The Clean Paper

WHAT THE PAPER SAYS · WHAT IT DOESN'T · WHY IT MATTERS

Kryptografický dôkaz môže skryť tajomstvo tým, že sťaží dokázanie, že simulátor chýba

Dôkazy s nulovou znalosťou umožňujú niekomu dokázať tvrdenie bez odhalenia svedka. Klasická teória hovorí, že ich v plnom zmysle nemožno mať s jedinou správou, bez dôveryhodného nastavenia a s dokonalou spoľahlivosťou. Práca Rahula Ilanga túto nemožnosť neruší. Mení cieľ: namiesto požiadavky, aby simulátor skutočne existoval, žiada, aby zvolený dôkazový systém nedokázal efektívne dokázať, že simulátor neexistuje. Za hlavných predpokladov z teórie zložitosti dôkazov a kryptografie to stačí na postupné obnovenie jednotlivých falzifikovateľných herných dôsledkov nulovej znalosti. Nejde o hotový praktický primitív. Je to dôkazovo-teoretický spôsob, ako z matematickej nepreukázateľnosti vytvoriť kryptografické krytie.

Written by Cinzia Vaglio · Cross-checked by Vera Rubin · AI-assisted, human-reviewed

Paper: *Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness*, Rahul Ilango, FOCS 2025 / IACR ePrint 2025/1296 · DOI: 10.1109/FOCS63196.2025.00058

Trik nie je dokázať, že tajomstvo je skryté

Začnime s najjednoduchšou verziou nulovej znalosti.

Alice chce presvedčiť Boba, že Sudoku hádanka má riešenie. Ak pošle riešenie, Bob je presvedčený, ale hádanka je zničená. To, čo chce, je zvláštnejšie: dôkaz, že riešenie existuje, bez toho, aby ho odhalila.

To je prísľub dôkazu s nulovou znalosťou. Dokazovateľka (Alice) presvedčí overovateľa (Boba), že tvrdenie je pravdivé, pričom neprezradí nič okrem samotnej pravdivosti tvrdenia.

Problémom je, že tento prísľub niečo stojí. Bežný matematický dôkaz má dve príjemné vlastnosti. Tvorí ho **jedna správa**: zapíšete ho, odovzdáte a odídete. Zároveň má **dokonalú spoľahlivosť**: nepravdivé tvrdenie nemá vôbec žiadny platný dôkaz. Klasické výsledky nemožnosti hovoria, že dôkaz s nulovou znalosťou sa musí vzdať oboch vlastností — a nielen ich kombinácie; neprípustná je každá z nich samostatne.

Po prvé, dôkaz s nulovou znalosťou vyžaduje komunikáciu tam a späť. Ak Alice pošle jedinú správu bez vopred pripraveného dôveryhodného nastavenia, záruka nulovej znalosti sa zrúti — bez ohľadu na to, akej miery spoľahlivosti ste ochotní sa výmenou vzdať.

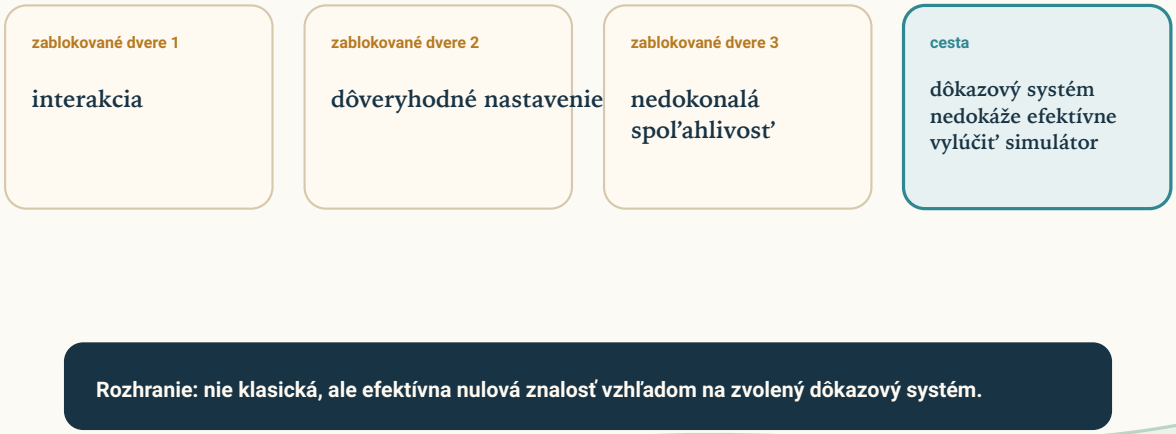
Po druhé, dôkaz s nulovou znalosťou potrebuje malú toleranciu chyby. Požiadavka dokonalej spoľahlivosti totiž nenápadne ruší aj interakciu: overovateľ, ktorého nemožno oklamať pri nijakej voľbe náhodných hodnôt, si ich môže rovno určiť vopred. Keď je overovateľ predvídateľný, Alice môže na všetko odpovedať jedinou správou — a práve tento prípad už zlyhal.

Práca Rahula Ilanga opisuje spôsob, ako túto dvojitú prekážku obísť. Nie predstieraním, že neexistuje, ani vytvorením klasickej nulovej znalosti v nemožnom prostredí. Ťah je jemnejší: oslabiť význam slov „nič neprezradiť“, ale tak, aby sa zachovali bezpečnostné vlastnosti, ktoré kryptografi dokážu skutočne testovať.

Výsledok sa nazýva **efektívna nulová znalosť**.

