The Clean Paper

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

Egy kriptográfiai bizonyítás úgy rejtheti el a titkát, hogy a hiányzó szimulátor hiányát nehéz bebizonyítani

A zéró tudású bizonyítások lehetővé teszik, hogy valaki egy állítást a tanú felfedése nélkül bizonyítson. A klasszikus elmélet szerint ez teljes értelemben nem lehetséges egyetlen üzenettel, megbízható beállítás nélkül és tökéletes megbízhatósággal. Rahul Ilango tanulmánya nem tünteti el ezt a lehetetlenséget. Megváltoztatja a célt: ahelyett, hogy valóban létező szimulátort követelne, azt kéri, hogy egy választott bizonyítási rendszer ne tudja hatékonyan bebizonyítani a szimulátor nemlétezését. Jelentős bizonyításkomplexitási és kriptográfiai feltevések mellett ez elég ahhoz, hogy tulajdonságonként visszanyerjük a zéró tudás cáfolható, játék-alapú következményeit. Nem egy kész internetes primitívről van szó, hanem egy bizonyításelméleti módszerről, amely a matematikai bizonyíthatatlanságot kriptográfiai fedezékké alakítja.

Written by Cinzia Vaglio · Cross-checked by Vera Rubin · Edited by Michele Renda · Figures by Nova Vela · 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

A trükk nem az, hogy bebizonyítsuk: a titok rejtve marad

Induljunk a zéró tudás legegyszerűbb változatától.

Alice meg akarja győzni Bobot arról, hogy egy Sudoku-feladványnak van megoldása. Ha elküldi a megoldást, Bob valóban meggyőződik róla, de ezzel a rejtvény értelmét veszti. Alice valami furcsábbat szeretne: bizonyítékot arra, hogy létezik megoldás, anélkül hogy magát a megoldást felfedné.

Ezt ígéri a zéró tudású bizonyítás. A bizonyító fél (Alice) meggyőzi az ellenőrzőt (Bobot) arról, hogy egy állítás igaz, miközben az állítás igazságán túl semmit sem fed fel.

Csakhogy ennek az ígéretnek ára van. Egy hétköznapi matematikai bizonyításnak két kényelmes tulajdonsága van. **Egyetlen üzenetből** áll: leírjuk, átadjuk, és kész. Emellett **tökéletesen megbízható**: hamis állításhoz egyáltalán nem létezik érvényes bizonyítás. A klasszikus lehetetlenségi eredmények szerint a zéró tudásnak mindkét tulajdonságról le kell mondania — és nem csupán arról, hogy egyszerre mindkettőt megtartsa; külön-külön sem tartható meg egyik sem.

Először is, a zéró tudású bizonyításhoz párbeszéd kell. Ha Alice egyetlen üzenetet küld, és előzetesen nincs megbízható beállítás, a zéró tudás garanciája összeomlik — függetlenül attól, hogy cserébe mennyit engednénk a megbízhatóságból.

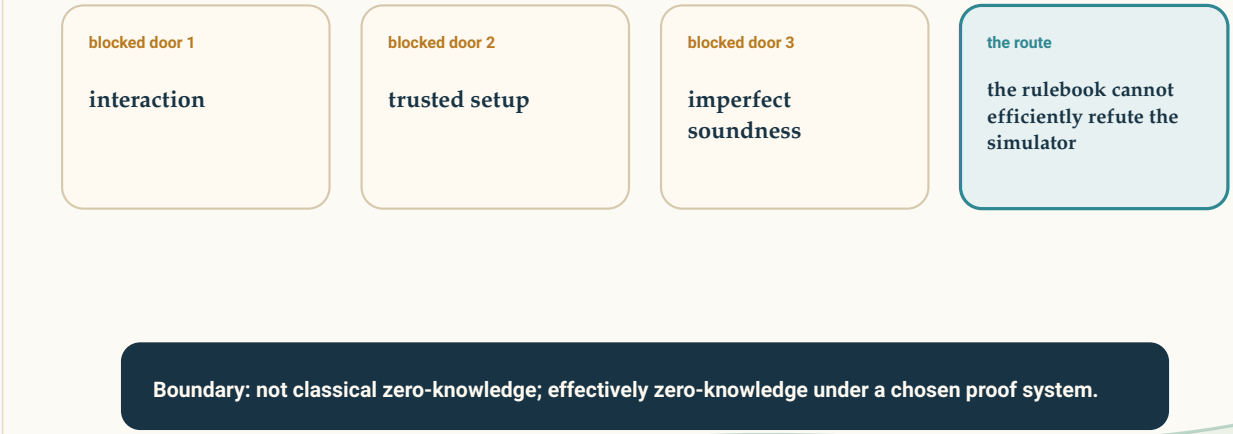
Másodszor, a zéró tudású bizonyításnak kis hibalehetőséget is el kell viselnie. A tökéletes megbízhatóság követelménye ugyanis csendben az interakciót is kiiktatja: ha egy ellenőrzőt semmilyen véletlen választás mellett sem lehet soha megtéveszteni, akkor akár előre is rögzítheti ezeket a választásokat. Ha pedig az ellenőrző kiszámítható, Alice egyetlen üzenetben előre megadhat minden választ — vagyis visszajutunk ahhoz az esethez, amely már eleve nem működött.

Rahul Ilango tanulmánya e kettős fal megkerüléséről szól. Nem úgy, hogy úgy tesz, mintha a fal nem létezne, és nem is úgy, hogy a lehetetlen helyzetben klasszikus zéró tudást állít elő. A lépés finomabb: gyengíti azt, mit értünk azon, hogy „semmit sem fed fel”, de úgy, hogy közben megőrzi azokat a biztonsági tulajdonságokat, amelyeket a kriptográfusok ténylegesen tesztelni tudnak.

Az eredmény neve **effektív zéró tudás** (*effectively zero-knowledge*).

