Univerzita Karlova v Prahe
Matematicko-fyzikálna fakulta

BAKALÁRSKA PRÁCA

Rudolf Barczi

Perfektný neinteraktívny dôkaz s nulovou znalosťou

Katedra algebry

Vedúci bakalárskej práce: Mgr. Štěpán Holub, Ph.D.

Študijný program: matematika
Študijný odbor: matematické metódy informačnej bezpečnosti

2007

Ďakujem svojmu vedúcemu bakalárskej práce Mgr. Štěpánovi Holubovi, Ph.D. za odborné vedenie, početné konzultácie, cenné rady a pripomienky pri vypracovaní a za všetok venovaný čas. Tiež ďakujem Bc. Ivanovi Štubňovi za to, že ma uviedol do sveta LaTeXu.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa 21. júla 2007 Rudolf Barczi

Obsah

Kapitola 1. Úvod **5**

1.1. Motivácia 5
1.2. Neinteraktívny dôkazový systém 5
1.3. Nulová znalosť 7

Kapitola 2. Stavebné kamene **9**

2.1. Rozhodovanie náležania podgrupe 9
2.2. Kryptosystém BGN 9
2.3. Záväzková schéma BGN 10

Kapitola 3. Perfektný NIZK argument pre všetky $\mathcal{NP}$ jazyky **12**

3.1. NIZK dôkaz obsahu správy 12
3.2. NIZK dôkaz pre CIRCSAT 16
3.3. Perfektný NIZK argument pre CIRCSAT 19

Kapitola 4. Záver **21**

Literatúra. **22**

Názov práce: Perfektný neinteraktívny dôkaz s nulovou znalosťou
Autor: Rudolf Barczi
Katedra: Katedra algebry
Vedúci bakalárskej práce: Mgr. Štěpán Holub, Ph.D.
e-mail vedúceho bakalárskej práce: holub@karlin.mff.cuni.cz

Abstrakt: V predloženej práci študujeme konštrukciu prvého neinteraktívneho argumentu pre všetky $\mathcal{NP}$ jazyky s vlastnosťou perfektnej nulovej znalosti. Na začiatku si zavedieme niektoré základné pojmy z teórie dôkazov s nulovou znalosťou a výpočtovej zložitosti. Ďalej sa oboznámime s predpokladom neefektívnosti rozhodovania náležania podgrupe z teórie čísel a so šifrovou a záväzkovou schémou BGN. Jadro práce tvorí predstavenie neinteraktívneho dôkazu s nulovou znalosťou a perfektnou správnosťou pre $\mathcal{NP}$-úplný jazyk CIRCSAT. Jeho jemnou modifikáciou nakoniec získame neinteraktívny argument s perfektnou nulovou znalosťou pre CIRCSAT, avšak za cenu uvoľnenia sily vlastnosti správnosti. V závere oba protokoly porovnáme a rozoberieme si vhodnosť ich použitia.

Kľúčové slová: NIZK, kryptosystém BGN, rozhodovanie náležania podgrupe

Title: Perfect Non-Interactive Zero Knowledge Proof
Author: Rudolf Barczi
Department: Department of Algebra
Supervisor: Mgr. Štěpán Holub, Ph.D.
Supervisor's e-mail address: holub@karlin.mff.cuni.cz

Abstract: In the present work we study construction of the first perfect non-interactive zero knowledge argument for any $\mathcal{NP}$ language. We start with the definition of some elementary notions from the theory of zero-knowledge proofs and computational complexity theory. We proceed with number-theoretic subgroup decision assumption and BGN cryptosystem and commitment scheme. The substance of this work is concentrated on the presentation of non-interactive zero knowledge proof of knowledge with perfect soundness for the $\mathcal{NP}$-complete language CIRCSAT. By a slight modification, we get the perfect non-interactive zero knowledge argument for CIRCSAT. This is achieved at cost of relaxing the soundness property. In the end, we compare both protocols and discuss their suitability for use.

Keywords: NIZK, BGN cryptosystem, subgroup decision assumption

1 Úvod

Náplňou tejto práce je predstavenie jedného z dvoch výsledkov publikovaných v článku [**6**], kde autori Groth, Ostrovsky a Sahai uvádzajú konštrukciu vôbec prvého neinteraktívneho argumentu s perfektnou nulovou znalosťou pre všetky $\mathcal{NP}$ jazyky. Tým podávajú riešenie problému, ktorý bol po takmer dve desaťročia otvorený.

1.1. Motivácia

Dôkazy s nulovou znalosťou sú veľmi zaujímavým a užitočným kryptografickým nástrojom založeným na interaktívnych dôkazových systémoch. Zaujímavá je najmä ich definícia, ktorá je na prvý pohľad rozporuplná – sú presvedčivé, no zároveň neprezrádzajú nič, okrem platnosti dokazovaného vyhlásenia.
Dôkazy s nulovou znalosťou sa po prvýkrát oficiálne objavili v roku 1985 v článku [**5**]. Ich štúdium bolo motivované výskumom v oblasti autentifikačných systémov. Cieľom bola realizácia procesu overenia identity užívateľa na základe nejakej tajnej informácie, ktorá s ním bola zviazaná (napríklad hesla). Samozrejme sa požadovalo, aby táto informácia ostala tajnou aj po ukončení autentifikácie. Dnes sú dôkazy s nulovou znalosťou vďaka svojim vlastnostiam najčastejšie využívané ako prostriedok vynucujúci korektné správanie účastníkov protokolu pri súčasnom zachovaní ich súkromia.
Neinteraktívne dôkazy s nulovou znalosťou sú špeciálnou variantou dôkazov s nulovou znalosťou. Predstavené boli v roku 1988 v článku [**1**], kde autori ukázali, že interakcia medzi dokazovateľom a overovateľom sa dá nahradiť zdieľaným prístupom k náhodne vygenerovanému spoločne používanému reťazcu. Neinteraktívne dôkazy s nulovou znalosťou sa používajú v rôznych kryptografických protokoloch – napríklad v digitálnych podpisoch, kde je spoločne používaný reťazec súčasťou verejného kľúča. Ich hlavnou výhodou je, že pri spúšťaní viacerých inštancií fungujú nezávisle na kompozícii vždy rovnako dobre – to sa nedá povedať o interaktívnych dôkazoch s nulovou znalosťou, ktoré pri súbežnom spúšťaní vykazujú určité problémy.

1.2. Neinteraktívny dôkazový systém

V nasledujúcich oddieloch si zavedieme potrebné značenie a definujeme väčšinu pojmov, s ktorými budeme ďalej pracovať.

Definícia. Funkciu $\nu : \mathbb{N} \to [0, 1]$ budeme nazývať *zanedbateľnou*, ak

$$(\forall c > 0)\ (\exists K \in \mathbb{N})\ (\forall k > K) : \nu(k) < \frac{1}{k^c}.$$

Značením $f_1(k) \approx f_2(k)$ budeme pre dve funkcie $f_1, f_2 : \mathbb{N} \to [0,1]$ rozumieť, že $|f_1(k) - f_2(k)|$ je zanedbateľná funkcia.
Ďalším často používaným symbolom bude $\leftarrow$ v zápisoch tvaru $vystup \leftarrow A(vstup)$. Takto budeme skrátene vyjadrovať proces výberu náhodnosti r a stanovenia $vystup = A(vstup; r)$.

Poznámka. Pokiaľ nebude uvedené inak, nepriateľské správanie budeme vždy modelovať neuniformným pravdepodobnostným polynomiálnym (skrátene PPT, z anglického probabilistic polynomial time) interaktívnym Turingovým strojom (skrátene ITM, z anglického interactive Turing machine) a všetky ostatné entity budeme implicitne pokladať za uniformné PPT ITM.

Definícia. Hovoríme, že jazyk $L \in \mathcal{NP}$, ak existuje binárna relácia $R \subseteq \{0,1\}^* \times \{0,1\}^*$ a polynóm $p(\cdot)$ tak, že

- R je rozpoznateľná v polynomiálnom čase
- $(x \in \text{Ł}) \Leftrightarrow (\exists w : |w| < p(|x|) \ \& \ (x, w) \in R)$

V každej usporiadanej dvojici $(x, w) \in R$ budeme x nazývať *tvrdením* a w *svedkom*. Jazyk L teda pozostáva zo všetkých tvrdení v R.