Dôkaz bez odhalenia svedka

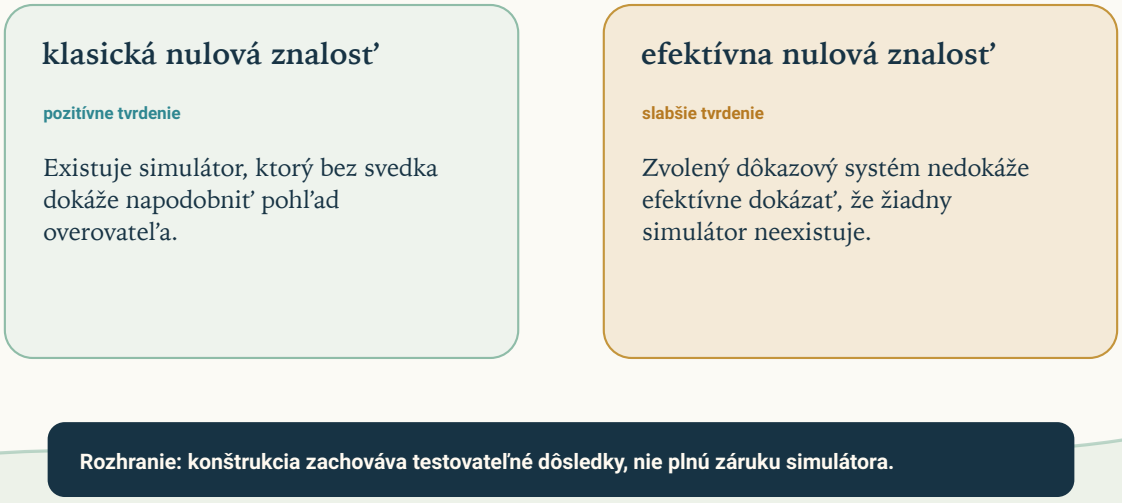
Práca zachováva podobu bežného dôkazu tým, že oslabuje, čo musí súkromie preukázať.



Nulovú znalosť blokujú troje dvere — interakcia, dôveryhodné nastavenie a nedokonalá spoľahlivosť. Ilangova konštrukcia prejde inými: dôkazový systém nedokáže efektívne vyvrátiť existenciu simulátora.

Klasické a efektívne súkromie

Jadrom je oslabenie podmienky: práca mení, čo musí tvrdenie o súkromí preukázať.



Klasická nulová znalosť sa pýta, či simulátor existuje; „efektívna nulová znalosť“ sa pýta iba to, či zvolený dôkazový systém dokáže efektívne preukázať, že simulátor existovať nemôže. Táto slabšia otázka umožňuje

konštrukcii zachovať jednu správu, žiadne počiatočné nastavenie a dokonalú spoľahlivosť.

Starý test: simulátor existuje

Klasický spôsob formalizácie nulovej znalosti využíva fiktívneho pomocníka nazývaného **simulátor**.

Myšlienka je takáto: predstavte si Jane, ktorá **ne** pozná Aliceino tajomstvo. Ak Jane dokáže úplne sama vytvoriť dôkazy, ktoré vyzerajú presne ako dôkazy, ktoré by Bob dostal od Alice, potom Aliceine dôkazy Bobovi nič nové nepriniesli. Jane už dokázala predstierať zážitok bez Aliceinho tajomstva.

Klasická nulová znalosť teda vyžaduje skutočný simulátor. Musí existovať efektívny algoritmus, ktorý vytvorí vierohodne vyzerajúce dôkazy bez znalosti tajomstva — v odbornej reči *svedka*; pri sudoku je svedkom jednoducho vyriešená mriežka.

Táto definícia je silná, ale práve tu sa prejavuje starý výsledok nemožnosti. Intuícia je takáto: skutočne neinteraktívny dôkaz je iba reťazec. Keď ho Bob dostane, môže ho ukázať niekomu ďalšiemu. Získal schopnosť dokazovať tvrdenie iným, čo už znie ako viac než „nič“. Klasické vety túto intuíciu spresňujú do uvedených výsledkov nemožnosti.

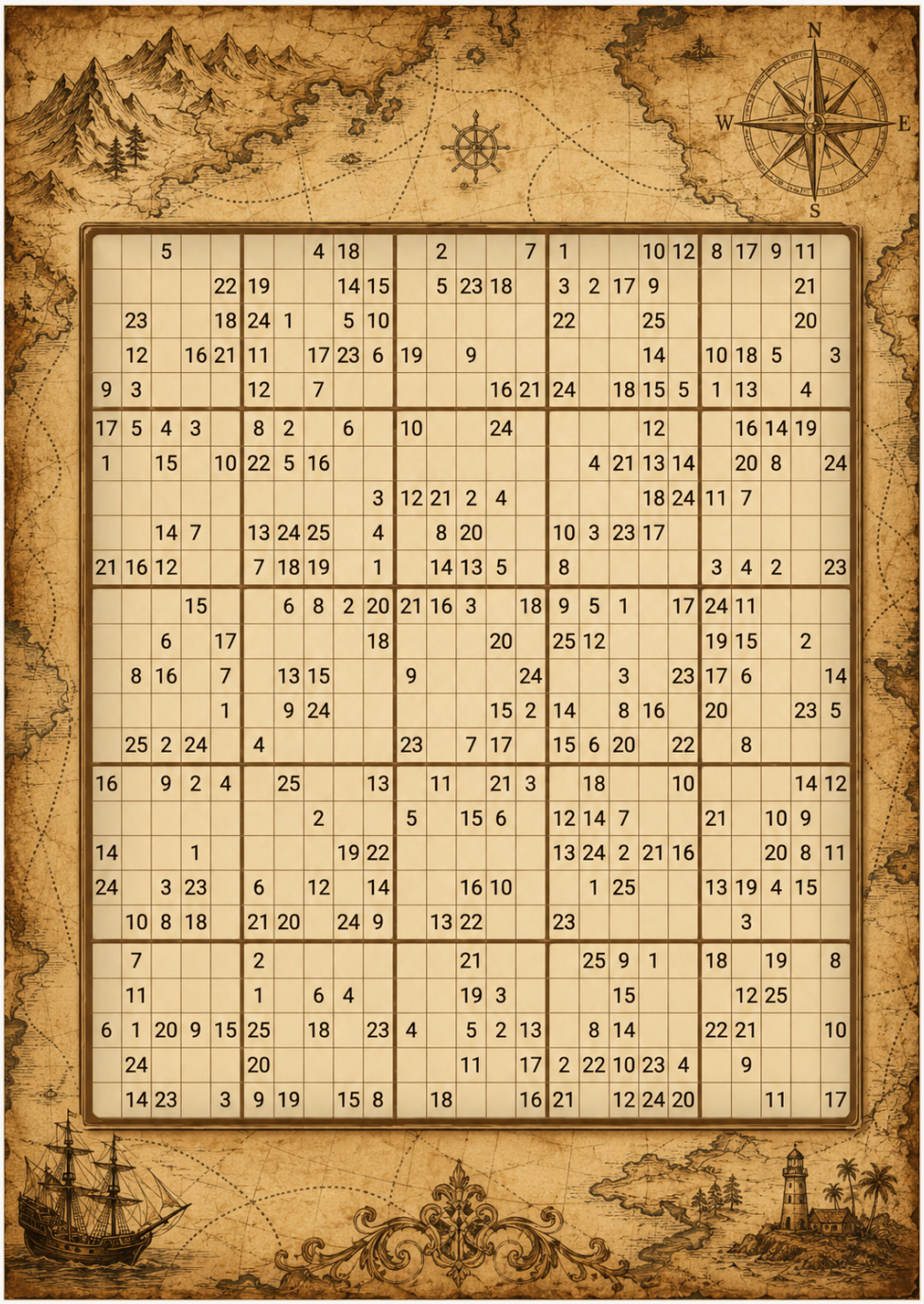
> **Tri vlastnosti, na ktorých táto práca trvá**
>
> Názov článku uvádza tri obmedzenia:
> **Žiadna interakcia:** Alice pošle jediný reťazec dôkazu. Protokol neobsahuje komunikáciu tam a späť.
> **Žiadne počiatočné nastavenie:** Alice a Bob sa nespoliehajú na dôveryhodný spoločný referenčný reťazec ani na inú vopred pripravenú verejnú náhodnosť. Mnohé systémy označované ako „neinteraktívna nulová znalosť“ sa na nastavenie stále spoliehajú; táto práca nevyžaduje nijaké.
> **Dokonalá spoľahlivosť:** nepravdivé tvrdenie nemá platný dôkaz. Nie „takmer nikdy nebude prijaté“; platný dôkaz vôbec neexistuje.
> Tieto tri vlastnosti má bežná písaná matematika — a ako bolo vysvetlené vyššie, klasická nulová znalosť si ich nemôže zachovať.