A proof without leaking the witness

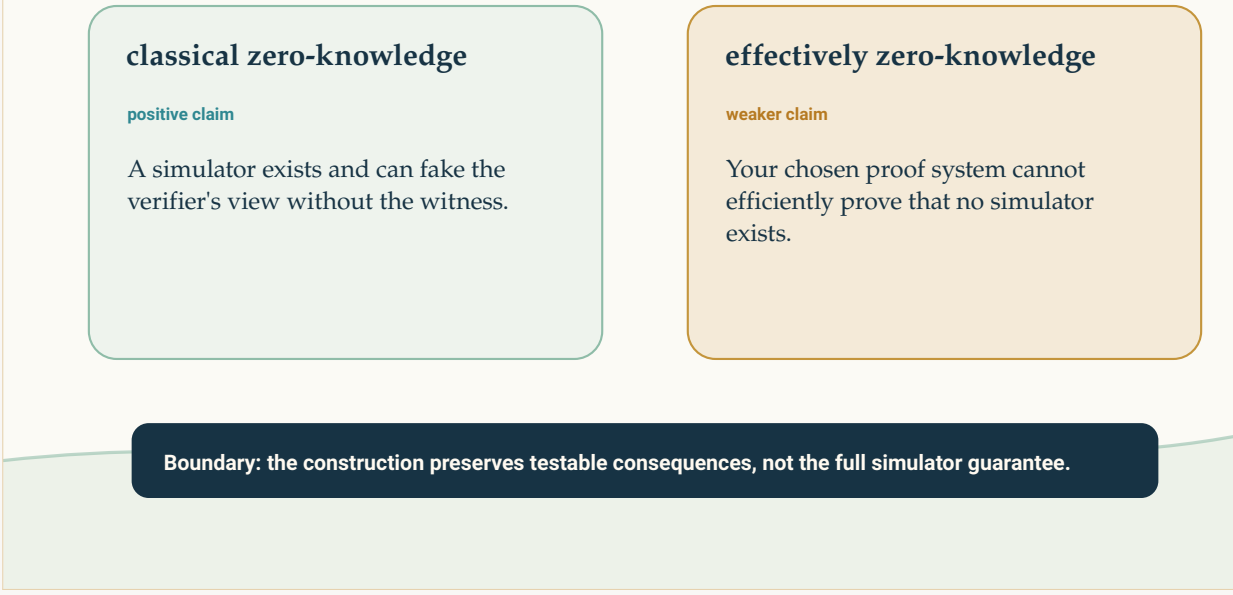
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



A zéró tudást három ajtó zárja el — az interakció, a megbízható beállítás és a nem tökéletes megbízhatóság követelménye. Ilango konstrukciója egy másik ajtón jut át: a választott szabálykönyv nem képes hatékonyan megcáfolni a szimulátor létezését.

Classical privacy vs effective privacy

The relaxation is the point: the paper changes what the privacy claim has to establish.



A klasszikus zéró tudás azt kérdezi, létezik-e szimulátor; az „effektív zéró tudás” csak azt, hogy a választott

szabálykönyv képes-e hatékonyan bebizonyítani, hogy nem létezhet. Ez a gyengébb kérdés teszi lehetővé, hogy a konstrukció megtartsa az egyetlen üzenetet, a beállítás hiányát és a tökéletes megbízhatóságot.

A régi teszt: létezik egy szimulátor

A zéró tudás klasszikus formalizálásához egy képzeletbeli segédet, úgynevezett **szimulátort** használunk.

Az ötlet a következő. Képzeljük el Jane-t, aki **nem** ismeri Alice titkát. Ha Jane teljesen egyedül képes olyan bizonyításokat előállítani, amelyek ugyanolyannak látszanak, mint amelyeket Bob Alice-től kapott volna, akkor Alice bizonyításai nem tanítottak Bobnak semmi újat. Jane Alice titka nélkül is elő tudta volna állítani ugyanazt az élményt.

A klasszikus zéró tudás tehát valóban létező szimulátort követel. Kell lennie egy hatékony algoritmusnak, amely a titok ismerete nélkül is hitelesnek látszó bizonyításokat képes gyártani — a szaknyelvben ezt a titkot *tanúnak* (*witness*) nevezik; Sudoku esetén a tanú egyszerűen a kitöltött rács.

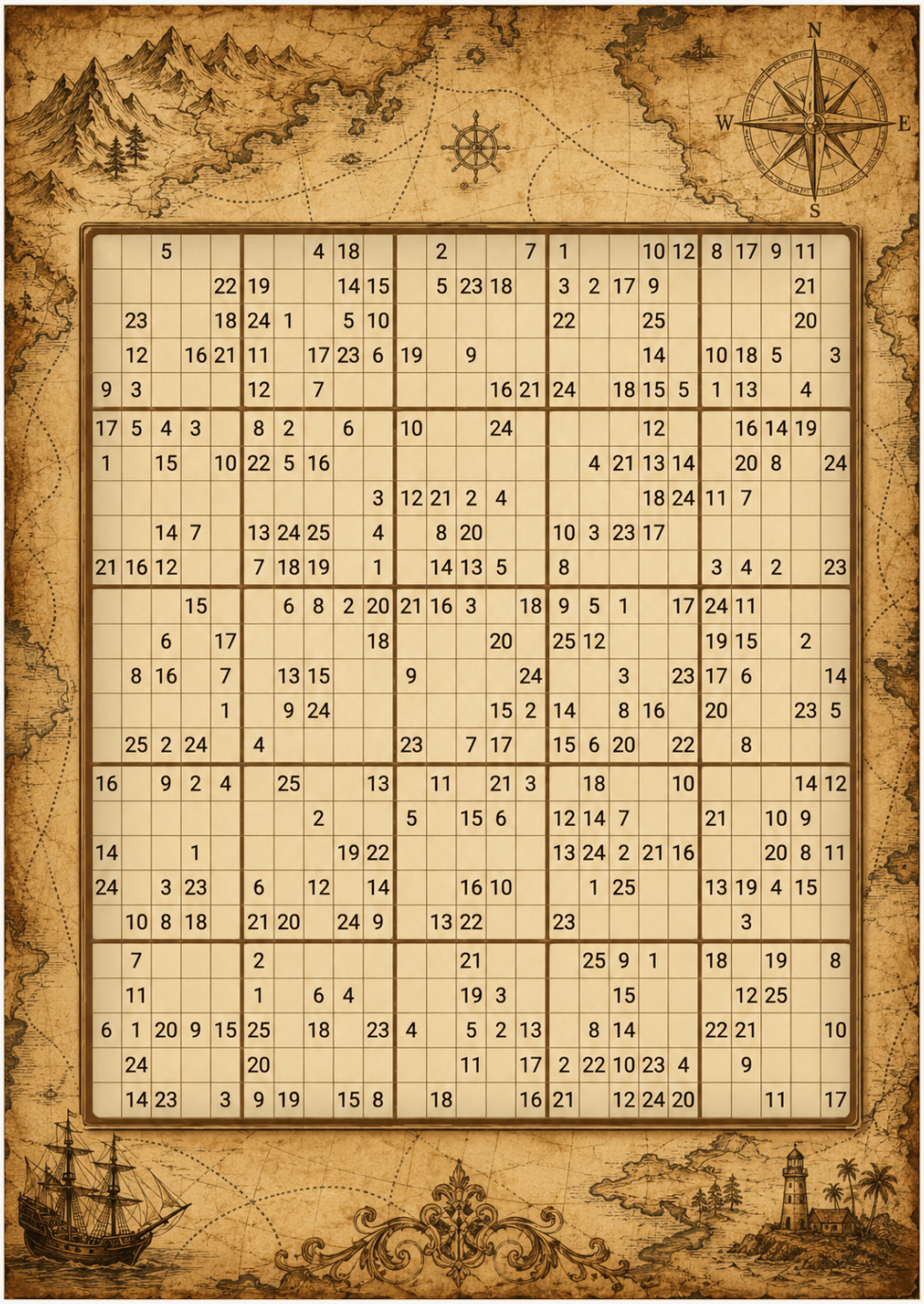
Ez a definíció erős, de éppen itt harapnak a régi lehetetlenségi tételek. Az intuíció a következő. Egy valóban nem interaktív bizonyítás csak egy karakterlánc. Ha Bob egyszer megkapta ezt a karakterláncot, megmutathatja valaki másnak is: megszerezte azt a képességet, hogy az állítást mások előtt is bizonyítsa, ami már önmagában többnek hangzik a „semminél”. A klasszikus tételek ezt az intuíciót teszik precízzé a fenti lehetetlenségi eredményekben.

