Nech $y, y' \in D_Y$ a $x \in D_X$, nech ďalej t je transkript protokolu Π. Potom, ak $f(x, y) = f(x, y')$ a $Pr(t|x) \neq 0$, potom podmienky 1 a 2 sú ekvivalentné:*

1. $Pr(t|x, y) = Pr(t|x, y')$
2. $Pr(y|x, t) = Pr(y'|x, t)$

Dôkaz: Z vlastností podmienenej pravdepodobnosti:

$$Pr(t|x, y) = \frac{Pr(t, y|x)}{Pr(y|x)} = Pr(y|x, t)\frac{Pr(t|x)}{Pr(y|x)}$$

Podobne, $Pr(t|x, y') = Pr(y'|x, t)\frac{Pr(t|x)}{Pr(y|x)}$. Keďže podľa predpokladov $Pr(y|x) = Pr(y'|x)$, dostávame

$$Pr(t|x, y) = Pr(t|x, y') \Longleftrightarrow Pr(y|t, x) = Pr(y'|t, x)$$

□

Poznámka: Predpoklad rovnomernej distribúcie pravdepodobnosti na množinách D_X a D_Y sme zaviedli iba pre účely predchádzajúcej lemy. Vo zvyšku kapitoly nezávadzame žiadne špecifické predpoklady ohľadom distribúcie pravdepodobnosti na množinách D_X a D_Y.

Poznámka: Všimnime si, že v prípade funkcie XOR protokol, pri ktorom hráč X pošle svoj vstup hráčovi Y a hráč Y svoj vstup hráčovi X, je privátny. Obaja hráči si síce prezradia navzájom svoje vstupy, vstup spoluhráča je však možné vypočítať aj na základe výsledku.

Definícia 2.12 *Funkcia je* **privátna**, *ak existuje privátny protokol Π, ktorý ju počíta. Funkcia je* **deterministicky privátna**, *ak existuje taký deterministický protokol.*

2.1.3 Komunikačná a kolová zložitosť

Definícia 2.13 Komunikačná zložitosť protokolu Π *(označujeme $C(\Pi)$) je dĺžka najdlhšieho možného transkriptu komunikácie v protokole Π. Ak protokol nie je konečný, v tom prípade píšeme $C(\Pi) = \infty$.*

Komunikačná zložitosť funkcie f *(označujeme $C(f)$) je minimum $C(\Pi)$ pre všetky protokoly Π, ktoré počítajú funkciu f.*

Poznámka: Ak navyše zavedieme požiadavku, aby protokoly boli explicitne oznamujúce, zhorší sa komunikačná zložitosť funkcie nanajvýš o $\log |H|$ bitov. Požiadavka striktnej striedavosti nemá vplyv na komunikačnú zložitosť.

Definícia 2.14 Kolová zložitosť protokolu Π *(označujeme $R(\Pi)$) je najväčší možný počet správ, z ktorého sa môže skladať transkript v protokole Π. Ak protokol nie je konečný, v tom prípade píšeme $R(\Pi) = \infty$.*

Kolová zložitosť funkcie f *(označujeme $R(f)$) je minimum $R(\Pi)$ pre všetky protokoly Π, ktoré počítajú funkciu f.*

Poznámka: Prípadná požiadavka, aby protokol bol explicitne oznamujúci, alebo striktne striedavý, nemá vplyv na kolovú zložitosť.

Definícia 2.15 Privátna komunikačná zložitosť *funkcie f (označujeme $C_P(f)$) je minimum $C(\Pi)$ pre všetky privátne protokoly, ktoré počítajú funkciu f. Podobne,* **privátna kolová zložitosť** *funkcie f (označujeme $R_P(f)$) je minimum $R(\Pi)$ pre všetky privátne protokoly, ktoré počítajú funkciu f.*

2.2 Charakterizácia privátnych funkcií

2.2.1 Rozdeliteľnosť funkcií

V tejto podkapitole zavedieme pojem *rozdeliteľnosti funkcií*. Ako neskôr uvidíme, rozdeliteľné funkcie budú hrať kľúčovú úlohu pri charakterizácii privátnych funkcií.

Poznamenajme, že funkciu f dvoch premenných nad konečnou doménou $D_X \times \times D_Y$ možno chápať aj ako maticu $(f(x,y))_{x \in D_X, y \in D_Y}$. Vybranou podmaticou matice budeme rozumieť maticu funkcie, ktorá je zúžením funkcie f na definičný obor $D'_X \times \times D'_Y$, kde $D'_X \subseteq D_X$ a $D'_Y \subseteq D_Y$. V nasledujúcom texte budeme pojem funkcie a príslušnej matice voľne zamieňať a nebudeme na to zvlášť upozorňovať.

Označenie 2.16 *Nech je daná funkcia $f : D_X \times D_Y \to H$, pričom D_X, D_Y a H sú konečné. Nech ďalej $X \subseteq D_X$ a $Y \subseteq D_Y$. Potom pre ľubovoľné $y \in D_Y$ označme $f(X,y) := \{f(x,y) | x \in X\}$ a podobne pre ľubovoľné $x \in D_X$ bude $f(x,Y) : := \{f(x,y) | y \in Y\}$.*

Teraz zavedieme pojmy *riadkovej* a *stĺpcovej* rozdeliteľnosti.

Definícia 2.17 (Riadková (stĺpcová) rozdeliteľnosť) *Funkcia f je* **riadkovo rozdeliteľná**, *ak existuje rozklad množiny D_X na neprázdne množiny $P_1, \ldots, P_n$ (pričom $n \geq 2$), pričom pre ľubovoľnú dvojicu P_i, P_j $(i \neq j)$ platí:*

$$(\forall y \in D_Y)(f(P_i, y) \cap f(P_j, y) = \emptyset).$$

Ak pre každé P_i označíme f_{P_i} zúženie funkcie f na definičný obor $P_i \times D_Y$ potom hovoríme, že funkcia f je **riadkovo rozdeliteľná na funkcie** $f_{P_1}, \ldots, f_{P_n}$.

Podobne, funkcia f je **stĺpcovo rozdeliteľná**, *ak existuje rozklad množiny D_Y na neprázdne množiny $P_1, \ldots, P_n$ (pričom $n \geq 2$), pričom pre ľubovoľnú dvojicu P_i, P_j $(i \neq j)$ platí:*

$$(\forall x \in D_X)(f(x, P_i) \cap f(x, P_j) = \emptyset).$$

Ak pre každé P_i označíme f_{P_i} zúženie funkcie f na definičný obor $D_X \times P_i$ potom hovoríme, že funkcia f je **stĺpcovo rozdeliteľná na funkcie** $f_{P_1}, \ldots, f_{P_n}$.

Definícia 2.18 (Podobnosť riadkov (stĺpcov)) *Ak pre nejaké dva riadky $x_1, x_2 \in \in D_X$ platí $(\exists y \in D_Y)(f(x_1, y) = f(x_2, y))$ hovoríme, že riadky x_1 a x_2 sú* **podobné** *(a píšeme $x_1 \sim x_2$).*

Podobne, ak pre nejaké dva stĺpce $y_1, y_2 \in D_Y$ platí $(\exists x \in D_X)(f(x, y_1) = f(x, y_2))$ hovoríme, že stĺpce y_1 a y_2 sú **podobné** *(a píšeme $y_1 \sim y_2$).*

Označenie 2.19 *Tranzitívny uzáver riadkovej (stĺpcovej) relácie podobnosti riadkov $\sim$ označíme $\equiv$. Relácia $\equiv$ je triviálne reflexívna a symetrická, preto ide o reláciu ekvivalencie.*

Lema 2.2 (Riadková (stĺpcová) rozdeliteľnosť) *Funkcia f je riadkovo (stĺpcovo) rozdeliteľná práve vtedy, ak relácia $\equiv$ vytvára aspoň dve triedy ekvivalencie.*

Dôkaz: Tvrdenie dokážeme pre riadkovú rozdeliteľnosť, pre stĺpcovú rozdeliteľnosť je dôkaz analogický.

Majme teda $x_1, x_2 \in D_X$ a nech $x_1 \sim x_2$. Potom z definície riadkovej rozdeliteľnosti x_1 aj x_2 musia v ľubovoľnom riadkovom rozdelení patriť do tej istej triedy rozkladu. Ak teda v relácii ekvivalencie $\equiv$ patria všetky riadky do tej istej triedy, musia byť všetky v tej istej množine a teda funkcia nie je riadkovo rozdeliteľná.

Naopak, nech v relácii ekvivalencie $\equiv$ existuje n $(n \geq 2)$ tried ekvivalencie $P_1, \ldots, P_n$. Potom pre ľubovoľné P_i, P_j platí

$$(\forall y \in D_Y)(f(P_i, y) \cap f(P_j, y) = \emptyset).$$

To ale znamená, že funkcia je riadkovo rozdeliteľná na funkcie $f_{P_1}, \ldots, f_{P_n}$. □

Všimnime si vlastnosti niekoľkých špeciálnych funkcií: napríklad funkcia XOR je riadkovo aj stĺpcovo rozdeliteľná. Naproti tomu funkcia AND nie je rozdeliteľná ani riadkovo, ani stĺpcovo a funkcia $f(x, y) = x$ je rozdeliteľná riadkovo, nie je však rozdeliteľná stĺpcovo. Nasledujúca funkcia takisto nie je riadkovo, ani stĺpcovo rozdeliteľná:

4	7	7
4	8	2
1	1	2

Teraz už ľahko môžeme zaviesť (rekurzívne) pojem **rozdeliteľnosti**:

Definícia 2.20 *Funkcia f je* **rozdeliteľná**, *ak*

- *je konštantná (jej matice je monochromatická),*
- *alebo je riadkovo rozdeliteľná na $f_{P_1}, \ldots, f_{P_n}$, pričom $f_{P_1}, \ldots, f_{P_n}$ sú rozdeliteľné funkcie*
- *alebo je stĺpcovo rozdeliteľná na $f_{P_1}, \ldots, f_{P_n}$, pričom $f_{P_1}, \ldots, f_{P_n}$ sú rozdeliteľné funkcie*

Zavedieme ešte pojem **stromu rozdelenia**. Z definície bude jasné, že každá rozdeliteľná funkcia má aspoň jeden strom rozdelenia a ak má funkcia strom rozdelenia, je rozdeliteľná.

Definícia 2.21 *Strom T_f budeme nazývať* **stromom rozdelenia** *funkcie f, ak*

- *Každý vrchol stromu T_f reprezentuje maticu niektorej funkcie.*
- *Koreň stromu reprezentuje maticu funkcie f.*
- *Ak vrchol v reprezentuje maticu funkcie g a jeho synovia $v_1, \ldots, v_n$ matice funkcií $g_1, \ldots, g_n$, potom funkcia g je riadkovo alebo stĺpcovo rozdeliteľná na funkcie $g_1, \ldots, g_n$.*
- *Listy stromu reprezentujú monochromatické matice.*

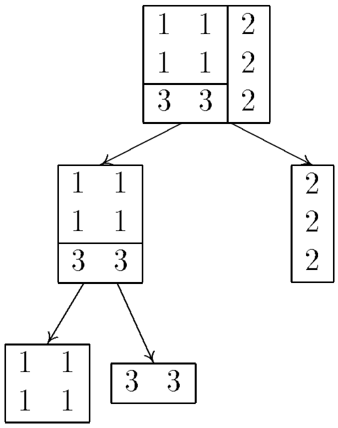
Pre nasledujúcu funkciu sa jeden z možných stromov rozdelenia nachádza na obrázku 2.2:

1	1	2
1	1	2
3	3	2

Na záver tejto časti uveďme ešte nutnú a postačujúcu podmienku pre rozdeliteľnosť funkcie. Táto podmienka nám často poslúži pri dôkazoch nerozdeliteľnosti niektorých funkcií.

Definícia 2.22 *Maticu M nazveme* **zakázanou**, *ak nie je monochromatická a súčasne nie je ani riadkovo ani stĺpcovo rozdeliteľná.*

Lema 2.3 (O zakázaných podmaticiach) *Funkcia je rozdeliteľná práve vtedy, ak jej matica neobsahuje ako vybranú podmaticu zakázanú maticu.*



Obrázok 2.2: Strom rozdelenia

Dôkaz: Nech funkcia f obsahuje zakázanú vybranú podmaticu $(f(x,y))_{x\in C, y\in D}$ a nech je naša funkcia rozdeliteľná. Vezmime jej ľubovoľný strom rozdelenia. Keďže v žiadnom vrchole nemožno rozdeliť ani riadky z C, ani stĺpce z D, musí byť naša matica vybranou podmaticou niektorého z listov stromu. Z toho ale vyplýva, že tento list nereprezentuje monochromatickú maticu, čo je spor.

Nech naopak funkcia f neobsahuje zakázanú podmaticu. Potom ale ľubovoľná nemonochromatická podmatica je rozdeliteľná riadkovo, alebo stĺpcovo. Postupným delením teda dostaneme z funkcie f monochromatické matice a teda funkcia f je rozdeliteľná. □

Z lemy 2.3 triviálne vychádza kritérium, ktoré často používame na dôkazy nerozdeliteľnosti funkcií.

Dôsledok 2.4 (Rohová lema) *Nech $x_1, x_2 \in D_X$ a $y_1, y_2 \in D_Y$. Potom ak platí $f(x_1,y_1) = f(x_1,y_2) = f(x_2,y_1) = a$ a $f(x_2,y_2) \neq a$, tak funkcia f nie je rozdeliteľná.*

2.2.2 Každá rozdeliteľná funkcia je privátna

Platnosť nasledujúceho tvrdenia dokážeme konštrukčným spôsobom (pre každú rozdeliteľnú funkciu nájdeme príslušný privátny protokol):

Veta 2.5 ([26, 2]) *Ak je funkcia $f : D_X \times D_Y \to H$ (pričom D_X, D_Y a H sú konečné množiny) rozdeliteľná, potom existuje deterministický privátny protokol pre výpočet f.*

Dôkaz: Tvrdenie dokážeme indukciou vzhľadom na $|D_X| + |D_Y|$ (triviálne platí $|D_X| + |D_Y| \geq 2$, keďže uvažujeme neprázdne domény).

Nech $|D_X| + |D_Y| = 2$, t.j. $D_X = \{x\}$ a $D_Y = \{y\}$. Potom je ale funkcia konštantná (keďže doména obsahuje jediný prvok) a obaja hráči poznajú výsledok. Hráči si nevymenia žiadnu správu a protokol je triviálne privátny.

Nech teraz naše tvrdenie platí pre všetky $|D_X| + |D_Y| < \alpha$ a nech $|D_X| + |D_Y| = \alpha$. Potom (keďže funkcia je rozdeliteľná) môže nastať jedna z troch možností:

Funkcia f je konštantná. Potom obaja hráči poznajú výsledok pre ľubovoľnú dvojicu x, y, nie je potrebná žiadna komunikácia a teda protokol je triviálne privátny.

Funkcia f je riadkovo rozdeliteľná na funkcie $f_{P_1}, \ldots, f_{P_n}$. Potom podľa indukčného predpokladu existujú pre výpočet funkcií $f_{P_1}, \ldots, f_{P_n}$ (v tomto poradí) privátne deterministické protokoly $\Pi_1, \ldots, \Pi_n$. Navrhnime teraz nový protokol Π pre výpočet funkcie f takto: ak $x \in P_i$, potom hráč X vyšle $\lceil \log n \rceil$ bitový zápis čísla i (označme tento zápis $\bar{\imath}$) a ďalej obaja hráči pokračujú podľa protokolu Π_i. Ukážeme, že protokol Π je tiež privátny.

Aby bol protokol privátny, musí byť splnená podmienka privátnosti pre hráča Y: pre ľubovoľné $x \in D_X$ a $y_1, y_2 \in D_Y$, ak $f(x, y_1) = f(x, y_2)$, potom transkript protokolu je rovnaký (x, y_1) aj (x, y_2). Skutočne, nech $x \in P_i$ pre niektoré i, potom z privátnosti pre Π_i pre ľubovoľné $y_1, y_2 \in D_Y$ také, že $f(x, y_1) = f(x, y_2)$ platí:

$$\Pi(x, y_1) = \bar{\imath} \cdot \Pi_i(x, y_1) = \bar{\imath} \cdot \Pi_i(x, y_2) = \Pi(x, y_2).$$

Zostáva dokázať podmienku privátnosti pre hráča Y, t.j. pre ľubovoľné $x_1, x_2 \in \in D_X$ a $y \in D_Y$ také, že $f(x_1, y) = f(x_2, y)$ bude transkript protokolu rovnaký. Z $f(x_1, y) = f(x_2, y)$ a z vlastnosti rozdeliteľnosti však vyplýva, že x_1 aj x_2 patria do tej istej množiny P_i. Potom z privátnosti Π_i:

$$\Pi(x_1, y) = \bar{\imath} \cdot \Pi_i(x_1, y) = \bar{\imath} \cdot \Pi_i(x_2, y) = \Pi(x_2, y),$$

čím je podmienka privátnosti pre hráča Y splnená.

Funkcia f je stĺpcovo rozdeliteľná na funkcie $f_{P_1}, \ldots, f_{P_n}$. Potom podľa indukčného predpokladu existujú pre výpočet funkcií $f_{P_1}, \ldots, f_{P_n}$ (v tomto poradí) privátne deterministické protokoly $\Pi_1, \ldots, \Pi_n$. Navrhnime teraz nový protokol Π pre výpočet funkcie f takto: ak $y \in P_i$, potom hráč X vyšle $\lceil \log n \rceil$ bitový zápis čísla i a ďalej obaja hráči pokračujú podľa protokolu Π_i. Dôkaz privátnosti je obdobný, ako v predchádzajúcom prípade.