Mega-Sudoku verzia rozdielu

Tu je zámerne zjednodušený spôsob, ako cítiť rozdiel.

Pri vážnej časti analógie nepoužívajme obyčajné sudoku 9×9. Je príliš malé a konečné: počítač ho jednoducho vyrieši alebo dokáže, že riešenie nemá. Predstavme si namiesto neho rodinu hlavolamov **MegaSudoku(n)**. Zovšeobecnime bežné pravidlo: zvoľme veľkosť bloku n, položme $N = n^2$ a vytvorme mriežku $N \times N$ rozdelenú na bloky $n \times n$ s N symbolmi. Bežné sudoku je iba malý

prípad $n = 3$, $N = 9$: mriežka 9×9, bloky 3×3 a deväť symbolov. Príbeh zložitosti dôkazov sa začína až vtedy, keď n môže rásť a mriežka môže obsahovať ďalšie konštrukčné prvky, vďaka ktorým sa správa ako formula SAT v prestrojení za sudoku. Formula SAT je zoznam podmienok typu áno/nie: možno premenným priradiť hodnoty pravda alebo nepravda tak, aby boli splnené všetky podmienky?



Sudoku 25x25: jeho pravidlá sa dajú skontrolovať bez odhalenia hotovej mriežky — vizuálny zástupca dôkazu, ktorý overuje skryté riešenie, svedka.

Sudoku a SAT: tá istá hádanka v dvoch kostýmoch

Tvrdenie, že Sudoku sa môže "správať ako SAT vzorec", nie je metafora. Preklad prebieha oboma smermi a jednoduchý smer sa dá zapísať celý.

Od sudoku k SAT. SAT pracuje iba s hodnotami pravda/nepravda, preto mu priradíme jednu booleovskú premennú ku každej trojici (riadok, stĺpec, hodnota): *x(r,c,v)* znamená „bunka v riadku *r* a stĺpci *c* obsahuje hodnotu *v*". Sudoku 4 × 4 (bloky 2 × 2, hodnoty 1–4) potrebuje 4·4·4 = 64 premenných; klasické sudoku 9 × 9 ich potrebuje 729. Každé pravidlo sudoku sa potom zmení na súbor klauzúl. (Klauzula je disjunkcia OR premenných alebo ich negácií; celá formula je konjunkciou AND všetkých klauzúl.)

Každá bunka obsahuje aspoň jednu hodnotu — jednu klauzulu na bunku:

x(1,1,1) ∨ x(1,1,2) ∨ x(1,1,3) ∨ x(1,1,4)

Každá bunka obsahuje najviac jednu hodnotu — klauzula „nie obe" pre každú dvojicu hodnôt:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … a tak ďalej pre všetkých šesť párov.

Každý riadok obsahuje každú hodnotu — pre riadok 1 a hodnotu 3: aspoň raz,

x(1,1,3) ∨ x(1,2,3) ∨ x(1,3,3) ∨ x(1,4,3)

a najviac raz: ¬x(1,1,3) ∨ ¬x(1,2,3) a tak ďalej pre každý pár buniek v rade.

Stĺpce a bloky — rovnaké skupiny klauzúl; mení sa iba skupina buniek. Pre ľavý horný blok a hodnotu 2:

x(1,1,2) ∨ x(1,2,2) ∨ x(2,1,2) ∨ x(2,2,2)

plus párové klauzuly „nie obe".

Vytlačené zadania — najjednoduchšia časť: každé zadané číslo je klauzulou s jedinou premennou. Vytlačená trojka v ľavom hornom rohu sa zmení na klauzulu

x(1,1,3)

Konjunkcia všetkých týchto klauzúl je splniteľná práve vtedy, keď má sudoku riešenie — a spĺňajúce priradenie *je* riešením: zistíme, ktoré premenné x(r,c,v) sú pravdivé, a podľa nich vyplníme mriežku. Pri sudoku 9 × 9 dostaneme 729 premenných a niekoľko tisíc klauzúl, ktoré moderný riešič SAT spracuje za milisekundy. Všimnime si klauzulu zadania x(1,1,3): hovorí „táto bunka sa rovná presne 3", nie „všetky tieto bunky sú odlišné". Rovnaká asymetria si v protokolovej poznámke nižšie vyžiada osobitný trik pre bunky zadania.