> **A tanulmány által ragaszkodott három tulajdonság**
>
> A tanulmány címe három megszorítást nevez meg:
> **Nincs interakció:** Alice egyetlen bizonyítási karakterláncot küld. Nincs oda-vissza zajló protokoll.
> **Nincs beállítás:** Alice és Bob nem támaszkodik megbízható közös referencia-karakterláncra vagy más előre elrendezett nyilvános véletlen adatra. Sok, „nem interaktív zéró tudásúnak” nevezett rendszer továbbra is igényel beállítást; ez a tanulmány valóban zéró beállítást ért alatta.
> **Tökéletes megbízhatóság:** hamis állításhoz nincs érvényes bizonyítás. Nem arról van szó, hogy „szinte soha nem fogadják el”; érvényes bizonyítás egyáltalán nem létezik.
> Pontosan ez a három tulajdonság jellemzi a hétköznapi írott matematikai bizonyítást — és, ahogy fent láttuk, a klasszikus zéró tudás nem tudja mindet megtartani.

A különbség egy MegaSudoku-változattal

A következő, szándékosan leegyszerűsített kép segít megérezni a különbséget.

A hasonlat komoly részéhez ne egy közönséges 9×9-es Sudokut használjunk. Túl kicsi és túl véges: egy számítógép egyszerűen megoldhatja, vagy bebizonyíthatja, hogy nincs megoldása. Képzeljünk inkább egy **MegaSudoku(n)** feladványcsaládot. Nagyítsuk fel a szokásos szabályt: válasszunk egy n blokkméretet, legyen $N = n^2$, majd építsünk egy $N \times N$ rácsot, amely $n \times n$ blokkokra oszlik, és N különböző szimbólumot használ. A közönséges Sudoku csupán az apró $n = 3$, $N = 9$ eset: 9×9-es rács, 3×3-as blokkok és kilenc szimbólum. A bizonyításkomplexitási történet csak akkor kezd igazán érdekessé válni, amikor n növekedhet, és a rács olyan kiegészítő szerkezeteket — gadgeteket — is tartalmazhat, amelyek SAT-formulaként viselkednek Sudoku-jelmezben. Egy SAT-formula lényegében igen/nem típusú megszorítások listája: lehet-e úgy igaz/hamis értékeket rendelni a változókhoz, hogy minden feltétel teljesüljön?



Egy 25×25-ös Sudoku: a szabályai ellenőrizhetők a teljes kitöltött rács felfedése nélkül — vizuális megfelelője annak a bizonyításnak, amely egy rejtett megoldás, vagyis a tanú létezését igazolja.

Sudoku és SAT: ugyanaz a feladvány két jelmezben

Az az állítás, hogy egy Sudoku „SAT-formulaként viselkedhet”, nem metafora. Az átalakítás mindkét irányban működik, és a könnyebbik irány teljes egészében leírható.

Sudokuból SAT. A SAT csak igaz/hamis értékeket ismer, ezért rendeljünk egy logikai változót minden (sor, oszlop, érték) hármashoz: az *x(r,c,v)* jelentése legyen „az *r*. sor *c*. oszlopában lévő cella értéke *v*”. Egy 4×4-es Sudokuhoz (2×2-es blokkokkal, 1–4 értékekkel) 4·4·4 = 64 változó kell; a klasszikus 9×9-eshez 729. Ezután minden Sudoku-szabály klózok egy csoportjává válik. (Egy klóz változók vagy negációik VAGY-kapcsolata; a teljes formula az összes klóz ÉS-kapcsolata.)

Minden cellában van legalább egy érték — cellánként egy klóz:

$$x(1,1,1) \vee x(1,1,2) \vee x(1,1,3) \vee x(1,1,4)$$

Minden cellában legfeljebb egy érték van — minden értékpárhoz egy „nem lehet mindkettő” klóz:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \text{… és így tovább mind a hat párra.}$$

Minden sor minden értéket tartalmaz — az 1. sor és a 3-as érték esetén legalább egyszer:

$$x(1,1,3) \vee x(1,2,3) \vee x(1,3,3) \vee x(1,4,3)$$

és legfeljebb egyszer: $\neg x(1,1,3) \vee \neg x(1,2,3)$, majd ugyanígy a sor minden cellapárjára.

Oszlopok és blokkok — ugyanilyen klózcsoportok, csak a cellák halmaza változik. A bal felső blokk és a 2-es érték esetén:

$$x(1,1,2) \vee x(1,2,2) \vee x(2,1,2) \vee x(2,2,2)$$

plusz a páronkénti „nem lehet mindkettő” klózok.

A megadott számok — ez a legegyszerűbb rész: minden megadott érték egyetlen változóból álló klóz. Ha a bal felső sarokban eleve 3 áll, abból ez a klóz lesz:

$$x(1,1,3)$$

Mindezek ÉS-kapcsolata pontosan akkor kielégíthető, ha a Sudokunak van megoldása — és egy kielégítő értékadás maga *a* megoldás: meg kell nézni, mely x(r,c,v) változók igazak, és ezekkel kitölteni a rácsot. Egy 9×9-es Sudoku esetén ez 729 változót és néhány ezer klózt jelent, amit egy korszerű SAT-megoldó ezredmásodpercek alatt elintéz. Érdemes észrevenni az x(1,1,3) megadottérték-klózt: azt mondja, hogy „ez a cella pontosan 3”, nem azt, hogy „ezek a cellák mind különböznek egymástól” — ugyanaz az aszimmetria, amely a későbbi protokolljegyzetben külön trükköt tesz szükségessé a megadott cellákhoz.

