The Clean Paper

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

Kryptografický důkaz může skrýt tajemství tím, že ztíží prokázání nepřítomnosti simulátoru

Důkazy s nulovou znalostí umožňují prokázat tvrzení bez odhalení svědka. Klasická teorie říká, že v plném smyslu toho nelze dosáhnout jedinou zprávou, bez důvěryhodného počátečního nastavení a s dokonalou spolehlivostí. Práce Rahula Ilanga tuto nemožnost neruší. Mění cíl: místo požadavku, aby simulátor skutečně existoval, žádá, aby žádný zvolený důkazový systém nedokázal efektivně prokázat, že simulátor neexistuje. Za významných předpokladů z teorie složitosti důkazů a kryptografie to stačí k tomu, aby se — vlastnost po vlastnosti — obnovily falzifikovatelné důsledky nulové znalosti založené na hrách. Nejde o hotový internetový primitiv. Je to způsob vycházející z teorie důkazů, jak proměnit matematickou neprokazatelnost v kryptografické krytí.

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 není v tom, dokázat, že tajemství je skryté

Začněme nejjednodušší podobou nulové znalosti.

Alice chce Boba přesvědčit, že Sudoku hádanka má řešení. Pokud pošle řešení, Bob je přesvědčen, ale hádanka je zničená. To, co chce, je ještě podivnější – důkaz, že řešení existuje, aniž by ho odhalila.

To je příslib důkazu s nulovou znalostí. Dokazovatelka (Alice) přesvědčí ověřovatele (Boba), že tvrzení je pravdivé, aniž odhalí cokoli nad rámec jeho pravdivosti.

Problém je, že tento příslib něco stojí. Běžný matematický důkaz má dvě pohodlné vlastnosti. Je **jedinou zprávou**: sepíšete jej, předáte a odejdete. A je **dokonale spolehlivý**: nepravdivé tvrzení nemá žádný platný důkaz. Klasické výsledky o nemožnosti říkají, že nulová znalost se musí vzdát obou vlastností — a nejen jejich kombinace; každá je nedostupná i samostatně.

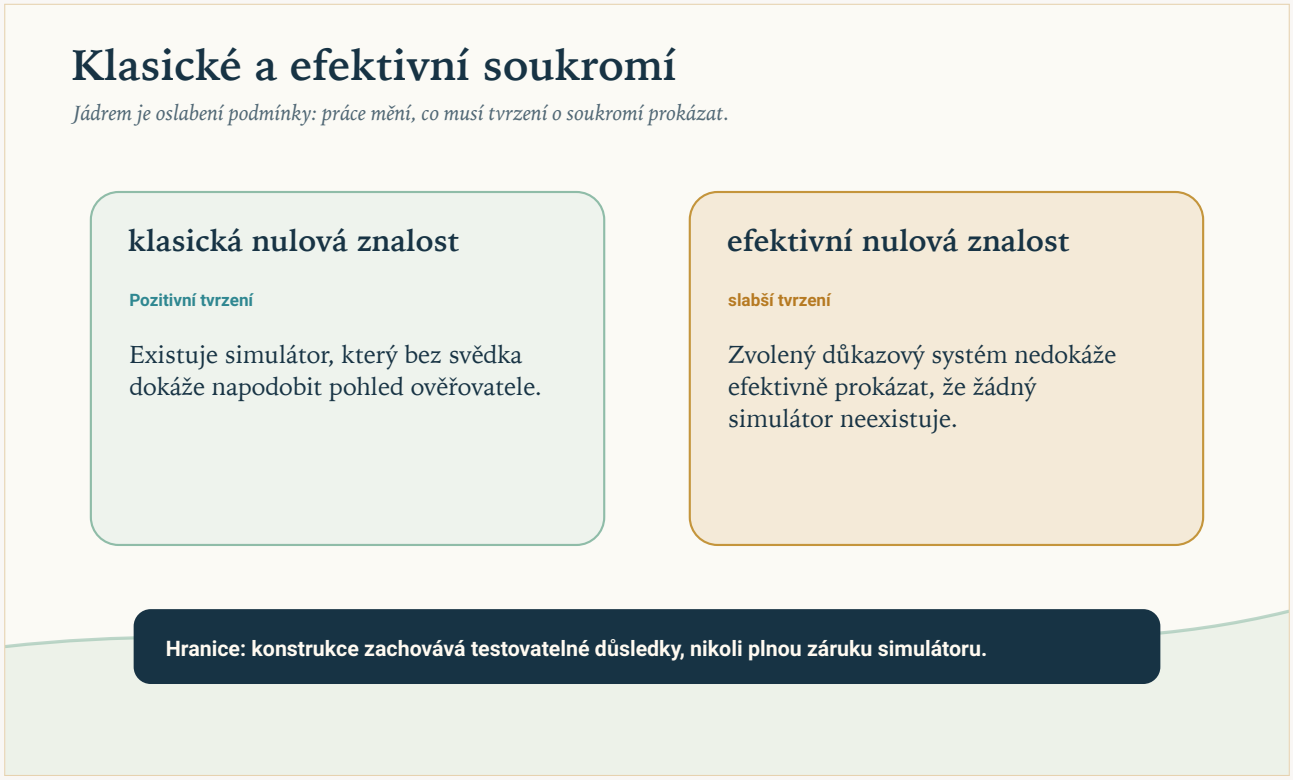
Za prvé, důkaz s nulovou znalostí vyžaduje komunikaci. Pokud Alice pošle jedinou zprávu bez předem připraveného důvěryhodného nastavení, záruka nulové znalosti se zhroutí — bez ohledu na to, jak velkou spolehlivost jsme ochotni obětovat.