Od SAT k sudoku. Práca potrebuje opačný a ťažší smer: z *ľubovoľnej* formuly SAT zostrojiť MegaSudoku, ktoré má riešenie práve vtedy, keď je formula splniteľná. Prirodzené pravidlá sudoku vedia povedať iba „všetky tieto bunky sú odlišné", takže ľubovoľné logické obmedzenia treba *zostrojiť* — a práve na to slúžia pomocné konštrukcie. Ide o malé vopred navrhnuté zhluky buniek, po jednom pre každú klauzulu formuly. Vybrané bunky v nich zastupujú premenné (ich symbol kóduje pravdu alebo nepravdu) a vnútorné obmedzenia sú navrhnuté tak, aby povolené vyplnenia zodpovedali iba priradeniam spĺňajúcim klauzulu. Ide o štandardnú

konštrukciu z dôkazov NP-úplnosti; pre zovšeobecnené sudoku ju v roku 2003 opísali Yato a Seta.
Oba smery spolu hovoria, že sudoku N × N a SAT sú rovnakým problémom v dvoch rôznych podobách. Vďaka tomu môže tento text — aj pôvodná práca — pomocou mriežok a symbolov rozprávať príbeh o celej triede NP.

Svedka si stále možno ľahko predstaviť. Alice pozná úplné platné vyplnenie MegaSudoku. Bob sa chce presvedčiť, že také vyplnenie existuje, ale Alice ho nechce prezradiť. Ak ho pošle celé, Bob bude presvedčený, no tajomstvo zmizne.

V klasickej verzii nulovej znalosti Alice s Bobom interagujú. Starší myšlienkový model používa zakryté doštičky. Alice skryje vyriešenú mriežku, pred každým kolom tajne premenuje symboly a Bobovi dovolí skontrolovať jedno náhodne zvolené miestne obmedzenie: riadok, stĺpec, blok alebo pomocnú konštrukciu. Ak odkryté bunky obsahujú navzájom odlišné symboly, Bobova istota vzrastie. Potom sa všetko znovu zakryje a symboly nanovo premenujú. (Je tu jeden háčik: zadané čísla hlavolamu si vyžadujú osobitný trik, pretože premenovanie skryje aj ich. Nasledujúca poznámka vysvetľuje riešenia klasických protokolov; pre ďalší výklad stačí tento zjednodušený obraz.)

Ako klasické protokoly skutočne riešia zadané bunky

Trik s premenovaním má slepé miesto. Pravidlá riadkov, stĺpcov a blokov hovoria „všetky tieto bunky sú odlišné“ a vlastnosť *všetky odlišné* prežije ľubovoľné premenovanie symbolov. Zadanie však hovorí „táto bunka obsahuje presne 5“ a Bob po premenovaní vidí iba $\sigma(5)$, teda zamaskovaný symbol, bez toho, aby poznal premenovanie σ. Nemôže nič overiť. Bez nápravy by Alice mohla dokázať existenciu *nejakej* platnej mriežky a úplne ignorovať vytlačené zadania, čo o *tomto* hlavolame nič nedokazuje. Klasická literatúra ponúka dve štandardné riešenia.
Paleta. Do skrytej mriežky pridáme jeden riadok s N bunkami — paletu, ktorú Alice vyplní symbolmi 1…N v pevnom verejnom poradí a premenuje spolu so všetkým ostatným, takže obsahuje $\sigma(1)$…$\sigma(N)$. Bobova náhodná výzva teraz dostane ďalšiu možnosť. Okrem riadka, stĺpca, bloku alebo pomocnej konštrukcie môže zvoliť **paletu spolu s jednou zadanou bunkou**. Alice odkryje obe; paleta ukáže premenovanie daného kola a Bob overí, že zadaná bunka obsahuje presne premenovanú podobu vytlačeného čísla. Nulová znalosť zostáva zachovaná, pretože Bob sa dozvie iba σ — v každom kole nanovo náhodne zvolené a samo osebe bezcenné — a hodnotu bunky, ktorú už zo zadania poznal. O tajných bunkách nič neunikne a simulátor môže pohľad napodobniť pomocou náhodného σ. Protokol je spoľahlivý, pretože podvádzajúcu Alicu odhalí v každom kole s pevnou pravdepodobnosťou a kolá sa opakujú, kým sa pochybnosť nestane zanedbateľnou.
Zakódovanie zadaní do obmedzení. Štrukturálnejší variant osobitnú výzvu nepridá, ale odstráni. Hodnotu zadania namiesto *overovania* vynúti obmedzeniami nerovnosti: zadanú bunku spojí so všetkými bunkami palety okrem tej, ktorá nesie jej vlastnú hodnotu — „odlišná od $\sigma(1)$, odlišná od $\sigma(2)$, …, odlišná od všetkého okrem $\sigma(5)$“. Jediným symbolom, ktorý môže bunka legálne obsahovať, zostane zadaná hodnota. Každé obmedzenie má opäť tvar „tieto dve hodnoty sa líšia“ — je invariantné voči premenovaniu a možno ho kontrolovať

rovnako ako riadok. Rovnaký postup sa používa pri vopred zafarbených vrcholoch v klasickom protokole farbenia grafov a vystihuje význam vyššie uvedených pomocných konštrukcií: v obraze MegaSudoku ako SAT sa zadania zakódujú do konštrukcií nerovnosti rovnako ako ostatné obmedzenia.
Fyzický protokol. Skutočný kartový protokol pre sudoku (Gradwohl, Naor, Pinkas a Rothblum, 2007) nepoužíva premenovanie a zadané čísla rieši ešte pred začiatkom skrývania. Alice položí na každú bunku tri rovnaké karty s jej hodnotou — lícom nadol pri tajných bunkách, ale **lícom nahor pri zadaných bunkách**, aby Bob na vlastné oči videl dodržanie zadania skôr, než sa karty obrátia. Jedna karta z každej bunky potom putuje do balíčka príslušného riadka, druhá do balíčka stĺpca a tretia do balíčka bloku. Každý balíček sa zamieša a odkryje a Bob overí, že obsahuje všetkých N symbolov. Miešanie zničí informáciu o pozícii, čím zachová nulovú znalosť, zatiaľ čo zadania sa overili už pri rozkladaní kariet.
V oboch prípadoch zostáva rovnaké poučenie, ku ktorému sa tento text vracia: protokol s nulovou znalosťou musí presne evidovať, *ktoré* fakty prežijú skrytie. Premenovanie zachová „všetky odlišné“ a vymaže „rovná sa 5“, preto sa fakt „rovná sa 5“ musí vrátiť iným spôsobom.