SAT-ból Sudoku. A tanulmánynak az ellenkező, nehezebb irányra van szüksége: egy *tetszőleges* SAT-formulából kell olyan mega-Sudokut építeni, amelynek pontosan akkor van megoldása,

ha a formulának is. A Sudoku saját szabályai lényegében csak azt tudják kimondani, hogy „ezek a cellák mind különböznek”, ezért az általános logikai megszorításokat *fel kell építeni* — erre szolgálnak a gadgetek. Egy gadget egy kicsi, előre megtervezett cellacsoport, a formula egy-egy klózához; kijelölt cellái változóként működnek (a bennük álló szimbólum kódolja az igaz vagy hamis értéket), belső megszorításait pedig úgy alakítják ki, hogy csak azok a kitöltések legyenek szabályosak, amelyek a klózt kielégítő értékadásoknak felelnek meg. Ez az NP-teljességi bizonyítások klasszikus mesterségbeli fogása; az általánosított Sudoku esetére Yato és Seta dolgozta ki 2003-ban.
A két irány együtt azt mondja ki, hogy az N×N-es Sudoku és a SAT ugyanaz a probléma két különböző jelmezben. Ez teszi indokolttá, hogy ez a cikk — és maga a tanulmány — rácsokkal és szimbólumokkal meséljen az egész NP problémakörről.

A tanút továbbra is könnyű elképzelni. Alice ismeri a mega-Sudoku teljes, szabályos kitöltését. Bob meg akar bizonyosodni arról, hogy létezik ilyen kitöltés, Alice viszont nem akarja felfedni. Ha elküldi az egészet, Bob meggyőződik, de a titok elveszik.

A klasszikus zéró tudású változatban Alice és Bob interakcióba lép. Egy régi szemléltető modell letakart lapkákat használ. Alice elrejti a megoldott rácsot, minden kör előtt titokban átnevezi a szimbólumokat, majd megengedi Bobnak, hogy véletlenszerűen kiválasztott helyi megszorítást ellenőrizzen: egy sort, egy oszlopot, egy blokkot vagy egy gadgetet. Ha a felfedett cellákban minden szimbólum különböző, Bob bizalma nő. Ezután mindent újra letakarnak, és a szimbólumok új átnevezést kapnak. (Van egy bökkenő: a feladvány előre megadott számai külön trükköt igényelnek, mert a szimbólumok átnevezése ezeket is elrejti. Az alábbi jegyzet elmagyarázza, hogyan oldják meg ezt a klasszikus protokollok; a továbbiakhoz elég ez az egyszerű kép.)

Hogyan kezelik a klasszikus protokollok valójában a megadott cellákat

Az átnevezési trükknek van egy vakfoltja. A sorokra, oszlopokra és blokkokra vonatkozó szabály mind azt mondja, hogy „ezek a cellák mind különböznek”, és a *minden különböző* tulajdonság bármilyen szimbólum-átnevezés után megmarad. Egy megadott szám viszont azt mondja, hogy „ebben a cellában pontosan 5 áll”, átnevezés után pedig Bob csak $\sigma(5)$-öt — valamilyen maszkolt szimbólumot — lát, miközben magát a σ átnevezést nem ismeri. Így semmit sem tud ellenőrizni. Ha ezt nem javítanánk ki, Alice bizonyíthatná, hogy *valamilyen* szabályos rács létezik, miközben teljesen figyelmen kívül hagyja a nyomtatott számokat — ami erről a konkrét feladványról semmit sem bizonyít. A klasszikus irodalom két szokásos megoldást használ.
A paletta. Adjunk a rejtett rácshoz egy N cellából álló extra sort — egy palettát —, amelyet Alice nyilvánosan rögzített sorrendben az 1…N szimbólumokkal tölt ki, majd minden mással együtt átnevez; így a sor $\sigma(1)$…σ(N)-et tartalmazza. Bob véletlen kihívása most eggyel több lehetőséget kap. Egy sor, oszlop, blokk vagy gadget felfedése mellett kiválaszthatja **a palettát és egy megadott cellát** is. Alice mindkettőt felfedi; a paletta megmutatja az adott kör átnevezését, Bob pedig ellenőrzi, hogy a megadott cella pontosan a nyomtatott érték átnevezett változatát tartalmazza. Ez továbbra is zéró tudású, mert Bob csak σ-t tanulja meg — amely minden

körben frissen, véletlenszerűen készül, ezért önmagában értéktelen —, valamint egy olyan cella értékét, amelyet már eleve ismert a feladványból. A titkos cellákról semmi nem szivárog ki, a szimulátor pedig egy véletlen σ választásával elő tudja állítani ugyanazt a látványt. A módszer megbízható, mert egy csaló Alice minden körben rögzített valószínűséggel lebukik; a köröket addig ismétlik, amíg a bizonytalanság elhanyagolhatóvá nem válik.

A megadott számok beépítése a megszorításokba. Egy szerkezeti megoldás a külön kihívás hozzáadása helyett megszünteti annak szükségességét. A megadott érték *ellenőrzése* helyett kényszerítsük ki különbözőségi megszorításokkal: kössük össze a megadott cellát a paletta minden olyan cellájával, amely nem a saját értékét hordozza — „különbözik $\sigma(1)$-től, különbözik $\sigma(2)$-től, …, minden mástól különbözik, kivéve $\sigma(5)$-öt”. Így az egyetlen szimbólum, amelyet a cella szabályosan tartalmazhat, éppen a megadott érték. Minden megszorítás újra „ez a két érték különbözik” alakú lesz — vagyis invariáns az átnevezésre, és ugyanúgy ellenőrizhető, mint egy sor. Ugyanezt a fogást használják az előre színezett csúcsokra a klasszikus gráfszínezési protokollban; és ugyanez a fenti *gadget* szó lényege is: a MegaSudoku-mint-SAT képben a megadott számok ugyanúgy egyenlőtlenségi gadgetekbe épülnek, mint minden más megszorítás.