Neinteraktívny dôkazový systém pre reláciu R sa skladá z generátora kľúča K, dokazovateľa P a overovateľa V. Generátor K vyprodukuje spoločne používaný reťazec σ. K môžeme vnímať ako dôveryhodnú tretiu stranu poskytujúcu rovnaký náhodný reťazec dokazovateľovi aj overovateľovi. Dokazovateľ P dostane ako vstup trojicu (σ, x, w) a skontroluje, či $(x, w) \in R$. Ak áno, vyrobí dôkaz π. V opačnom prípade bude jeho výstupom hláška `zlyhanie`. Vstupom pre overovateľa V je trojica (σ, x, π). Jeho výstupom je 1 v prípade, že dôkaz prijal, a 0 inak.

Definícia. Nižšie popísanú usporiadanú trojicu nazývame *neinteraktívnym dôkazovým systémom* pre R, ak sú splnené nasledujúce dve podmienky:

- *Úplnosť.* Pre každého nepriateľa A platí

$$\Pr[\sigma \leftarrow K(1^k); (x, w) \leftarrow A(\sigma); \pi \leftarrow P(\sigma, x, w) : V(\sigma, x, \pi) = 1 \mid (x, w) \in R] \approx 1.$$

- *Správnosť.* Pre každého nepriateľa A platí

$$\Pr[\sigma \leftarrow K(1^k); (x, \pi) \leftarrow A(\sigma) : V(\sigma, x, \pi) = 0 \mid x \notin L] \approx 1.$$

Poznámka. Nás bude zaujímať predovšetkým neuniformný PPT nepriateľ, pretože takýto nepriateľ slúži ako horný odhad pri realistických výpočtoch. Ak je podmienka správnosti z predchádzajúcej definície splnená len pre týchto (výpočtovo obmedzených) nepriateľov, nazývame trojicu (K, P, V) *neinteraktívnym argumentovým systémom* pre R a dokazovateľom produkované π nazývame v tomto prípade argumentom.

Vysvetlíme si notáciu použitú v definícii na podmienke správnosti. Tá je splnená, ak pravdepodobnosť, že overovateľ V, ktorý na vstupe dostane spoločne používaný reťazec σ vygenerovaný K a dvojicu (x, π) vygenerovanú ľubovoľným A, odmietne π ako dôkaz tvrdenia x, je za podmienky $x \notin L$ blízka 1.
Slovo neinteraktívny v názve dôkazového systému vystihuje fakt, že interakcia odohrávajúca sa medzi dokazovateľom a overovateľom je skutočne minimálna – pozostáva z jedinej správy odoslanej overovateľovi.

Poznámka. Ďalej budeme neinteraktívny dôkazový (resp. argumentový) systém všade, kde nebude hroziť nedorozumenie, stručne označovať už len ako dôkaz (resp. argument).

Existujú vôbec nejaké dôkazové (argumentové) systémy? Je zrejmé, že pre každý jazyk z $\mathcal{P}$ (alebo skôr z $\mathcal{BPP}$) existuje triviálny dôkazový (argumentový) systém, v ktorom overovateľ vždy rozhodne príslušnosť tvrdenia x k danému jazyku sám, bez potreby použitia nejakej dodatočnej informácie a teda bez nutnosti akejkoľvek interakcie s dokazovateľom. Celý koncept dôkazového (resp. argumentového) systému ako taký je preto užitočný iba v prípade, keď medzi zložitosťou overenia pravdivosti vyhlásenia a jeho dokázaním existuje istá asymetria. Tú ponúka práve zložitostná trieda $\mathcal{NP}$. Každý jazyk z $L \in \mathcal{NP}$ má efektívnu verifikáciu vyhlásenia typu $x \in L$ na základe znalosti w – overovateľ obdrží od dokazovateľa potenciálneho svedka w tvrdenia x a jednoducho aplikuje (polynomiálny) algoritmus rozpoznávajúci reláciu R, pomocou ktorého pravdivosť vyhlásenia $x \in L$ overí. Na druhej strane, nájsť k danému tvrdeniu x platného svedka w môže byť ťažšie. Preto má v súvislosti s dôkazovými (argumentovými) systémami praktický zmysel venovať sa len zaujímavej triede $\mathcal{NP}$.

Definícia. Usporiadanú trojicu (K, P, V) nazývame *neinteraktívnym dôkazom* (resp. *argumentom*) *znalosti* pre R, ak existuje usporiadaná dvojica $E = (E_1, E_2)$ nazývaná *extraktor znalosti*, splňujúca nasledujúce podmienky:

- Pre každého nepriateľa A je
$$\Pr[\sigma \leftarrow K(1^k) : A(\sigma) = 1] \approx \Pr[(\sigma, \tau) \leftarrow E_1(1^k) : A(\sigma) = 1].$$
- Pre každého nepriateľa A je
$$\Pr[(\sigma, \tau) \leftarrow E_1(1^k); (x, \pi) \leftarrow A(\sigma); w \leftarrow E_2(\sigma, \tau, x, \pi) : \\ (x, w) \in R \text{ alebo } V(\sigma, x, \pi) = 0] \approx 1.$$

Definovaný extraktor znalosti $E = (E_1, E_2)$ teda dokáže simulovať tvorbu spoločne používaného reťazca, pričom vyprodukuje nejaké dodatočné informácie τ (časť E_1). V prípade, že má k dispozícii dôkaz tvrdenia, ktorý by overovateľ prijal, je z neho za použitia dodatočných informácií τ schopný extrahovať svedka pre toto tvrdenie (časť E_2).

1.3. Nulová znalosť

Definícia. Hovoríme, že usporiadaná trojica (K, P, V) je *neinteraktívnym dôkazom* (resp. *argumentom*) *s nulovou znalosťou* pre R, ak existuje simulátor $S = (S_1, S_2)$, ktorý splňuje
$$\Pr[\sigma \leftarrow K(1^k) : A^{P(\sigma,\cdot,\cdot)}(\sigma) = 1] \approx \Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{S'(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1],$$
kde $S'(\sigma, \tau, \cdot, \cdot) = S_2(\sigma, \tau, x)$ pre $(x, w) \in R$, pričom S_2 spočíta $\pi \leftarrow S_2(\sigma, \tau, x)$ a vráti π. Inak je výstupom $S'(\sigma, \tau, \cdot, \cdot)$ hláška `zlyhanie`.

Poznámka. Neinteraktívny dôkaz (resp. argument) s nulovou znalosťou budeme v ďalšom texte označovať ako NIZK (z anglického non-interactive zero knowledge) dôkaz (resp. argument).

Vysvetlíme si notáciu z predchádzajúcej definície na príklade. $A^{P(\sigma,\cdot,\cdot)}$ vyjadruje, že nepriateľ A má prístup k orákulu P – kedykoľvek v priebehu výpočtu

môže A na ním zadanom vstupe získať výstup dokazovateľa P, pričom dobu výpočtu P zanedbávame (pri behu A sa to celé prejaví ako jeden krok).
Vlastnosť nulovej znalosti neinteraktívneho dôkazu (resp. argumentu) podľa definície potom prakticky znamená, že všetko, čo môže nepriateľ vypočítať z dôkazu (resp. argumentu) vytvoreného skutočným dokazovateľom, môže byť vypočítané aj z tvrdenia samotného. Takže π neprezrádza o dokazovanom tvrdení x nič okrem jeho platnosti – faktu, že k tvrdeniu x existuje nejaký svedok w tak, že $(x, w) \in R$.

Definícia. Hovoríme, že NIZK dôkaz (resp. argument) pre R má schopnosť *rekonštrukcie cti dokazovateľa*, ak existuje simulátor $S = (S_1, S_2, S_3)$ taký, že pre každého nepriateľa A platí

$$\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] \approx \Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1],$$

kde T spočíta $r \leftarrow \{0,1\}^{\ell_P(k)}; \pi = P(\sigma, x, w; r)$ a ako výstup vydá π, r a F spočíta $\rho \leftarrow \{0,1\}^{\ell_S(k)}; \pi = S_2(\sigma, \tau, x; \rho); r = S_3(\sigma, \tau, x, w; \rho)$ a takisto vráti π, r. Obe orákulá vrátia ako výstup hlášku `zlyhanie`, ak $(x, w) \notin R$.