Toto nie je protokol z práce. Je to myšlienkový model klasickej nulovej znalosti:

- Alice a Bob komunikujú tam a späť.
- Bob vyberá náhodné kontroly.
- Alice odhaľuje iba lokálnu konzistenciu, nie celé riešenie.
- Dôkaz súkromia funguje tak, že ukazuje, že Bobov pohľad mohol byť generovaný aj bez Aliceinho tajného riešenia.

Klasická nulová znalosť teda stojí na pozitívnom fakte:

> Simulátor naozaj existuje.

Teraz odstráňme pohodlné prvky. Alice pošle jediný reťazec dôkazu a odíde. Neexistuje dôveryhodné počiatočné nastavenie ani vopred pripravený spoločný náhodný reťazec a Bob nesmie nikdy prijať nepravdivý hlavolam. V takom prostredí klasická nulová znalosť nemôže existovať.

Pred vysvetlením triku potrebujeme ešte jednu postavu. Zvoľme si **dôkazový systém** v logickom zmysle — pevnú množinu axióm a mechanické pravidlá na kontrolu zapísaných matematických dôkazov. Kánonickým príkladom je ZFC, štandardný axiomatický systém matematiky. Všetko ďalšie sa vzťahuje na vopred zvolený dôkazový systém; voľba je pritom flexibilná a konštrukcia funguje pre každý pevne zvolený systém vrátane ZFC.

(Terminologická poznámka prevzatá priamo z práce: „dôkazový systém“ tu vždy znamená formálny systém kontrolujúci matematické dôkazy, nikdy správy, ktoré posiela Alice. Mechanizmy Alice a Boba sa nazývajú „dokazovateľ a overovateľ“.)

Gödelovská verzia zachováva príbeh MegaSudoku, ale mení dôkaz.

Zvoľme druhý systém obmedzení rovnakej zobrazenej veľkosti a nazvime ho **D**. V našom príbehu sú

S a D dva hlavolamy MegaSudoku(n) v rovnakom formáte. V pozadí mohlo D vzniknúť z ťažkej logickej formuly inej veľkosti; v prípade potreby sa dá doplniť neškodnými pomocnými obmedzeniami, aby sa zmestilo do rovnakej mriežky. D je zostrojené z logickej formuly, ktorá je v skutočnosti **nesplniteľná**: neexistuje nijaké priradenie hodnôt, ktoré by splnilo všetky jej obmedzenia, rovnako ako chybný hlavolam nemá platne vyplnenú mriežku. Jednoduchým príkladom by bola formula vyžadujúca zároveň „X je pravda“ aj „X je nepravda“. D teda nemá platné vyplnenie.

D však nesmie byť chybným hlavolamom, ktorého chybu možno *ľahko odhaliť*. Uvedený jednoduchý príklad túto podmienku nespĺňa: každý dôkazový systém vyvráti „X a nie X“ jediným riadkom. D musí byť nepravdivé spôsobom, ktorý zvolený systém nedokáže potvrdiť krátkym argumentom. Ak by systém vedel vyvrátiť D krátkym dôkazom, ďalšia konštrukcia by sa zrútila: alternatívnu cestu umožňujúcu vytvárať dôkazy bez Alicinho tajomstva by bolo možné formálne vylúčiť a spolu s ňou aj záruku súkromia. D sa preto vyberá z rodiny, ktorú pevne zvolený dôkazový systém nedokáže efektívne vyvrátiť: v tomto systéme neexistuje krátky dôkaz, že D nemá riešenie.

Alicin dôkaz tvorený jedinou správou sa teda týka výroku buď–alebo:

> buď skutočný mega-Sudoku S má riešenie, alebo návnada D má riešenie.

Toto je logická väzba. D sa **nevytvára** nijakým magickým spôsobom, ktorý by robil S pravdivým. Dôkaz netvrdí „D nemá riešenie, preto S riešenie má“. Dokazuje disjunkciu **S alebo D**. Dokonalá spoľahlivosť znamená, že nepravdivá disjunkcia nemôže mať platný dôkaz. Keďže D je v skutočnosti nepravdivé — nemá riešenie — disjunkcia môže byť pravdivá iba vtedy, ak je pravdivé S. Ak sa teda dôkaz prijme, S musí mať riešenie. Návnada nemôže z nepravdivého S urobiť pravdivé.

Pri časti podobnej nulovej znalosti sa však pýtajme, čo by nastalo, keby D riešenie *malo*. Riešenie návnady by slúžilo ako alternatívny svedok. Umožnilo by vytvárať dôkazy bez znalosti Alicinho skutočného riešenia MegaSudoku — inými slovami, fungovalo by ako simulátor. V skutočnosti D riešenie nemá, takže táto cesta simulácie je uzavretá. Podstatné je, že dôkazový systém nedokáže efektívne preukázať jej uzavretosť.

D teda plní dve úlohy. Pre **spoľahlivosť** je D nepravdivé, takže platný dôkaz výroku „S alebo D“ vynucuje pravdivosť S. Pre **efektívnu nulovú znalosť** sa D ťažko vyvracia, preto dôkazový systém nemôže rýchlo vylúčiť návnadovú cestu, ktorá by umožnila simuláciu.

Takže bezpečnostný test už nie je:

> Môžeme dokázať, že simulátor naozaj existuje?

Znie to:

> Dokáže váš dôkazový systém efektívne preukázať, že simulátor nemôže existovať?