Za druhé, důkaz s nulovou znalostí potřebuje malou toleranci chyby. Požadavek dokonalé spolehlivosti nenápadně ničí i interakci: ověřovatel, kterého nelze oklamat bez ohledu na jeho náhodné volby, je může stejně dobře stanovit předem. Jakmile je předvídatelný, Alice dokáže na vše odpovědět jedinou zprávou — tedy právě v případě, který už selhal.

Práce Rahula Ilanga hledá cestu kolem této dvojité zdi. Nepředstírá, že zeď neexistuje, ani nevytváří klasickou nulovou znalost v nemožných podmínkách. Postup je jemnější: oslabit význam slov „nic neodhaluje“, ale způsobem, který zachová bezpečnostní vlastnosti, jež kryptografové skutečně dokážou testovat.

Výsledek se nazývá **efektivní nulová znalost**.

Nulovou znalost blokují troje dveře — interakce, důvěryhodné nastavení a nedokonalá spolehlivost. Ilangova konstrukce prochází jinudy: důkazový systém nedokáže efektivně vyloučit simulátor.



Klasická nulová znalost se ptá, zda simulátor existuje; „efektivní nulová znalost“ se ptá jen na to, zda zvolený důkazový systém dokáže efektivně prokázat, že simulátor existovat nemůže. Tato slabší otázka dovoluje

konstrukci zachovat jedinou zprávu, žádné počáteční nastavení a dokonalou spolehlivost.

Starý test: simulátor existuje

Klasický způsob formalizace nulové znalosti využívá fiktivního pomocníka zvaného **simulátor**.

Myšlenka je tato: představte si Jane, která **nezná** Alicino tajemství. Pokud Jane dokáže sama vytvořit důkazy, které vypadají přesně jako důkazy, které by Bob dostal od Alice, pak Aliceiny důkazy Bobovi nic nového nepřinesly. Jane už dokázala napodobit jeho zkušenost bez Alicina tajemství.

Takže klasická nulová znalost vyžaduje skutečný simulátor. Musí existovat efektivní algoritmus, který dokáže vytvořit zdánlivě pravé důkazy, aniž by znal tajemství — *svědka*, jak se říká v žargonu; pro Sudoku je svědkem jednoduše vyplněná mřížka.

Tato definice je silná, ale právě zde se projeví starý výsledek o nemožnosti. Intuice je následující. Skutečně neinteraktivní důkaz je jen řetězec. Jakmile Bob tento řetězec má, může jej ukázat někomu jinému: získal schopnost dokázat tvrzení ostatním, což už zní jako víc než „nic“. Klasické věty tuto intuici zpřesňují do výše uvedených výsledků o nemožnosti.

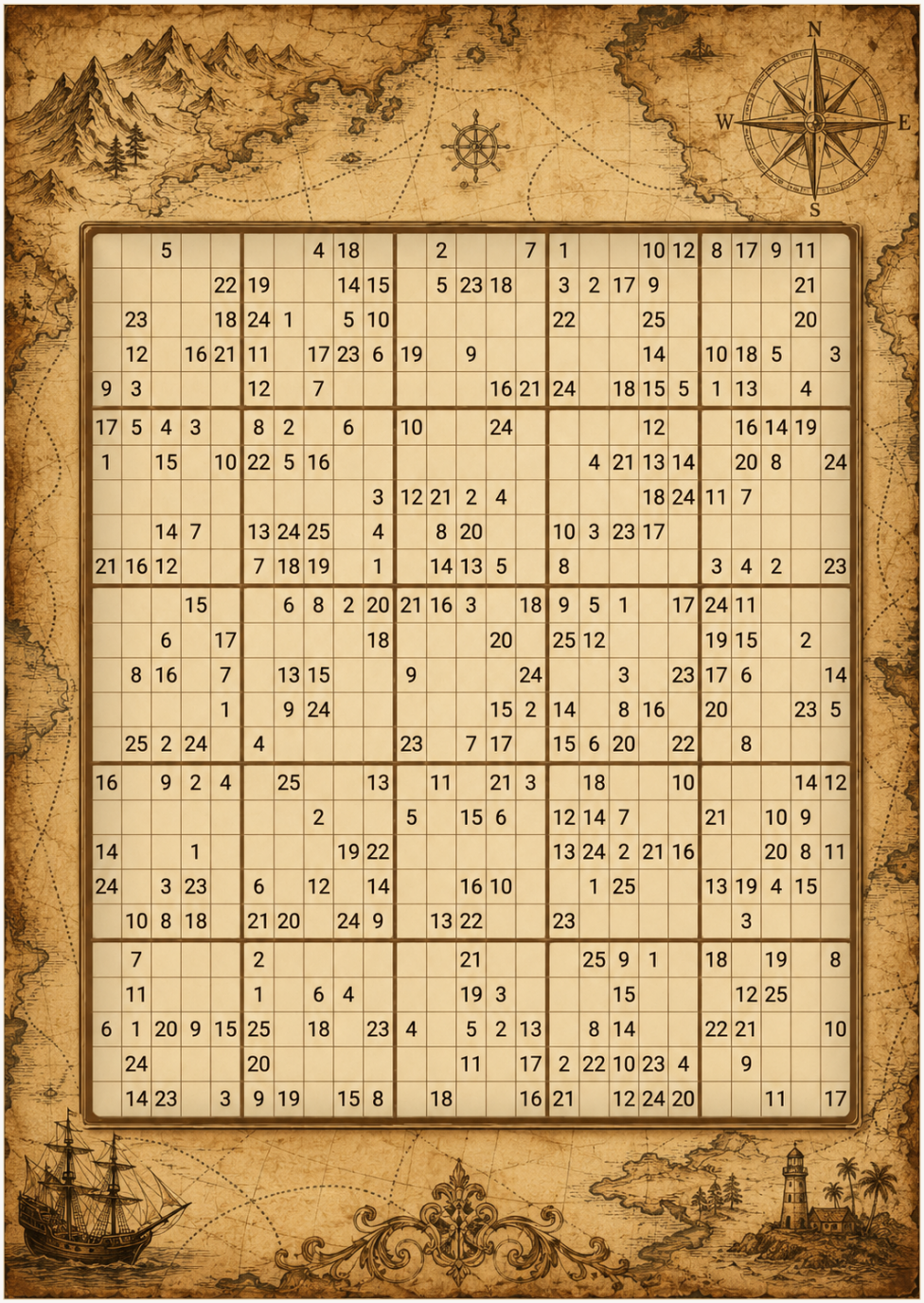
> **Tři vlastnosti, na nichž tato práce trvá**
>
> Název práce uvádí tři omezení:
> **Žádná interakce:** Alice pošle jediný řetězec tvořící důkaz. Nenásleduje žádná výměna zpráv.
> **Žádné počáteční nastavení:** Alice a Bob se nespoléhají na důvěryhodný společný referenční řetězec ani jiné předem připravené veřejné náhodné hodnoty. Mnoho systémů označovaných jako „neinteraktivní nulová znalost“ přesto nastavení vyžaduje; tato práce nevyžaduje žádné.
> **Dokonalá spolehlivost:** nepravdivé tvrzení nemá žádný platný důkaz. Nejde o to, že bude „téměř vždy odmítnuto“; platný důkaz vůbec neexistuje.
> Tyto tři vlastnosti jsou přesně tím, co má běžná psaná matematika — a jak bylo vysvětleno výše, klasická nulová znalost je nemůže zachovat.