Týmto je naše tvrdenie dokázané. □

Poznámka: Z dôkazu vety 2.5 vyplýva dôsledok, ku ktorému sa ešte v budúcnosti vrátime. Sformulujeme ho v nasledujúcom tvrdení.

Dôsledok 2.6 *Ku každému stromu rozdelenia T_f existuje deterministický privátny protokol Π, pričom $R_\Pi = H(T_f)$, kde $H(T_f)$ je výška stromu T_f.*

2.2.3 Každá privátna funkcia je rozdeliteľná

V tejto časti ukážeme, ako zostrojiť pre ľubovoľnú privátnu funkciu f niektorý jej strom rozdelenia. Tým dokážeme, že každá privátna funkcia je rozdeliteľná. Príslušné rozdelenie budeme konštruovať na základe niektorého privátneho protokolu Π, ktorý počíta f. Pripomeňme si, že tento protokol môže byť randomizovaný a dokonca nemusí jeho výpočet vždy skončiť. O protokole Π však môžeme predpokladať, že je **striktne striedavý** (pripomeňme si, že táto požiadavka nevedie k zhoršeniu ani komunikačnej, ani kolovej zložitosti).

Označenie 2.23 *Nech f je funkcia $f : D_X \times D_Y \to H$, kde D_X, D_Y a H sú konečné množiny. Majme ďalej protokol Π pre privátny výpočet tejto funkcie (môže byť randomizovaný, je striktne striedavý). Zostrojíme strom T_Π pre protokol Π takto:*

1. *Koreňom stromu bude matica funkcie f.*

2. *Ak vrchol v v strome reprezentuje monochromatickú maticu, potom v je listom stromu.*

3. *V opačnom prípade, nech sa vrchol v reprezentujúci funkciu $g : P_X \times P_Y \to \to H$ ($P_X \subseteq D_X, P_Y \subseteq D_Y$) nachádza v hĺbke l. Keďže náš protokol je striktne striedavý, podľa parity l je po l krokoch na ťahu vždy ten istý hráč, bez ujmy na všeobecnosti nech je to X. Potom jeho synov určíme takto:*

   - *Nech pre ľubovoľné $x_1, x_2 \in P_X$ platí $x_1 \approx x_2$ práve vtedy, keď pre ľubovoľný transkript prvých l ťahov t_l taký, že $(\forall x \in P_X)(\forall y \in P_Y)(Pr(t_l|x, y) > 0)$ a pre ľubovoľnú správu m_{l+1} v protokole Π platí:*

     $$Pr(m_{l+1}|x_1, t_l) = Pr(m_{l+1}|x_2, t_l).$$

   - *Relácia $\approx$ je relácia ekvivalencie, jej triedy ekvivalencie označme $P_1, \ldots, P_n$.*
   - *Zúženia funkcie g na domény $P_1 \times P_Y, \ldots, P_n \times P_Y$ označme (v tomto poradí) $g_{P_1}, \ldots, g_{P_n}$.*
   - *Synovia vrcholu v budú reprezentovať práve funkcie $g_{P_1}, \ldots, g_{P_n}$.*

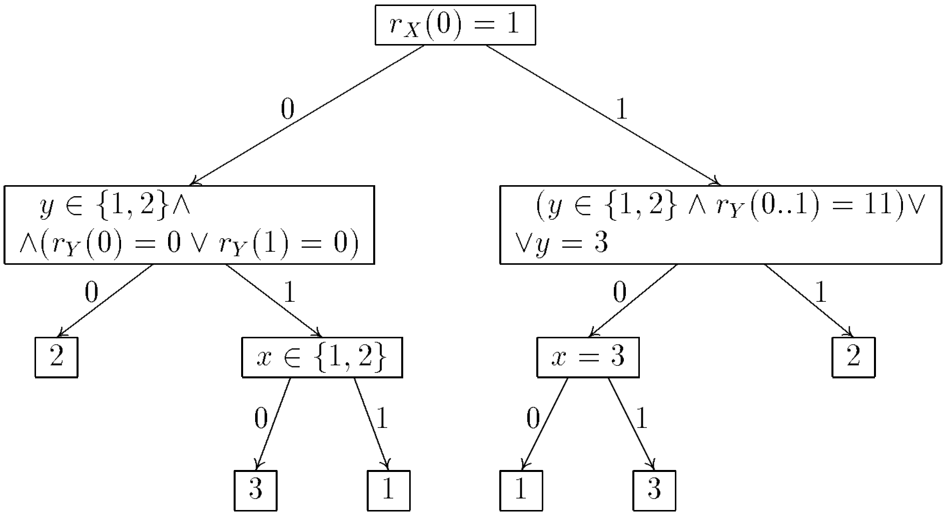
Majme napríklad nasledujúcu funkciu $f : \{1, 2, 3\} \times \{1, 2, 3\} \to \{1, 2, 3\}$:

	1	2	3
1	1	1	2
2	1	1	2
3	3	3	2

a protokol Π pre jej výpočet zobrazený na obrázku 2.3. Ľahko sa možno presvedčiť, že protokol pravdepodobnostne počíta funkciu f (pre $y = 3$ počíta prokol správnu hodnotu vždy, pre $y = 1$ resp. $y = 2$ a pre ľubovoľné x s pravdepodobnosťou $\frac{3}{4}$). Takisto sa ľahko presvedčíme, že protokol spĺňa podmienky privátnosti. Strom skonštruovaný podľa vyššie uvedeného postupu sa nachádza na obrázku 2.4.

Označenie 2.24 *Označme $Kontr(T_\Pi)$ strom, ktorý vznikne zo stromu T_Π po skontrahovaní všetkých hrán, ktoré spájajú vrcholy reprezentujúce tú istú funkciu.*

V ďalšom texte dokážeme, že pre privátny protokol Π, ktorý počíta funkciu f, bude $Kontr(T_\Pi)$ stromom rozdelenia funkcie f. Pripomeňme si, že o T_Π musíme dokázať tri veci:



Obrázok 2.3: Randomizovaný privátny protokol

- že neobsahuje nekonečné vetvy,
- že jeho listy reprezentujú monochromatické matice,
- že ak vrchol v reprezentujúci funkciu g má synov $v_1, \ldots, v_n$ reprezentujúcich funkcie $g_1, \ldots, g_n$, potom g je rozdeliteľná na $g_1, \ldots, g_n$.

Za týchto predpokladov nám operácie *Kontr* zabezpečí, že v strome sa nebudú vyskytovať vrcholy s jediným následovníkom a strom $Kontr(T_\Pi)$ bude stromom rozdelenia funkcie f.

Lema 2.7 ([*]) *Nech Π je ľubovoľný privátny protokol pre výpočet funkcie $f : D_X \times D_Y \to H$. Ak pre nejaké $x_1, x_2 \in D_X$ a pre niektoré $y \in D_Y$ platí $f(x_1, y) = f(x_2, y)$, potom pre ľubovoľný transkript t_r prvých r ťahov platí* [3]*:*

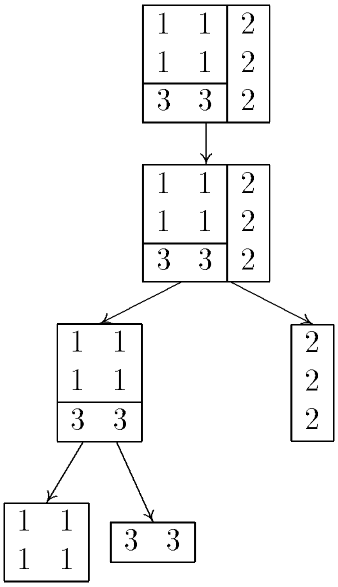
$$Pr(t_r | x_1, y) = Pr(t_r | x_2, y).$$

Dôkaz: Ak $Pr(t_r|x_1, y) = Pr(t_r|x_2, y) = 0$, tvrdenie triviálne platí. Nech teda $Pr(t_r|x_1, y) \neq 0$, alebo $Pr(t_r|x_2, y) \neq 0$. Označme $\tau(t_r, x, y)$ množinu všetkých transkriptov t, ktoré začínajú transkriptom t_r a súčasne $Pr(t|x, y) > > 0$. Z privátnosti protokolu vyplýva $\tau(t_r, x_1, y) = \tau(t_r, x_2, y) \neq \emptyset$, označme τ.

Teraz pre ľubovoľné $t \in \tau$ platí:

$$\begin{aligned} Pr(t_r|x_1, y)Pr(t|x_1, y, t_r) &= \\ = Pr(t|x_1, y) &= Pr(t|x_2, y) = \\ &= Pr(t_r|x_2, y)Pr(t|x_2, y, t_r) \end{aligned}$$

[3] Symetrické tvrdenie pre druhého hráča je možné dokázať obdobne



Obrázok 2.4: Skonštruovaný strom

Z toho ale vyplýva:

$$\begin{aligned} Pr(t_r|x_1, y)\sum_{t\in\tau} Pr(t|x_1, y, t_r) &= Pr(t_r|x_2, y)\sum_{t\in\tau} Pr(t|x_2, y, t_r) \\ Pr(t_r|x_1, y).1 &= Pr(t_r, x_2, y).1, \end{aligned}$$

čo bolo treba dokázať. $\square$

Lema 2.8 ([*]) *Nech v je vrchol stromu T_Π, ktorý sa nachádza v hĺbke l (koreň sa nachádza v hĺbke 0). Nech vrchol v reprezentuje zúženie funkcie f na doménu $C \times D$. Označme τ_l množinu všetkých možných transkriptov prvých l ťahov. Potom pre vrchol v musí platiť:*

$$(\forall t_l \in \tau_l)(\forall (x_1, y_1), (x_2, y_2) \in C \times D)(Pr(t_l|x_1, y_1) = Pr(t_l|x_2, y_2))$$

Dôkaz: Tvrdenie dokážeme indukciou vzhľadom na hĺbku vrcholu. Pre koreň stromu (matica funkcie f) tvrdenie triviálne platí (jediná možná správa je prázdna správa).

Majme teraz vrchol v v hĺbke l, ktorý nie je koreňom a nech tvrdenie platí pre jeho otca. Nech vrchol v reprezentuje vybranú podmaticu $C \times D$ matice funkcie f, nech $(x_1, y_1), (x_2, y_2) \in C \times D$ a ďalej nech $t_l \in \tau_l$. Ďalej nech m_l je posledná správa (bez ujmy na všeobecnosti vyslaná hráčom X — pre hráča Y tvrdenie dokážeme obdobne) a teda $t_l = t_{l-1} \cdot m_l$.

Potom z indukčného predpokladu ($Pr(t_{l-1}|x_1, y_1) = Pr(t_{l-1}|x_2, y_2)$) a ďalej z vlastností konštrukcie ($Pr(m_l|x_1, t_{l-1}) = Pr(m_l|x_2, t_{l-1})$, ak $Pr(t_{l-1}|x_1, y_1) \neq$ $\neq 0$):

$$\begin{aligned} Pr(t_l|x_1, y_1) &= Pr(m_l|x_1, t_{l-1})Pr(t_{l-1}|x_1, y_1) = \\ &= Pr(m_l|x_2, t_{l-1})Pr(t_{l-1}|x_2, y_2) = Pr(t_l|x_2, y_2)), \end{aligned}$$

čo bolo treba dokázať. □

Lema 2.9 ([*]) *Strom T_Π neobsahuje nekonečné vetvy.*

Dôkaz: Nech sa v našom strome nachádza nekonečná vetva. Potom od určitej úrovne vrcholy ležiace na tejto vetve reprezentujú tú istú maticu $A = (f(x,y))_{x \in C, y \in D}$, kde $C \subseteq D_X$, $D \subseteq D_Y$ (keďže funkciu f možno rozdeliť iba konečný počet krát). Matica A nie je monochromatická (inak by naša vetva bola konečná). Existuje teda $(x_1, y_1), (x_2, y_2) \in C \times D$ také, že $f(x_1, y_1) \neq f(x_2, y_2)$.

Podľa definície 2.6 pravdepodobnosť, že protokol skončí s výsledkom $f(x,y)$, je:

$$Pr(\mathcal{A}_\Pi = f(x,y)|x,y) = \sum_{t \in \mu_{f(x,y)}(x,y)} Pr(t|x,y).$$

Všetky vrcholy našej nekonečnej vetvy obsahujú (x_1, y_1) aj (x_2, y_2) (vrchol reprezentuje buď maticu $C \times D$, alebo jej nadmaticu). Preto možno použiť lemu 2.8 a teda pre všetky t platí:

$$Pr(t|x_1, y_1) = Pr(t|x_2, y_2),$$

a teda

$$Pr(\mathcal{A}_\Pi = f(x_1, y_1)|x_1, y_1) = Pr(\mathcal{A}_\Pi = f(x_1, y_1)|x_2, y_2).$$

Náš protokol ale počíta funkciu f, musí teda platiť $Pr(\mathcal{A}_\Pi = f(x_1, y_1)|x_1, y_1) > \frac{1}{2}$ a teda

$$Pr(\mathcal{A}_\Pi = f(x_2, y_2)|x_2, y_2) \leq 1 - Pr(\mathcal{A}_\Pi = f(x_1, y_1)|x_2, y_2) < \frac{1}{2},$$

čo je spor. □

Lema 2.10 ([*]) *Pre každý vrchol stromu T_Π, ktorý reprezentuje vybranú podmaticu $(f(x,y))_{x \in C, y \in D}$, platí: $(\forall x_1, x_2 \in C)(x_1 \sim x_2 \Rightarrow x_1 \approx x_2)$, ak je na ťahu hráč X (resp. $(\forall y_1, y_2 \in D)(y_1 \sim y_2 \Rightarrow y_1 \approx y_2)$ ak je na ťahu hráč Y).*

Dôkaz: Budeme dokazovať prvé z tvrdení, dôkaz druhého je veľmi podobný. Nech sa náš vrchol nachádza v strome v hĺbke l (koreň sa nachádza v hĺbke 0). Nech je dané $x_1, x_2 \in C$. Ak v matici $C \times D$ platí $x_1 \sim x_2$, potom existuje také $y \in D$, že $f(x_1, y) = f(x_2, y)$. Potom ale z podmienky privátnosti protokolu (lema 2.7) musí platiť (označme τ_l množinu všetkých možných transkriptov prvých l ťahov):

$$(\forall t_l \in \tau_l)(Pr(t_l|x_1, y) = Pr(t_l|x_2, y)) \tag{2.1}$$

$$(\forall t_{l+1} \in \tau_{l+1})(Pr(t_{l+1}|x_1, y) = Pr(t_{l+1}|x_2, y)) \tag{2.2}$$

Pre každé $t_{l+1} \in \tau_{l+1}$ nech $t_{l+1} = t_l \cdot m_{l+1}$, kde m_{l+1} je posledná vyslaná správa a t_l je transkript zvyšku komunikácie. Potom ale platí (keďže m_{l+1} vyslal hráč X):

- ak $Pr(t_l|x_1, y) = 0$, potom z lemy 2.8 aj $(\forall x \in C)(\forall y \in D)(Pr(t_l|x, y) = 0)$,

- ak $Pr(t_l|x_1,y) \neq 0$, potom:

$$Pr(t_{l+1}|x_1,y) = Pr(m_{l+1}|x_1,t_l)Pr(t_l|x_1,y))$$
$$Pr(t_{l+1}|x_2,y) = Pr(m_{l+1}|x_2,t_l)Pr(t_l|x_2,y))$$

a teda z 2.1 a 2.2 vyplýva:

$$Pr(m_{l+1}|x_1,t_l) = Pr(m_{l+1}|x_2,t_l).$$

Z toho ale podľa konštrukcie vyplýva, že $x_1 \approx x_2$, čo sme chceli dokázať. □

Veta 2.11 ([26, 2]) *Nech f je privátna funkcia. Potom funkcia f je rozdeliteľná.*

Dôkaz: ([*]) Keďže f je privátna, existuje pre jej výpočet privátny protokol Π. Zostrojme k tomuto protokolu strom $Kontr(T_\Pi)$. Ukážeme, že tento strom je stromom rozdelenia funkcie f.

Vezmime si vrchol v reprezentujúci funkciu g, ktorá je zúžením funkcie f na definičný obor $C \times D$. Bez ujmy na všeobecnosti, nech je na ťahu X (pre Y ukážeme obdobne). Vrchol v má synov $g_{P_1}, \ldots, g_{P_n}$ $(n \geq 2)$, ktoré reprezentujú (v tomto poradí) zúženia funkcie g na definičné obory $P_1 \times D, \ldots, P_n \times D$. Podľa lemy 2.10, ak pre $x_1, x_2 \in C$ platí $x_1 \sim x_2$, potom aj $x_1 \approx x_2$, a teda

$$(\forall i,j)(\forall y \in D)(g(P_i,y) \cap g(P_j,y) = \emptyset)$$

Z toho ale vyplýva, že funkcia g je rozdeliteľná na funkcie $g_{P_1}, \ldots, g_{P_n}$.

Keďže navyše podľa lemy 2.9 je náš strom konečný a jeho listy reprezentujú monochromatické matice, je tento strom súčasne aj stromom rozdelenia funkcie f, čo bolo treba dokázať. □

Poznámka: Veta 2.11 neurčuje žiadny vzťah medzi kolovou zložitosťou protokolu Π a výškou zostrojeného stromu rozdelenia. Tento vzťah však bezprostredne vyplýva z jej dôkazu a sformulujeme ho ako dôsledok.