A fizikai protokoll. A Sudoku valódi kártyás protokollja (Gradwohl, Naor, Pinkas és Rothblum, 2007) egyáltalán nem használ átnevezést, és már a rejtés megkezdése előtt rendezi a megadott számokat. Alice minden cellához három azonos, a cella értékét hordozó kártyát tesz le — a titkos celláknál képpel lefelé, a **megadott celláknál viszont képpel felfelé**, így Bob saját szemével látja, hogy a megadott számokat betartották, mielőtt a kártyákat lefordítják. Ezután minden cella egy-egy kártyája a megfelelő sor csomagjába, egy az oszlop csomagjába, egy pedig a blokk csomagjába kerül; minden csomagot megkevernek és felfednek, Bob pedig ellenőrzi, hogy mind az N szimbólum szerepel benne. A keverés eltünteti a pozícióinformációt — ez adja a zéró tudást —, a megadott számokat viszont már az osztáskor rögzítették.

Bármelyik megoldást választjuk, ugyanoda jutunk vissza, ahová ez a cikk újra és újra: a zéró tudású protokoll gondos könyvelése annak, hogy *mely* tények élik túl a rejtést. Az átnevezés megőrzi azt, hogy „mind különböző”, de eltörli azt, hogy „egyenlő 5-tel” — ezért az „egyenlő 5-tel” tényt más módon kell visszacsempészni.

Ez nem a tanulmány protokollja. Csupán a klasszikus zéró tudás szemléleti modellje:

- Alice és Bob oda-vissza kommunikál.
- Bob véletlenszerű ellenőrzéseket választ.
- Alice csak a helyi konzisztenciát fedi fel, a teljes megoldást nem.
- Az adatvédelem bizonyítása arra épül, hogy Bob nézete Alice titkos megoldása nélkül is előállítható lenne.

A klasszikus zéró tudás tehát egy pozitív tényre épül:

> Valóban létezik egy szimulátor.

Most vegyük el a kényelmes részeket. Alice egyetlen bizonyítási karakterláncot küld, majd távozik. Nincs megbízható beállítás, nincs előre elkészített közös véletlen karakterlánc, és Bob soha nem

fogadhat el hamis feladványt. Ebben a környezetben a klasszikus zéró tudás nem maradhat fenn.

A trükkhöz még egy szereplő kell. Rögzítsünk egy **szabálykönyvet**: a logika értelmében vett formális bizonyítási rendszert — axiómák rögzített halmazát és a leírt matematikai bizonyítások mechanikus ellenőrzési szabályait. A kanonikus példa a ZFC, a matematika szokásos axiómarendszere. Innentől minden állítást egy előre kiválasztott szabálykönyvhöz viszonyítunk, de a választás rugalmas: a konstrukció bármely rögzített szabálykönyvvel működik, a ZFC-vel is.

(A tanulmány szóhasználatát követő megjegyzés: a „bizonyítási rendszer" itt mindig ezt a szabálykönyvet jelenti — azt a formális rendszert, amely matematikai bizonyításokat ellenőriz —, soha nem az Alice által küldött üzeneteket. Alice és Bob gépezetét „bizonyítónak" és „ellenőrzőnek" nevezzük.)

A Gödel-jellegű változat megtartja a mega-Sudoku történetét, de megváltoztatja a bizonyítást.

Válasszunk egy második, ugyanakkora megjelenített méretű megszorításrendszert, és nevezzük **D**-nek. A történetben S és D két azonos formátumú MegaSudoku(n) feladvány. A háttérben D akár más méretű, nehéz logikai formulából is indulhatott; szükség esetén ártalmatlan, üres megszorításokkal kiegészíthető, hogy ugyanabba a rácsméretbe férjen. D egy olyan logikai formulából készül, amely valóban **kielégíthetetlen**: nincs olyan értékadás, amely minden megszorítását igazzá tenné, ahogyan egy hibás feladványnak sincs szabályos teljes kitöltése. Játékpélda lenne egy olyan formula, amely egyszerre követeli, hogy „X igaz" és „X hamis". D-nek tehát nincs érvényes kitöltése.

Csakhogy D nem lehet olyan hibás feladvány, amelynek hibáját *könnyű kimutatni*. A fenti játékpélda ezért rossz: bármely szabálykönyv egy sorban megcáfolja az „X és nem-X" formulát. D-nek úgy kell hamisnak lennie, hogy a választott szabálykönyv ezt ne tudja rövid érveléssel tanúsítani. Ha a szabálykönyv rövid bizonyítással meg tudná cáfolni D-t, az alábbi történet összeomlana: formálisan kizárható lenne az az alternatív út, amely Alice titka nélkül is lehetővé tehette volna a bizonyításokat, vele együtt pedig az adatvédelmi garancia is. Ezért D-t olyan családból választjuk, amelyet a rögzített szabálykönyv nem tud hatékonyan megcáfolni: a szabálykönyvön belül nincs rövid bizonyítás arra, hogy D-nek nincs megoldása.

Alice egyetlen üzenetből álló bizonyítása ezután egy vagy-vagy állításról szól:

> vagy a valódi mega-Sudokunak, S-nek van megoldása, vagy a D csalinak van megoldása.

Ez a logikai kapocs. D-t **nem** valamilyen mágikus eljárás állítja elő úgy, hogy attól S igaz legyen. A bizonyítás nem azt mondja, hogy „D-nek nincs megoldása, tehát S-nek van". A **S vagy D** diszjunkciót bizonyítja. A tökéletes megbízhatóság azt mondja, hogy hamis diszjunkciónak nem lehet érvényes bizonyítása. Mivel D a valóságban hamis — nincs megoldása —, a diszjunkció csak úgy lehet igaz, ha S igaz. Ha tehát a bizonyítást elfogadják, S-nek szükségképpen van megoldása. A csali nem tehet igazzá egy hamis S-t.

A zéró tudáshoz hasonló részhez viszont tegyük fel, mi történne, ha D-nek *mégis* lenne megoldása. Ez a csalimegoldás alternatív tanúként működne. Lehetővé tenné, hogy valaki Alice valódi mega-Sudoku-megoldásának ismerete nélkül állítson elő bizonyításokat — vagyis szimulátorként szolgálna. A valóságban D-nek nincs megoldása, tehát ez a szimulációs út zárva van. A lényeg azonban az, hogy a szabálykönyv nem képes hatékonyan bebizonyítani, hogy zárva van.

D-nek tehát két feladata van. A **megbízhatóság** szempontjából D hamis, ezért az „S vagy D” érvényes bizonyítása kikényszeríti S igazságát. Az **effektív zéró tudás** szempontjából D nehezen cáfolható, ezért a szabálykönyv nem tudja gyorsan kizárni azt a csaliutat, amely szimulációt tett volna lehetővé.