Rozdíl na příkladu mega-Sudoku

Tady je záměrně zjednodušený způsob, jak ten rozdíl vnímat.

Pro vážnější část analogie nepoužívejme běžné sudoku 9×9. Je příliš malé a příliš konečné: počítač je může jednoduše vyřešit nebo dokázat, že řešení nemá. Místo toho si představme rodinu hádanek **MegaSudoku(n)**. Zobecněme obvyklé pravidlo: zvolme velikost bloku n, položme $N = n^2$ a vytvořme mřížku $N \times N$, rozdělenou na bloky $n \times n$ a používající N symbolů. Běžné sudoku je jen malý případ $n = 3$, $N = 9$: mřížka 9×9, bloky 3×3 a devět symbolů. Příběh složitosti důkazů začíná až tehdy, když n

může růst a mřížka může obsahovat další gadgety, díky nimž se chová jako formule SAT převlečená za sudoku. Formule SAT je pouze seznam logických omezení: lze proměnným přiřadit hodnoty pravda či nepravda tak, aby byla splněna všechna omezení?



Sudoku 25 × 25: jeho pravidla lze zkontrolovat bez odhalení hotové mřížky — názorná obdoba důkazu ověřujícího skryté řešení, tedy svědka.

Sudoku a SAT: stejná hádanka ve dvou kostýmech

Tvrzení, že se sudoku může „chovat jako formule SAT“, není metafora. Překlad funguje oběma směry a snadnější směr lze popsat celý.

Od sudoku k SAT. SAT pracuje pouze s hodnotami pravda a nepravda, proto zaveďme jednu booleovskou proměnnou pro každou trojici (řádek, sloupec, hodnota): *x(r,c,v)* znamená „buňka v řádku *r* a sloupci *c* obsahuje hodnotu *v*“. Sudoku 4 × 4 (bloky 2 × 2, hodnoty 1–4) potřebuje 4 · 4 · 4 = 64 proměnných; klasické sudoku 9 × 9 jich potřebuje 729. Každé pravidlo sudoku se pak stane souborem klauzulí. (Klauzule je disjunkce proměnných nebo jejich negací; celá formule je konjunkcí všech klauzulí.)

Každá buňka obsahuje alespoň jednu hodnotu — jednu klauzuli na buňku:

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

Každá buňka má nejvýše jednu hodnotu — klauzuli “ne obě” pro každou dvojici hodnot:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … a tak dále pro všech šest párů.

Každý řádek obsahuje každou hodnotu — pro řádek 1 a hodnotu 3: alespoň jednou,

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

a nejvýše jednou: ¬x(1,1,3) ∨ ¬x(1,2,3) a tak dále pro každý pár buněk v řadě.

Sloupce a bloky — identické šarže; mění se pouze skupina buněk. Pro blok vlevo nahoře a hodnotu 2:

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

plus párové věty “ne obě”.

Tištěné nápovědy — nejjednodušší část: každá nápověda je klauzule s jednou proměnnou. Vytištěná trojka v levém horním rohu se stává klauzulí

x(1,1,3)

Konjunkce všech těchto klauzulí je splnitelná právě tehdy, když má sudoku řešení — a splňující přiřazení *je* řešením: stačí přečíst, které proměnné x(r,c,v) jsou pravdivé, a vyplnit mřížku. Pro mřížku 9 × 9 to znamená 729 proměnných a několik tisíc klauzulí, které moderní řešič SAT zpracuje během milisekund. Všimněte si klauzule pro zadanou hodnotu x(1,1,3): říká „tato buňka se rovná právě 3“, nikoli „tyto buňky jsou všechny navzájem různé“ — jde o tutéž asymetrii, která si v protokolární poznámce níže vyžádá další trik pro buňky se zadanými hodnotami.