V skutočnom svete sa väčšinou pohybujeme v prostredí, kde je nepriateľ schopný dokazovateľa skorumpovať. Toto (okrem iného) modeluje sada nástrojov UC od Canettiho, popísaná v [**3**]. Každý protokol vyhovujúci prostrediu UC splňuje vďaka jeho vlastnostiam silné bezpečnostné požiadavky, ako napríklad nefalzifikovateľnosť (anglicky non-malleability) alebo zachovanie bezpečnosti pri súbežnom (anglicky concurrent) spúšťaní – obe uvedené vzhľadom na ľubovoľné a dopredu neznáme množstvo inštancií toho istého alebo iných protokolov, ktoré sú potenciálne koordinované nepriateľom. NIZK argument s perfektnou nulovou znalosťou, ktorého predstavenie je náplňou tejto práce, po určitom rozšírení podľa [**6**] vyhovuje prostrediu UC (ďalej sa tým zaoberať nebudeme).
Podstatná pre význam rekonštrukcie cti dokazovateľa je skutočnosť, že nepriateľ sa po skorumpovaní dokazovateľa dozvie svedka w a náhodnosť r, použitú pri konštrukcii dôkazu (resp. argumentu) π. Aby bolo možné simulovať aj korupciu, je potrebné definíciu nulovej znalosti rozšíriť. Preto požadujeme pri obdržaní w schopnosť simulovať hodnoverne aj náhodnosť r, ktorá by pre dvojicu $(x, w) \in R$ viedla čestného dokazovateľa P práve k produkcii π.

Poznámka. Ak v niektorej z definícií v tomto oddieli dostaneme namiesto $\approx$ pre všetky dostatočne veľké $k \in \mathbb{N}$ rovnosť, pridávame príslušnému definovanému pojmu prívlastok perfektný – hovoríme teda o perfektnej úplnosti, perfektnej správnosti, atď.

2
Stavebné kamene

V nasledujúcich riadkoch si predstavíme základy, na ktorých stojí NIZK dôkaz z ďalšieho oddielu. Zdrojom sa stal článok [**2**] od autorov Boneh, Goh a Nissim.

2.1. Rozhodovanie náležania podgrupe

Nech $\mathcal{G}$ je generátor, ktorému je ako vstup daný bezpečnostný parameter $k \in \mathbb{N}$. Ako výstup vracia $\mathcal{G}$ usporiadanú trojicu (p, q, e), pričom

- p, q sú prvočísla bitovej dĺžky k
- $\mathbb{G}$ je cyklická grupa rádu $n = pq$ v multiplikatívnej notácii
- $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ je bilineárne zobrazenie zachovávajúce generátory, teda
  (1) $\forall u, v \in \mathbb{G}\ \forall a, b \in \mathbb{Z} : e(u^a, v^b) = e(u, v)^{ab}$
  (2) ak je $g \in \mathbb{G}$ generátorom $\mathbb{G}$, potom $e(g, g) \in \mathbb{G}$ je generátorom $\mathbb{G}$.

Množinu všetkých generátorov grupy $\mathbb{G}$ budeme označovať ako $\mathbb{G}_{gen}$ (namiesto tradičného $\mathbb{Z}_n^*$, používaného pre cyklickú grupu v aditívnej notácii). Ďalej si ešte zavedieme značenie $\mathbb{G}_q$ pre podgrupu $\mathbb{G}$ rádu q a tiež symbol $\in_R$, ktorý budeme používať v kontexte $g \in_R \mathbb{G}$. Takto budeme skrátene značiť výber náhodného prvku grupy $\mathbb{G}$.
Pre vyššie popísanú trojicu $(p, q, e) \leftarrow \mathcal{G}(1^k)$ definujeme výhodu nepriateľa pri rozhodovaní náležania podgrupe ako

$$\text{SD-Adv}_A(1^k) = |\Pr[g, h \in_R \mathbb{G}_{gen} : A(n, e, g, h) = 1] - \Pr[g \in_R \mathbb{G}_{gen}, h \in_R \mathbb{G}_q \setminus \{1\} : A(n, e, g, h) = 1]|.$$

Definícia. *Predpoklad neefektívnosti rozhodovania náležania podgrupe* pre generátor $\mathcal{G}$ platí, ak existuje zanedbateľná funkcia $\nu_{SD} : \mathbb{N} \to [0, 1]$ taká, že pre každého nepriateľa A je $\text{SD-Adv}_A(1^k) < \nu_{SD}(k)$ pre všetky dostatočne veľké $k \in \mathbb{N}$.

Rozhodovacím problémom náležania podgrupe je teda bez znalosti faktorizácie n pre daný prvok $x \in \mathbb{G}$ stanoviť, či $x \in \mathbb{G}_q$ alebo nie. Dodajme, že výpočtovo obmedzený nepriateľ A nedokáže (v dnešnej dobe) efektívne faktorizovať dostatočne veľké $n = pq$.

2.2. Kryptosystém BGN

Generácia kľúča

Najprv vygenerujeme $(p, q, e) \leftarrow \mathcal{G}(1^k)$, položíme $n = pq$ a zvolíme g ako náhodný generátor $\mathbb{G}$ a h ako náhodný generátor $\mathbb{G}_q$. Verejný kľúč potom tvorí štvorica (n, e, g, h) a privátnym kľúčom je q.

Šifrovanie

Správu $m \in \{0,1\}$ šifrujeme tak, že náhodne zvolíme $w \in_R \mathbb{Z}_n^*$ a spočítame šifrový text ako $c = g^m h^w$.

Dešifrácia

Pre dešifrovanie správy m zo šifrového textu c spočítame $c^q = g^{mq} h^{wq} = (g^q)^m$ a vyskúšaním možností $\{0,1\}$ dostaneme m.

2.3. Záväzková schéma BGN

Formálnu definíciu záväzkovej schémy kvôli jej rozsiahlosti vynechávame. Priblížime si preto tento pojem aspoň voľnými slovami. Všetky podrobnosti je možné nájsť v [**4**]. Záväzková schéma je dvojstranový protokol odohrávajúci sa vo dvoch fázach, v ktorom sa jedna strana (odosielateľ) zaviaže druhej strane (príjemcovi) k nejakej hodnote tak, že sú splnené nasledujúce protichodné požiadavky:

- *Utajenie.* Na konci prvej (zaväzujúcej) fázy nezíska príjemca znalosť hodnoty, ku ktorej sa odosielateľ zaviazal. Podmienka musí byť splnená, aj keď sa príjemca pokúsi podvádzať.
- *Záväznosť.* Existuje najviac jedna hodnota, ktorú môže príjemca, disponujúci výsledkom interakcie z prvej fázy, prijať na konci druhej (odhaľujúcej) fázy ako správne odhalenie odosielateľovho záväzku. Podmienka musí byť splnená, aj keď sa odosielateľ pokúsi podvádzať.

Záväzková schéma môže mať vlastnosť perfektnej záväznosti alebo perfektného utajenia, nie však obe naraz. V prvom prípade je požiadavka na utajenie výpočtová, takže platí len pre neuniformného pravdepodobnostného polynomiálneho nepriateľa, pričom požiadavka na záväznosť je splnená pre nepriateľa ľubovoľného. V záväzkových schémach s perfektným utajením je to naopak.
Ak pri generácii kľúča pre kryptosystém BGN z predchádzajúceho oddielu zvolíme h ako náhodný generátor $\mathbb{G}$ namiesto pôvodného $h \in_R \mathbb{G}_q \setminus \{1\}$, dostaneme záväzkovú schému BGN:

Generácia spoločne používaného reťazca

Na začiatku vygenerujeme trojicu $(p,q,e) \leftarrow \mathcal{G}(1^k)$, položíme $n = pq$ a zvolíme $g, h \in_R \mathbb{G}_{gen}$. Spoločne používaný reťazec potom tvorí štvorica (n,e,g,h).