Dôsledok 2.12 *Pre ľubovoľný privátny protokol Π (môže byť aj randomizovaný), ktorý počíta funkciu f, existuje strom rozdelenia funkcie f (označme ho T_Π), pre ktorý platí $H(T_\Pi) \leq R(\Pi)$, kde $H(T_\Pi)$ označuje výšku stromu T_Π.*

Dôkaz: Ak je protokol striktne striedavý, potom hľadaným stromom je priamo strom T_Π zostrojený v dôkaze vety 2.11. Ak protokol nie je striktne striedavý, možno jednoduchou konštrukciou (zlúčenie po sebe nasledujúcich ťahov toho istého hráča do jedného ťahu) zostrojiť striktne striedavý protokol Π', pre ktorý platí $R(\Pi') \leq$ $\leq R(\Pi)$. Keďže k Π' existuje strom $T_{\Pi'}$ taký, že $H(T_{\Pi'}) \leq R(\Pi')$, tak súčasne aj platí $H(T_{\Pi'}) \leq R(\Pi)$ a teda $T_{\Pi'}$ je súčasne hľadaným stromom pre protokol Π. □

2.2.4 Hlavné tvrdenie

Veta 2.13 ([26, 2]) *Nasledujúce tri tvrdenia sú ekvivalentné:*

1. *Funkcia f je privátna.*
2. *Funkcia f je rozdeliteľná.*
3. *Matica funkcie f neobsahuje zakázanú vybranú podmaticu.*

Dôkaz: Tvrdenia 1 a 2 sú ekvivalentné na základe viet 2.5 a 2.11. Tvrdenia 2 a 3 sú ekvivalentné na základe tvrdenia 2.3. □

Príklad: Vráťme sa k milionárskemu problému, ktorý sme uviedli na strane 7. Alica a Bob sú dvaja milionári a chcú vedieť, kto z nich je bohatší. Alica má i miliónov, Bob má j miliónov $1 \leq i, j \leq 10$. Uviedli sme riešenie pri kryptografickom prístupe.

Vezmime si teraz funkciu $f(i, j)$ definovanú pre $1 \leq i, j \leq 10$, pričom $f(i, j) = 1$, práve keď $i < j$, inak $f(i, j) = 0$. Táto funkcia je vlastne priamym prepisom nášho problému. Všimnime si teraz, že $f(1, 1) = f(10, 1) = f(10, 10) = 0$ a súčasne $f(1, 10) = 1$. Podľa rohovej lemy (lema 2.4) teda táto funkcia nie je rozdeliteľná, a preto podľa vety 2.13 **neexistuje bezpodmienečne privátny protokol pre riešenie tohoto problému.**

2.3 Komunikačná a kolová zložitosť privátnych funkcií

V tejto časti ukážeme dva podstatné zložitostné výsledky, a to konkrétne:

- Pomocou konštrukcie uvedenej v dôkaze vety 2.5 zostrojíme **optimálny protokol** vzhľadom na počet kôl komunikácie.
- Ukážeme, že existuje funkcia, ktorej privátna komunikačná zložitosť je **exponenciálne horšia** ako jej bežná komunikačná zložitosť.

2.3.1 Optimálny protokol

Pre danú privátnu funkciu f označme T_{opt} strom rozdelenia s najmenšou výškou. Nasledujúce tvrdenie ukazuje vzťah medzi kolovou zložitosťou a výškou tohoto stromu.

Lema 2.14 *Nech $H(T_{opt})$ je výška stromu rozdelenia T_{opt}. Potom*

$$R_P(f) = H(T_{opt}).$$

Dôkaz:

$R_P(f) \geq H(T_{opt})$. Majme privátny protokol Π pre výpočet funkcie f. Podľa dôsledku 2.12 existuje strom rozdelenia T_Π taký, že $H(T_{opt} \leq H(T_\Pi) \leq R(\Pi)$.

$R_P(f) \leq H(T_{opt})$. Majme ľubovoľný strom rozdelenia T_f. Podľa dôsledku 2.6 existuje protokol Π, kde $R_P(f) \leq R(\Pi) = H(T_f)$.

□

Z predchádzajúcej lemy vyplýva, že pri hľadaní protokolu optimálneho vzhľadom na kolovú zložitosť sa stačí zamerať na hľadanie stromu rozdelenia T_{opt}. Príslušný optimálny protokol potom možno zostrojiť zo stromu T_{opt} pomocou konštrukcie uvedenej v dôkaze vety 2.5.

Označenie 2.25 *Pre danú funkciu f označme $T_{\equiv R}$ strom, ktorý je definovaný* **za predpokladu riadkovej rozdeliteľnosti** *funkcie f nasledujúcim spôsobom:*

- *Koreň stromu reprezentuje funkciu f.*
- *Nech vrchol v v stromu reprezentuje funkciu g s definičným oborom $D_X \times D_Y$. Potom ak funkcia g*

  je riadkovo rozdeliteľná, *tak synmi vrcholu v budú vrcholy reprezentujúce funkcie $g_{P_1}, \ldots, g_{P_n}$, kde $P_1, \ldots, P_n$ sú triedy ekvivalencie riadkovej relácie $\equiv$ na D_X.*

  je stĺpcovo, ale nie riadkovo rozdeliteľná, *tak synmi vrcholu v budú vrcholy reprezentujúce funkcie $g_{P_1}, \ldots, g_{P_n}$, kde $P_1, \ldots, P_n$ sú triedy ekvivalencie stĺpcovej relácie $\equiv$ na D_Y.*

  nie je riadkovo ani stĺpcovo rozdeliteľná, *tak vrchol v je listom.*

Poznámka: Z vlastností rozdeliteľnosti je zrejmé, že ak f je privátna funkcia, potom strom $T_{\equiv R}$ (ak existuje) je stromom rozdelenia funkcie f a je striktne striedavý. Takisto z definície vyplýva, že synovia koreňa stromu vzniknú vždy riadkovým rozdelením funkcie f.

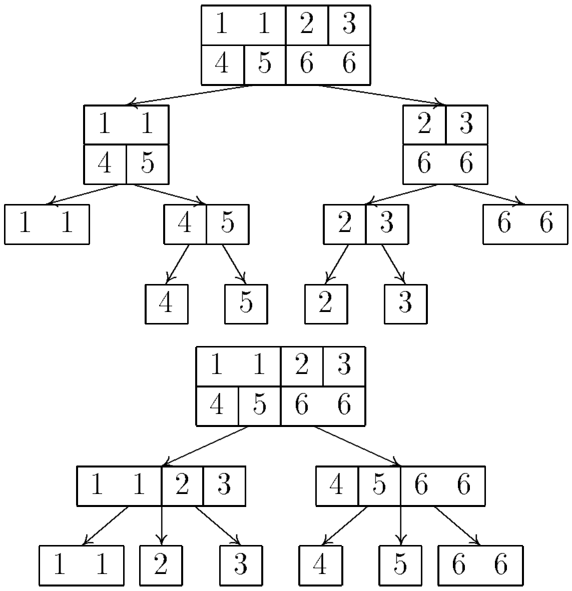
Označenie 2.26 *Pre danú funkciu f označme $T_{\equiv S}$ strom, ktorý je definovaný* **za predpokladu stĺpcovej rozdeliteľnosti** *funkcie f nasledujúcim spôsobom:*

- *Koreň stromu reprezentuje funkciu f.*
- *Nech vrchol v v stromu reprezentuje funkciu g s definičným oborom $D_X \times D_Y$. Potom ak funkcia g*

  je stĺpcovo rozdeliteľná, *tak synmi vrcholu v budú vrcholy reprezentujúce funkcie $g_{P_1}, \ldots, g_{P_n}$, kde $P_1, \ldots, P_n$ sú triedy ekvivalencie stĺpcovej relácie $\equiv$ na D_Y.*

  je riadkovo, ale nie stĺpcovo rozdeliteľná, *tak synmi vrcholu v budú vrcholy reprezentujúce funkcie $g_{P_1}, \ldots, g_{P_n}$, kde $P_1, \ldots, P_n$ sú triedy ekvivalencie riadkovej relácie $\equiv$ na D_X.*

  nie je riadkovo ani stĺpcovo rozdeliteľná, *tak vrchol v je listom.*



Obrázok 2.5: Stromy $T_{\equiv R}$ a $T_{\equiv S}$

Poznámka: Podobne, ako v predchádzajúcom prípade, aj strom $T_{\equiv S}$ (ak existuje) je pre privátnu funkciu f striktne striedavým stromom rozdelenia, pričom synovia koreňa vzniknú stĺpcovým rozdelením. Je ďalej zrejmé, že vždy existuje aspoň jeden zo stromov $T_{\equiv R}$ a $T_{\equiv S}$ (keďže privátna funkcia je vždy buď riadkovo, alebo stĺpcovo rozdeliteľná).

Označenie 2.27 *Označme $T_{\equiv}$ ten zo stromov $T_{\equiv S}$ a $T_{\equiv R}$, ktorý má menšiu výšku. Ak jeden zo stromov neexistuje, je $T_{\equiv}$ druhý z nich.*

Dôležité je uvedomiť si, že stromy $T_{\equiv S}$ a $T_{\equiv R}$ nemusia mať rovnakú výšku, a to aj v prípade, že pominieme špeciálne prípady (ako napríklad funkciu, ktorá nie je riadkovo rozdeliteľná a pod.). Všimnime si napríklad nasledujúcu funkciu:

1	1	2	3
4	5	6	6

Táto funkcia je aj riakovo, aj stĺpcovo rozdeliteľná. Jej stromy rozdelenia $T_{\equiv R}$ a $T_{\equiv S}$ sú na obrázku 2.5, pričom $H(T_{\equiv R}) = 4$ a $H(T_{\equiv S}) = 3$. Stromom $T_{\equiv}$ bude teda $T_{\equiv S}$.[4]

Veta 2.15 ([26],[*]) *Strom $T_{\equiv}$ je stromom rozdelenia s optimálnou výškou.*

Dôkaz: Ukážeme, že ľubovoľný strom rozdelenia T možno pretransformovať na jeden zo stromov $T_{\equiv R}$, $T_{\equiv S}$ tak, že jeho výšku nezväčšíme. Z toho ale vyplýva, že pre ľubovoľný strom rozdelenia T platí $H(T) \geq H(T_{\equiv})$, čo chceme dokázať.

[4]Tento príklad súčasne poukazuje na chybu, ktorej sa dopustil Kushilevitz v článku [26]. Kushilevitz totiž považuje za optimálny vždy strom $T_{\equiv R}$ (okrem prípadov, kedy funkcia nie je riadkovo rozdeliteľná).

Majme teda strom T, ktorý nie je stromom $T_{\equiv R}$, ani stromom $T_{\equiv S}$. Nazvime optimálnym rozdelením vrcholu v (bez ujmy na všeobecnosti predpokladáme riadkové rozdelenie, pri stĺpcovom rozdelení definujeme obdobne) reprezentujúceho maticu $C \times D$ rozdelenie na podmatice $C_1 \times D, \dots C_n \times D$ také, že $C_1, \dots C_n$ sú triedy ekvivalencie relácie $\equiv$ na C. Potom v strome T musí existovať vrchol, ktorého rozdelenie nie je optimálne. Vezmime taký, ktorého všetky podstromy obsahujú iba optimálne rozdelené vrcholy a označme ho w.

Nech vrchol w reprezentuje maticu $C \times D$. Keďže nie je rozdelený optimálne, musí aspoň jeden z jeho synov reprezentovať maticu $C' \times D$, pričom C' je zjednotením niekoľkých tried ekvivalencie relácie $\equiv C_1, \dots, C_n$. Označme podstrom zodpovedajúci tomuto synovi T'.

Nahraďme teraz T' podstromami $T_1, \dots, T_n$, pričom strom T_i vznikne zo stromu T' tak, že ak vrchol v T' reprezentuje maticu $C'' \times D''$, tak zodpovedajúci vrchol v T_i bude reprezentovať maticu $C'' \cap C_i \times D''$. Výsledný strom označme T^+. Pre strom $Kontr(T^+)$ zrejme platí:

- Strom $Kontr(T^+)$ je stromom rozdelenia.
- $H(Kontr(T^+)) \leq H(T)$.

Po konečnom počte aplikovaní tejto operácie dostaneme strom rozdelenia, u ktorého je každý vrchol rozdelený optimálne a teda je to buď strom $T_{\equiv R}$, alebo $T_{\equiv S}$, a teda $H(T) \geq H(T_{\equiv})$, čo sme chceli dokázať. □

2.3.2 Funkcie s vysokou privátnou komunikačnou zložitosťou

Uvažujme nekonečnú postupnosť funkcií $\{f_n\}$, pričom funkcia f_n je definovaná na obore $\{0,1\}^n \times \{0,1\}^n$. Vezmime teraz takúto postupnosť funkcií:

$$f_n(x,y) = \begin{cases} 2x & \text{ak } x \leq y \\ 2y+1 & \text{ak } x > y \end{cases}$$

Optimálny privátny protokol pre túto funkciu vyžaduje (pozri obrázok 2.6) $2^{n+1} - 2 = \Theta(2^n)$ kôl komunikácie a teda jej privátna komunikačná zložitosť $C_P(f_n) = \Omega(2^n)$ (v každom kole každý účastník musí poslať aspoň 1 bit). Naproti tomu, známe techniky horných odhadov bežnej komunikačnej zložitosti (viď. napr. [22]) dávajú pre túto funkciu odhad $C(f_n) = O(n)$. Pre túto funkciu je teda **privátna komunikačnú zložitosť exponenciálne horšia**, ako bežná komunikačná zložitosť.

2.4 Randomizované vs. deterministické protokoly

Označme pojmom **deterministicky privátne funkcie** množinu takých funkcií, pre ktorých výpočet existuje deterministický privátny protokol. Na základe tvrdení 2.11 a 2.5 v tejto časti ukážeme nasledujúce tvrdenie:

f	0	1	2	3	...	2^n-2	2^n-1
0	0	0	0	0	...	0	0
1	1	2	2	2	...	2	2
2	1	3	4	4	...	4	4
3	1	3	5	6	...	6	6
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
2^n-2	1	3	5	7	...	$2^{n+1}-4$	$2^{n+1}-4$
2^n-1	1	3	5	7	...	$2^{n+1}-3$	$2^{n+1}-2$

Obrázok 2.6: Matica funkcie f_n

Veta 2.16 ([26]) *Triedy deterministicky privátnych funkcií a privátnych funkcií sú totožné. Navyše, pre ľubovoľnú funkciu nemožno zlepšiť jej privátnu kolovú zložitosť použitím randomizovaného protokolu.*

Dôkaz: Majme funkciu f a randomizovaný privátny protokol Π pre jej výpočet. Podľa vety 2.11 existuje strom rozdelenia T_f pre túto funkciu taký, že $H(T_f) \leq R(\Pi)$. Podľa vety 2.5 ďalej k takémuto stromu existuje deterministický privátny protokol Π', pričom $R(\Pi') = H(T_f)$. Teda pre ľubovoľný randomizovaný privátny protokol Π pre výpočet funkcie f existuje deterministický privátny protokol Π' pre jej výpočet taký, že $R(\Pi') \leq R(\Pi)$. □

2.5 Silná vs. slabá privátnosť

V doterajších úvahách sme sa zaoberali výlučne tzv. slabou privátnosťou. Okrem tohoto pojmu je však často používaná aj tzv. silná privátnosť funkcií podľa nasledujúcej definície.

Definícia 2.28 *Protokol* Π *je* **silne privátny**, *ak platia nasledujúce podmienky:*

- *Protokol skončí s pravdepodobnosťou 1.*
- *Pre ľubovoľné $y, y' \in D_Y$ a $x \in D_X$, pre ktoré $f(x,y) = f(x,y')$, pre ľubovoľný reťazec náhodných bitov hráča X r_X a pre ľubovoľný transkript protokolu t:*

$$Pr(t|x,y,r_X) = Pr(t|x,y',r_X).$$

- *Pre ľubovoľné $x, x' \in D_X$ a $y \in D_Y$, pre ktoré $f(x,y) = f(x',y)$, pre ľubovoľný reťazec náhodných bitov hráča Y r_Y a pre ľubovoľný transkript protokolu t:*

$$Pr(t|x,y,r_Y) = Pr(t|x',y,r_Y).$$

Poznámka: Oproti definícii (slabej) privátnosti uvažujeme pri výpočte pravdepodobností aj náhodné reťazce bitov účastníkov. Všimnime si, že ak uvažujeme deterministické protokoly, pojmy slabej a silnej privátnosti protokolu sú ekvivalentné.

Ukážeme, že pojmy slabej a silnej privátnosti vymedzujú tú istú triedu funkcií.

Veta 2.17 ([26]) *Funkcia je slabo privátna práve vtedy, keď je silne privátna*

Dôkaz: Nech je funkcia silne privátna. Potom je triviálne z definície aj slabo privátna.

Naopak, majme slabo privátnu funkciu. Potom existuje pre jej výpočet deterministický privátny protokol. Keďže pojmy slabá a silná privátnosť sú na deterministických protokoloch ekvivalentné, je naša funkcia aj silne privátna. □

2.6 Bibliografia a ďalšie smery

Podmienkou privátnosti nad uvedeným komunikačným modelom sa prvý krát zaoberal Yao v [32]. Išlo však o kryptografickú privátnosť (predpoklad ohraničenia jednotlivých účastníkov na triedu BPP a využitie tzv. "ťažkých problémov").