A biztonsági teszt tehát már nem ez:

> Be tudjuk bizonyítani, hogy valóban létezik szimulátor?

Hanem ez:

> A szabálykönyved képes hatékonyan bebizonyítani, hogy a szimulátor lehetetlen?

Ha a válasz nem, meglepően erős következmény adódik: minden olyan biztonsági garancia ténylegesen teljesül, amely (a) egy teszt futtatásával megfigyelhető, és (b) a szabálykönyvön belül bizonyíthatóan következne egy szimulátor létezéséből. Ha ezek bármelyike ellen sikeres támadás létezne, az maga adná a hiányzó rövid cáfolatot — márpedig ilyen rövid cáfolat nincs. Ez az „effektív” az effektív zéró tudásban.

A tantermi kontraszt tehát:

Klasszikus zéró tudás: a bizonyítások azért biztonságosak, mert létezik szimulátor.

Gödel-jellegű effektív zéró tudás: a bizonyításokat a megfigyelhető biztonsági tesztek szempontjából azért kezelhetjük biztonságosként, mert a szabálykönyv nem képes hatékonyan bebizonyítani, hogy a szimulátor lehetetlen.

A második állítás gyengébb. És éppen ezért tarthatja meg a tanulmány azt a három tulajdonságot, amely a klasszikus változatot ellehetetlenítette: egyetlen üzenet, nincs beállítás, tökéletes megbízhatóság.

Az új teszt: nem tudod bebizonyítani, hogy nincs szimulátor

Ilango enyhített definíciója megváltoztatja a kérdést.

A klasszikus zéró tudás ezt kérdezi:

> Létezik szimulátor?

Az effektív zéró tudás ennél gyengébbet kérdez:

> A választott szabálykönyved képes hatékonyan bebizonyítani, hogy nem létezik szimulátor?

Ez technikai kibúvónak hangozhat, de éppen ez a központi ötlet. A konstrukció különös állapotban él: szimulátor valójában nem létezik — ezt a tanulmány egyértelműen kimondja —, a rögzített szabálykönyv azonban nem képes hatékonyan bebizonyítani, hogy nincs. Ha minden fontos rossz következményhez ilyen cáfolatra lenne szükség, a rendszer e következmények tekintetében továbbra is úgy viselkedik, mint egy zéró tudású rendszer.

Itt lép be Gödel. Nem díszítésként, és nem úgy, hogy „Gödel biztonságossá teszi a kriptográfiát". A kapcsolat bizonyításelméleti. Egy szabálykönyv **optimális**, ha pontos értelemben a lehető legjobb: ha bármely más szabálykönyv az adott típusú formulát rövid bizonyítással meg tudja cáfolni, az optimális szabálykönyv is képes rá, legfeljebb polinomiálisan hosszabb bizonyítással. Krajíček és Pudlák 1989-ben azt sejtette, hogy **nem létezik optimális bizonyítási rendszer**: bármely rögzített szabálykönyv mellett akad egy másik, amely igaz állítások valamely családját sokkal tömörebben bizonyítja. Ez a bizonyításkomplexitás egyik központi nyitott sejtése, és Gödel nemteljességi tételének véges, komplexitáselméleti rokona: vannak igaz állítások, amelyekhez az általunk rögzített szabálykönyvben nincs rövid bizonyítás — nem azért, mert elvben bizonyíthatatlanok, hanem mert minden rögzített szabálykönyv hagy olyan röviden megfogalmazható igazságokat, amelyekhez csak hosszú bizonyítás tartozik.

A tanulmány feltételezi ezt a sejtést (egy enyhén erősebb, „végtelen sokszor" változatban, amely kriptográfiai sejtések használatakor szokásos). Krajíček és Pudlák tétele révén a nyereség konkrét: minden szabálykönyvhöz létezik olyan, ténylegesen kielégíthetetlen formulákból álló sorozat, amelyet a szabálykönyv nem tud rövid bizonyításokkal megcáfolni — és, ami döntő, amelyet egy hatékony algoritmus *elő is tud állítani*. Ez az utóbbi tulajdonság, az uniformitás teszi az egész gondolatot puszta létezési állításból Alice által ténylegesen futtatható algoritmussá: a D csalik futószalagról érkeznek, nem a semmiből.

A kriptográfiai lépés ezt a bizonyítási erőhiányt fordítja haszonra.

Mit csinál a konstrukció?

A tanulmány konstrukciója a lényegére csupaszítva így néz ki.

Rögzítsünk egy szabálykönyvet — mondjuk a ZFC-t. A bizonyításkomplexitási feltevés szerint létezik hatékonyan előállítható olyan formulasorozat, amely valójában kielégíthetetlen, de amelynek kielégíthetetlenségére a szabálykönyvben nincs rövid bizonyítás.

Most készítsünk egyetlen üzenetből álló bizonyítást a következő formában:

> vagy a valódi állítás kielégíthető, vagy ez a különleges, nehéz formula kielégíthető.

A különleges nehéz formula nem kielégíthető. Ha tehát az alapul szolgáló bizonyítási mechanizmus tökéletesen megbízható, az üzenet elfogadása továbbra is azt jelenti, hogy a valódi állítás igaz. Ez adja a tökéletes megbízhatóságot.

A zéró tudáshoz hasonló biztonság érdekében viszont képzeljük el, hogy a különleges, nehéz for-

mula *mégis* kielégíthető lenne. Ekkor a tanúja felhasználható lenne bizonyítások szimulálására a valódi tanú ismerete nélkül. A formula a valóságban nem kielégíthető — a szabálykönyv azonban nem képes ezt hatékonyan bebizonyítani. Így azt sem képes hatékonyan bizonyítani, hogy a szimulátor lehetetlen.

Ez a fordulópont. A rendszer nem klasszikus szimulátor előállításával rejti el a titkot. A megfigyelhető biztonsági tesztek széles osztálya számára a szabálykönyv azon képtelensége mögé rejti, hogy tanúsítsa a szimulátor hiányát.

Mit állít a tanulmány?

A főtétel több rétegből áll. A központi eredmény ez:

Egy szokásos kriptográfiai feltevés — a **nem interaktív, tanú-megkülönböztethetetlen bizonyítások** (*non-interactive witness indistinguishable proofs*) létezése; ezek jól tanulmányozott objektumok, és több bevett feltevéscsomagból is következnek —, valamint a **nem létezik (végtelen sokszor) optimális bizonyítási rendszer** bizonyításkomplexitási sejtése mellett a tanulmány minden választott szabálykönyvhöz felépít NP/SAT problémákra egyetlen üzenetből álló, beállítás nélküli, **tökéletesen megbízható** bizonyítót és ellenőrzőt, amely az adott szabálykönyvhöz képest effektíven zéró tudású. (Az NP/SAT a feladványszerű problémák szokásos „legnehezebb közös nevezője”; a mega-Sudoku csupán az egyik jelmez, amelyet felvehet.)