Od SAT k Sudoku. Práce potřebuje opačný, tvrdší směr: s *libovolným* SAT vzorcem vytvořit mega-Sudoku, které má řešení právě tehdy, když je formule splnitelná. Vlastní pravidla sudoku dokážou říci jen “tyto buňky jsou všechny různé”, takže je třeba *postavit* libovolná logická omezení — a přesně to tyto gadgety jsou. Gadget je malý předpřipravený shluk buněk, jeden na každou klauzuli vzorce, ve kterém určené buňky hrají roli proměnných (symbol, který drží, kóduje pravdivé nebo nepravdivé) a vnitřní omezení shluku jsou navržena tak, že jeho

jediná legální vyplnění odpovídají ohodnocením splňujícím danou klauzuli. To je standardní řemeslná práce na důkazech NP-úplnosti; pro generalizované sudoku ji provedli Yato a Seta v roce 2003.
Oba směry společně říkají, že sudoku $N \times N$ a SAT jsou tentýž problém v různých převlecích. Právě proto může tento článek — a také vědecká práce — vyprávět pomocí mřížek a symbolů příběh o celé třídě NP.

Svědka si lze stále snadno představit. Alice zná úplné platné vyplnění mega-Sudoku. Bob chce být přesvědčen, že takové vyplnění existuje, ale Alice je nechce prozradit. Když je pošle celé, Bob je přesvědčen, ale tajemství je pryč.

V klasické verzi s nulovou znalostí Alice a Bob interagují. Jeden starý mentální model používá zakryté destičky. Alice schová vyřešenou mřížku, před každým kolem tajně přejmenuje symboly a nechá Boba prohlédnout si jedno náhodně vybrané lokální omezení: řádek, sloupec, blok nebo gadget. Pokud odkryté buňky ukazují různé symboly, Bob získává jistotu. Pak se vše znovu zakryje a symboly se znovu přejmenují. (Je tu jedna zvláštnost: zadané hodnoty hádanky potřebují další trik, protože přejmenování symbolů skryje i je. Poznámka níže vysvětluje, jak klasické protokoly tento problém řeší; pro další výklad tento zjednodušený obraz stačí.)

Jak klasické protokoly skutečně zacházejí s buňkami nápovědy

Trik s přejmenováním má slepou skvrnu. Pravidla řádků, sloupců a políček říkají "tyto buňky jsou všechny odlišné" a *všechny odlišné* přežijí jakékoli přejmenování symbolů. Ale nápověda říká "tato buňka obsahuje přesně 5" a po přejmenování Bob vidí jen $\sigma(5)$ — nějaký maskovaný symbol — aniž by znal σ přejmenování. Nemůže nic zkontrolovat. Bez opravy by Alice, mohla by dokázat, že *nějaká* platná mřížka existuje, a přitom zcela ignorovala tištěné nápovědy, což nic nedokazuje o *této* hádance. Klasická literatura má dvě standardní opravy.
Paleta. Přidejte do skryté mřížky jeden další řádek N buněk — paletu, kterou Alice vyplní symboly 1…N v pevném veřejném pořadí a pak ji přejmenovává spolu se vším ostatním, takže obsahuje $\sigma(1)$…σ(N). Bobova náhodná výzva má nyní jednu možnost navíc. Kromě výběru řádku, sloupce, bloku nebo gadgetu k otevření může zvolit **paletu spolu s jednou buňkou se zadanou hodnotou**. Alice odhalí obojí; paleta ukáže přejmenování použité v daném kole a Bob zkontroluje, zda buňka ukazuje právě přejmenovanou podobu zadané hodnoty. Protokol si zachovává nulovou znalost, protože Bob se dozvídá pouze σ — která se v každém kole nově náhodně volí a sama o sobě je bezcenná — a hodnotu buňky, kterou už znal ze zadání. Z tajných buněk nic neunikne a simulátor může pohled napodobit volbou náhodné permutace σ. Protokol je spolehlivý, protože podvádějící Alice je v každém kole odhalena s pevnou pravděpodobností a kola se opakují, dokud není pravděpodobnost omylu zanedbatelná.
Zabudování zadaných hodnot. Strukturálnější varianta zvláštní výzvu nepřidává, ale odstraňuje. Místo *ověření* zadané hodnoty ji vynutí pomocí omezení nerovnosti: buňku se zadanou hodnotou propojí se všemi buňkami palety kromě té, která nese její vlastní hodnotu — „odlišná od $\sigma(1)$, odlišná od $\sigma(2)$, …, odlišná od všeho kromě $\sigma(5)$". Jediným symbolem, který pak buňka může legálně obsahovat, je symbol zadané hodnoty. Každé omezení je opět typu

> „tyto dvě hodnoty se liší“ — je invariantní vůči přejmenování a kontrolovatelné stejně jako řádek. Jde o tentýž postup, jaký se používá pro předem obarvené vrcholy v klasickém protokolu barvení grafů, a vystihuje smysl výše zmíněných *gadgetů*: v obrazu mega-Sudoku jako SAT jsou zadané hodnoty převedeny na gadgety nerovnosti stejně jako každé jiné omezení.
> **Fyzický protokol.** Skutečný karetní protokol pro sudoku (Gradwohl, Naor, Pinkas a Rothblum, 2007) nepoužívá žádné přejmenování a zadané hodnoty ověří ještě před začátkem skrývání. Na každou buňku Alice položí tři stejné karty s její hodnotou — lícem dolů u tajných buněk, ale **lícem nahoru u buněk se zadanými hodnotami**, takže Bob na vlastní oči vidí, že jsou dodrženy, ještě než se karty otočí. Potom jde jedna karta z každé buňky do balíčku pro řádek, jedna do balíčku pro sloupec a jedna do balíčku pro blok; každý balíček se zamíchá a odkryje a Bob zkontroluje, zda obsahuje všech N symbolů. Míchání zničí informaci o poloze (a tím zachová nulovou znalost), zatímco zadané hodnoty byly pevně ověřeny už při rozdávání.
> V obou případech je poučení stejné a práce se k němu opakovaně vrací: protokol s nulovou znalostí musí pečlivě sledovat, *které* skutečnosti skrývání přežijí. Přejmenování zachovává vlastnost „všechny různé“ a maže vlastnost „rovná se 5“ — takže „rovná se 5“ se musí do protokolu vrátit jinou cestou.