Štúdium bezpodmienečne privátnych funkcií iniciovali Ben-Or, Goldwasser a Wigderson v [6]. Chor a Kushilevitz charakterizovali privátne booleovské funkcie [16]. Kompletná charakterizácia bezpodmienečne privátnych funkcií (veta 2.13) pre dvojúčastnícky privátne funkcie sa prvýkrát objavila v roku 1989 nezávisle v článkoch [25, 3]. V oboch týchto článkoch však bol uvedený chybný dôkaz vety 2.11. Autori článkov v neskorších verziách ([26, 2]) publikovali odlišné dôkazy (oba založené na myšlienke dôkazu sporom). Konštrukčný dôkaz uvedený v tejto práci je pôvodný, inšpirovaný myšlienkou uvedenou v [26]. Na vlastnostiach tejto konštrukcie je založený aj dôkaz optimality deterministického privátneho protokolu uvedený v časti 2.3. Výsledok bol uvedený už v [26], avšak s chybným dôkazom. V tejto práci predkladáme opravený dôkaz. Prínosom tejto práce je aj rozšírenie tvrdení z konečných protokolov na potenciálne nekonečné protokoly končiace s pravdepodobnosťou 1.

Ďalšie smery

Pre funkcie, ktoré nie sú privátne vypočítateľné je prirodzené študovať, koľko najmenej informácie o jednotlivých vstupoch je nutné prezradiť súperovi. Množstvom tejto informácie (na základe rôznych mier) sa zaoberajú Bar-Yehuda, Chor, Kushilevitz a Orlitsky v [1].

Každá funkcia je vypočítateľná pomocou dvoch správ. Ak sa obmedzíme na privátne protokoly, môže počet potrebných správ vzrásť exponenciálne. Existuje však nejaký kompromis medzi úrovňou privátnosti a medzi kolovou zložitosťou funkcie? Bar-Yehuda, Chor, Kushilevitz a Orlitsky v [1] ukazujú:

- Prezradením k bitov informácie možno dosiahnuť, že ľubovoľnú funkciu možno vypočítať na $O(k2^{\frac{2n+1}{k+1}})$ správ.

- Pre niektoré funkcie už prezradením jedného bitu informácie možno znížiť počet potrebných správ z 2^{n+1} na 2.

Kapitola 3

Mnohoúčastnícke privátne protokoly

V tejto kapitole sa budeme venovať privátnosti funkcií viac argumentov z hľadiska, ktoré sme vymedzili v kapitole 1. V kapitole opäť zavedieme základné pojmy (aj keď menej formálne, ako v predchádzajúcej kapitole) a vybudujeme podobný pohľad na protokol ako v prípade dvojúčastníckych privátnych výpočtov.

Okrem základných charakteristík mnohoúčastníckych privátnych protokolov sa v tejto kapitole podrobne venujeme problematike hierarchie privátnosti v mnohoúčastníckych výpočtoch.

Keďže ide o veľmi rozsiahlu oblasť, na záver kapitoly uvádzame podrobnú bibliografiu s prehľadom dosiahnutých výsledkov.

3.1 Definície a model

Podobne, ako v kapitole 2.1, zavedieme v ďalšom texte model privátnych výpočtov pre viac účastníkov. Komunikačnému modelu sa však nebudeme venovať tak podrobne, ako v kapitole 2.1, táto snaha by totiž viedla iba k sérii neprehľadných (a v budúcnosti nie veľmi použiteľných) definícií. Uvedený popis modelu však samozrejme možno sformalizovať (na úkor čitateľnosti) do podoby uvedenej v kapitole 2.1.

3.1.1 Komunikačný model

Nech F je konečné pole. Nech je ďalej daná funkcia $f : F^n \rightarrow F$, pričom platí $|F| > n$. Uvažujme množinu n hráčov $S = \{P_1, \ldots, P_n\}$, ktorí chcú vypočítať hodnotu funkcie $f(x_1, \ldots, x_n)$. Pritom ale každý hráč P_i pozná iba hodnotu vstupu x_i. Hráči teda musia medzi sebou komunikovať.

Predpokladajme teda, že hráči sú pospájaní v synchrónnej sieti každý s každým, pričom na komunikáciu používajú bezpečné kanály (t.j. kanály nie je možné odpočúvať). Komunikácia prebieha v kolách, pričom v každom kole pošle každý hráč po jednej správe každému hráčovi (pre jednoduchosť môžeme predpokladať, že hráč v každom kole posiela správu aj sebe samému). Formálne môžeme každé kolo komunikácie zapísať ako maticu M typu $n \times n$ prvkov z $\{0,1\}^*$, pričom $M(i,j)$ je správa, vyslaná hráčom P_i hráčovi P_j. Hráč P_i teda v danom kole prijal správy v i-tom stĺpci matice M a vyslal správy v i-tom riadku matice M.

Hráči komunikujú na základe tzv. *protokolu*. Protokol musí pre každého hráča P_i, pre každú hodnotu x_i a postupnosť doteraz ním prijatých správ T určovať správy, ktoré hráč P_i vyšle všetkým ostatným hráčom. Navyše umožňujeme hráčom ďalší vstup r_i, čo je nekonečná postupnosť náhodných bitov.

Označenie 3.1 *Nech G je množina. Potom $[G]$ označíme množinu všetkých konečných postupností prvkov z množiny G. Ďalej označme $T = \{0,1\}^*$.*

Definícia 3.2 *Predpis protokolu m je usporiadaná n-tica $(m_1, \ldots, m_n)$, pričom m_i je funkcia $[T] \times F \times T \to T^n$. Funkcia $m_i(t_i, x_i, r_i)$ pre každú postupnosť t_i doteraz prijatých správ hráčom P_i, vstup x_i a náhodný vektor r_i určuje správy, ktoré majú byť vyslané ostatným účastníkom komunikácie.*

Označenie 3.3 *Transkript protokolu s predpisom $m = (m_1, \ldots, m_n)$ pre vstupy jednotlivých hráčov $(x_1, \ldots, x_n)$ a vektory náhodných bitov pre jednotlivých hráčov $r_1, \ldots, r_n$ budeme zapisovať postupnosťou matíc typu $n \times n$ $M = (M_1, M_2, \ldots, M_l)$, kde*

$$M_k(i,*) = m_i((M_1(*,i), \ldots, M_{k-1}(*,i)), x_i, r_i),$$

pričom $M_k(i,*)$ je i-ty riadok matice M_k a $M_k(*,i)$ je i-ty stĺpec matice M_k.

Nami zostavené protokoly budú obvykle fungovať nasledujúcim spôsobom: hráč 1 pomocou komunikácie s ostatnými hráčmi vypočíta výsledok a pošle tento výsledok všetkým ostatným hráčom. Teraz sformalizujeme to, čo myslíme pod pojmom "vypočítať výsledok".

Označenie 3.4 *Funkcia $v : [T] \times F \times T \to F \cup \{\perp\}$ definuje výsledok protokolu, ak pre ľubovoľný transkript protokolu $M = (M_1, M_2, \ldots, M_l)$ bude platiť:*

- *ak $v((M_1(*,1), M_2(*,1), \ldots, M_l(*,1)), x_1, r_1) = \perp$ (nedefinované), potom aj pre všetky $k < l$ platí $v((M_1(*,1), M_2(*,1), \ldots, M_k(*,1)), x_1, r_1) = \perp$.*
- *ak $v((M_1(*,1), M_2(*,1), \ldots, M_k(*,1)), x_1, r_1) = a$ pre nejaké $a \in F$ a $k \leq l$, potom pre všetky $k \leq i \leq l$ platí $v((M_1(*,1), M_2(*,1), \ldots, M_i(*,1)), x_1, r_1) = a$*

Definícia 3.5 *Protokol Π je usporiadaná dvojica (m, v), kde m je predpis protokolu a v definuje jeho výsledok.*

Podobným spôsobom, ako v kapitole 2.1 môžeme zadefinovať pravdepodobnostný pohľad na protokol Π. Označme $x = (x_1, \ldots, x_n)$ vstupy jednotlivých hráčov, $r = (r_1, \ldots, r_n)$ ich náhodné bitové vektory, $M = (M_1, M_2, \ldots, M_l)$ niektorý transkript. Definície sú veľmi podobné (aj keď o niečo málo zložitejšie), ako v kapitola 2.1, preto uvádzame iba prehľad označení.

$Pr(M|x)$ je pravdepodobnosť priebehu protokolu Π podľa transkriptu M (počítaná cez všetky možné r).

$Pr(M_{l+1}|x, M)$, kde M_{l+1} je matica správ typu $n \times n$, je pravdepodobnosť vyslania správ podľa M_{l+1} v kole $l + 1$, ak transkript predchádzajúcej komunikácie je M (pričom ak platí $Pr(M|x) \neq 0$, potom $Pr((M_1, \dots, M_l, M_{l+1}|x)) = Pr(M_{l+1}|x, M)Pr(M|x)$).

$Pr(\mathcal{A}_\Pi(x) = a|x)$ je pravdepodobnosť, že protokol pri vstupe x skončí s výsledkom a (skrátene tiež $Pr(\mathcal{A}_\Pi = a|x)$).

Definícia 3.6 *Protokol* Π **počíta funkciu** $f : F^n \to F$, *ak pre každé* $x \in F^n$ *platí*

$$Pr(\mathcal{A}_\Pi = f(x)|x) > \frac{1}{2}.$$

Protokol $\Pi = (m, v)$ **počíta funkciu** $f : F^n \to F$ **bez chyby**, *ak pre každé* $x = (x_1, \dots, x_n)$ $(x_i \in F)$ *a pre každý transkript* $M = (M_1, \dots, M_l)$ *taký, že* $Pr(M|x) \neq 0$, *existuje transkript* $M' = (M_1, \dots, M_l, \dots, M_k)$ *taký, že* $Pr(M'|x) \neq 0$ *a súčasne platí:*

$$v((M_1(*, 1), M_2(*, 1), \dots, M_k(*, 1)), x_1, r_1) = f(x).$$

Nasledujúce označenie zavádza do nášho modelu tzv. lokálny pohľad skupiny hráčov.

Označenie 3.7 (Pohľad) *Nech* T *je ľubovoľná podmnožina hráčov* $\{P_1, \dots, P_n\}$. *Potom označíme:*

$\textsc{view}_T(x)$, *(pričom* $x = (x_1, \dots, x_n)$ *je vstup) vektor* $(x_i)_{P_i \in T}$,

$\textsc{view}_T(r)$, *(pričom* $r = (r_1, \dots, r_n)$ *sú náhodné vektory jednotlivých hráčov) vektor* $(r_i)_{P_i \in T}$,

$\textsc{view}_T(M_k)$, *(pričom* M_k *je matica vyslaných/prijatých správ) riadky* $i_1, \dots, i_t$ *a stĺpce* $i_1, \dots, i_t$ *matice* M_k, *pričom* $T = \{P_{i_1}, \dots, P_{i_t}\}$,

$\textsc{view}_T(M)$, *(pričom* $M = (M_1, \dots, M_l)$ *je transkript) postupnosť* $M' = (\textsc{view}_T(M_1), \dots, \textsc{view}_T(M_l))$.

3.1.2 Mnohoúčastnícka privátnosť

Protokol pre výpočet funkcie $f : F^n \to F$ je t-privátny, ak žiadna skupina T nanajvýš t hráčov nemôže získať z ich pohľadu na vstup, náhodné reťazce a transkript protokolu, žiadnu dodatočnú informáciu. Dodatočná informácia je ľubovoľná informácia o vstupoch hráčov, ktorí nepatria do skupiny T, a nevyplýva zo vstupov hráčov z T a z hodnoty $f(x_1, \dots, x_n)$. Formálne zapísané:

Definícia 3.8 *Konečný protokol* Π *je* t-**privátny**, *ak pre ľubovoľnú skupinu* T *hráčov, kde* $|T| \leq t$, *pre ľubovoľný transkript* M, *pre ľubovoľné vstupné vektory* $x, y \in F^n$ *také, že* $f(x) = f(y)$ *a* $\textsc{view}_T(x) = \textsc{view}_T(y)$ *a pre ľubovoľné náhodné vektory jednotlivých hráčov* r *platí:*

$$Pr(\textsc{view}_T(M)|x, \textsc{view}_T(r)) = Pr(\textsc{view}_T(M)|y, \textsc{view}_T(r)).$$

Definícia 3.9 *Funkcia je* t-**privátna**, *ak existuje protokol* Π, *ktorý ju počíta, a súčasne protokol* Π *je* t*-privátny.*

3.1.3 Úloha randomizácie

Pozastavme sa na chvíľu nad úlohou randomizácie u t-privátnych funkcií. V dvojúčastníckom prípade veta 2.16 ukázala, že randomizácia nijakým spôsobom nerozširuje triedu funkcií, ktoré možno vypočítať privátne. V mnohoúčastníckom prípade je však situácia iná. Nasledujúce tvrdenie ukazuje, že už ani takú jednoduchú funkciu, ako je XOR nemožno spočítať bez použitia náhodných bitov.

Veta 3.1 ([20]) *Nech* Π *je protokol pre* $n \geq 3$ *hráčov, ktorý počíta* t*-privátne funkciu XOR . Potom pre* Π *existuje vstup a priebeh protokolu, pri ktorom* Π *použije aspoň* t *náhodných bitov.*

Ako vidíme, trieda deterministicky t-privátnych funkcií je veľmi obmedzená, preto sa deterministickými výpočtami v tejto kapitole nebudeme zaoberať.

3.1.4 Základné vlastnosti viacúčastníckej privátnosti

Skôr, ako sa pustíme do skúmania t-privátnosti, všimnime si niektoré (triviálne) vlastnosti t-privátnych funkcií.

Lema 3.2 *Keď je funkcia* t*-privátna, je funkcia aj* t'*-privátna pre všetky* $t' < t$.

Dôkaz: Funkcia je t-privátna, ak pre ľubovoľnú podmnožinu hráčov T, kde $|T| \leq t$ platí podmienka privátnosti podľa definície 3.8. Táto podmienka je teda splnená aj pre ľubovoľnú podmnožinu hráčov T', kde $|T'| \leq t' < t$, čo bolo treba dokázať. □

Lema 3.3 *Keď je funkcia* n *argumentov* $(n-1)$*-privátna, je aj* n*-privátna.*

Dôkaz: Nech funkcia je $(n-1)$-privátna. Potom pre ľubovoľnú podmnožinu hráčov T, kde $|T| \leq n-1$, je splnená podmienka privátnosti podľa definície 3.8. Navyše, ak $T = \{P_1, \ldots, P_n\}$, je táto podmienka splnená triviálne (táto skupina hráčov pozná všetku informáciu). Preto je naša funkcia podľa definície aj n-privátna. □

Ďalšie dve tvrdenia sú aplikáciou výsledkov v dvojúčastníckom modeli na mnohoúčastnícky model.

Lema 3.4 (Rohová lema) *Nech funkcia f je t-privátna. Potom pre ľubovoľnú podmnožinu hráčov T takú, že $|T| \leq t$, a pre ľubovoľné dva vstupy x a x' platí: ak $f(\textsc{view}_T(x), \textsc{view}_{S-T}(x)) = f(\textsc{view}_T(x), \textsc{view}_{S-T}(x')) = f(\textsc{view}_T(x'), \textsc{view}_{S-T}(x)) = a$, potom $f(\textsc{view}_T(x'), \textsc{view}_{S-T}(x') = a$.*

Lema 3.5 (Redukčná lema) *Nech funkcie $f : F^n \to F$ je t-privátna. Potom T je ľubovoľná podmnožinu hráčov taká, že $|T| \leq t$. Definujme funkciu $f_T : F^{|T|} \times F^{n-|T|} \to F$ takto: $f_T(x, y) = f(z)$, kde z je taký vstup, že $x = \textsc{view}_T(z)$ a $y = \textsc{view}_{S-T}(z)$. Potom funkcia f_T je rozdeliteľná.*

Dôkaz: Tvrdenia sme dostali aplikáciou výsledkov z dvojúčastníckeho modelu. Ak totiž vezmeme množinu hráčov z T ako jedného hráča a množinu hráčov z $S - T$ ako druhého hráča, potom ak je nejaký protokol t-privátny, musí byť príslušný dvojúčastnícky protokol privátny. Na takýchto hráčov teda možno aplikovať tvrdenia z dvojúčastníckeho modelu. Prvé z tvrdení sme dostali aplikovaním dvojúčastníckej rohovej lemy a druhé aplikáciou charakterizácie dvojúčastnícky privátnych funkcií. □

Tieto tvrdenia možno výhodne využiť pri dokazovaní toho, že daná funkcia nie je t-privátna.

3.2 Hierarchie mnohoúčastníckej privátnosti

V prípade dvoch účastníkov sa nám podarilo nájsť jednoznačnú kombinatorickú charakterizáciu funkcií, ktoré možno vypočítať privátne. U mnohoúčastníckych výpočtov je situácia o niečo zložitejšia. Každá funkcia totiž spadá do určitej úrovne privátnosti. Podľa vyššie uvedeného by sa dalo predpokladať, že takýchto úrovní je $n - 1$: 1-privátne a nie 2-privátne funkcie, 2-privátne a nie 3-privátne funkcie, ..., $(n - 2)$-privátne a nie $(n - 1)$-privátne funkcie a n-privátne funkcie (všimnime si, že sme vynechali úroveň $n - 1$ – pre bližšie vysvetlenie pozri tvrdenie 3.3). O to zaujímavejší je nasledujúci výsledok: *Každá funkcia je $\lfloor \frac{n-1}{2} \rfloor$-privátna.*

Inými slovami: ak z n hráčov väčšina nevyzradí svoje informácie, funkciu možno vypočítať bez toho, aby sa ktokoľvek dozvedel dodatočnú informáciu o vstupoch spoluhráčov.