A cáfolható biztonsági tulajdonságok megőrzéséről szóló szélesebb állításhoz a tanulmány még egy szokásos feltevést ad: a derandomizációs **P = BPP** hipotézist (nagyjából: a véletlenszerűség nem ad az algoritmusoknak lényegi többleterőt).

A tétel nyelvéről lefordítva:

- A bizonyítás egyetlen üzenet.
- Nincs megbízható beállítás.
- Hamis állítások nem bizonyíthatók.
- A bizonyító nem klasszikusan zéró tudású — nincs szimulátora.
- A klasszikus zéró tudás minden cáfolható, játék-alapú biztonsági következménye elérhető ebben a környezetben.

A „cáfolható” szó fontos. Azt jelenti, hogy egy biztonsági hiba egy ellenféllel futtatott játékban tesztelhető. Sok kriptográfiai biztonsági definíció ilyen alakú: meg tudja-e különböztetni az ellenfél két titkosítás eredményét, invertálni tud-e egy függvényt, vissza tud-e szerezni egy tanút, vagy meg tud-e nyerni valamilyen pontosan meghatározott kísérletet? A tétel minden egyes cáfolható tulajdonsághoz külön-külön ad egy bizonyítót. Egyetlen olyan bizonyító, amely *minden* cáfolható tulajdonságot egyszerre élvez, valószínűleg lehetetlen — a régi újrafelhasználhatósági támadás („Bob megmutathatja a bizonyítást másoknak”) maga is cáfolható tulajdonság, és itt valóban nem teljesül. A tanulmány javaslata az, hogy egyetlen bizonyító hihetően lefedheti az összes *természetes* cáfolható tulajdonságot — azokat, amelyek a kriptográfiai gyakorlatban ténylegesen előfordulnak —, de ez a rész egy

feltételes tétel, amely a „természetes” informális fogalmára és egy explicit sejtésre támaszkodik. A garancia megfigyelhető hibákra irányul, nem a titkosság minden filozófiai vagy szimuláció-alapú értelmezésére.

Egy konkrét következményt érdemes külön megnevezni: a konstrukció létrehozza az első, uniform bizonyítóval rendelkező nem interaktív *tanúrejtő* (*witness hiding*) bizonyításokat — vagyis olyan rendszert, ahol „egy feladvány bizonyítása nem segít megtalálni a megoldását”, interakció és beállítás nélkül. Ez szerényen hangzó objektum, amelynek megalkotása évtizedekig ellenállt a próbálkozásoknak.

Mit nem állít mindez?

Ez a rész tartja földön a cikket.

Nem azt mondja, hogy a régi lehetetlenségi tételek tévesek voltak. A konstrukció a definíció megváltoztatásával kerüli meg őket.

Nem ad szokásos, klasszikus zéró tudást interakció és beállítás nélkül, tökéletes megbízhatósággal. A tanulmány kifejezetten kimondja, hogy a megkonstruált bizonyítónak nincs szimulátora.

Nem jelenti azt, hogy a bizonyítás nem használható újra. Egyetlen üzenetből álló bizonyítást továbbra is meg lehet mutatni valaki másnak; a tanulmány nem őriz meg tagadhatósági jellegű tulajdonságokat. (A megbízható beállítást használó nem interaktív zéró tudásnak ugyanez a korlátja.)

Nem jelenti azt sem, hogy ez gyakorlati, bevetésre kész protokoll. Ez komplexitáselméleti és kriptográfiai alapkutatás. Az eredmény jelentős bizonyításkomplexitási és kriptográfiai feltevésektől függ, és arról szól, mi lehetséges elvben.

És **nem** teszi „Gödelt” valamiféle mágikus biztonsági primitívvé. A Gödel-kapcsolat a bizonyítási rendszereken, az optimális bizonyítási rendszereken és a nemteljesség véges analógiáin keresztül jelenik meg. A használható intuíció nem az, hogy „a nemteljesség megvédi a jelszavadat”. Hanem ez: ha egy szabálykönyv nem képes hatékonyan bebizonyítani, hogy egy szimulátor lehetetlen, akkor az ilyen bizonyítást igénylő támadások a biztonsági definíciók szintjén blokkolhatók.

Miért érdekes mégis?

A kriptográfia gyakran alakítja a nehézséget biztonsággá. A faktorizáció nehéz, ezért az RSA-jellegű feltevések hasznosak. A rácsproblémák nehezek, ezért a rácsalapú kriptográfia hasznos. Itt azonban a nehézség furcsább: nem az, hogy „nehéz kiszámítani egy titkot”, hanem hogy „nehéz bebizonyítani, hogy egy bizonyos bizonyítási objektum nem létezhet”.

Ezért hat szokatlannak a tanulmány. Az axiómákat és szabálykönyveket szinte kriptográfiai erőforrásként kezeli. A szokásos lehetetlenségi eredmény szerint feszültség van a megbízhatóság és a sz-

imuláció között. Ilango lépése ezt a feszültséget egy bizonyításelméleti függöny mögé helyezi: a szimulátor hiányzik, de a formális rendszer nem képes hatékonyan felfedni a hiányát.

Az olvasó számára nem az a meglepő, hogy ez a módszer leváltaná a mai zéró tudású rendszereket. Valószínűleg nem fogja, legalábbis közvetlenül. Az a meglepő, hogy a matematikai logika egyik korlátja konstruktívan használható: nem csupán falként, hanem egyfajta fedezékként is.

Mennyire erős a bizonyíték?

Ez egy tételközpontú tanulmány, ezért a „bizonyíték” itt mást jelent, mint egy biológiai vagy csillagászati cikkben. Nem az a kérdés, hogy egy kísérletet megismételtek-e, hanem az, hogy a definíciók, a feltevések és a bizonyítási lánc alátámasztják-e az állítást.

A bizonyítás formális, a tanulmány pedig egyértelműen felsorolja a feltevéseit. Ezek nem mellékes feltételek. A nem interaktív, tanú-megkülönböztethetetlen bizonyítások a kriptográfia bevett objektumai, és több megalapozott feltevéscsomagból is következnek. A „nincs optimális bizonyítási rendszer” sejtés a bizonyításkomplexitás egyik központi sejtése. A P = BPP egy szokásos derandomizációs feltevés, amelyre csak a cáfolható tulajdonságokról szóló szélesebb tételhez van szükség.