Zaviazanie

K správe $m \in \{0,1\}$ sa odosielateľ zaviaže tak, že náhodne zvolí $w \in_R \mathbb{Z}_n^*$ a spočíta záväzok ako $c = g^m h^w$.

Odhalenie

Pre odhalenie správy m zo záväzku c pošle odosielateľ dvojicu (m,w) príjemcovi. Ten overí korektnosť vytvorenia záväzku c, teda platnosť rovnosti $c = g^m h^w$.

Lemma 2.1. *Práve popísaná* BGN *schéma je záväzková schéma s vlastnosťou perfektného utajenia.*

Dôkaz. *Perfektné utajenie.* Nech $\gamma \in \mathbb{Z}_n$ je také, že $g = h^\gamma$. Potom $c = g^m h^w = h^{\gamma m + w}$. Keďže g, h volíme ako náhodné generátory $\mathbb{G}$, je hodnota γ náhodná. Rovnako je náhodná hodnota w, takže prvok $h^{\gamma m+w}$ je náhodným prvkom $\mathbb{G}$. Preto ani výpočtovo neobmedzený príjemca nedokáže zistiť hodnotu $m \in \{0, 1\}$ skôr, ako dôjde k jej odhaleniu.
Výpočtová záväznosť. BGN schéma má vlastnosť perfektného utajenia, nemôže mať teda zároveň vlastnosť perfektnej záväznosti. Je to naozaj tak, lebo výpočtovo neobmedzený odosielateľ dokáže riešiť problém diskrétneho logaritmu – zo znalosti g, h zistiť hodnotu γ. Pretože $c = g^m h^w = h^{\gamma m+w}$, môže potom taký odosielateľ pri odhaľovaní odoslať hodnotu $m \in \{0, 1\}$ podľa vlastnej vôle, lebo vďaka znalosti γ si k zvolenému m vie dopočítať vhodné w. Z toho plynie, že záväznosť záväzkovej schémy BGN je najviac výpočtová. Ukážeme, že jej prelomenie znamená získanie hodnoty diskrétneho logaritmu.
Aby odosielateľ vedel podvádzať, musí byť schopný z odoslaného záväzku c odhaliť príjemcovi ľubovoľnú zo správ $m_0 = 0, m_1 = 1$. Preto musí poznať dva prvky $w_0, w_1 \in \mathbb{Z}_n^*$, pre ktoré je $c = g^{m_0} h^{w_0} = g^{m_1} h^{w_1}$, teda $g^0 h^{w_0} = g^1 h^{w_1}$. Odtiaľ dostávame platnosť vzťahu $g = h^{w_0 - w_1}$, pričom hodnotu výrazu $w_0 - w_1$ si odosielateľ ľahko spočíta.

□

3

Perfektný NIZK argument pre všetky $\mathcal{NP}$ jazyky

Názov kapitoly napovedá, že našim cieľom v nej bude zostrojiť NIZK argument s perfektnou nulovou znalosťou pre všetky $\mathcal{NP}$ jazyky. K tomu budeme potrebovať nasledujúcu definíciu:

Definícia. Množinu $\{C \mid \exists w : C(w) = 1\}$, kde C je booleovský obvod a w ohodnotenie jeho vstupných vrcholov, nazveme *jazykom splniteľných booleovských obvodov*. Tento jazyk budeme označovať ako CIRCSAT.

Ako je ukázané napríklad v [**7**], tento jazyk je $\mathcal{NP}$-úplný, takže každý jazyk z $\mathcal{NP}$ je na neho polynomiálne prevediteľný. Preto nám k dosiahnutiu cieľa bude stačiť skonštruovať NIZK argument s perfektnou nulovou znalosťou pre jazyk CIRCSAT. Čerpať budeme opäť z [**6**].

3.1. NIZK dôkaz obsahu správy

Pre naše účely budeme potrebovať šifrovať logické hodnoty vo vrcholoch obvodu. Dokazovateľ musí byť schopný presvedčiť overovateľa, že takto vzniknuté šifrové texty boli vytvorené korektne. Preto začneme zostrojením NIZK dôkazu, že k danému šifrovému textu c kryptosystému BGN je odpovedajúcim otvoreným textom $m \in \{0, 1\}$.

Lemma 3.1. *Nech $c = g^m h^w$ je šifrovým textom* BGN *kryptosystému. Potom*

$$m \in \{0, 1\} \Leftrightarrow e(c, cg^{-1})^q = 1.$$

Dôkaz. '$\Rightarrow$'. Ak šifrový text c obsahuje ako otvorený text $m \in \{0, 1\}$, potom buď $c \in \mathbb{G}_q$ (máme $c = g^0 h^w = h^w \in \mathbb{G}_q$), alebo $cg^{-1} \in \mathbb{G}_q$ (máme $c = g^1 h^w \Rightarrow cg^{-1} = h^w \in \mathbb{G}_q$). Z toho vyplýva, že prvok $e(c, cg^{-1}) \in \mathbb{G}$ má rád q.
'$\Leftarrow$'. Označme si diskrétny logaritmus z h pri základe g ako δ, teda nech $\delta \in \mathbb{Z}_n$ je také, že $h = g^\delta$. Dosadením za c a jednoduchou úpravou dostávame

$$e(c, cg^{-1}) = e(g^m h^w, g^{m-1} h^w) = e(g^{m+\delta w}, g^{m-1+\delta w}) = e(g, g)^{m(m-1)+\delta w(2m-1+\delta w)}.$$

Predpoklad $e(c, cg^{-1})^q = 1$ nám hovorí, že $m(m-1) + \delta w(2m - 1 + \delta w) = 0 \mod p$. Pretože $h \in \mathbb{G}_q$ má rád q a zároveň $h = g^\delta$, platí $p|\delta$. To nám dáva

$$m(m-1) = 0 \mod p.$$

Odtiaľ máme $m = 0 \mod p$ alebo $m = 1 \mod p$ a vďaka obmedzeniu obsahu šifrovanej správy je $m \in \{0, 1\}$.

□

Podľa Lemmy 3.1 overovateľovi môžeme (a budeme) namiesto tvrdenia, že daný šifrový text c vznikol z otvoreného textu $m \in \{0,1\}$, ekvivalentne dokazovať, že prvok $e(c, cg^{-1})$ má rád q.
Ak poznáme (m, w), pre ktoré je $c = g^m h^w$, potom

$$m = 0 \Rightarrow e(c, cg^{-1}) = e(h^w, g^{-1}h^w) = e(h, (g^{-1}h^w)^w)$$
$$m = 1 \Rightarrow e(c, cg^{-1}) = e(gh^w, h^w) = e(h^w, gh^w) = e(h, (gh^w)^w).$$

V oboch prípadoch teda pre príslušné m platí vzťah

$$e(c, cg^{-1}) = e(h, (g^{2m-1}h^w)^w).$$

Aby sme dostali nulovú znalosť, zvolíme náhodný exponent $r \in \mathbb{Z}_n^*$ a spočítame

$$e(c, cg^{-1}) = e(h, (g^{2m-1}h^w)^w) = e(h^r, (g^{2m-1}h^w)^{wr^{-1}}).$$

Overovateľovi odošleme prvky $\pi_1 = h^r, \pi_2 = (g^{2m-1}h^w)^{wr^{-1}}$. Budeme ho chcieť presvedčiť, že π_1 má rád q. Preto mu ukážeme aj prvok $\pi_3 = g^r$. To stačí, lebo

$$e(\pi_1, g) = e(h^r, g) = e(h, g^r) = e(h, \pi_3).$$

Spoločne používaný reťazec:
1. $(p, q, e) \leftarrow \mathcal{G}(1^k)$
2. $n = pq$
3. $h \in_R \mathbb{G}_q \setminus \{1\}$
4. $g \in_R \mathbb{G}_{gen}$
5. Vráť $\sigma = (n, e, g, h)$.

Tvrdenie: Tvrdením je prvok $c \in \mathbb{G}$. Vyhlásením je, že existuje dvojica $(m, w) \in \mathbb{Z}_n^2$ tak, že $m \in \{0,1\}$ a zároveň $c = g^m h^w$.