Prvú časť tejto kapitoly budeme venovať dôkazu tohoto výsledku. Potom sa budeme venovať hierarchii privátnosti pre všeobecné funkcie.

3.2.1 Každá funkcia je $\lfloor \frac{n-1}{2} \rfloor$-privátna

Ukážeme platnosť tohoto tvrdenia tak, že pre ľubovoľnú funkciu f zostavíme protokol, ktorý ju počíta a o tomto protokole ukážeme, že je privátny.

Veta 3.6 ([6, 13]) *Nech F je konečné pole, nech ďalej $f : F^n \to F$ je funkcia, pričom $|F| > n + 1$. Potom funkciu f možno vypočítať $\lfloor \frac{n-1}{2} \rfloor$-privátne.*

Dôkaz: ([6]) Označme $t = \lfloor \frac{n-1}{2} \rfloor$. Uvažujme nasledujúci protokol:

1. Každý hráč P_i vezme svoj vstup x_i a rozdistribuuje jeho podiely pomocou Shamirovej $(t+1, n)$-threshold schémy pre zdieľanie tajomstva (pozri dodatok A).

2. Každý hráč vypočíta na základe svojho podielu tajomstva nový podiel tajomstva $f(x_1, \ldots, x_n)$ (pričom prípadná komunikácia medzi hráčmi bude nezávislá od ich vstupov – pozri kapitolu A.2).

   Poznámka: Všimnite si, že t sme museli vybrať tak, aby $2t+1 \leq n$. Pri násobení sa totiž v medzivýsledku zvýši stupeň threshold schémy na $(2t+1, n)$; ak by $2t+1 > n$, potom by výsledok nebolo možné zrekonštruovať.

3. Každý hráč pošle svoj podiel tajomstva $f(x_1, \ldots, x_n)$ hráčovi 1, ktorý z týchto podielov vypočíta hodnotu $f(x_1, \ldots, x_n)$.

4. Hráč 1 rozpošle výsledok ostatným hráčom.

Ukážeme, že uvedený protokol je t-privátny. Správy, ktoré hráč i prijal počas behu protokolu možno rozdeliť na niekoľko skupín.

Podiely vstupov jednotlivých hráčov, tzn. správy, ktoré hráči prijali v prvom kroku (označme podiel i-teho hráča na vstupe j-teho hráča t_{ij}).

Podiely randomizačných polynómov, tzn. správy prijaté v druhom kroku.

Podiely výsledku, získava iba hráč 1 v treťom kroku (podiel výsledku od hráča i označme q_i).

Označme S skupinu hráčov, pričom $|S| \leq t$. Ďalej nech $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ sú vstupy, pričom $f(x) = f(y)$, $\textsc{view}_S(x) = \textsc{view}_S(y)$ a $r = (r_1, \ldots, r_n)$ sú náhodné vektory jednotlivých hráčov. O vstupe hráča $P_j \notin S$ majú hráči z S informáciu $T_j = \{t_{ij} | P_i \in S\}$ (ostatné podiely vstupov sú jednoznačne určené $\textsc{view}_S(x)$ resp. $\textsc{view}_S(y)$ a $\textsc{view}_S(r)$). Keďže z hľadiska použitej schémy pre zdieľanie tajomstva ide o nekvalifikovanú skupinu hráčov, platí podľa tvrdenia A.1

$$Pr(T_j|x_j) = Pr(T_j|y_j) \tag{3.1}$$

Označme R podiely randomizačných polynómov prijaté skupinou S v druhom kroku. Keďže tieto podiely sú generované nezávisle od vstupných hodnôt a od predchádzajúcich správ, môžeme písať

$$Pr(R|\textsc{view}_S(x), \textsc{view}_S(r)) = Pr(R|\textsc{view}_S(y), \textsc{view}_S(r)) \tag{3.2}$$

Označme M priebeh protokolu. Rozoberieme teraz dva prípady:

Hráč 1 nie je v S. Potom (keďže vyššie uvedené skupiny správ sú nezávislé):

$$\begin{gathered} Pr(\textsc{view}_S(M)|x, \textsc{view}_S(r)) = \\ = Pr(R|x, \textsc{view}_S(r)) \textstyle\prod_{P_i \notin S} Pr(T_i|x_i) \overset{3.1,3.2}{=} \\ \overset{3.1,3.2}{=} Pr(R|y, \textsc{view}_S(r)) \textstyle\prod_{P_i \notin S} Pr(T_i|y_i) = \\ = Pr(\textsc{view}_S(M)|y, \textsc{view}_S(r)). \end{gathered}$$

Hráč 1 je v S. Potom oproti predchádzajúcemu prípadu treba ešte dokázať (označme $Q = (q_1, \ldots, q_n)$):

$$Pr(Q|x, \text{VIEW}_S(r)) = Pr(Q|y, \text{VIEW}_S(r))$$

Keďže však ide o podiely **náhodného polynómu** tajomstva $f = f(x) = f(y)$, platí: $Pr(Q|x, \text{VIEW}_S(r)) = Pr(Q|f, \text{VIEW}_S(r)) = Pr(Q|y, \text{VIEW}_S(r))$.

□

Príklad: Opäť sa vrátime k nášmu milionárskemu problému, ktorý sme uviedli na strane 7. Pripomeňme si, že Alica a Bob chcú vedieť, kto z nich je bohatší. Alica má i miliónov, Bob má j miliónov, pričom $1 \leq i, j \leq 10$. Pritom ale nikto z nich nechce prezradiť protihráčovi, aký veľký majetok vlastní.

Zistili sme (pozri stranu 27), že tento problém nemožno riešiť v dvojúčastníckom modeli. Veta 3.6 nám však ponúka riešenie vo viacúčastníckom modeli — pridáme do nášho modelu ďalšieho hráča (volajme ho Dano). Dano nevlastní žiaden vstup, iba pomáha Alici a Bobovi vyriešiť ich problém. V takomto modeli už existuje podľa vety 3.6 1-privátny protokol. Pridaním jedného hráča, ktorý je "dôveryhodný" (t.j. nevytvorí koalíciu s Alicou ani Bobom) tak môžeme výrazne rozšíriť triedu funkcií, ktoré Alica a Bob môžu vypočítať privátne.

3.2.2 Hierarchia privátnosti má práve $\lceil \frac{n+1}{2} \rceil$ tried

Veta 3.6 obmedzila počet možných tried hierarchie privátnosti. Vyplýva z nej totiž, že každá funkcia spadá do jednej z týchto tried: $\lfloor \frac{n-1}{2} \rfloor$-privátne, $\lceil \frac{n}{2} \rceil$-privátne, $\lceil \frac{n}{2} + 1 \rceil$-privátne, ..., $(n-2)$-privátne a n-privátne funkcie (pričom trieda označená ako t-privátne funkcie je trieda funkcií, ktoré možno vypočítať t-privátnym protokolom, ale nemožno vypočítať $(t+1)$-privátnym protokolom). Teraz ukážeme, že každá z týchto tried je neprázdna.

Veta 3.7 ([14]) *Nech t je celé číslo, pričom $\lceil \frac{n}{2} \rceil \leq t \leq n-2$. Potom existuje funkcia f_t n argumentov, ktorá je t-privátna a nie je $(t+1)$-privátna.*

Dôkaz: Uvažujme funkciu $f_t : \{0,1\}^n \to \{0,1\}^{t+2} \cup \{0,1\}$ definovanú takto:

$$f_t(x_1, \ldots, x_n) = \begin{cases} 0 & \text{ak } x_i = 0 \text{ pre } 1 \leq i \leq t+1, \\ x_{t+2} & \text{ak } x_i = 1 \text{ pre } 1 \leq i \leq t+1, \\ (x_1, \ldots, x_{t+2}) & \textit{inak.} \end{cases}$$

Na dôkaz nášho tvrdenia bude stačiť, ak o funkcii f_t dokážeme, že:

- nie je $(t+1)$-privátna,
- je t-privátna.

Funkcia f_t nie je $(t+1)$-privátna. Na dôkaz tohoto tvrdenia využijeme rohovú lemu (lema 3.4). Vezmime si totiž množinu hráčov $T = \{x_1, \dots, x_{t+1}\}$ a množinu $\bar{T} = \{x_{t+2}, x_{t+3}, \dots, x_n\}$. Vezmime si teraz nasledujúcu podmaticu matice funkcie f_t:

		$(x_{t+2}, \dots, x_n) =$	
		$(0, \dots, 0)$	$(1, \dots, 1)$
$(x_1, \dots, x_{t+1}) =$	$(0, \dots, 0)$	0	0
	$(1, \dots, 1)$	0	1

Podľa rohovej lemy však takáto situácia nemôže nastať, ak je f_t $(t+1)$-privátna. Teda f_t nie je $(t+1)$-privátna.

Funkcia f_t je t-privátna Uvažujme nasledujúci protokol pre výpočet funkcie f_t:

1. Hráč P_{t+2} vygeneruje $t+1$ náhodných bitov $m_1, \dots, m_{t+1}$ tak, aby platilo $(\sum_{i=1,\dots,t+1} m_i) \bmod 2 = x_{t+2}$. Hodnotu m_i pošle i-temu hráčovi[1]
2. Nech U je množina hráčov $U = \{P_1, \dots, P_{t+1}\}$. Hráči z tejto množiny si navzájom rozpošlú svoje vstupy (t.j. každý hráč z T pozná po tomto kroku $x_1, \dots, x_{t+1}$).
3. Ak $(x_1, \dots, x_{t+1}) = (0, \dots, 0)$, hráč 1 rozpošle všetkým hráčom výsledok 0.
4. V opačnom prípade všetci hráči z U pošlú hráčovi P_1 svoje hodnoty m_i. Hráč 1 zrekonštruuje $x_{t+2} = (\sum_{i=1,\dots,t+1} m_i) \bmod 2$ a rozpošle výsledok (určený hodnotami $x_1, \dots, x_{t+2}$) ostatným hráčom.

Ukážeme, že uvedený protokol je t-privátny. Nech T je ľubovoľná skupina hráčov, pričom $|T| \leq t$. Majme vstupy x, y také, že $f_t(x) = f_t(y)$ a $\textsc{view}_T(x) = \textsc{view}_T(y)$. Nech ďalej r sú príslušné náhodné reťazce a nech M je transkript protokolu. Dokážeme podmienku privátnosti, t.j.

$$Pr(\textsc{view}_T(M) | x, \textsc{view}_T(r)) = Pr(\textsc{view}_T(M) | y, \textsc{view}_T(r)).$$

Označme $U^+ = U \cup \{x_{t+2}\}$. Najskôr si uvedomme, že ak T neobsahuje hráča z U^+, nezískajú hráči z T žiadnu informáciu z komunikácie okrem výsledku (počas behu protokolu prijmú totiž iba oznámenie hodnoty funkcie a funkcia f_t nezávisí od ich vstupov). Preto v takomto prípade podmienka privátnosti nemôže byť porušená. Z toho istého dôvodu, podmienka privátnosti pre T platí práve vtedy, keď platí pre $T \cap U^+$ (ostatní hráči z T totiž neprinesú žiadnu informáciu). Preto sa stačí zaoberať množinami $T \subseteq U^+$.

Zvyšok dôkazu rozdelíme na prípady podľa hodnoty $f_t(x) = f_t(y)$ takto:

[1] Všimnime si, že hráč P_{t+2} týmto vytvoril jednoduchú $(t+1, t+1)$-threshold schému pre zdieľanie tajomstva.

Nech $f_t(x) \notin \{0, 1\}$. Potom výstup jednoznačne určuje všetky vstupy hráčov $P_1, \ldots, P_{t+2}$, a preto podľa definície je podmienka privátnosti splnená (keďže vstupy $x_{t+3}, \ldots, x_n$ neovplyvňujú priebeh komunikácie).

Nech $f_t(x) = 1$. Potom $x_1 = x_2 = \ldots = x_{t+2} = 1$ a teda (podobne ako v predchádzajúcom prípade) podmienka privátnosti je opäť splnená.

Nech $f_t(x) = 0$. Potom $x_1 = x_2 = \ldots = x_{t+1} = 0$ a $x_{t+2} = 0$ alebo $x_{t+2} = 1$, alebo $x_1 = \ldots = x_{t+1} = 1$ a $x_{t+2} = 0$. Uvažujme možné zloženie T ($|T| \leq$ $\leq t$), pričom berieme ohľad iba na účastníkov z U^+, na ostatných hráčoch nezáleží (pozri vyššie):

$T \subseteq U$. Takáto skupina neobsahuje hráča P_{t+2}, preto nesmie vedieť rozlíšiť medzi vstupmi $x_1 = \ldots = x_{t+1} = 1, x_{t+2} = 0$ a $y_1 = \ldots = y_{t+1} =$ $= 1, y_{t+2} = 1$. Keďže v kroku 1 protokolu sú $m_1, \ldots, m_{t+1}$ vyberané náhodne, tak pre ľubovoľnú **vlastnú** podmnožinu U, sú (v prípade oboch vstupov x a y) distribúcie pravdepodobnosti jednotlivých správ triviálne rovnaké (z podmnožiny nanajvýš t hodnôt z $m_1, \ldots, m_{t+1}$ nemožno určiť žiadnu informáciu o $\sum_{i=1}^{t+1} m_i$. Kroky 2 a 3 nezávisia od vstupu hráča P_{t+2}, a preto priebeh protokolu je identický pre x aj pre y (v tomto prípade sa protokol zastaví v kroku 3). V tomto prípade je teda podmienka privátnosti protokolu splnená.

$T = \{P_{t+2}\}$. V tomto prípade T nesmie vedieť rozlíšiť medzi vstupmi $x_1 =$ $= \ldots = x_{t+1} = x_{t+2} = 0$ a $y_1 = \ldots = y_{t+1} = 1, y_{t+2} = 0$. V tomto prípade však P_{t+2} neprijme počas vykonávania protokolu žiadnu správu (okrem výstupu) a preto distribúcia pravdepodobnosti jednotlivých správ je rovnaká pre x aj pre y.

T **obsahuje** P_{t+2} **a aspoň jedného hráča z** U. V tomto prípade sú hodnoty vstupov hráčov $P_1, \ldots, P_{t+2}$ jednoznačne určené a teda podmienka privátnosti je splnená triviálne.

Tým sme dokázali, že funkcia f_t je t-privátna a teda aj platnosť nášho tvrdenia.

□

Dôsledok 3.8 *Hierarchia privátnosti funkcií definovaných nad konečnými doménami pozostáva z práve* $\lceil \frac{n+1}{2} \rceil$ *neprázdnych tried zodpovedajúcich* $\lfloor \frac{n-1}{2} \rfloor$, $\lceil \frac{n}{2} \rceil$, $\lceil \frac{n}{2} \rceil + 1$, ..., $n - 2$ *a* n*-privátnosti.*

Dôkaz: Vyplýva priamo z tvrdení 3.6 a 3.7. □

3.3 Bibliografia a ďalšie smery

Model mnohoúčastníckych bezpodmienečne privátnych výpočtov v tej podobe, ako ho uvádzame v tejto práci, bol prvýkrát skúmaný v roku 1988 nezávisle v článkoch [6, 13].

Model uvedený v tomto článku, ako aj formulácia a dôkaz tvrdenia 3.6, vychádza z práce [6]. Práca [13] uvádza rovnaké výsledky, používa však mierne odlišnú techniku.

Množstvom náhodných bitov, ktoré je potrebné použiť na t-privátny výpočet funkcie, sa zaoberá Kushilevitz a Mansour v [20]. Z tohoto článku pochádza aj tvrdenie 3.1.

Triedam hierarchie privátnosti sa prvýkrát venujú Chor a Kushilevitz v [16], ktorí sa venujú hierarchii booleovských funkcií. Hierarchie privátnosti na všeobecných funkciách skúmajú Chor, Geréb-Graus a Kushilevitz v [14]. Z tejto práce pochádza aj tvrdenie 3.7.

V oblasti mnohoúčastníckej privátnosti existuje množstvo ďalších zaujímavých prác zameraných rôznymi smermi. Nie je v našich možnostiach podať podrobný opis všetkých výsledkov dosiahnutých v tejto oblasti. Na nasledujúcich stranách preto podávame aspoň stručný prehľad výsledkov výskumu v tejto oblasti, rozčlenený podľa jednotlivých zameraní. Na záver uvádzame stručný prehľad aplikácií mnohoúčastníckej privátnosti a súvisiacich výsledkov.

3.3.1 Hierarchie mnohoúčastníckej privátnosti

Články [6, 13] sa okrem uvedených výsledkov (3.6) venujú aj modelu s byzantínskymi chybami (jednotliví hráči nemusia postupovať podľa predpísaného protokolu). V tomto modeli ukázali, že žiadna koalícia $t < \frac{n}{3}$ hráčov nemôže narušiť komunikáciu, ani nemôže získať žiadnu dodatočnú informáciu. Vzhľadom k známym výsledkom z oblasti distribuovaných algoritmov (pozri napr. [27]) je tento odhad tesný.

Vyššieuvedené výsledky sú zaujímavé aj v kontexte kryptografickej privátnosti. V takom prípade (pozri napr. [11]):

- Ak neuvažujeme byzantínske chyby, žiadna koalícia hráčov nemôže vypočítať žiadnu dodatočnú informáciu.
- Ak uvažujeme byzantínske chyby, žiadna koalícia o veľkosti $t < \frac{n}{2}$ nemôže narušiť komunikáciu, ani vypočítať žiadnu dodatočnú informáciu.