Ak je odpoveď záporná, vyplýva z nej niečo prekvapivo silné: skutočne platí každá bezpečnostná záruka, ktorú (a) možno pozorovať vykonaním testu a (b) podľa daného dôkazového systému

preukázateľne zaručuje existencia simulátora. Úspešný útok na ktorúkoľvek z nich by sám predstavoval chýbajúce krátke vyvrátenie — a také krátke vyvrátenie neexistuje. V tom spočíva „efektívna“ časť efektívnej nulovej znalosti.

Rozdiel možno teda zhrnúť takto:

Klasická nulová znalosť: dôkazy sú bezpečné, pretože existuje simulátor.

Gödelovská efektívna nulová znalosť: dôkazy sa považujú za bezpečné vzhľadom na pozorovateľné bezpečnostné testy, pretože dôkazový systém nedokáže efektívne preukázať nemožnosť simulátora.

Druhé tvrdenie je slabšie. Práve preto si práca môže zachovať tri vlastnosti, ktoré narušili klasickú verziu: jednu správu, žiadne počiatočné nastavenie a dokonalú spoľahlivosť.

Nový test: nemôžete dokázať, že simulátor chýba

Ilangova relaxácia mení otázku.

Klasická nulová znalosť sa pýta:

> Existuje simulátor?

Efektívna nulová znalosť kladie slabšiu otázku:

> Dokáže váš zvolený dôkazový systém efektívne preukázať, že nijaký simulátor neexistuje?

Znie to ako technická obchádzka, ale ide o ústrednú myšlienku. Konštrukcia sa nachádza v nezvyčajnom stave: simulátor v skutočnosti neexistuje — práca to výslovne uvádza — no pevne zvolený dôkazový systém nedokáže efektívne preukázať jeho neexistenciu. Ak by každý nežiaduci dôsledok, na ktorom nám záleží, vyžadoval takéto vyvrátenie, systém sa vzhľadom na tieto dôsledky stále správa ako systém s nulovou znalosťou.

Tu vstupuje do príbehu Gödel. Nie ako ozdoba ani ako tvrdenie „Gödel robí kryptografiu bezpečnou“. Súvislosť patrí do teórie dôkazov. Dôkazový systém sa nazýva **optimálny**, ak je v presnom zmysle najlepší možný: kedykoľvek iný systém dokáže príslušnú formulu vyvrátiť krátkym dôkazom, optimálny systém to dokáže tiež a jeho dôkaz je nanajvýš polynomiálne dlhší. Krajíček a Pudlák v roku 1989 vyslovili hypotézu, že **nijaký optimálny dôkazový systém neexistuje**: nech pevne zvolíme ktorýkoľvek systém, iný dokáže určitú rodinu pravdivých tvrdení omnoho stručnejšie. Ide o jednu z ústredných otvorených hypotéz zložitosti dôkazov a o konečného, komplexnostnoteoretického príbuzného Gödelovej vety o neúplnosti. Niektoré pravdivé tvrdenia nemajú vo zvolenom systéme krátky dôkaz — nie preto, že by sa v zásade nedali dokázať, ale preto, že každý pevný systém ponecháva niektoré krátke pravdy bez krátkeho dôkazu.

Práca túto hypotézu predpokladá v mierne silnejšej podobe „nekonečne často“, ktorá je štandardná pri kryptografickom použití hypotéz. Odmena je podľa vety Krajíčka a Pudláka konkrétna: pre

každý dôkazový systém existuje postupnosť skutočne nesplniteľných formúl, ktoré systém nedokáže vyvrátiť krátkymi dôkazmi — a čo je kľúčové, efektívny algoritmus ich dokáže *generovať*. Táto posledná vlastnosť, uniformita, mení myšlienku z tvrdenia o existencii na skutočný algoritmus, ktorý môže Alice spustiť: jej návnady D prichádzajú z výrobnej linky, nie z ničoho.

Kryptografickým krokom je využiť tento nedostatok dôkaznej sily.

Čo konštrukcia robí

Tu je konštrukcia práce v základných obrysoch.

Pevne zvoľme dôkazový systém, napríklad ZFC. Za predpokladu zo zložitosti dôkazov existuje efektívne generovateľná postupnosť formúl, ktoré sú v skutočnosti nesplniteľné, ale systém nemá krátky dôkaz ich nesplniteľnosti.

Teraz vytvorte dôkaz v jednej správe tohto formátu:

> buď je reálne tvrdenie splniteľné, alebo je splniteľná táto špeciálna tvrdá formula.

Osobitná ťažká formula nie je splniteľná. Ak má teda základný dôkazový mechanizmus dokonalú spoľahlivosť, prijatie správy naďalej znamená, že skutočné tvrdenie je pravdivé. Tým získavame dokonalú spoľahlivosť.

Pri bezpečnosti podobnej nulovej znalosti si však predstavme, že by osobitná ťažká formula *bola* splniteľná. Jej svedok by potom umožnil simulovať dôkazy bez znalosti skutočného svedka. Formula v skutočnosti splniteľná nie je, ale dôkazový systém to nedokáže efektívne preukázať. Nemôže teda efektívne preukázať ani nemožnosť simulátora.

To je rozhodujúci bod. Systém neskrýva tajomstvo vytvorením klasického simulátora. Pri veľkej triede pozorovateľných bezpečnostných testov ho ukrýva za neschopnosťou dôkazového systému potvrdiť, že simulátor neexistuje.

Čo práca tvrdí

Hlavná veta prichádza vo vrstvách. Základný výsledok je tento:

Za štandardného kryptografického predpokladu — existencie **neinteraktívnych dôkazov s nerozlíšiteľnými svedkami**, dobre preskúmaných objektov vyplývajúcich z viacerých zavedených balíkov predpokladov — a za hypotézy zo zložitosti dôkazov, že **neexistuje (nekonečne často) optimálny dôkazový systém**, práca pre každý zvolený dôkazový systém konštruuje dokazovateľa a overovateľa pre NP/SAT s jednou správou, **dokonalou spoľahlivosťou** a bez počiatočného nastavenia, ktorý má vzhľadom na tento systém efektívnu nulovú znalosť. (NP/SAT je štandardným „najťažším spoločným menovateľom“ úloh podobných hlavolamom; MegaSudoku je jednou z jeho podôb.)