Dôkaz: Vstup $(\sigma, c, (m, w))$.
1. Skontroluj, či $c \in \mathbb{G}, m \in \{0,1\}$ a $c = g^m h^w$. Vráť `zlyhanie`, ak nie.
2. $r \in_R \mathbb{Z}_n^*$
3. $\pi_1 = h^r, \pi_2 = (g^{2m-1}h^w)^{wr^{-1}}, \pi_3 = g^r$
4. Vráť $\pi = (\pi_1, \pi_2, \pi_3)$.

Overenie: Vstup $(\sigma, c, \pi = (\pi_1, \pi_2, \pi_3))$.
1. Skontroluj, či $c \in \mathbb{G}$ a zároveň $\pi \in \mathbb{G}^3$.
2. Skontroluj, či $e(c, cg^{-1}) = e(\pi_1, \pi_2)$ a zároveň $e(\pi_1, g) = e(h, \pi_3)$.
3. Vráť 1, ak oba testy prebehli úspešne. Inak vráť 0.

Tabuľka 1. NIZK dôkaz obsahu správy z $\{0,1\}$

Tvrdenie 3.2. *Protokol uvedený v Tabuľke 1 je* NIZK *dôkazom s rekonštrukciou cti dokazovateľa, že šifrový text $c \in \mathbb{G}$ kryptosystému* BGN *má otvorený text $m \in \{0,1\}$.*

Dôkaz. *Perfektná úplnosť.* Nech $\delta \in \mathbb{Z}_n$ je diskrétnym logaritmom z h o základe g, teda $h = g^\delta$. Vieme, že $c = g^m h^w$, kde $m \in \{0,1\}$. Odtiaľ máme

$$e(c, cg^{-1}) = e(g^{m+\delta w}, g^{m-1+\delta w}) = e(g,g)^{m(m-1)+\delta w(2m-1+\delta w)} =$$
$$e(g,g)^{r\delta(2m-1+\delta w)wr^{-1}} = e(h^r, (g^{2m-1}h^w)^{wr^{-1}}) = e(\pi_1, \pi_2).$$

Tiež platí $e(\pi_1, g) = e(h^r, g) = e(h, g^r) = e(h, \pi_3)$. Dokázali sme, že ak c má otvorený text $m \in \{0, 1\}$, potom overovateľ vždy také c, π prijme.
Perfektná správnosť. Opäť, nech $\delta \in \mathbb{Z}_n$ je také, že $g^\delta = h \in \mathbb{G}_q$. Uvažujme c, π, pre ktoré platí $e(c, cg^{-1}) = e(\pi_1, \pi_2)$ a zároveň $e(\pi_1, g) = e(h, \pi_3)$. Existuje $0 \leq m < p$ a $w \in \mathbb{Z}_n$ tak, že $c = g^{\delta w+m} = g^m h^w$. Platí, že π_1 má rád 1 alebo q, lebo

$$e(\pi_1^q, g) = e(\pi_1, g)^q = e(h, \pi_3)^q = e(h^q, \pi_3) = e(1, \pi_3) = 1.$$

Takže existuje nejaké $r \in \mathbb{Z}_n$, pre ktoré $\pi_1 = h^r$. Preto $e(c, cg^{-1}) = e(\pi_1, \pi_2) = e(h^r, \pi_2)$ a tiež $e(c, cg^{-1})^q = e(h^{rq}, \pi_2) = e(1, \pi_2) = 1$. Odtiaľ a z $e(c, cg^{-1}) = e(g, g)^{m(m-1)+\delta w(2m-1+\delta w)}$ dostávame

$$m(m-1) + \delta w(2m - 1 + \delta w) = 0 \mod p,$$

pričom $g^\delta = h \in \mathbb{G}_q$ znamená, že $p|\delta$. To nám dáva $m(m-1) = 0 \mod p$ a keďže predpokladáme $0 \leq m < p$, je $m \in \{0, 1\}$. Ukázali sme, že ak overovateľ prijme c, π, potom c musí mať otvorený text $m \in \{0, 1\}$. Takže overovateľ nikdy neprijme nevyhovujúce c.
Nulová znalosť a rekonštrukcia cti dokazovateľa. Začneme popisom simulátora $S = (S_1, S_2, S_3)$. S_1 spustí algoritmus na generáciu spoločne používaného reťazca s tým rozdielom, že namiesto $h \in_R \mathbb{G}_q \setminus \{1\}$ zvolí h ako náhodný generátor $\mathbb{G}$, ďalej zvolí $\gamma \in_R \mathbb{Z}_n^*$ a položí $g = h^\gamma$, takže bude $h, g \in \mathbb{G}_{gen}$. Pri tejto generácii si simulátor zapamätá p, q. Výstupom S_1 je teda

$$(\sigma, \tau) = ((n, e, g, h), (p, q, \gamma)).$$

S_2 na vstupe (σ, τ, c) simuluje dôkaz π. Ako prvé vyberie $r \in_R \mathbb{Z}_n^*$. Voľba $h \in_R \mathbb{G}_{gen}$ pri simulovanej generácii spoločne používaného reťazca časťou S_1 nám hovorí, že aspoň jeden z prvkov c, cg^{-1} je generátorom grupy $\mathbb{G}$. Ak ním je c, S_2 položí

$$\pi_1 = c^r, \pi_2 = (cg^{-1})^{r^{-1}}, \pi_3 = \pi_1^\gamma.$$

Ak c nie je generátorom $\mathbb{G}$, S_2 položí

$$\pi_1 = (cg^{-1})^r, \pi_2 = c^{r^{-1}}, \pi_3 = \pi_1^\gamma.$$

Ako svoj výstup S_2 teda vracia usporiadanú trojicu $\pi = (\pi_1, \pi_2, \pi_3)$.
S_3 obdrží na vstupe okrem (σ, τ, c) tiež svedka $(m, w) \in \mathbb{Z}_n^2$ tak, že $m \in \{0, 1\}$ a zároveň $c = g^m h^w$. Jeho úlohou je na základe znalosti tohto svedka zrekonštruovať náhodnosť, použitím ktorej by reálny dokazovateľ vyprodukoval dôkaz π simulovaný časťou S_2. Pretože S_3 pozná hodnotu γ, dostáva $c = g^m h^w = h^{\gamma m+w}$. Uvažujme najprv prípad, keď c je generátorom $\mathbb{G}$. Máme $\gcd(n, \gamma m + w) = 1$, takže prvok $\gamma m + w$ je v $\mathbb{Z}_n$ invertibilný. Simulovaný dôkaz môžeme preto s využitím vyššie odvodenej rovnosti $e(c, cg^{-1}) = e(h, (g^{2m-1}h^w)^w)$ písať ako $\pi_1 = h^{r(\gamma m+w)}, \pi_2 = (g^{2m-1}h^w)^{w(r(\gamma m+w))^{-1}}$ a $\pi_3 = g^{r(\gamma m+w)}$. Ako simulovanú dokazovateľovu náhodnosť teda S_3 vráti

$$r(\gamma m + w) \mod n.$$

Podobne postupujeme, ak c nie je generátorom $\mathbb{G}$. Vieme, že v tomto prípade je generátorom prvok $cg^{-1} = h^{\gamma(m-1)+w}$ a preto $\gcd(n, \gamma(m-1)+w) = 1$. Simulovaný dôkaz potom môžeme písať ako $\pi_1 = h^{r(\gamma(m-1)+w)}, \pi_2 = (g^{2m-1}h^w)^{w(r(\gamma(m-1)+w))^{-1}}$ a $\pi_3 = g^{r(\gamma(m-1)+w)}$. V tomto prípade teda S_3 ako simulovanú náhodnosť vráti

$$r(\gamma(m-1) + w) \mod n.$$

Aby sme dokázali nulovú znalosť, uvažujme najprv hybridný experiment, v ktorom S_1 vygeneruje spoločne používaný reťazec σ, ale ako simulované orákulum použijeme reálneho dokazovateľa P. Ukážeme si, že pre každého nepriateľa A platí