Okrem uvedených výsledkov týkajúcich sa hierarchie privátnosti nad všeobecnými funkciami (veta 3.7) sa skúmali aj rôzne podtriedy funkcií. Pre funkcie s booleovským oborom hodnôt ([16]) a tzv. husté symetrické funkcie (pozri [19]) sa podarilo dokázať nasledujúci výsledok:

Veta 3.9 ([16, 19]) *Ak uvažujeme funkcie s booleovským oborom hodnôt (resp. husté symetrické funkcie), potom hierarchia privátnosti nad týmito funkciami pozostáva práve z dvoch neprázdnych tried: funkcie, ktoré sú n-privátne a funkcie, ktoré sú $\lfloor\frac{n-1}{2}\rfloor$ privátne, ale nie $\lceil\frac{n}{2}\rceil$ privátne.*

Otvorené problémy

Problém 3.1 ([14, 19]) *Pri dokazovaní vlastností tried privátnosti je často potrebné ukázať pre nejaké t, že daná funkcia f (resp. trieda funkcií) nie je t-privátna. Známe* *dôkazy využívajú na tento účel nutné podmienky formulované v tzv. rohovej (3.4) a redukčnej (3.5) leme. Doposiaľ nie je známa funkcia, ktorá by vyhovovala týmto podmienkam a napriek tomu by nebola t-privátna. Prirodzenou otázkou teda je, či sú tieto dve podmienky aj postačujúce.*

Problém 3.2 ([19]) *Pre booleovské a husté symetrické funkcie je známa nielen hierarchia tried privátnosti, ale aj kompletná charakterizácia funkcií patriacich do týchto tried. Naproti tomu, charakterizácia funkcií patriacich do jednotlivých tried t-privátnosti pre $t \geq \lceil \frac{n}{2} \rceil$ pre všeobecné funkcie nad konečnými doménami je stále otvoreným problémom.*

3.3.2 Úloha randomizácie v mnohoúčastníckych privátnych výpočtoch, komunikačná a kolová zložitosť

Ako sme už uviedli v kapitole 3.1.3, randomizácia hrá v prípade mnohoúčastníckych výpočtov oveľa dôležitejšiu úlohu, ako v prípade dvojúčastníckych (v prípade dvojúčastníckych výpočtov sme ukázali ekvivalenciu deterministického a randomizovaného modelu výpočtov).

Úloha randomizácie

Kvantitatívnou úlohou randomizácie vo mnohoúčastníckych privátnych výpočtoch sa zaoberajú Kushilevitz a Mansour v [20]. Vo svojej práci ukazujú, že na výpočet funkcie XOR n vstupov t-privátne **stačí** $O(t^2 \log(\frac{n}{t}))$ náhodných bitov a **je potrebných** aspoň t náhodných bitov.

Vzťah medzi počtom náhodných bitov a kolovou zložitosťou

Vzťahom medzi počtom náhodných bitov a kolovou zložitosťou 1-privátnych výpočtov sa zaoberajú Kushilevitz a Rosén v [24]. Z vyššie uvedeného vyplýva, že funkciu XOR nemožno 1-privátne vypočítať deterministicky. Ak máme k dispozícii jeden náhodný bit, možno túto funkciu vypočítať nasledujúcim protokolom:

1. Hráč P_n si zvolí náhodný bit r a pošle P_1 hodnotu $x_n \oplus r$.

i. $(2 \leq i \leq n)$ Hráč P_{i-1} zoxoruje svoj vstup x_{i-1} so správou, ktorú prijal a pošle novú správu hráčovi P_i.

Je pomerne ľahké a priamočiare ukázať korektnosť a 1-privátnosť tohto protokolu. Hlavnou jeho nevýhodou však je, že jeho kolová zložitosť je n. Iný protokol počíta XOR s kolovou zložitosťou 2, vyžaduje však lineárny počet náhodných bitov:

1. Každý hráč P_i si zvolí náhodný bit r_i. Potom pošle $x_i \oplus r_i$ hráčovi P_1 a r_i hráčovi P_2.
2. Hráč P_2 spočíta $\sum_{i=1}^{n} r_i \bmod 2$ a pošle výsledok hráčovi P_1, ktorý zoxorovaním všetkých prijatých správ zistí výsledok.

Opäť nie je problém overiť korektnosť a 1-privátnosť uvedeného protokolu. Tieto dva protokoly poukazujú na možný vzťah medzi počtom kôl a počtom náhodných bitov potrebných na 1-privátne výpočty funkcií (čím viac náhodných bitov, tým lepšia kolová zložitosť).

Kushilevitz a Rosén sa zaoberajú práve vzťahom medzi počtom náhodných bitov a kolovou zložitosťou v 1-privátnych výpočtoch funkcie XOR . Pre jeden náhodný bit je potrebných a stačí $\Theta(n)$ kôl komunikácie. Pre $d \geq 2$ náhodných bitov je potrebných $\Omega(\log n/d)$ kôl komunikácie a stačí $O(\frac{\log n}{\log d})$ kôl komunikácie. Dolný odhad rozširujú aj na ostatné booleovské funkcie. Ukazujú, že pre výpočet funkcie so senzitivitou[2] $S(f)$ je v prípade jedného náhodného bitu potrebných $\Omega(S(f))$ a v prípade $d \geq 2$ náhodných bitov $\Omega(\frac{\log S(f)}{d})$ kôl.

Na túto prácu nadväzuje práca [8], kde sa autori venujú vzťahu medzi počtom náhodných bitov a kolovou zložitosťou pre t-privátne výpočty.

Vzťah medzi privátnosťou a komunikačnou zložitosťou

Odhadom komunikačnej zložitosti tzv. nevedomých[3] t-privátnych protokolov pre výpočet modulárneho sčítania sa zaoberajú Chor a Kushilevitz v [17]. Uvádzajú nevedomý protokol, ktorý t-privátne vypočíta modulárny súčet, pričom použijú $n \cdot \lceil \frac{t+1}{2} \rceil$ správ. Súčasne dokazujú tesný dolný odhad $\lceil n \cdot \frac{t+1}{2} \rceil$ správ.

Amortizovaná komunikačná zložitosť

Nech je daná funkcia $f : F^n \to F$ a k vstupných vektorov $x_1, \ldots, x_k$. Nech komunikačná zložitosť funkcie f je $g(n)$. Ak počítame hodnoty $f(x_i)$ postupne pre vektory $x_1, \ldots, x_k$, dostávame komunikačnú zložitosť $kg(n)$. Nemožno však navrhnúť protokol, ktorý by hodnoty $f(x_1), \ldots, f(x_k)$ vypočítal efektívnejšie, využijúc fakt, že už na začiatku máme k dispozícii všetky vstupy?

Touto otázkou sa zaoberajú Franklin a Yung v [9]. Konkrétne, ak f je n-árny XOR , potom na $\lfloor \frac{n}{2} \rfloor$-privátny výpočet jednoho vstupu je potrebných $\Omega(n^2)$ bitov komunikácie (t.j. na n vstupov potrebujeme pri sekvenčnom výpočte $\Omega(n^3)$ bitov). Ak však počítame hodnotu f pre n vstupov naraz, stačí nám $O(n^2 \log n)$ bitov komunikácie.

Otvorené problémy

Problém 3.3 ([24]) *Kushilevitz a Rosén dávajú dolný ($\Omega(\log n/d)$) a horný ($O(\frac{\log n}{\log d})$) odhad pre počet kôl komunikácie 1-privátneho výpočtu funkcie XOR za predpokladu, že hráči môžu použiť d náhodných bitov. Tradičným otvoreným problémom je zmenšenie rozdielu dolným a horným odhadom*

[2]Senzitivita funkcie f je počet jej argumentov, od ktorých funkcia závisí.

[3]Ide o protokoly, kde skutočnosť, či hráč P_i pošle v k-tom kole správu hráčovi P_j, závisí iba od hodnôt i, j, k, teda nie od vstupov ani náhodných vstupov.

Problém 3.4 **([9])** *Uviedli sme vzťah medzi počtom náhodných bitov a kolovou privátnou zložitosťou funkcie. Bolo by zaujímavé vyšetriť existenciu ďalších vzťahov medzi jednotlivými mierami (ako napríklad komunikačná zložitosť, úroveň privátnosti, pravdepodobnosť chyby a pod.)*

3.3.3 Redukovateľnosť a úplné funkcie

Kushilevitz, Micali a Ostrovsky v [21] zavádzajú redukovateľnosť funkcií takto:

Definícia 3.10 *Funkcia f je redukovateľná na funkciu g, ak existuje protokol, ktorý umožní n hráčom vypočítať hodnotu funkcie f n-privátne iba za pomoci čiernej skrinky (t.j. bez žiadnej ďalšej komunikácie), ktorá počíta funkciu g. To znamená, že v každom kole každý hráč odovzdá* **tajne** *(tzn. žiadny iný hráč sa túto informáciu nedozvie) argumenty pre funkciu g a čierna skrinka oznámi hodnotu tejto funkcie* **verejne** *(tzn. všetkých hráčom).*

Prirodzeným spôsobom môžeme definovať pojem **úplnosti** funkcie g. Funkcia g je teda úplná, práve keď ľubovoľná funkcia f je redukovateľná na g. Všimnime si, že ak by sme mali k dispozícii t-privátnu úplnú funkciu g, potom by bolo možné ľubovoľnú funkciu f vypočítať takisto t-privátne. To platí nielen pre model privátnych mnohoúčastníckych výpočtov, ale aj pre iné modely (ako napríklad pre kryptografickú privátnosť). Ak teda napríklad o nejakej funkcii f v modeli bezpodmienečnej privátnosti ukážeme, že je t-privátna a úplná pre nejakú triedu funkcií F, ak ďalej zistíme, že funkcia f je kryptograficky s-privátna, potom celá trieda funkcií F je kryptograficky s-privátna. Výsledky, získané v jednom modeli privátnych výpočtov, tak môžeme ľahko používať aj v iných modeloch.

V uvedenej práci sa autori zaoberajú skúmaním úplných funkcií pre mnohoúčastnícke n-privátne výpočty. Nasledujúce tvrdenie charakterizuje všetky úplné booleovské funkcie.

Veta 3.10 *Pre ľubovoľné $n \geq 2$, n-argumentová funkcia g je úplná, práve ak nie je n-privátna.*

Iným slovom: každá booleovská funkcia je buď "dostatočne jednoduchá", aby ju bolo možné vypočítať n-privátne, alebo má "dostatočnú vyjadrovaciu silu", aby pomocou nej bolo možné vypočítať všetky ostatné funkcie n-privátne.

3.3.4 Privátne výpočty nad spočítateľnými doménami

Doteraz sme sa zaoberali privátnymi výpočtami, pričom definičným oborom funkcie bola konečná množina. Avšak funkcie bývajú často definované nad spočítateľnými doménami (ako sú napr. množina všetkých reťazcov $\{0,1\}^*$ alebo prirodzených čísel).

Najprv si všimnime, že protokol, navrhnutý v dôkaze vety 3.6, nemožno v tomto prípade použiť. Jeho prvým krokom je totiž použitie perfektnej schémy pre zdieľania tajomstva. Chor a Kushilevitz však v práci [18] ukazujú, že nad spočítateľnou doménou neexistuje perfektná schéma pre zdieľanie tajomstva. Ako uvidíme neskôr, veta 3.6 v tomto modeli neplatí (t.j. existujú funkcie, ktoré nie sú ani 1-privátne).

Problémom privátnych výpočtov nad spočítateľnými doménami sa zaoberajú Chor, Geréb-Graus a Kushilevitz v [14]. Ukazujú, že privátnosť funkcie definovanej nad spočítateľnou doménou úzko súvisí s **komunikačnou zložitosťou tejto funkcie.** Hlavné výsledky tejto práce možno zhrnúť v troch tvrdeniach. Prvé z týchto tvrdení dáva postačujúcu podmienku pre $\lfloor\frac{n-1}{2}\rfloor$-privátnosť funkcií:

Veta 3.11 ([14]) [4] *Nech* $f : (\{0,1\}^*)^n \to \{0,1\}$ *je funkcia a* $0 < \varepsilon \leq \frac{1}{2}$*. Uvažujme protokoly, kde pravdepodobnosť správneho výsledku je aspoň* $\frac{1}{2} + \varepsilon$*. Potom ak možno komunikačnú zložitosť* f *ohraničiť na* d *bitov, kde* d *je konštanta, tak* f *je* $\lfloor\frac{n-1}{2}\rfloor$*-privátna.*

Druhé tvrdenie ukazuje, že existujú funkcie, ktoré nie sú ani 1-privátne:

Veta 3.12 ([14]) *Neexistuje ani 1-privátny protokol pre súčet* $n \geq 3$ *celých čísel.*

Tretie tvrdenie dáva charakterizáciu booleovských $\lfloor\frac{n-1}{2}\rfloor$-privátnych funkcií (v kombinácii s faktom, že 1-privátna booleovská funkcia je aj $\lfloor\frac{n-1}{2}\rfloor$-privátna[5]).

Veta 3.13 ([14]) *Ak je funkcia* f *1-privátna, potom je jej komunikačná zložitosť ohraničená na* d *bitov, kde* d *je nejaká konštanta.*

Otvorené problémy

Problém 3.5 ([14]) *Uviedli sme, že výsledok vo vete 3.11 možno generalizovať na funkcie so všeobecným oborom hodnôt. Nie je známe, či je možné rozšíriť aj výsledok vo vete 3.13 na iné, ako booleovské obory hodnôt.*

Problém 3.6 ([14]) *V tejto kapitole sme sa venovali mimo iné aj hierarchii privátnosti pre konečné domény. Techniky, použité v dôkaze vety 3.7 však nemožno použiť pre* $t \leq \lfloor\frac{n-1}{2}\rfloor$*. Veta 3.12 naznačuje v spočítateľných doménach možnú existenciu ďalších tried privátnosti práve pre takéto* t*. Otázka hierarchie privátnosti pre spočítateľné domény tak zostáva otvorená.*

Problém 3.7 ([*]) *Ak uvažujeme spočítateľné domény, má zmysel uvažovať aj o vypočítateľnosti funkcií. Konkrétne, vo vyššie uvedenom modeli umožňujeme hráčom počítať aj funkcie, ktoré nie sú vypočítateľné (napríklad riešiť problém zastavenia).*

Obmedzíme teda výpočty účastníkov na vypočítateľné funkcie. V takomto novom modeli prirodzene nemožno vypočítať privátne žiadnu nevypočítateľnú funkciu. Existuje však vypočítateľná funkcia, pre ktorú existuje privátny protokol v pôvodnom modeli, ale neexistuje privátny protokol v modeli s obmedzením na vypočítateľnosť?

[4] Tvrdenie uvádzame pre booleovské funkcie, je však možné ho rozšíriť na všeobecné funkcie — bližšie pozri [14]

[5] Dôkaz tohoto tvrdenia možno nájsť napríklad v [16]. Aj keď ide o dôkaz pre konečné domény, je priamo rozšíriteľný na spočítateľné domény.

3.3.5 Aplikácie

Na záver tejto kapitoly uvedieme prehľad niektorých aplikácií mnohoúčastníckeho modelu privátnych výpočtov. Uvedené aplikácie buď priamo súvisia s modelom výpočtov uvedeným v tejto kapitole, alebo z neho vychádzajú.

Privátne databázové dotazy

Verejne prístupné databázy sú dôležitým zdrojom informácií. Používanie takejto databázy môže veľa prezradiť o samotnom používateľovi. Operátor databázy, ktorý by zhromažďoval údaje o tom, na ktoré položky databázy sa pýtali jednotliví používatelia, môže týmto spôsobom získať nežiadúce privátne informácie. Preto je dôležité uvažovať nielen o ochrane dát v databáze voči nežiadúcemu prístupu, ale aj o ochrane užívateľa.

Uvažujme nasledujúci model. Nech U je používateľ, a D je databáza. Nech používateľ vlastní číslo $x \in \{1, 2, \ldots, n\}$ a databáza binárny reťazec $y = (y_1, y_2, \ldots, y_n)$. Zadefinujme funkciu $f(x, y) = y_x$. Komunikáciu (jej zápis označme t) medzi používateľom a databázou budeme považovať za **privátnu**, ak pre ľubovoľné dve hodnoty x a x' také, že $f(x, y) = f(x', z)$, databáza nemôže rozlíšiť medzi vstupmi používateľa x a x' (t.j. $Pr(t|x, y) = Pr(t|x', y)$).

Poznámka: Všimnime si podobnosť tejto definície s definíciou dvojúčastníckej privátnosti.

Ľahko možno ukázať (viď. napríklad [15]), že aby bola zaručená podmienka privátnosti, je potrebné prekomunikovať $O(n)$ bitov. To znamená, že protokol, kde databáza pošle používateľovi celý svoj obsah, je v tomto prípade optimálny.

Chor, Goldreich, Kushilevitz a Sudan v práci [15] rozoberajú, či je možné dosiahnuť lepšiu komunikačnú zložitosť za predpokladu, že máme k dispozícii viacero navzájom nekomunikujúcich kópií tejto databázy (ide o tzv. replikáciu databázy).