To není protokol z této práce. Je to mentální model pro klasickou nulovou znalost:

- Alice a Bob si vyměňují zprávy.
- Bob vybírá náhodné kontroly.
- Alice odhaluje pouze lokální konzistenci, nikoli celé řešení.
- Důkaz soukromí funguje tak, že ukazuje, že Bobův pohled mohl být generován i bez Aliceina tajného řešení.

Klasická nulová znalost je tedy založena na pozitivním faktu:

> Simulátor opravdu existuje.

Teď odstraňte ty pohodlné části. Alice pošle jeden řetězec tvořící důkaz a odejde. Neexistuje žádné důvěryhodné počáteční nastavení, žádný předem připravený sdílený náhodný řetězec a Bob nikdy nesmí přijmout nepravdivé tvrzení. To je prostředí, které klasická nulová znalost nemůže přežít.

Před vlastní myšlenkou potřebujeme ještě jednu postavu. Zvolme **soubor pravidel**: formální důkazový systém v logickém smyslu — pevnou sadu axiomů a mechanických pravidel pro kontrolu zapsaných matematických důkazů. Kanonickým příkladem je ZFC, standardní axiomatický systém matematiky. Vše další se vztahuje k předem zvolenému systému; volba je libovolná a konstrukce funguje pro každý pevně zvolený systém včetně ZFC.

(Terminologická poznámka převzatá z práce: „důkazový systém“ zde vždy znamená tento soubor pravidel — formální systém kontrolující matematické důkazy — nikdy zprávy, které posílá Alice. Mechanismy Alice a Boba se nazývají „dokazovatel a ověřovatel“.)

Gödelovská verze zachovává příběh mega-Sudoku, ale mění důkaz.

Vyberme druhý systém omezení stejné zobrazené velikosti a nazvěme jej **D**. Pro účely příběhu jsou S a D dvě hádanky MegaSudoku(n) ve stejném formátu. V zákulisí mohl D vzniknout jako obtížná logická formule jiné velikosti; je-li třeba, lze ji doplnit neškodnými fiktivními omezeními, aby se vešla do stejné mřížky. D je vytvořeno z logické formule, která je ve skutečnosti **nesplnitelná**: neexistuje přiřazení hodnot, jež by učinilo všechna její omezení pravdivými, stejně jako rozbitá hádanka nemá žádné legální úplné vyplnění. Jednoduchým příkladem by byla formule vyžadující zároveň „X je pravda“ a „X je nepravda“. D tedy nemá platné vyplnění.

Ale D nesmí být rozbitá hádanka, jejíž rozbitost lze *snadno odhalit*. Uvedený jednoduchý příklad nevyhovuje: každý důkazový systém vyvrátí „X a ne-X“ v jediné větě. D musí být nepravdivé způsobem, který zvolený důkazový systém nedokáže potvrdit krátkým argumentem. Kdyby důkazový systém dokázal D vyvrátit krátkým důkazem, následující příběh by se zhroutil: alternativní cesta k důkazům bez Alicina tajemství by mohla být formálně vyloučena, a s ní i záruka soukromí. D se proto vybírá z rodiny, kterou pevně zvolený důkazový systém nedokáže efektivně vyvrátit: v tomto systému neexistuje krátký důkaz, že D nemá řešení.

Alicin jednozprávový důkaz je pak o výroku buď–anebo:

> buď má skutečný mega-Sudoku S řešení, nebo návnada D má řešení.

To je logické spojení. D **není** generováno nějakým magickým způsobem, který by činil S pravdivým. Důkaz netvrdí “D nemá řešení, tedy S má řešení.” Dokazuje disjunkci **S nebo D**. Dokonalá spolehlivost říká, že falešná disjunkce nemůže mít platný důkaz. Protože D je ve skutečnosti nepravdivé — nemá řešení — jediný způsob, jak může být disjunkce pravdivá, je, aby S byla pravdivá. Pokud je důkaz přijat, musí mít S řešení. Falešná formule nemůže falešné S učinit pravdivým.

Pro část připomínající nulovou znalost se však ptejme, co by se stalo, kdyby D *mělo* řešení. Toto řešení nepravdivé formule by sloužilo jako alternativní svědek. Umožnilo by někomu vytvářet důkazy bez znalosti skutečného Alicina řešení mega-Sudoku — tedy fungovat jako simulátor. Ve skutečnosti D řešení nemá, takže tato simulační cesta je uzavřena. Podstatné je, že důkazový systém nedokáže efektivně dokázat, že je uzavřena.

D tedy plní dvě úlohy. Pro **spolehlivost** je D nepravdivé, takže platný důkaz „S nebo D“ vynucuje pravdivost S. Pro **efektivní nulovou znalost** je D obtížné vyvrátit, takže důkazový systém nemůže rychle vyloučit alternativní cestu, která by simulaci umožnila.

Takže bezpečnostní test už není:

> Můžeme dokázat, že simulátor skutečně existuje?

Stává se to:

> Dokáže váš důkazový systém efektivně dokázat, že simulátor nemůže existovat?