$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] - \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k),$$

kde $T(\sigma, c, (m, w))$ spočíta $r \in_R \mathbb{Z}_n^*; \pi = P(\sigma, c, (m, w); r)$ a vráti π, r. V prípade, že $m \notin \{0, 1\}$ alebo $c \neq g^m h^w$, vráti T hlášku `zlyhanie`. Jediným rozdielom medzi pôvodným a hybridným experimentom je voľba h. V prvom prípade je h náhodným generátorom $\mathbb{G}_q$, zatiaľ čo v druhom je náhodným generátorom $\mathbb{G}$. V žiadnom z týchto experimentov nevyužívame znalosť p, q alebo diskrétneho logaritmu z g pri základe h. Uvažujme predpoklad neefektívnosti rozhodovania náležania podgrupe pre dve štvorice (n, e, g, h) s rozdielnou voľbou h (v prvej štvorici $h \in_R \mathbb{G}_q \setminus \{1\}$, v druhej $h \in_R \mathbb{G}_{gen}$). Tieto dve štvorice odpovedajú presne spoločne používaným reťazcom vyrobeným generátormi K a S_1. Výhoda útočníka A je preto zhora ohraničená zanedbateľnou funkciou $\nu_{SD}(k)$.
Ďalším krokom bude prechod od hybridného experimentu k plnej simulácii. Ukážeme si, že pre každého nepriateľa A je

$$\Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] = \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1],$$

kde F spočíta $r \in_R \mathbb{Z}_n^*; \pi = S_2(\sigma, \tau, c; r); \rho = S_3(\sigma, \tau, c, (m, w); r)$ a vráti π, ρ. Opäť, ak $m \notin \{0, 1\}$ alebo $c \neq g^m h^w$, vráti F hlášku `zlyhanie`. Simulovaný dôkaz $\pi = (\pi_1, \pi_2, \pi_3)$ jednoznačne určuje náhodnosť $\rho \in \mathbb{Z}_n^*$ tak, že $\pi_1 = h^\rho$. Taká náhodnosť je naozaj výstupom S_3. Preto nám ostáva ukázať už len to, že simulované dôkazy sú distribuované rovnako, ako dôkazy vytvorené skutočným dokazovateľom v hybridnom experimente. V prípade, že c je generátorom $\mathbb{G}$, S_2 zvolí náhodne $r \in_R \mathbb{Z}_n^*$ a položí $\pi_1 = c^r$, čo nám dáva náhodný generátor $\mathbb{G}$. V hybridnom experimente je $\pi_1 = h^r$ taktiež náhodným generátorom $\mathbb{G}$, pretože použité h má rád n. Z faktu, že π_1 jednoznačne určuje π_2 a π_3 vyplýva, že distribúcie dôkazov v hybridnom experimente a simulácii sú identické. Na druhej strane, ak c nie je generátorom $\mathbb{G}$, je ním prvok cg^{-1}. Simulované $\pi_1 = (cg^{-1})^r$ je pre zvolené $r \in_R \mathbb{Z}_n^*$ opäť náhodným generátorom $\mathbb{G}$ a použitím rovnakého argumentu, ako pred chvíľou, dostávame aj v tomto prípade identitu uvažovaných distribúcií.
Teda

$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] - \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k)$$
$$\Downarrow$$
$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] - \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k)$$
$$\Downarrow$$
$$\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] \approx \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1]$$

a dôkaz je hotový.

□

3.2. NIZK dôkaz pre CIRCSAT

Majme nejaký booleovský obvod $C \in$ CIRCSAT. Chceme dokázať jeho splniteľnosť, teda existenciu takého ohodnotenia vstupných vrcholov w, že $C(w) = 1$. Aby sme pri tom dosiahli nulovú znalosť, budeme v každom vrchole obvodu C šifrovať logickú hodnotu vzniknutú pri danom ohodnotení w. Použitím NIZK dôkazu z Tabuľky 1 môžeme overovateľa presvedčiť, že všetky šifrové texty obsahujú korešpondujúce otvorené texty z $\{0, 1\}$. Hodnotu výstupu obvodu C budeme vždy šifrovať s použitím rovnakej "náhodnosti" 0, aby si overovateľ mohol priamo overiť, že táto hodnota je 1.

Definícia. Binárnu logickú spojku NAND definujeme ako

$$a \text{ NAND } b \equiv \neg(a \,\&\, b).$$

Booleovské obvody sú zostrojené pomocou logických spojok $\neg, \&, \vee$. Poslednú uvedenú vieme nahradiť pomocou zvyšných dvoch ako:

$$a \vee b \equiv \neg(\neg a \,\&\, \neg b).$$

Ostávajúce spojky sa dajú pomocou NAND prepísať nasledovne:

$$\neg a \equiv a \text{ NAND } a$$
$$a \,\&\, b \equiv (a \text{ NAND } b) \text{ NAND } (a \text{ NAND } b).$$

Každý booleovský obvod dokážeme preto lineárne redukovať na obvod pozostávajúci len z NAND-brán.

Poznámka. Ďalej budeme bez újmy na všeobecnosti uvažovať obvody skonštruované len pomocou NAND-brán.

Podľa predchádzajúcej poznámky ostáva ešte overovateľa presvedčiť, že všetky zašifrované hodnoty vo výstupných vrcholoch NAND-brán naozaj odpovedajú správnemu vyhodnoteniu týchto NAND-brán.

Lemma 3.3. *Nech* $b_0, b_1, b_2 \in \{0, 1\}$. *Potom*

$$b_0 + b_1 + 2b_2 - 2 \in \{0, 1\} \Leftrightarrow b_2 = b_0 \text{ NAND } b_1.$$

Dôkaz. '$\Rightarrow$'. Z predpokladu máme buď $b_0+b_1+2b_2-2 = 0$ alebo $b_0+b_1+2b_2-2 = 1$. V prvom prípade musí platiť $b_0 = b_1$ a v druhom $b_0 \neq b_1$. Rozbor ostávajúcich možností dáva platnosť vzťahu $b_2 = b_0$ NAND b_1.
'$\Leftarrow$'. Z predpokladu máme $b_2 = b_0$ NAND $b_1 = \neg(b_0 \,\&\, b_1) = 1 - b_0 b_1$. Preto $b_0 + b_1 + 2b_2 - 2 = b_0 + b_1 - 2b_0 b_1$. Skutočnosť, že tento výraz nadobúda hodnoty z $\{0, 1\}$, dostaneme opäť rozborom možností.

□

Z daných šifrových textov c_0, c_1, c_2, obsahujúcich otvorené texty b_0, b_1, b_2, môžeme vytvoriť šifrový text $c_0 c_1 c_2^2 g^{-2} = g^{b_0+b_1+2b_2-2} h^{r_0+r_1+2r_2}$. NIZK dôkaz, že $c_0 c_1 c_2^2 g^{-2}$ obsahuje otvorený text z $\{0, 1\}$, potom podľa Lemmy 3.3 implikuje $b_2 = b_0$ NAND b_1, ako je potrebné.

Tvrdenie 3.4. *Protokol uvedený v Tabuľke 2 je* NIZK *dôkazom znalosti s rekonštrukciou cti dokazovateľa pre jazyk* CIRCSAT.

Dôkaz. *Perfektná úplnosť.* Pretože dokazovateľ pozná splňujúce ohodnotenie w pre C, dokáže spočítať bitové hodnoty vo všetkých vrcholoch C tak, že tieto hodnoty dodržujú NAND-brány a zároveň je výstupom obvodu 1. Perfektnú úplnosť dostávame z perfektnej úplnosti použitých NIZK dôkazov hodnoty správy z $\{0, 1\}$.
Perfektná správnosť. Aby overovateľ prijal C, π, musí mu byť pomocou NIZK dôkazov z Tabuľky 1 dokázané, že k šifrovému textu pre každý vrchol existuje odpovedajúci otvorený text z $\{0, 1\}$. Overenie NIZK dôkazov pre NAND-brány zase podľa Lemmy 3.3 implikuje, že logické hodnoty v obovode dodržujú správne vyhodnocovanie NAND-brán. Všetky použité NIZK dôkazy majú podľa Tvrdenia 3.2 vlastnosť perfektnej správnosti. Nakoniec musí byť $c_{vystup} = g$, čo znamená hodnotu výstupu obvodu C rovnú 1. Z predchádzajúcich riadkov plynie, že ak overovateľ prijme C, π, potom obvod C musí byť splniteľný. Overovateľ teda nikdy neprijme obvod $C \notin$ CIRCSAT.
Perfektná extrakcia znalosti. Extraktor $E = (E_1, E_2)$ najprv vygeneruje spoločne

Spoločne používaný reťazec:
1. $(p, q, e) \leftarrow \mathcal{G}(1^k)$
2. $n = pq$
3. $h \in_R \mathbb{G}_q \setminus \{1\}$
4. $g \in_R \mathbb{G}_{gen}$
5. Vráť $\sigma = (n, e, g, h)$.