Príklad: Uvažujme prípad dvoch databáz D_1 a D_2 a nasledujúci protokol (používateľ chce získať i-ty bit databázy):

1. U náhodne vyberie podmnožinu $S \subseteq \{1, 2, \ldots, n\}$.
2. U pošle databáze D_1 množinu S a databáze D_2 množinu $S' = S \oplus i$.
3. Databáza D_1 pošle U správu $\sum_{k \in S} x_k \bmod 2$.
4. Databáza D_2 pošle U správu $\sum_{k \in S'} x_k \bmod 2$.

Tento protokol je triviálne privátny, pričom databázy posielajú účastníkovi U iba po 1 bite. Žiaľ, celková komunikačná zložitosť zostáva $O(n)$.

Aj keď sa nám v tomto prípade komunikačnú zložitosť nepodarilo znížiť, vychádzajú z tohoto protokolu v práci [15] protokoly:

- s komunikačnou zložitosťou $O(n^{\frac{1}{3}})$ pre dve kópie databázy,
- s komunikačnou zložitosťou $O(n^{\frac{1}{k}})$ pre konštantný počet k kópií databázy,

- s polylogaritmickou komunikačnou zložitosťou pre $\frac{1}{3}\log_2 n$ kópií databázy.

Privátne databázové dotazy teda umožňujú používateľovi získať i-ty bit dátového reťazca y, pričom reťazec je k dispozícii prostredníctvom $k \geq 2$ identických navzájom nekomunikujúcich databáz, tak, že je splnená podmienka zachovania privátnosti používateľa (žiadna databáza sa nedozvie žiadnu dodatočnú informáciu o vstupe i). Gertner, Ishai, Kushilevitz a Malkin v [10] sa zaoberajú tzv. **symetricky privátnymi databázovými dotazmi**. V tomto modeli je vyžadovaná nielen ochrana používateľa, ale aj databázy.

Tým sa nám celý problém redukuje na klasický problém mnohoúčastníckych privátnych výpočtov. Je daná množina účastníkov $\{U, D_1, \ldots, D_k)$, pričom účastník U má na vstupe číslo x a účastníci $D_1, \ldots, D_k$ majú na vstupe (rovnaký) n-bitový reťazec y. Úlohou je 1-privátne vypočítať hodnotu funkcie $f(x, y) = y_x$.

Aj keď ide o klasický problém, použitím klasických metód (konštrukcia $\lfloor\frac{n-1}{2}\rfloor$-privátnych protokolov podľa vety 3.6) získavame protokoly s neúnosne vysokou komunikačnou zložitosťou. Autori v článku uvádzajú niekoľko protokolov s výrazne lepšou komunikačnou zložitosťou:

- Protokol pre $k + 1$ databáz s komunikačnou zložitosťou $O(C_k(n) \log n)$, kde $C_k(n)$ je komunikačná zložitosť niektorého protokolu pre k databázové privátne dotazy.

- Protokol pre k databázové symetricky privátne dotazy s komunikačnou zložitosťou $O(\log n \cdot n^{\frac{1}{2k-1}})$ pre ľubovoľnú konštantu $k \geq 2$.

- Protokol pre $O(\log n)$ databázové symetricky privátne dotazy s komunikačnou zložitosťou $O(\log^2 n \cdot \log\log n)$.

Poznámka: Komunikačnú zložitosť možno zlepšiť z dvoch dôvodov:

- Ide o konkrétnu funkciu, takže sa stačí zamerať na protokoly, počítajúce priamo túto funkciu.

- Funkcia f má síce $n+1$ vstupov, je však definovaná iba v prípade, keď sú vstupy databáz rovnaké.

Problém 3.8 ([15]) *Zaujímavé by bolo nájsť dolné odhady komunikačnej zložitosti pre privátne databázové dotazy. Predpokladá sa, že pre k kópií databázy je potrebných* $\Omega(n^{\frac{1}{k+1}})$ *bitov komunikácie. Protokoly uvedené v [15] ukazujú, že komunikačná zložitosť privátneho databázového dotazu je* $O(n^{\frac{1}{k}})$. *Ak by teda aj vyššie uvedená hypotéza bola pravdivá, stále nám zostáva medzera medzi horným a dolným odhadom.*

Problém 3.9 ([10],[*]) *Aké výsledky možno dosiahnuť využitím techník uvedených v [10] alebo podobných na symetricky privátne dotazy na bloky dát (amortizovaná komunikačná zložitosť), prípadne na dotazy s vyššou úrovňou privátnosti? Aký je vzťah medzi úrovňou privátnosti a komunikačnou zložitosťou privátnych databázových dotazov?*

Problém 3.10 ([*]) *Privátnosť (resp. symetrickú privátnosť) databázového dotazu by bolo možné zabezpečiť aj bez replikácie databázy, a to za pomoci účastníkov, ktorí nemajú k dispozícii žiadny vstup. Aká je komunikačná zložitosť nášho problému v takomto prípade? Je možné pomocou takýchto "dôverníkov" dosiahnuť výsledky s podobnou komunikačnou zložitosťou, ako u replikácie databázy?*

Voľby

Tradičný problém volieb možno takisto formulovať ako problém mnohoúčastníckych privátnych výpočtov. V tomto prípade máme n voličov (účastníkov $P_1, \ldots, P_n$), pričom hlas voliča P_i označíme x_i. Výsledkom volieb je hodnota funkcie $f(x_1, \ldots, x_n)$. Ak máme napríklad hlasovanie áno/nie, funkciu f môžeme definovať takto:

$$f(x_1, \ldots, x_n) = \begin{cases} 1, & \text{ak } \sum x_i > \frac{n}{2}, \\ 0, & \text{inak.} \end{cases}$$

V takomto prípade môžeme tradičnými metódami (za pomoci vety 3.6) dosiahnuť, že menšina účastníkov nemôže zistiť žiadnu informáciu o tom, ako hlasovali ostatní účastníci.

Zdalo by sa, že pre naše potreby by stačilo, ak by sme nevedeli získať informáciu o tom, ako hlasoval konkrétny účastník volieb. To by zodpovedalo klasickému spôsobu "vhodenia" hlasovacieho lístka do urny. Opodstatnenosť vyššie uvedenej (silnejšej) požiadavky na privátnosť ukazuje nasledujúci príklad.

Príklad: V niektorých malých talianskych dedinách volebný systém umožňuje voličovi uviesť na hlasovacom lístku kandidátov v ľubovoľnom poradí podľa vlastných preferencií. Politickým lídrom tak stačí priradiť jednotlivým voličom rôzne permutácie (permutácií je dostatočne veľa, aby bolo možné vybrať dosť permutácií s "vhodným" poradím na prvých miestach) a "požiadať" týchto voličov, aby na svojom hlasovacom lístku uviedli práve túto permutáciu. Ak sa potom niektorá z takýchto permutácií nevyskytne v hlasovacej urne, líder môže zistiť, ktorí konkrétni voliči nevolili "správne", čo môže byť zdrojom neskorších perzekúcií.

Ďalším problémom, súvisiacim s voľbami, sa zaoberajú Benaloh a Tunistra v [5] a Sako a Kilian v [28]. Poukazujú na problém predchádzajúcich navrhnutých protokolov. Protokoly totiž umožňujú každému účastníkovi "odniesť" si so sebou "potvrdenie" o vlastnom hlasovaní. Táto zdanlivo nepodstatná skutočnosť má však nepríjemný dôsledok — môže sa stať zdrojom manipulácií volieb, ak niekto po voličoch začne tieto "potvrdenia" vyžadovať. [5, 28] uvádzajú privátne protokoly, kde účastníci nemôžu dokázať, ako hlasovali.

Problém 3.11 ([*]) *V predchádzajúcich úvahách sme použili vetu 3.6 na získanie $\lfloor \frac{n-1}{2} \rfloor$-privátneho protokolu pre voľby. Je možné nájsť volebnú funkciu a protokol s vyššou úrovňou privátnosti? Ak áno, pre ktoré volebné funkcie?*

Charakterizácia obvodov s lineárnou veľkosťou pomocou privátnosti

Uvažujme booleovské obvody, ktoré majú vstupy $x_1, \ldots, x_n$ a ich negácie $\bar{x_1}, \ldots, \bar{x_n}$. Obvody budú pozostávať z AND a OR hradiel so vstupným stupňom 2 a ľubovoľným výstupným stupňom. Pre obvod O označme $m_g(O)$ počet hradiel v obvode.

Označme ďalej f_n zúženie funkcie $f : \{0,1\}^* \to \{0,1\}$ na doménu $\{0,1\}^n$. Potom hovoríme, že funkcia f má **obvod s lineárnou veľkosťou**, ak existuje konštanta k taká, že pre všetky n existuje obvod o veľkosti nanajvýš kn, ktorý vypočíta funkciu f_n.

Skúmanie dolných odhadov veľkosti obvodov je jedným z hlavných cieľov teórie zložitosti. Kým Shannon už v roku 1947 [30] dokázal, že skoro všetky funkcie vyžadujú obvod exponenciálnej veľkosti, pre funkcie vypočítateľné nedeterministicky v polynomiálnom čase (NP funkcie) je doteraz najlepší známy dolný odhad je lineárny. Doteraz nie je známa NP funkcia, ktorá by nemohla byť vypočítaná obvodom lineárnej veľkosti. Preto je výskum triedy funkcií majúcich obvod lineárnej veľkosti dôležitý.

Kushilevitz, Ostrovsky a Rosén sa v článku [23] zaoberajú pomerne prekvapujúcim vzťahom medzi triedou funkcií, ktoré majú obvod lineárnej veľkosti, a mnohoúčastníckymi privátnymi protokolmi. Dokazujú nasledujúce tvrdenie.

Veta 3.14 *Nech f je booleovská funkcia. Potom f má obvod lineárnej veľkosti práve ak pre výpočet f existuje 1-privátny protokol používajúci konštantný počet náhodných bitov.*

Toto tvrdenie nám dáva charakterizáciu triedy funkcií majúcich obvod lineárnej veľkosti pomocou veľmi odlišného pojmu privátnosti funkcií. Súčasne konštrukcia [23] dáva vzťah medzi hĺbkou obvodu a počtom kôl príslušného privátneho protokolu.

Problém 3.12 ([23]) *Dokážte o niektorej NP funkcii f, že ju nemožno vypočítať 1-privátnym protokolom používajúcim konštantný počet bitov (na základe vety 3.14 možno usúdiť, že pôjde o ťažký problém).*

Problém 3.13 ([23]) *Každú funkciu možno vypočítať* 1*-privátne randomizovaným protokolom (pozri napríklad vetu 3.6). Nanešťastie, čo sa týka dolných odhadov počtu náhodných bitov, potrebných na* 1*-privátny výpočet funkcie f_n, jediným známym výsledkom je, že prakticky žiadne funkcie nemožno vypočítať deterministicky (pozri vetu 3.1). V tomto kontexte vyznieva zaujímavý aj problém hľadania funkcií, ktorých dolný odhad počtu náhodných bitov je nejaká konštanta d.*

Záver

Úlohou tejto práce bolo podať prehľad o informačno-teoretickom prístupe k privátnym výpočtom. Prinášame podrobný prehľad hlavných výsledkov dosiahnutých v tejto oblasti. V práci sa snažíme podať aj neformálny popis uvedených výsledkov a ukázať ich vzťah k príbuzným disciplínam (kryptografická privátnosť), na druhej strane, v mnohých prípadoch oproti pôvodnej literatúre namiesto "intuitívneho" chápania niektorých pojmov zavádzame a používame formálny model.

Aj keď ide prevažne o prácu kompilačnú, uvádzame v nej aj niektoré vlastné výsledky (viď. napr. dôkaz vety 2.11). Navyše, niektoré z pôvodných článkov obsahovali nepresnosti, prípadne aj chyby, ktoré sme sa snažili v tejto práci odstrániť. V niektorých prípadoch sa nám podarilo rozšíriť platnosť výsledkov (viď. napr. v kapitole 2 rozšírenie platnosti všetkých tvrdení z konečných protokolov na protokoly končiace s pravdepodobnosťou 1).

Záverečná časť každej kapitoly obsahuje podrobnú bibliografiu v kapitole uvedených výsledkov, ako aj prehľad ďalších výsledkov a odborných prác, súvisiacich s problematikou. Takisto sa snažíme formulovať otvorené problémy pre ďalšie riešenie. Práca tak môže slúžiť ako základný zdroj informácií o danej oblasti, aj ako zdroj doposiaľ nevyriešených problémov v oblasti bezpodmienečnej privátnosti.

Literatúra

[1] Reuven Bar-Yehuda, Benny Chor, and Eyal Kushilevitz. Privacy, additional information, and communication (extended abstract). In *Proceedings, Fifth Annual Structure in Complexity Theory Conference*, pages 55–65, Barcelona, Spain, 8–11 July 1990. IEEE Computer Society Press.

[2] Donald Beaver. Perfect privacy for two-party protocols. In J. Feigenbaum and M. Meritt, editors, *Proceedings of the DIMACS Workshop on Distributed Computing and Cryptography*, Princeton, NJ, October 1989.

[3] Donald Beaver. Perfert privacy for two party protocol. Technical Report TR-11-90, Harvard University, 1989.

[4] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD thesis, Technion – Israel Institute of Technology, June 1996.

[5] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, pages 544–553, Montréal, Québec, Canada, 23–25 May 1994.

[6] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 1–10, Chicago, Illinois, 2–4 May 1988.

[7] Garrett Birkhoff and Saunders MacLane. *Prehľad modernej algebry.* ALFA Bratislava, 1979.

[8] Carlo Blundo, Alfredo De Santis, Giuseppe Persiano, and Ugo Vaccaro. On the number of random bits in totally private computation. In Zoltán Fülöp and Ferenc Gécseg, editors, *Automata, Languages and Programming, 22nd International Colloquium*, volume 944 of *Lecture Notes in Computer Science*, pages 171–182, Szeged, Hungary, 10–14 July 1995. Springer-Verlag.

[9] Matthew Franklin and Moti Yung. Communication complexity of secure computation (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on the Theory of Computing*, pages 699–710, Victoria, British Columbia, Canada, 4–6 May 1992.

[10] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting data privacy in private information retrieval schemes. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, Dallas, Texas, 24–26 May 1998.

[11] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, 25–27 May 1987.

[12] Shafi Goldwasser. Multi-party computations: Past and present. In *Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing*, pages 1–6, Santa Barbara, California, 21–24 August 1997. Invited Talk.

[13] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 11–19, Chicago, Illinois, 2–4 May 1988.

[14] Benny Chor, Mihály Geréb-Graus, and Eyal Kushilevitz. On the structure of the privacy hierarchy. *Journal of Cryptology*, 7(1):53–60, Winter 1994.

[15] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *36th Annual Symposium on Foundations of Computer Science*, pages 41–50, Milwaukee, Wisconsin, 23–25 October 1995. IEEE.

[16] Benny Chor and Eyal Kushilevitz. A zero-one law for Boolean privacy (extended abstract). In *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, pages 62–72, Seattle, Washington, 15–17 May 1989.

[17] Benny Chor and Eyal Kushilevitz. A communication-privacy tradeoff for modular addition. *Information Processing Letters*, 45:205–210, 1993.

[18] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains. *Journal of Cryptology*, 6(2):87–95, 1993.

[19] Benny Chor and Netta Shani. The privacy of dense symmetric functions. *Computational Complexity*, 5(1):43–59, 1995.

[20] Eyal Kushilevitz and Yishay Mansour. Randomness in private computations. In *Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing*, pages 181–190, Philadelphia, Pennsylvania, USA, 23–26 May 1996.

[21] Eyal Kushilevitz, Silvio Micali, and Rafail Ostrovsky. Reducibility and completeness in multi-party private computations. In *35th Annual Symposium on Foundations of Computer Science*, pages 478–489, Santa Fe, New Mexico, 20–22 November 1994. IEEE.

[22] Eyal Kushilevitz and Noam Nisan. *Communication Complexity.* Cambridge University Press, 1997.

[23] Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Characterizing linear size circuits in terms of privacy. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 541–550, Philadelphia, Pennsylvania, 22–24 May 1996.

[24] Eyal Kushilevitz and Adi Rosén. A randomnesss-rounds tradeoff in private computation. In Yvo G. Desmedt, editor, *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 397–410. Springer-Verlag, 21–25 August 1994.

[25] Eyal Kushilevitz. Privacy and communication complexity. In *30th Annual Symposium on Foundations of Computer Science*, pages 416–421, Research Triangle Park, North Carolina, 30 October–1 November 1989. IEEE.

[26] Eyal Kushilevitz. Privacy and communication complexity. *SIAM Journal on Discrete Mathematics*, 5(2):273–284, May 1992.

[27] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27(2):228–234, April 1980.

[28] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology—EUROCRYPT 95*, volume 921 of *Lecture Notes in Computer Science*, pages 393–403. Springer-Verlag, 21–25 May 1995.

[29] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[30] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423,623–656, 1948.

[31] Martin Stanek. Kryptológia. nepublikovaný materiál, 25 November 1997.

[32] Andrew C. Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science*, pages 160–164, Chicago, Illinois, 3–5 November 1982. IEEE.

Príloha A

Schémy pre zdieľanie tajomstva

Pod pojmom schémy pre zdieľanie tajomstva rozumieme protokoly, ktorými možno medzi n hráčov rozdistribuovať časti nejakého tajomstva tak, aby ho bolo možné zrekonštruovať iba za určitých konkrétnych podmienok. Skupinu hráčov, ktorá týmto podmienkam vyhovuje, nazveme **kvalifikovaná skupina**. V tejto kapitole sa budeme zaoberať iba tzv. **threshold** schémami.