Pokud je odpověď ne, vyplývá z toho něco překvapivě silného: každá bezpečnostní záruka, kterou (a) lze pozorovat spuštěním testu a (b) prokazatelně vyplývá — v tomto důkazovém systému — z

existence simulátoru, skutečně platí. Úspěšný útok proti kterékoli z nich by sám o sobě znamenal chybějící krátké vyvrácení, a takové krátké vyvrácení neexistuje. To je ta “efektivní” část efektivní nulové znalosti.

Takže kontrast ve třídě je následující:

Klasická nulová znalost: důkazy jsou bezpečné, protože existuje simulátor.

Gödelovská efektivní nulová znalost: důkazy jsou považovány za bezpečné pro pozorovatelné bezpečnostní testy, protože důkazový systém nedokáže efektivně dokázat, že simulátor nemůže existovat.

Druhé tvrzení je slabší. Je to také důvod, proč si práce může zachovat tři rysy, které klasickou verzi zlomily: jednu zprávu, žádné počáteční nastavení a dokonalou spolehlivost.

Nový test: nelze dokázat, že simulátor chybí

Ilangovo oslabení mění otázku.

Klasická nulová znalost se ptá:

> Existuje nějaký simulátor?

Efektivní nulová znalost se ptá na něco slabšího:

> Dokáže váš zvolený důkazový systém efektivně dokázat, že žádný simulátor neexistuje?

Zní to jako technický úskok, ale je to základní myšlenka. Konstrukce žije v podivném stavu: simulátor ve skutečnosti neexistuje — práce to výslovně uvádí — ale důkazový systém, který jste zvolili, nemůže efektivně dokázat, že neexistuje. I kdyby každý špatný důsledek, na kterém vám záleží, vyžadoval takové vyvrácení, systém se vůči těmto důsledkům stále chová jako systém s nulovou znalostí.

Tady přichází na scénu Gödel. Ne jako ozdoba ani ve smyslu „Gödel zabezpečuje kryptografii“. Souvislost vede přes teorii důkazů. Důkazový systém se nazývá **optimální**, pokud je v přesném smyslu nejlepší možný: kdykoli libovolný systém dokáže příslušnou formuli vyvrátit krátkým důkazem, dokáže to i optimální důkazový systém, přičemž jeho důkaz je nanejvýš polynomiálně delší. Krajíček a Pudlák v roce 1989 vyslovili domněnku, že **žádný optimální důkazový systém neexistuje**: ať zvolíme jakýkoli systém, jiný systém dokáže určitou rodinu pravdivých tvrzení prokazovat mnohem stručněji. Jde o jednu z ústředních otevřených domněnek teorie složitosti důkazů a o konečný protějšek Gödelovy věty o neúplnosti z teorie složitosti: některá pravdivá tvrzení nemají ve zvoleném systému krátký důkaz — nikoli proto, že by byla z principu nedokazatelná, ale proto, že každý pevně zvolený důkazový systém ponechává některé stručně formulované pravdy bez krátkých důkazů.

Práce tuto domněnku předpokládá v mírně silnější podobě „nekonečně často“, která je při kryptografickém využití domněnek standardní. Věta Krajíčka a Pudláka pak dává konkrétní výsledek: pro

každý důkazový systém existuje posloupnost skutečně nesplnitelných formulí, které tento systém nedokáže vyvrátit krátkými důkazy — a především je dokáže efektivní algoritmus *generovat*. Poslední vlastnost, uniformita, mění tvrzení o existenci ve skutečný algoritmus, který Alice může spustit: její formule D vznikají systematicky, nikoli z ničeho.

Kryptografický tah spočívá v tom, že tento nedostatek důkazové síly je využit.

Co konstrukce dělá

Zde je konstrukce práce zbavená podrobností.

Zvolte důkazový systém — například ZFC. Za předpokladu z teorie složitosti důkazů existuje efektivně generovatelná posloupnost formulí, které jsou ve skutečnosti nesplnitelné, ale zvolený systém nemá žádný krátký důkaz jejich nesplnitelnosti.

Nyní vytvořte jednozprávový důkaz této formy:

> buď je reálné tvrzení splnitelné, nebo je tato speciální tvrdá formule splnitelná.

Speciální obtížná formule není splnitelná. Pokud je tedy základní důkazový mechanismus dokonale spolehlivý, přijetí zprávy stále znamená, že skutečné tvrzení je pravdivé. Tím se zachová dokonalá spolehlivost.

Ale pro bezpečnost typu nulové znalosti si představte, že by speciální tvrdý vzorec *byl* splnitelný. Pak by jeho svědek mohl být použit k simulaci důkazů bez znalosti skutečného svědka. Vzorec není ve skutečnosti splnitelný — ale důkazový systém to nedokáže efektivně dokázat. Takže nemůže efektivně dokázat, že simulátor nemůže existovat.

To je klíčový bod. Systém neskrývá tajemství vytvořením klasického simulátoru. Pro širokou třídu pozorovatelných bezpečnostních testů je chrání neschopnost důkazového systému potvrdit, že simulátor chybí.

Co práce tvrdí

Hlavní věta přichází ve vrstvách. Hlavní výsledek je tento:

Za standardního kryptografického předpokladu — existence **neinteraktivních důkazů s nerozlišitelnými svědky**, dobře prozkoumaných objektů odvozených z několika zavedených souborů předpokladů — a za domněnky z teorie složitosti důkazů, že **neexistuje žádný (nekonečně často) optimální důkazový systém**, práce pro každý zvolený důkazový systém konstruuje dvojici jednozprávového dokazovatele a ověřovatele pro NP/SAT, která nemá žádné počáteční nastavení, je **dokonale spolehlivá** a vůči tomuto systému má efektivní nulovou znalost. (NP/SAT je standardní „nejtěžší společný jmenovatel“ problémů podobných hádankám; mega-Sudoku je jedním z jeho

převleků.)