A tanulmány azt is megmutatja, hogy ezek a feltevések nem önkényesen felhúzott állványzatot jelentenek, hanem lényegében szükséges árat. Egy fordított irányú eredményt is bizonyít: ha ilyen konstrukciók egyáltalán léteznek, akkor nem interaktív, tanú-megkülönböztethetetlen bizonyításoknak is létezniük kell, és — a szokásos egyirányú függvények létezését feltételezve — optimális bizonyítási rendszer nem létezhet. A feltevések ráadásul „win-win” jellegűek: bármelyikük megcáfolása önmagában mérföldkő lenne a bizonyításkomplexitásban, a kriptográfiában vagy a komplexitáselméletben.

Mivel azonban az eredmény feltételes, a belé vetett bizalom is feltételes. Ha ezek a feltevések hamisak, a tétel értelmezése megváltozik. És még ha igazak is, a garancia akkor sem teljes klasszikus zéró tudás, hanem a tanulmány enyhített, bizonyításelméleti változata.

Ezért a megfelelő bizalmi szint: magas abban, hogy a tanulmány koherens, feltételes lehetőségi eredményt állapít meg; közepes abban, hogy a feltevések a tényleges kriptográfiai világot írják le; és alacsony bármilyen közvetlen gyakorlati következményt illetően.

Miért számít?

A tanulmány megnyit egy korábban lezártnak hitt útvonalat.

A klasszikus elmélet szerint a teljes zéró tudás beállítás nélkül nem szorítható egyetlen üzenetbe, és nem lehet tökéletesen megbízható. Ilango tanulmánya azt mondja: ha a zéró tudás azon következményeit kérjük számon, amelyek biztonsági játékokban tesztelhetők, és megengedjük, hogy a biztonsági definíció attól függjön, mit tud vagy nem tud egy szabálykönyv hatékonyan

megcáfolni, akkor a hasznos viselkedés nagy része visszanyerhető — egyetlen üzenettel, beállítás nélkül és tökéletes megbízhatósággal.

Ez nem apró definíciós finomítás. Más módja a kriptográfiai garanciákról való gondolkodásnak. Ne csak azt kérdezzük, mi létezik; kérdezzük azt is, mit képes kizárni a szabálykönyvünk. Ne pusztán filozófiai kellemetlenségként kezeljük a bizonyíthatatlanságot, hanem szerkezeti erőforrásként.

A gyakorlati világ talán nem változik meg holnap. A fogalmi térkép viszont igen. Most már van formális értelemben vett helyzet, amelyben az, hogy „senki sem tudja hatékonyan bebizonyítani, hogy a titok kiszivárgott", elég erős lehet ahhoz, hogy visszanyerjük azokat a játék-alapú védelmeket, amelyeket eredetileg abból szerettünk volna, hogy „a titok nem szivárgott ki".

Ezért van Gödel a címben.

Röviden

A zéró tudású bizonyítások lehetővé teszik, hogy a bizonyító meggyőzze az ellenőrzőt egy állítás igazságáról anélkül, hogy felfedné a tanút. A klasszikus lehetetlenségi eredmények szerint a zéró tudás beállítás nélkül nem sűríthető egyetlen üzenetbe, és nem lehet tökéletesen megbízható. Rahul Ilango tanulmánya nem cáfolja ezeket a lehetetlenségi eredményeket. Egy gyengébb fogalmat vezet be, az effektív zéró tudást: ahelyett, hogy valóban létező szimulátort követelne, azt követeli, hogy a választott bizonyítási rendszer — egy formális szabálykönyv, például a ZFC — ne tudja hatékonyan bebizonyítani, hogy szimulátor nem létezik. Jelentős kriptográfiai (nem interaktív, tanú-megkülönböztethetetlen bizonyítások) és bizonyításkomplexitási (nem létezik optimális bizonyítási rendszer) feltevések mellett a tanulmány NP/SAT problémákra olyan együzenetes, beállítás nélküli, tökéletesen megbízható bizonyítókat konstruál, amelyek tulajdonságonként elérik a zéró tudás cáfolható, játék-alapú következményeit. Az, hogy egyetlen bizonyító az összes „természetes" ilyen tulajdonságot lefedje, további, részben sejtésen alapuló kiterjesztés — és szó szerint minden cáfolható tulajdonság együttes lefedése valószínűleg lehetetlen, mert a bizonyítások továbbra is újrafelhasználhatók. Az eredmény elméleti és feltételes, nem bevethető primitív, de új módot mutat arra, hogyan válhat a bizonyításelméleti bizonyíthatatlanság kriptográfiai erőforrássá.

Tárgyilagos mérleg

Mit mutat meg a tanulmány? A megadott feltevések mellett NP/SAT problémákra felépíthetők olyan együzenetes, beállítás nélküli, tökéletesen megbízható bizonyítók, amelyek bármely választott bizonyítási rendszerhez képest effektíven zéró tudásúak, és külön-külön elérik a klasszikus zéró tudás minden cáfolható, játék-alapú következményét.

Mi hihető, de nincs feltétel nélkül bizonyítva? Hogy a szükséges bizonyításkomplexitási és kriptográfiai feltevések igazak. Komoly, jól tanulmányozott feltevésekről van szó — a tanulmány ráadásul azt mutatja, hogy lényegében szükségesek és elégségesek is —, de továbbra is feltevések.

Mit nem mutat meg? Klasszikus zéró tudást interakció és beállítás nélkül, tökéletes megbízhatósággal; bevetésre kész gyakorlati rendszert; a bizonyítások tagadhatóságát vagy újrafelhasználhatatlanságát; illetve azt, hogy Gödel nemteljességi tétele önmagában biztonságossá teszi a kriptográfiát.

Fő korlátok: A garancia a zéró tudás enyhített változata; a legszélesebb verzió több feltevéstől függ; az egyetlen univerzális bizonyítóra vonatkozó állítások részben továbbra is sejtésesek; az eredmény elsősorban alapkutatási jelentőségű.

Mekkora bizalom indokolt egy általános olvasó részéről? Magas abban, hogy a definíciók elfogadása esetén ez fontos feltételes elméleti eredmény. Közepes abban, hogy a feltevések a valóságot írják le. Alacsony a közvetlen gyakorlati alkalmazhatóságot illetően. A biztonságos tanulság: a tanulmány nem dönti meg a zéró tudás lehetetlenségi eredményeit; új, bizonyításelméleti módot talál arra, hogy megkerülje azoknak a részeit, amelyek sok biztonsági játékban számítanak.

Források

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`