Označenie A.1 *Pod pojmom (t, n)-threshold schéma pre zdieľanie tajomstva budeme rozumieť schému pre zdieľanie tajomstva, pri ktorej je tajomstvo rozdistribuované medzi n hráčov a kvalifikovaná je ľubovoľná skupina hráčov T taká, že $|T| \geq t$.*

Schému pre zdieľanie tajomstva budeme určovať vždy dvoma algoritmami:

Distribúcia tajomstva, t.j. postup, akým pre každého účastníka vygenerujeme jeho podiel tajomstva;

Rekonštrukcia tajomstva, t.j. postup, akým kvalifikovaná skupina dokáže zrekonštruovať obsah tajomstva.

Zvyšok kapitoly je organizovaný nasledovne. Najprv uvedieme príklad schémy pre zdieľanie tajomstva a ukážeme niektoré jej vlastnosti (nekvalifikovaná skupina hráčov zo svojich podielov nezíska z informačno-teoretického hľadiska žiadnu informáciu o obsahu tajomstva). Potom sa budeme venovať možnostiam výpočtu funkcií nad podielmi tajomstva.

Keďže schémy pre zdieľanie tajomstva nie sú hlavným predmetom tejto práce, obmedzíme sa v tejto kapitole iba na tzv. Shamirovu schému. Uvedené výsledky však možno generalizovať, pozri napr. [4]

A.1 Shamirova schéma pre zdieľanie tajomstva

Uvažujme konečné pole F o veľkosti q (pričom q je mocninou prvočísla) $q > n + 1$. Označme jednotlivých hráčov $P_1, \ldots, P_n$. Zostrojíme (t, n)-threshold schému.

A.1.1 Distribúcia tajomstva

Nech je dané tajomstvo $s \in F$. Distribúcia tajomstva bude prebiehať podľa nasledujúceho algoritmu.

- Nezávisle s uniformnou distribúciou pravdepodobnosti vyberieme $t-1$ náhodných prvkov $r_1, \ldots, r_{r-1}$ z F. Definujme polynóm $p(x)$ nad poľom F takto (všimnime si, že $p(0) = s$):

$$p(x) = r_{t-1}x^{t-1} + r_{t-2}x^{t-2} + \ldots + r_1 x + s.$$

- Každý účastník P_i dostane podiel tajomstva $s_i = p(i)$.

A.1.2 Rekonštrukcia tajomstva

Nech $T = \{P_{i_1}, \ldots, P_{i_l}\}$ je kvalifikovaná skupina hráčov (t.j. $|T| = l \geq t$); nech hráč P_{i_j} vlastní podiel tajomstva s_{i_j}. Takáto množina môže vypočítať ľubovoľnú hodnotu $p(x)$ pomocou Lagrangeovej interpolácie:

$$p(x) = \sum_{j=1}^{t} s_{i_j} \prod_{d \neq j} \frac{i_d - x}{i_d - i_j}.$$

Pôvodné tajomstvo teda zrekonštruujeme dosadením 0 za x v tomto polynóme.

Príklad: Uvažujme Shamirovu $(3,5)$-schému nad poľom Z_7. Nech tajomstvo je $s = 3$. Zvolíme polynóm druhého stupňa $p(x) = 2x^2 + x + 3$. Jednotlivým hráčom teda (v tomto poradí) rozdistribuujeme ich podiely tajomstva takto: $s_1 = 6$, $s_2 = 6$, $s_3 = 3$, $s_4 = 4$ a $s_5 = 2$. Ak vezmeme napríklad skupinu hráčov $\{P_2, P_4, P_5\}$, dostaneme Lagrangeovou interpoláciou polynóm

$$6 \cdot \frac{(4-x)(5-x)}{(4-2)(5-2)} + 4 \cdot \frac{(2-x)(5-x)}{(2-4)(5-4)} + 2 \cdot \frac{(2-x)(4-x)}{(2-5)(4-5)},$$

a dosadením $x = 0$ dostaneme zrekonštruované tajomstvo 3.

A.1.3 Vlastnosti Shamirovej schémy

Ukážeme, že žiadna nekvalifikovaná skupina hráčov použitím Shamirovej schémy nezíska žiadnu informáciu o zdieľanom tajomstve.

Lema A.1 *Nech $s, s' \in F$ sú dve tajomstvá a nech $S = \{s_1, \ldots, s_l\}$ $(l < t)$ sú podiely tajomstva nekvalifikovanej skupiny hráčov. Potom*

$$Pr(S|s) = Pr(S|s').$$

Dôkaz: Bez ujmy na všeobecnosti uvažujme nekvalifikovanú skupinu hráčov $T = \{P_1, \ldots, P_{t-1}\}$ s podielmi tajomstva $S = \{s_1, \ldots, s_{t-1}\}$ (dôkaz pre inú skupinu hráčov prebieha obdobne). Pokúsme sa určiť koeficienty $r_1, \ldots, r_{t-1}$ polynómu použitého na konštrukciu Shamirovej schémy. Pre tajomstvo s musí platiť:

$$\begin{aligned}
s_1 &= r_{t-1} + r_{t-2} + \ldots + r_1 + s \\
s_2 &= r_{t-1}.2^{t-1} + r_{t-2}.2^{t-2} + \ldots + r_1.2 + s \\
&\ldots \\
s_{t-1} &= r_{t-1}.(t-1)^{t-1} + r_{t-2}.(t-1)^{t-2} + \ldots + r_1.(t-1) + s
\end{aligned}$$

Pre každé s máme teda sústavu $(t-1)$ rovníc o $(t-1)$ neznámych. Keďže determinant sústavy (jedná sa o Vandermondov determinant) je v našom prípade nenulový, naša sústava má jediné riešenie. Pre každé tajomstvo s teda existuje práve jedna sada koeficientov určujúca taký polynóm, ktorý hráčom z T určuje podiely tajomstva podľa S. Vzhľadom k spôsobu výberu koeficientov teda platí $Pr(S|s) = Pr(S|s') = \frac{1}{|F|^{t-1}}$, čo bolo treba dokázať.

Pre menšiu skupinu l hráčov postupujeme obdobne, podiely tajomstiev doplníme do počtu $t-1$. To možno urobiť $|F|^{t-l-1}$ spôsobmi a teda v tomto prípade bude $Pr(S|s) = Pr(S|s') = \frac{1}{|F|^l}$. $\square$

A.2 Počítanie nad podielmi tajomstva

Je daných k tajomstiev $s_1, \ldots, s_k$, ktoré sú rozdistribuované medzi jednotlivých hráčov $\{P_1, \ldots, P_n\}$ pomocou Shamirovej (t,n)-threshold schémy pre zdieľanie tajomstva nad konečným poľom F. Hráč P_i teda vlastní podiely $s_{i1}, s_{i2}, \ldots, s_{ik}$ jednotlivých tajomstiev $s_1, s_2, \ldots, s_k$ (v tomto poradí).

Našou úlohou bude počítať funkcie nad týmito tajomstvami a to bez toho, aby hráči boli nútení rekonštruovať jednotlivé tajomstvá. Ukážeme, že to ide bez toho, aby hráča získali akúkoľvek ďalšiu informáciu o pôvodných tajomstvách. Výsledok, ktorý získame, bude opäť distribuovaný medzi jednotlivých hráčov pomocou Shamirovej (t,n)-threshold schémy.

Vzhľadom k tomu, že sa v našich úvahách obmedzujeme na konečné polia, postačí, keď sa budeme zaoberať elementárnymi operáciami sčítanie a násobenie. Z týchto operácií je možné zostrojiť ľubovoľnú funkciu nad takýmto poľom (pričítanie a vynásobenie konštantou možno ľahko previesť na sčítanie).

Poznámka: Schémy s vlastnosťou, ktorú vyjadruje u Shamirovej schémy lema A.1, sa obvykle zvyknú nazývať **perfektné schémy pre zdieľanie tajomstva.**

A.2.1 Sčítanie nad podielmi tajomstva

Majme teda dve tajomstvá s_1, s_2, nech ďalej $p_1(x)$ a $p_2(x)$ sú polynómy ($(t-1)$-vého stupňa) použité na vygenerevanie podielov tajomstva v Shamirovej (t,n)-threshold schéme.

Položme $p_3(x) = p_1(x) + p_2(x)$. Všimnime si, že tento polynóm má v bode 0 hodnotu $s_1 + s_2$ a jeho stupeň je opäť $t-1$. Môžeme teda vytvoriť Shamirovu (t, n)-threshold schému pomocou tohoto polynómu. Uvedomme si ale, že každý hráč môže svoj podiel vypočítať aj bez znalosti podielov s_1 a s_2 ostatných hráčov. Pre každého hráča P_i totiž platí $s_{i3} = p_3(i) = p_1(i) + p_2(i) = s_{i1} + s_{i2}$.

Keďže sme nerozdistribuovali žiadnu ďalšiu informáciu, hráči sa nemohli týmto krokom dozvedieť nič nové o jednotlivých tajomstvách. Navyše polynóm $p_3(x)$ je náhodný polynóm.

Z vyššiuevedeného ako priamy dôsledok dostávame nasledujúce tvrdenie.

Lema A.2 (O lineárnych funkciách) *Nech $s_1, \ldots, s_k$ sú tajomstvá rozdistribuované medzi hráčmi $P_1, \ldots, P_n$ pomocou Shamirovej (t, n)-threshold schémy. Potom pre ľubovoľnú lineárnu funkciu*

$$F(x_1, \ldots, x_k) = a_0x_0 + \cdots + a_kx_k$$

možno hodnotu $F(s_1, \ldots, s_n)$ vypočítať bez akejkoľvek komunikácie medzi hráčmi tak, že výsledok bude distribuovaný medzi jednotlivých hráčov vo forme podielov Shamirovej (t, n)-threshold schémy.

Dôsledok A.3 (O maticiach) *Nech $s_1, \ldots, s_k$ sú tajomstvá rozdistribuované medzi hráčmi $P_1, \ldots, P_n$ pomocou Shamirovej (t, n)-threshold schémy. Nech A je ľubovoľná konštantná matica typu $k \times k$. Označme*

$$(s'_1, \ldots, s'_k) = (s_1, \ldots, s_k)A.$$

Potom hodnoty $s'_1, \ldots, s'_k$ možno vypočítať bez akejkoľvek komunikácie medzi hráčmi tak, že výsledok bude distribuovaný medzi jednotlivých hráčov vo forme podielov Shamirovej (t, n)-threshold schémy.

Dôkaz: Použijeme k krát lemu o lineárnych funkciách. □

A.2.2 Násobenie nad podielmi tajomstva

Opäť máme dve tajomstvá s_1, s_2 a nech ďalej $p_1(x)$ a $p_2(x)$ sú polynómy ($(t-1)$-vého stupňa) použité na vygenerevanie podielov tajomstva v Shamirovej (t, n)-threshold schéme. Predpokladajme ďalej $2t - 1 \leq n$.

Položme $p_3(x) = p_1(x)p_2(x)$. Tento polynóm má v bode 0 hodnotu $s_1.s_2$ a súčasne podiel v Shamirovej schéme môže každý hráč vypočítať zo svojich vlastných podielov na s_1 a s_2 takto: $s_{i3} = p_3(i) = p_1(i)p_2(i) = s_{i1}s_{i2}$. Polynóm $p_3(x)$ však môže mať stupeň až $2(t-1)$, preto už ide nie o (t, n)-threshold ale o $(2t-1, n)$-threshold schému. Keďže (podľa predpokladu) $2t - 1 \leq n$, stále je možné tajomstvo $s_3 = s_1s_2$ zrekonštruovať z vypočítaných podielov. Namiesto t hráčov však na tento účel potrebujeme $2t - 1$ hráčov.

Našim cieľom v nasledujúcich niekoľkých odstavcoch bude získať podiely tajomstva s_3 jednotlivých hráčov vo forme podielov (t, n)-threshold schémy.

Všimnime si, že na rozdiel od sčítania, v tomto prípade nezískavame náhodný polynóm. O polynóme $p_3(x)$ totiž minimálne platí, že je reducibilný. Ak by účastníci tento polynóm neskôr zrekonštruovali, mohli by zistiť informácie o členoch, ktorých vynásobením tento polynóm vznikol.

Príklad: Predpokladajme, že máme troch účastníkov a že pracujeme nad poľom Z_5. Nech hráči P_2 a P_3 vlastnia tajomstvá $s_2 = 1$ a $s_3 = 3$ (v tomto poradí), ktorých podiely rozdistribuovali medzi hráčov pomocou náhodných polynómov $x + 1$ a $x + 3$ (oba tieto polynómy sú ireducibilné nad Z_5). Uplatnením súčinu dostaneme polynóm $x^2 + 4x + 3$ (rozdistribuovaný medzi hráčov). Ak sa hráči rozhodú toto tajomstvo zrekonštruovať, získa každý z nich tento polynóm. Tento polynóm však možno jednoznačne rozložiť (až na asociovanosť). V kombinácii so svojim podielom tajomstva sa môže takto napríklad hráč P_2 dozvedieť vstup hráča P_3. Takáto situácia by nemohla nastať, ak by išlo o náhodný polynóm.

Poznámka: Problém nie je v tom, že by hráči priamo výpočtom nad svojou lokálnou informáciou získali nejakú informáciu o vstupoch iných hráčov. Problémy nastávajú až vtedy, keď sa rozhodne príslušný počet hráčov zrekonštruovať pôvodné tajomstvo. V takom prípade dôjde k výmene informácií a ak polynóm, ktorý účastníci rekonštrukcie získajú, obsahuje "v sebe" aj časť histórie svojho výpočtu, ľubovoľný hráč túto informáciu môže získať (v našom prípade to bola spolu s lokálnou informáciou aj informácia o vstupoch ostatných hráčov, môže však ísť aj o čiastočnú informáciu). Preto je potrebné pri rekonštrukciách dôsledne pracovať s náhodnými polynómmi.

Aby sme teda ďalej pracovali s náhodným polynómom, musíme výsledné podiely tajomstva počítať v dvoch krokoch: **randomizácia** polynómu $p_3(x)$ a **zníženie stupňa** polynómu $p_3(x)$.

Randomizácia

Tento krok prebehne nasledovne: každý hráč P_i vygeneruje Shamirovu $(2t-1, n)$-threshold schému, pričom zdieľané tajomstvo bude 0. Jednotlivé podiely rozdistribuuje medzi hráčov a každý hráč si pričíta príslušné podiely ku svojmu podielu $p_3(x)$. Výsledný polynóm:

- je náhodný (keďže vznikol sčítaním $p_3(x)$ a n náhodných polynómov),
- reprezentuje pôvodné tajomstvo (keďže sme pričítavali polynómy reprezentujúce tajomstvo 0),
- žiadny hráč nezíska žiadnu dodatkovú informáciu (keďže všetci distribuovali podiely konkrétnej konštanty a tieto nezáviseli od vstupov jednotlivých hráčov).

Zníženie stupňa

Nech $p_3(x) = r_0 + r_1x + \ldots + r_{2t-2}x^{2t-2}$. Nech ďalej $s_{i3} = p_3(i) = p_1(i)p_2(i)$. Označme $p_3'(x) = r_0 + r_1x + \ldots + r_{t-1}x^{t-1}$, a $s_{i3}' = p_3'(i)$.

Všimnime si, že polynóm $p_3'(x)$ reprezentuje to isté tajomstvo ako $p_3(x)$, má však oproti polynómu $p_3(x)$ požadovaný stupeň $t-1$. Preto by bolo dobré, ak by sa nám podarilo hodnoty $s_{13}, \ldots, s_{n3}$ prepočítať na hodnoty $s'_{13}, \ldots, s'_{n3}$ a to bez použitia komunikácie. Nasledujúca lema hovorí, ako to urobiť.

Lema A.4 *Nech* $S = (s_{13}, \ldots, s_{n3})$ *a* $S' = (s'_{13}, \ldots, s'_{n3})$. *Potom existuje* **konštantná** *matica* A *typu* $n \times n$ *taká, že* $S' = S \cdot A$.

Dôkaz: Vezmime vektor R dĺžky n:

$$R = (r_0, \ldots, r_{t-1}, \ldots, r_{2t-2}, 0, \ldots, 0).$$

Nech ďalej R' bude vektor dĺžky n

$$R' = (r_0, \ldots, r_{t-1}, 0, \ldots, 0).$$

Označme $B = (j^i)_{i=1,\ldots,n; j=1,\ldots n}$ Vandermondovu maticu typu $n \times n$. Triviálne platí:

$$\begin{aligned} R \cdot B &= S \\ R' \cdot B &= S' \end{aligned}$$

Ak súčasne označíme P lineárne zobrazenie $P(x_1, \ldots, x_n) = (x_1, \ldots, x_{t-1}, 0, \ldots, 0)$, máme triviálne $R \cdot P = R'$. Z toho, keďže Vandermondova matice B je regulárna, dostávame

$$S \cdot (B^{-1} P B) = S',$$

a teda matica $A = B^{-1} P B$ je hľadanou konštantnou maticou. □

Podľa lemy o maticiach a podľa predchádzajúcej lemy teda hodnoty $s_{13}, \ldots, s_{n3}$ skutočne možno **bez použitia komunikácie** prepočítať na hodnoty $s'_{13}, \ldots, s'_{n3}$.

A.3 Bibliografia

Shamirova schéma pre zdieľanie tajomstva sa prvýkrát objavila v roku 1979 v [29]. Väčšinu informácií pre túto kapitolu sme čerpali hlavne z práce [4]. Počítaním nad Shamirovou schémou pre zdieľanie tajomstva sa zaoberajú Ben-Or, Goldwasser, Wigderson v [6].