Pri širšom tvrdení o zachovaní falzifikovateľných bezpečnostných vlastností práca pridáva ešte jeden štandardný predpoklad, derandomizačnú domnienku **P = BPP** (približne: náhodnosť nedáva algoritmom nijakú podstatnú dodatočnú silu).

Preložené z jazyka vety:

- Dôkaz tvorí jedna správa.
- Neexistuje dôveryhodné počiatočné nastavenie.
- Nepravdivé tvrdenia nemožno dokázať.
- Dokazovateľ nemá klasickú nulovú znalosť — nemá simulátor.
- V tomto prostredí však možno dosiahnuť každý falzifikovateľný herný bezpečnostný dôsledok klasickej nulovej znalosti.

Na slove „falzifikovateľné“ záleží. Znamená, že bezpečnostné zlyhanie možno otestovať spustením protivníka v hre. Mnohé kryptografické definície bezpečnosti majú takúto podobu: dokáže protivník rozlíšiť dve šifrovania, invertovať funkciu, získať svedka alebo vyhrať určený experiment? Veta poskytuje dokazovateľa pre každú falzifikovateľnú vlastnosť osobitne. Jediný dokazovateľ, ktorý by spĺňal *všetky* falzifikovateľné vlastnosti naraz, pravdepodobne nie je možný — starý útok opätovným použitím („Bob môže ukázať dôkaz ďalším ľuďom“) je sám falzifikovateľnou vlastnosťou a v tomto prípade skutočne uspeje. Práca navrhuje, že jediný dokazovateľ by mohol pokrývať všetky *prirodzené* falzifikovateľné vlastnosti, ktoré sa reálne vyskytujú v kryptografickej praxi. Táto časť je však podmienenou vetou založenou na neformálnom pojme „prirodzené“ a na výslovnej hypotéze. Záruka sa zameriava na pozorovateľné zlyhania, nie na každý filozofický alebo simulačný význam utajenia.

Za zmienku stojí jeden konkrétny dôsledok: konštrukcia prináša prvé neinteraktívne dôkazy *skrývajúce svedka* s uniformným dokazovateľom — „dôkaz existencie riešenia hlavolamu vám nepomôže toto riešenie nájsť“ — bez interakcie a počiatočného nastavenia. Tento nenápadne znejúci objekt odolával konštrukcii celé desaťročia.

Čo toto nehovorí

Táto časť udržiava text poctivý.

Nehovorí, že staré vety o nemožnosti boli nesprávne. Konštrukcia sa im vyhýba zmenou definície.

Nedáva bežnú klasickú nulovú znalosť bez interakcie a počiatočného nastavenia a s dokonalou spoľahlivosťou. Práca výslovne uvádza, že zostrojený dokazovateľ nemá simulátor.

Neznamená, že dôkaz nemožno opätovne použiť. Dôkaz v podobe jedinej správy možno stále ukázať niekomu ďalšiemu; práca nezachováva vlastnosti podobné popierateľnosti. (Rovnaké obmedzenie má aj neinteraktívna nulová znalosť s dôveryhodným nastavením.)

To **neznamená**, že ide o praktický protokol pripravený na nasadenie. Ide o teóriu komplexity a kryptografické základy. Výsledok závisí od hlavných predpokladov z dôkazovej zložitosti a kryptografie,

pričom konštrukcia je o tom, čo je možné v princípe.

Nerobí z „Gödela“ magický bezpečnostný primitív. Gödelovská súvislosť vedie cez dôkazové systémy, optimálne dôkazové systémy a konečné analógie neúplnosti. Užitočná intuícia neznie „neúplnosť chráni vaše heslo“. Znie takto: ak dôkazový systém nedokáže efektívne preukázať nemožnosť simulátora, útoky vyžadujúce taký dôkaz možno zablokovať na úrovni bezpečnostných definícií.

Prečo je to vlastne zaujímavé

Kryptografia často premieňa výpočtovú náročnosť na bezpečnosť. Rozklad na prvočísla je ťažký, preto sú užitočné predpoklady typu RSA. Mriežkové problémy sú ťažké, preto je užitočná mriežková kryptografia. Tu je náročnosť nezvyčajnejšia: nie „ťažko vypočítať tajomstvo“, ale „ťažko dokázať, že určitý dôkazový objekt nemôže existovať“.

Preto práca pôsobí nezvyčajne. S axiómami a dôkazovými systémami zaobchádza takmer ako s kryptografickými zdrojmi. Bežný výsledok nemožnosti vyjadruje napätie medzi spoľahlivosťou a simuláciou. Ilangov ťah toto napätie umiestňuje za oponu teórie dôkazov: simulátor neexistuje, ale formálny systém nedokáže jeho neprítomnosť efektívne odhaliť.

Pre čitateľa nie je prekvapením, že by výsledok nahradil dnešné systémy s nulovou znalosťou. Pravdepodobne ich nenahradí, prinajmenšom nie priamo. Prekvapujúce je, že obmedzenie matematickej logiky možno použiť konštruktívne: nielen ako stenu, ale aj ako istý druh krytia.

Aké silné sú dôkazy?

Ide o teoretickú prácu s vetami, takže „dôkazy“ tu znamenajú niečo iné než v biológii alebo astronómii. Nejde o to, či sa experiment podarilo zopakovať, ale či tvrdenie podporujú definície, predpoklady a reťazec matematických dôkazov.

Dôkaz je formálny a práca svoje predpoklady uvádza výslovne. Nie sú zvolené náhodne. Neinteraktívne dôkazy s nerozlíšiteľnými svedkami sú štandardnými objektmi kryptografie a vyplývajú z viacerých zavedených balíkov predpokladov. Hypotéza o neexistencii optimálneho dôkazového systému je ústrednou hypotézou zložitosti dôkazov. P = BPP je štandardná derandomizačná domnienka použitá iba pri širšej vete o falzifikovateľných vlastnostiach.