Tvrdenie: Tvrdením je obvod C zložený z NAND-brán. Vyhlásením je, že existuje postupnosť vstupných bitov w, splňujúca $C(w) = 1$.

Dôkaz: Vstup (C, w), kde $C(w) = 1$.
1. Pripoj k w bity zo všetkých vrcholov C pri ohodnotení w.
2. Zašifruj každý bit w_i ako $c_i = g^{w_i} h^{r_i}$ s použitím $r_i \in_R \mathbb{Z}_n^*$.
3. Pre všetky c_i vytvor NIZK dôkaz existencie $(w_i, r_i) \in \mathbb{Z}_n^2$ takých, že $w_i \in \{0, 1\}$ a zároveň $c_i = g^{w_i} h^{r_i}$.
4. Zašifruj výstup obvodu C ako $c_{vystup} = g^1 h^0 = g$.
5. Pre všetky NAND-brány so vstupnými vrcholmi j_0, j_1 a výstupným vrcholom j_2 vytvor pre $c_{j_0} c_{j_1} c_{j_2}^2 g^{-2}$ NIZK dôkaz existencie $(m, r) \in \mathbb{Z}_n^2$ takých, že $m \in \{0, 1\}$ a $c_{j_0} c_{j_1} c_{j_2}^2 g^{-2} = g^m h^r$.
6. Vráť π zložené zo všetkých uvedených šifrových textov a príslušných NIZK dôkazov.

Overenie: Vstup (C, π).
1. Skontroluj, či ku všetkým vrcholom existuje korešpondujúci šifrový text a či šifrovým textom odpovedajúcim výstupu obvodu C je $c_{vystup} = g$.
2. Skontroluj NIZK dôkazy obsahu správy z $\{0, 1\}$ pre všetky šifrové texty.
3. Skontroluj NIZK dôkazy validity vyhodnocovania pre všetky NAND-brány.
4. Vráť 1, ak všetky testy prebehli úspešne. Inak vráť 0.

Tabuľka 2. NIZK dôkaz znalosti pre CIRCSAT

používaný reťazec spustením generátora pre NIZK dôkaz, teda $(\sigma, \tau) \leftarrow E_1(1^k)$, kde $(\sigma, \tau) = ((n, e, g, h), (p, q))$. Pri tomto procese sa naučí (p, q), vďaka čomu môže $E_2(\sigma, \tau, C, \pi)$ dešifrovať jednotlivé c_i. Tak získa bitové hodnoty prislúchajúce všetkým vrcholom obvodu C. Keďže sme si pred chvíľou ukázali perfektnú správnosť uvažovaného protokolu, dešifrované hodnoty vstupných vrcholov musia korešpondovať so svedkom w, pre ktorého je $C(w) = 1$.

Nulová znalosť a rekonštrukcia cti dokazovateľa. Začneme popisom simulátora $S = (S_1, S_2, S_3)$. Časť S_1 ostane rovnaká, ako v dôkaze Tvrdenia 3.2.

S_2 bude simulovať dôkaz π nasledovne. Výstupu priradí šifrový text g. Pre všetky ostatné vrcholy položí $c_i = h^{r_i}$, kde $r_i \in_R \mathbb{Z}_n^*$. Neskôr, keď bude mať S_3 k dispozícii svedka w, bude poznať $w_i \in \{0, 1\}$ odpovedajúce každému c_i. To ale nevadí, pretože pre $w_i \in \{0, 1\}$ platí $c_i = g^{w_i} h^{r_i - w_i \gamma^{-1}} = h^{r_i}$. Ďalej S_2 pokračuje pre všetky c_i simuláciou NIZK dôkazu obsahu správy z $\{0, 1\}$. Nakoniec, S_2 pre všetky NAND-brány so vstupnými vrcholmi j_0, j_1 a výstupným vrcholom j_2 simuluje pre šifrový text $c_{j_0} c_{j_1} c_{j_2}^2 g^{-2}$ NIZK dôkaz obsahu správy z $\{0, 1\}$ a vráti π pozostávajúce zo všetkých šifrových textov a odpovedajúcich NIZK dôkazov. Všetky uvedené NIZK dôkazy simuluje S_2 rovnako, ako časť S_2 z dôkazu Tvrdenia 3.2.

S_3 dostane na vstupe svedka w, vďaka ktorému sa dozvie bitové hodnoty w_i vo všetkých vrcholoch C. Zároveň pozná náhodnosti $r_i - w_i \gamma^{-1}$ použité pri tvorbe šifrových textov, takže pre každé $c_i = g^{w_i} h^{r_i - w_i \gamma^{-1}}$ spustí rekonštruktor cti S_3 z dôkazu Tvrdenia 3.2. Tak dostane celkovú náhodnosť, ktorá by viedla reálneho dokazovateľa k produkcii simulovaného π.

Aby sme dokázali nulovú znalosť, budeme opäť najprv uvažovať hybridný experiment, v ktorom spoločne používaný reťazec vyrobí simulátor, ale dôkazy bude produkovať reálny dokazovateľ. Podobne, ako v dôkaze Tvrdenia 3.2, pre každého nepriateľa A platí

$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] - \Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k),$$

kde $T(\sigma, C, w)$ spočíta $\pi = P(\sigma, C, w; r)$ a v prípade, že $C(w) = 1$, vráti π, r. Inak je výstupom `zlyhanie`.

V ďalšom kroku modifikujeme spôsob produkcie dôkazov v hybridnom experimente. Šifrové texty c_i budeme naďalej vytvárať ako skutočný dokazovateľ, ale všetky NIZK dôkazy obsahu správy z $\{0, 1\}$ budeme simulovať. Ako sme si ukázali v dôkaze Tvrdenia 3.2, táto zmena neovplyvní pravdepodobnosť, že nepriateľ A vráti 1. Preto pre každého nepriateľa A máme

$$\Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] = \Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{M(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1],$$

kde $M(\sigma, \tau, C, w)$ vytvorí šifrové texty korektne a všetky NIZK dôkazy obsahu správy z $\{0, 1\}$ simuluje. Ak $C(w) \neq 1$, výstupom M je `zlyhanie`.

Nakoniec prejdeme k plnej simulácii. Pre každého nepriateľa A je

$$\Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{M(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1] = \Pr[(\sigma, \tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1],$$

kde F spočíta $\pi = S_2(\sigma, \tau, C; \rho); r = S_3(\sigma, \tau, C, w; \rho)$ a vráti π, r. Ak $C(w) \neq 1$, vráti hlášku `zlyhanie`. Uvedená rovnosť platí, lebo jediným rozdielom medzi orákulami M a F je spôsob tvorby šifrových textov. Ale pretože S_1 pri generácii spoločne používaného reťazca volí g, h ako náhodné generátory grupy $\mathbb{G}$, sú šifrové texty vyprodukované orákulom M záväzkami s perfektným utajením podľa Lemmy 2.1. Orákulum F zasa vytvorí šifrové texty podľa predpisu $c_i = h^{r_i}$, kde

$r_i \in_R \mathbb{Z}_n^*$. Hodnoty c_i sú teda náhodnými prvkami grupy $\mathbb{G}$. Preto posledné dva experimenty nepriateľ taktiež rozlíšiť nedokáže.
Podobne, ako v dôkaze Tvrdenia 3.2, dostávame

$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] -$$
$$\Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k)$$
$$\Downarrow$$
$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] -$$
$$\Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{M(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k)$$
$$\Downarrow$$
$$|\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] -$$
$$\Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1]| < \nu_{SD}(k)$$
$$\Downarrow$$
$$\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] \approx \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{F(\sigma,\tau,\cdot,\cdot)}(\sigma) = 1]$$

a dôkaz je hotový.