Pro širší tvrzení o zachování falzifikovatelných bezpečnostních vlastností práce přidává další standardní předpoklad, derandomizační domněnku **P = BPP** (přibližně: náhodnost algoritmům nedává žádnou podstatnou dodatečnou moc).

Přeloženo z jazyka vět:

- Důkaz tvoří jediná zpráva.
- Neexistuje žádné důvěryhodné počáteční nastavení.
- Nepravdivá tvrzení nelze prokázat.
- Dokazovatel nemá klasickou nulovou znalost — neexistuje pro něj simulátor.
- Lze však dosáhnout každého falzifikovatelného bezpečnostního důsledku klasické nulové znalosti definovaného hrou.

„Falzifikovatelné“ je důležité. Znamená to, že bezpečnostní selhání lze otestovat spuštěním protivníka ve hře. Mnoho kryptografických bezpečnostních definic má tuto podobu: dokáže útočník rozlišit dva šifrové texty, obrátit funkci, získat svědka nebo vyhrát určitý experiment? Věta poskytuje dokazovatele pro každou falzifikovatelnou vlastnost, jednu po druhé. Jeden dokazovatel, který by měl *všechny* falzifikovatelné vlastnosti současně, je pravděpodobně nemožný — starý útok na znovupoužitelnost („Bob může ukázat důkaz ostatním“) je sám falzifikovatelnou vlastností a právě ta zde skutečně neplatí. Práce navrhuje, že jeden dokazovatel by mohl věrohodně pokrýt všechny *přirozené* falzifikovatelné vlastnosti — ty, které se skutečně vyskytují v kryptografické praxi — tato část je však podmíněným tvrzením založeným na neformálním pojmu „přirozenosti“ a na explicitní domněnce. Záruka míří na pozorovatelná selhání, nikoli na všechny filozofické či simulační významy skrývání.

Jeden konkrétní důsledek stojí za zmínku: konstrukce přináší první neinteraktivní důkazy *skrývající svědka* s uniformním dokazovatelem — „důkaz řešitelnosti hádanky vám nepomůže najít její řešení“, bez interakce a bez počátečního nastavení — skromně znějící objekt, který konstrukci odolával desítky let.

Co práce neříká

Tato část udržuje text poctivý.

Neříká, že staré věty o nemožnosti byly špatné. Konstrukce se jim vyhýbá změnou definice.

Nedává běžnou klasickou nulovou znalost bez interakce, bez počátečního nastavení a s dokonalou spolehlivostí. Práce výslovně uvádí, že zkonstruovaný dokazovatel nemá simulátor.

To neznamená, že důkaz nelze znovu použít. Důkaz tvořený jedinou zprávou lze stále ukázat někomu jinému; práce nezachovává vlastnosti, jako je popiratelnost. (Neinteraktivní nulová znalost s důvěryhodným počátečním nastavením má stejné omezení.)

Neznamená to, že jde o praktický protokol připravený k nasazení. Práce patří k teorii složitosti a

základům kryptografie. Výsledek závisí na hlavních předpokladech teorie složitosti důkazů a kryptografie a konstrukce ukazuje, co je možné v principu.

To z „Gödla“ nedělá magický bezpečnostní primitiv. Souvislost s Gödlem vede přes důkazové systémy, optimální důkazové systémy a konečné obdoby neúplnosti. Užitečná intuice nezní „neúplnost chrání vaše heslo“. Zní takto: pokud důkazový systém nedokáže efektivně dokázat, že simulátor nemůže existovat, lze na úrovni bezpečnostních definic zablokovat útoky, které by takový důkaz vyžadovaly.

Proč je to vlastně zajímavé

Kryptografie často proměňuje obtížnost v bezpečnost. Rozklad na prvočinitele je obtížný, a proto jsou užitečné předpoklady ve stylu RSA. Mřížkové problémy jsou obtížné, a proto je užitečná mřížková kryptografie. Zde je obtížnost nezvyklejší: nikoli „je těžké vypočítat tajemství“, ale „je těžké dokázat, že určitý důkazový objekt nemůže existovat“.

Proto tato práce působí neobvykle. S axiomy a důkazovými systémy zachází téměř jako s kryptografickými zdroji. Obvyklá nemožnost říká, že existuje napětí mezi spolehlivostí a simulací. Ilango se snaží umístit napětí za důkazově-teoretickou oponu: simulátor chybí, ale formální systém tuto absenci nedokáže efektivně odhalit.

Překvapením nemá být, že by tento přístup měl nahradit dnešní systémy s nulovou znalostí. Pravděpodobně je nenahradí, alespoň ne přímo. Překvapivé je, že omezení matematické logiky lze využít konstruktivně: nejen jako zeď, ale také jako určitý druh krytí.

Jak silné jsou důkazy?

Jde o teoretickou práci, takže „důkazy“ zde znamenají něco jiného než v biologii nebo astronomii. Otázkou není, zda byl experiment zopakován, ale zda tvrzení podporují definice, předpoklady a řetězec formálních důkazů.

Důkazní řetězec je formální a práce své předpoklady výslovně uvádí. Nejde o nahodilé volby. Neinteraktivní důkazy s nerozlišitelnými svědky jsou standardními objekty kryptografie a vycházejí z několika zavedených souborů předpokladů. Domněnka o neexistenci optimálního důkazového systému je ústřední domněnkou teorie složitosti důkazů. P = BPP je standardní derandomizační domněnka použitá pouze pro širší větu o falzifikovatelných vlastnostech.