Práca tiež ukazuje, že predpoklady sú primeranou cenou, nie svojvoľnou oporou: dokazuje opačný smer, podľa ktorého sú v podstate nevyhnutné. Ak takéto konštrukcie vôbec existujú, musia existovať neinteraktívne dôkazy s nerozlíšiteľnými svedkami a pri predpoklade štandardných jednosmerných funkcií nemôže existovať optimálny dôkazový systém. Predpoklady sú navyše výhodné v oboch prípadoch: vyvrátenie ktoréhokoľvek z nich by samo bolo prelomovým objavom v zložitosti dôkazov, kryptografii alebo teórii zložitosti.

Ale keďže výsledok je podmienený, jeho istota je tiež podmienená. Ak tieto predpoklady zlyhajú,

interpretácia vety sa mení. A aj keby predpoklady platili, záruka nie je úplná klasická nulová znalosť; je to oslabená verzia z práce založená na teórii dôkazov.

Primeraná dôvera je teda vysoká v to, že práca stanovuje koherentný podmienený výsledok možnosti; stredná v to, že jej predpoklady opisujú kryptografický svet, v ktorom skutočne žijeme; a nízka v akýkoľvek bezprostredný praktický dôsledok.

Prečo je to dôležité

Práca otvára cestu, ktorá sa považovala za uzavretú.

Klasická teória hovorí: úplná nulová znalosť nemôže mať podobu jedinej správy bez počiatočného nastavenia a nemôže mať dokonalú spoľahlivosť. Ilangova práca hovorí: ak požadujeme tie dôsledky nulovej znalosti, ktoré možno testovať v bezpečnostných hrách, a dovolíme definícii bezpečnosti závisieť od toho, čo dôkazový systém dokáže alebo nedokáže efektívne vyvrátiť, môžeme obnoviť veľkú časť užitočného správania — s jednou správou, bez nastavenia a s dokonalou spoľahlivosťou.

Nejde o drobnú zmenu definície. Je to iný spôsob uvažovania o kryptografických zárukách. Namiesto otázky iba o tom, čo existuje, sa pýtame, čo dokáže dôkazový systém vylúčiť. Namiesto toho, aby sme nedokázateľnosť chápali ako filozofickú nepríjemnosť, použijeme ju ako štruktúru.

Praktický svet sa možno zajtra nezmení, ale pojmová mapa áno. Teraz existuje formálny význam, v ktorom tvrdenie „nikto nedokáže efektívne preukázať, že tajomstvo uniklo“ môže stačiť na obnovenie mnohých herných ochrán, ktoré sme požadovali od tvrdenia „tajomstvo neuniklo“.

Preto Gödel patrí do názvu.

Čisté zhrnutie

Dôkazy s nulovou znalosťou umožňujú dokazovateľovi presvedčiť overovateľa o pravdivosti tvrdenia bez prezradenia svedka. Klasické výsledky nemožnosti hovoria, že nulovú znalosť nemožno vtesnať do jedinej správy bez počiatočného nastavenia a že nemôže mať dokonalú spoľahlivosť. Práca Rahula Ilanga tieto výsledky nevyvracia. Definuje slabší pojem, efektívnu nulovú znalosť: namiesto požiadavky skutočnej existencie simulátora vyžaduje, aby zvolený dôkazový systém — formálny systém ako ZFC — nedokázal efektívne preukázať, že simulátor neexistuje. Za hlavných predpokladov z kryptografie (neinteraktívne dôkazy s nerozlíšiteľnými svedkami) a zložitosti dôkazov (neexistencia optimálneho dôkazového systému) práca konštruuje dokazovateľov pre NP/SAT s jednou správou, bez počiatočného nastavenia a s dokonalou spoľahlivosťou, ktoré postupne dosahujú falzifikovateľné herné dôsledky nulovej znalosti. Jediný dokazovateľ pokrývajúci všetky takéto „prirodzené“ vlastnosti je ďalším, čiastočne hypotetickým rozšírením — a pokrytie doslova každej falzifikovateľnej vlastnosti je pravdepodobne nemožné, pretože dôkazy zostávajú opätovne použiteľné. Výsledok je teoretický a podmienený, nie je nasadeným primitívom, ukazuje však nový spôsob využitia nedokázateľnosti v teórii dôkazov ako kryptografického zdroja.

Kontrola bez nezmyslov

Čo práca ukazuje: Za uvedených predpokladov možno vytvoriť dokazovateľov pre NP/SAT s jednou správou, bez počiatočného nastavenia a s dokonalou spoľahlivosťou, ktorí majú efektívnu nulovú znalosť vzhľadom na ľubovoľný zvolený dôkazový systém a dosahujú každý falzifikovateľný herný dôsledok klasickej nulovej znalosti.

Čo je pravdepodobné, ale nie bezpodmienečne dokázané: Že platia potrebné predpoklady zo zložitosti dôkazov a kryptografie. Sú to seriózne, dobre preskúmané predpoklady — a práca ukazuje, že sú v podstate nevyhnutné aj postačujúce — stále však zostávajú predpokladmi.

Čo neukazuje: Klasickú nulovú znalosť bez interakcie a počiatočného nastavenia a s dokonalou spoľahlivosťou; praktický systém pripravený na nasadenie; popierateľnosť alebo nemožnosť opätovného použitia dôkazov; ani to, že samotná Gödelova veta o neúplnosti zabezpečuje kryptografiu.

Hlavné obmedzenia: Záruka je oslabením nulovej znalosti; najširšia verzia závisí od viacerých predpokladov; tvrdenia o jedinom univerzálnom dokazovateľovi zostávajú sčasti hypotetické; a výsledok má predovšetkým základný teoretický význam.

Koľko dôvery by mal mať bežný čitateľ? Vysokú v to, že pri prijatí definícií ide o významný podmienený teoretický výsledok. Strednú v to, že predpoklady vystihujú realitu. Nízku v okamžité praktické nasadenie. Bezpečný záver znie: práca nevyvracia výsledky nemožnosti nulovej znalosti; nachádza nový spôsob založený na teórii dôkazov, ako obísť tie ich časti, ktoré sú dôležité pre mnohé bezpečnostné hry.

Zdroje

Ilango, IACR ePrint 2025/1296
https://eprint.iacr.org/2025/1296

FOCS 2025, DOI 10.1109/FOCS63196.2025.00058
https://doi.org/10.1109/FOCS63196.2025.00058