□

3.3. Perfektný NIZK argument pre CIRCSAT

Ukázali sme si, že protokol v Tabuľke 2 je NIZK dôkazom pre všetky $\mathcal{NP}$ jazyky. Stále mu však chýba vlastnosť perfektnej nulovej znalosti, ktorá je našim cieľom.
Dosiahneme ju tak, že pri generácii spoločne používaného reťazca $\sigma = (n, e, g, h)$ budeme namiesto $h \in_R \mathbb{G}_q \setminus \{1\}$ voliť $h \in_R \mathbb{G}_{gen}$. Tým pádom sa z každého šifrového textu $c = g^m h^r$ stane záväzok k hodnote m s perfektným utajením. Je zrejmé, že takto pozmenený protokol bude naďalej splňovať podmienku perfektnej úplnosti. Z dôkazu Tvrdenia 3.4 dostávame taktiež vlastnosť perfektnej nulovej znalosti, pretože pri prvom hybridnom experimente bude platiť

$$\Pr[\sigma \leftarrow K(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1] = \Pr[(\sigma,\tau) \leftarrow S_1(1^k) : A^{T(\sigma,\cdot,\cdot)}(\sigma) = 1],$$

pričom rovnosti vo zvyšných dvoch experimentoch ostanú zachované.
Trocha väčším problémom je ukázať splnenie podmienky správnosti, ktorej sila sa po vykonanej zmene uvoľní z perfektnej na výpočtovú. To je daň, ktorú v uvedenom protokole vďaka vlastnostiam záväzkových schém zaplatíme za získanie perfektnej nulovej znalosti.

TVRDENIE 3.5. *Označme časť S_1 simulátora S z dôkazu Tvrdenia 3.4, ktorá ako výstup produkuje namiesto dvojice (σ, τ) len σ, ako S_σ. Potom protokol z Tabuľky 2 je pre trojicu (S_σ, P, V)* NIZK *argumentom s perfektnou nulovou znalosťou a rekonštrukciou cti dokazovateľa pre obvody z* CIRCSAT.

DÔKAZ. Z dôkazu Tvrdenia 3.4 dostávame podľa predchádzajúceho odstavca perfektnú úplnosť, perfektnú nulovú znalosť a rekonštrukciu cti dokazovateľa.
Správnosť. Uvažujme ľubovoľný obvod $C \notin$ CIRCSAT a nepriateľa A. Označme pravdepodobnosť, s ktorou A dokáže prelomiť podmienku správnosti, ako $\mathrm{SoAdv}_A(1^k)$. To znamená, že ak A obdrží spoločne používaný reťazec, potom s

pravdepodobnosťou $\text{So-Adv}_A(1^k)$ vyprodukuje platný argument π pre nesplniteľný obvod C. K nášmu cieľu sa dostaneme tak, že skonštruujeme nepriateľa B, ktorý rozhoduje problém náležania podgrupe s pravdepodobnosťou

$$\text{SD-Adv}_B(1^k) = \text{So-Adv}_A(1^k).$$

Úlohou B bude po obdržaní spoločne používaného reťazca (n, e, g, h) stanoviť, či dané h je rádu n alebo q. To odpovedá rozhodnutiu, či spoločne používaný reťazec vygeneroval generátor S_σ, alebo generátor K z Tabuľky 2. Nepriateľ B najskôr posunie obdržaný spoločne používaný reťazec nepriateľovi A, ktorý sa následne pokúsi vytvoriť platný argument pre C. Nakoniec, B vydá ako svoj výstup 1, práve keď A pri konštrukcii platného argumentu pre C uspel.
Rozoberme si teraz pravdepodobnosť úspechu A. Ak je h rádu n, A dostal spoločne používaný reťazec vygenerovaný S_σ. Preto je v tomto prípade pravdepodobnosť vytvorenia platného argumentu rovná $\text{So-Adv}_A(1^k)$. Na druhej strane, ak je h rádu q, spoločne používaný reťazec bol vygenerovaný K. Tým pádom dostávame NIZK dôkaz z Tabuľky 2. Keďže tento NIZK dôkaz má podľa Tvrdenia 3.4 vlastnosť perfektnej správnosti, je uvažovaná pravdepodobnosť rovná 0.
Ukázali sme, že za predpokladu neefektívnosti rozhodovania náležania podgrupe platí

$$\text{So-Adv}_A(1^k) = \text{SD-Adv}_B(1^k) < \nu_{SD}(k),$$

kde $\nu_{SD}(k)$ je zanedbateľná funkcia z definície tohto predpokladu. Odtiaľ dostávame

$$\begin{aligned}\Pr[\sigma \leftarrow S_\sigma; (C, \pi) \leftarrow A(\sigma) : V(\sigma, C, \pi) = 0 \mid C \notin \text{CIRCSAT}] = \\ = 1 - \text{So-Adv}_A(1^k) \approx 1,\end{aligned}$$

a dôkaz je hotový.

□

4
Záver

V poslednej kapitole sme si ukázali konštrukciu dvoch NIZK protokolov za predpokladu neefektívnosti rozhodovania náležania podgrupe – na jednej strane stojí NIZK dôkaz s perfektnou správnosťou predstavený v oddieli 3.2, na strane druhej zasa NIZK argument s perfektnou nulovou znalosťou prezentovaný v oddieli 3.3. Je možné povšimnúť si vzájomnú výmenu medzi silou vlastností správnosti a nulovej znalosti týchto protokolov.

Vynára sa teda logická otázka – ktorý z týchto NIZK protokolov je lepšie použiť v praxi? Odpoveď síce nie je jednoznačná, ale podľa [**4**] by sa mal brať ohľad na:

- **relatívnu dôležitosť prisúdenú správnosti a nulovej znalosti v špecifickej aplikácii.** V prípade jasnej priority niektorej z týchto vlastností by mal byť uskutočnený odpovedajúci výber.
- **výpočtové zdroje rôznych užívateľov aplikácie.** O niektorom z užívateľov môže byť známe, že má k dispozícii veľmi silné výpočtové zdroje a môže byť preto vhodné požadovať, aby nebol schopný podvádzať ani v teoretickom zmysle. Tu sa viac hodí protokol z Tabuľky 2 s vlastnosťou perfektnej správnosti.
- **trvácnosť výsledku.** V mnohých aplikáciách môže byť nulová znalosť v záujme ešte dlho po úspešnom overení. V tomto prípade je zase výhodnejšie použiť NIZK argument s perfektnou nulovou znalosťou.

Literatúra

[1] Manuel Blum, Paul Feldman, Silvio Micali: *Non-Interactive Zero-Knowledge and Its Applications.* Proceedings of the twentieth annual ACM symposium on Theory of computing, 103–112, 1988.

[2] Dan Boneh, Eu-Jin Goh, Kobbi Nissim: *Evaluating 2-DNF Formulas on Ciphertexts.* Proceedings of TCC'05, 325–341, 2005.

[3] Ron Canetti: *Universally Composable Security: A New Paradigm for Cryptographic Protocols.* Proceedings of FOCS'01, 136–145, 2001. Plná verzia dostupná na http://eprint.iacr.org/2000/067.

[4] Oded Goldreich: *Foundations of Cryptography.* Cambridge University Press, 2001.

[5] Shafi Goldwasser, Silvio Micali, Charles Rackoff: *The knowledge complexity of interactive proof-systems.* Proceedings of the seventeenth annual ACM symposium on Theory of computing, 291–304, 1985.

[6] Jens Groth, Rafail Ostrovsky, Amit Sahai: *Perfect Non-Interactive Zero Knowledge for NP.* Cryptology ePrint Archive, Report 2005/290, 2005.

[7] Štěpán Holub: *Složitost pro kryptografii.* Skriptá pre MFF UK, 2004. Dostupné na http://www.karlin.mff.cuni.cz/∼holub/skripta/slozitost.ps.