Práce také tvrdí, že předpoklady jsou odpovídající cenou, nikoli svévolnou konstrukcí: dokazuje obrácené tvrzení, že jsou v podstatě nezbytné — pokud takové konstrukce vůbec existují, musí existovat neinteraktivní důkazy s nerozlišitelnými svědky, a (při standardních jednocestných funkcích) nemůže existovat žádný optimální důkazový systém. A předpoklady jsou „win-win“: vyvrácení kterékoli z nich by samo o sobě bylo průlomovým objevem v teorii složitosti důkazů, kryptografii nebo teorii složitosti.

Protože je výsledek podmíněný, je podmíněná i míra jistoty. Pokud tyto předpoklady selžou, interpretace věty se změní. A i kdyby platily, zárukou není úplná klasická nulová znalost; jde o oslabenou verzi založenou na teorii důkazů.

Správné hodnocení tedy zní: vysoká jistota, že práce stanovuje koherentní podmíněný výsledek; střední jistota, že její předpoklady popisují kryptografický svět, ve kterém skutečně žijeme; a nízká jistota ohledně jakéhokoli bezprostředního praktického důsledku.

Proč je to důležité

Práce otevírá cestu, která měla být uzavřena.

Klasická teorie říká: plné nulové znalosti nelze dosáhnout jedinou zprávou bez počátečního nastavení a zároveň jí nelze dát dokonalou spolehlivost. Ilangova práce říká: požadujeme-li důsledky nulové znalosti, které lze testovat v bezpečnostních hrách, a necháme-li definici bezpečnosti záviset na tom, co důkazový systém může či nemůže efektivně vyvrátit, lze obnovit mnoho užitečných vlastností — s jedinou zprávou, bez počátečního nastavení a s dokonalou spolehlivostí.

Nejde o drobnou úpravu definice. Je to jiný způsob uvažování o kryptografických zárukách. Místo abychom se ptali pouze na to, co existuje, ptáme se, co může náš důkazový systém vyloučit. Místo abychom neprokazatelnost považovali za filozofickou nepříjemnost, využijeme ji jako součást konstrukce.

Praktický svět se možná zítra nezmění, ale konceptuální mapa ano. Nyní máme formální smysl, v němž tvrzení „nikdo nedokáže efektivně prokázat, že tajemství uniklo“ může být dostatečně silné k obnovení mnoha herních ochran, které jsme očekávali od tvrzení „tajemství neuniklo“.

Proto Gödel patří do názvu.

Čisté shrnutí

Důkazy s nulovou znalostí umožňují dokazovateli přesvědčit ověřovatele, že tvrzení je pravdivé, aniž odhalí svědka. Klasické výsledky o nemožnosti říkají, že nulovou znalost nelze vměstnat do jediné zprávy bez počátečního nastavení a nelze jí dát dokonalou spolehlivost. Práce Rahula Ilanga tyto výsledky nevyvrací. Definuje slabší pojem, efektivní nulovou znalost: místo požadavku, aby simulátor skutečně existoval, vyžaduje, aby zvolený formální soubor pravidel — například ZFC — nedokázal efektivně dokázat, že žádný simulátor neexistuje. Za zásadních předpokladů kryptografie (neinteraktivní důkazy s nerozlišitelnými svědky) a teorie složitosti důkazů (neexistence optimálního důkazového systému) práce konstruuje jednozprávové dokazovatele pro NP/SAT bez počátečního nastavení a s dokonalou spolehlivostí, kteří postupně dosahují jednotlivých falzifikovatelných herních důsledků nulové znalosti. Jediný dokazovatel pokrývající všechny takové „přirozené“ vlastnosti je dalším, částečně spekulativním rozšířením — a pokrytí doslova všech falzifikovatelných vlastností je pravděpodobně nemožné, protože důkazy zůstávají znovupoužitelné. Výsledek je

teoretický a podmíněný, nikoli hotový primitiv, ale ukazuje nový způsob využití důkazově-teoretické neprokazatelnosti jako kryptografického zdroje.

Kontrola bez nesmyslů

Co práce ukazuje: Za uvedených předpokladů lze vytvořit jednozprávové dokazovatele a ověřovatele pro NP/SAT bez počátečního nastavení, kteří jsou dokonale spolehliví, mají efektivní nulovou znalost vzhledem k libovolnému zvolenému důkazovému systému a dosahují každého falzifikovatelného herního důsledku klasické nulové znalosti.

Co je pravděpodobné, ale není bezpodmínečně dokázáno: Že platí potřebné předpoklady složitosti důkazu a kryptografie. Jsou to vážné, dobře prozkoumané předpoklady — a práce ukazuje, že jsou v podstatě nezbytné i dostačující — ale stále jen předpoklady.

Co neukazuje: Klasická nulová znalost bez interakce, bez počátečního nastavení a s dokonalou spolehlivostí; praktický systém připravený k nasazení; popíratelnost nebo nemožnost opětovného použití důkazů; nebo že Gödelova věta o neúplnosti sama o sobě zajišťuje kryptografii.

Hlavní omezení: Záruka je oslabením nulové znalosti; nejširší verze závisí na několika předpokladech; tvrzení o jediném univerzálním dokazovateli zůstávají částečně spekulativní; a výsledek je především fundamentální.

Jakou důvěru by měl mít běžný čtenář? Vysokou v to, že jde při přijetí definic o důležitý podmíněný teoretický výsledek. Střední v to, že předpoklady zachycují realitu. Nízkou ohledně okamžitého praktického nasazení. Bezpečné poučení zní: práce neporušuje výsledky o nemožnosti nulové znalosti; nachází nový důkazově-teoretický způsob, jak obejít ty jejich části, které jsou důležité pro mnoho bezpečnostních her.

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