The Clean Paper

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

Krüptograafiline tõestus võib saladust varjata, muutes puuduva simulaatori puudumise raskesti tõestatavaks

Nullteadmustõestused võimaldavad väidet tõestada tunnistajat paljastamata. Klassikaline teooria ütleb, et täielikus tähenduses ei saa seda saavutada ühe sõnumi, usaldatud seadistuse puudumise ja täiusliku korrektsusega. Rahul Ilango artikkel ei kaota seda võimatust. See muudab sihtmärki: selle asemel et nõuda simulaatori tegelikku olemasolu, nõutakse, et ükski valitud tõestussüsteem ei suudaks tõhusalt tõestada, et simulaatorit ei ole. Oluliste tõestuskeerukuse ja krüptograafiliste eelduste korral piisab sellest, et taastada nullteadmuse falsifitseeritavad mängupõhised tagajärjed omadus omaduse järel. Mõte ei ole valmis internetiprimitiivis, vaid tõestusteoreetilises viisis muuta matemaatiline tõestamatus krüptograafiliseks katteks.

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

Nipp ei seisne selles, et tõestada saladuse varjatust

Alustame nullteadmuse kõige lihtsamast versioonist.

Alice tahab Bobi veenda, et Sudoku ülesandel on lahendus. Kui ta saadab lahenduse, on Bob veendunud, kuid mõistatus on rikutud. Alice tahab midagi kummalisemat: tõestust, et lahendus on olemas, ilma lahendust ennast paljastamata.

Seda lubab **nullteadmustõestus**. Tõestaja (Alice) veenab kontrollijat (Bob), et väide on tõene, paljastamata midagi peale väite tõesuse enda.

Probleem on selles, et sellel lubadusel on hind. Tavalisel matemaatilisel tõestusel on kaks mugavat omadust. See on **üks sõnum**: kirjutad tõestuse üles, annad selle üle ja võid lahkuda. Ja sellel on **täiuslik korrektsus (perfect soundness)**: vääral väitel ei ole üldse kehtivat tõestust. Klassikalised võimatustulemused ütlevad, et nullteadmus peab mõlemast omadusest loobuma — ja mitte ainult nende kombinatsioonist; kumbki neist eraldi on samuti kättesaamatu.

Esiteks vajab nullteadmustõestus suhtlust. Kui Alice saadab ainult ühe sõnumi ja eelnevalt pole korraldatud usaldatud seadistust, variseb nullteadmuse garantii kokku — olenemata sellest, kui palju korrektsusest oleksime valmis selle nimel loovutama.

Teiseks vajab nullteadmustõestus väikest veataluvust. Nõue, et korrektsus oleks täiuslik, hävitab märkamatult ka interaktiivsuse: kontrollija, keda ei saa petta sõltumata sellest, milliseid juhuslikke valikuid ta teeb, võiks need valikud sama hästi ette ära fikseerida. Kui kontrollija on etteaimatav, saab Alice vastata kõigele üheainsa sõnumiga — ja just see juhtum juba ei töötanud.

Rahul Ilango artikkel kirjeldab viisi sellest kahekordsest müürist mööda pääseda. Mitte teeseldes, et müüri pole olemas, ega luues klassikalist nullteadmust võimatus olukorras. Võte on peenem: nõrgendada tähendust „ei paljasta midagi“, kuid teha seda viisil, mis säilitab turvaomadused, mida krüptograafid saavad tegelikult testida.

Tulemust nimetatakse **efektiivseks nullteadmuseks (effectively zero-knowledge)**.

A proof without leaking the witness

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

blocked door 1
interaction

blocked door 2
trusted setup

blocked door 3
imperfect soundness

the route
the rulebook cannot efficiently refute the simulator

Boundary: not classical zero-knowledge; effectively zero-knowledge under a chosen proof system.

Nullteadmus jääb kolme ukse taha kinni — interaktiivsus, usaldatud seadistus ja ebatäiuslik korrektsus. Ilango konstruktsioon läheb läbi teisest uksest: reeglistik ei suuda simulaatorit tõhusalt ümber lükata.

Original diagram — The Clean Paper CC BY 4.0

Classical privacy vs effective privacy

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

classical zero-knowledge

positive claim

A simulator exists and can fake the verifier's view without the witness.

effectively zero-knowledge

weaker claim

Your chosen proof system cannot efficiently prove that no simulator exists.

Boundary: the construction preserves testable consequences, not the full simulator guarantee.

Klassikaline nullteadmus küsib, kas simulaator on olemas; „efektiivne nullteadmus“ küsib ainult, kas valitud reeglistik suudab tõhusalt tõestada, et simulaatorit ei saa olla. Just see nõrgem küsimus võimaldab

konstruktsioonil säilitada ühe sõnumi, seadistuse puudumise ja täiusliku korrektsuse.

Original diagram — The Clean Paper CC BY 4.0

Vana test: simulaator on olemas

Klassikaline nullteadmuse formaliseering kasutab kujuteldavat abilist, keda nimetatakse **simulaatoriks**.

Mõte on järgmine: kujutleme Jane'i, kes **ei tea** Alice'i saladust. Kui Jane suudab täiesti iseseisvalt tekitada tõestusi, mis näevad välja täpselt nagu need, mille Bob oleks saanud Alice'ilt, siis ei õpetanud Alice'i tõestused Bobile midagi uut. Jane oleks saanud sama kogemuse võltsida juba ilma Alice'i saladuseta.

Seega nõuab klassikaline nullteadmus tegelikku simulaatorit. Peab leiduma tõhus algoritm, mis suudab luua usutavana näivaid tõestusi saladust teadmata — erialakeeles **tunnistajat (witness)** teadmata; Sudoku puhul on tunnistaja lihtsalt täidetud lahendusruudustik.

See definitsioon on võimas, kuid just siin hakkab vana võimatus kehtima. Intuitsioon on lihtne. Tõeliselt mitteinteraktiivne tõestus on lihtsalt üks sõne. Kui Bobil on see sõne käes, võib ta seda näidata kellelegi teisele: ta on saanud võime väidet teistele tõestada, mis kõlab juba millegi enama kui „mitte millegi" saamisena. Klassikalised teoreemid muudavad selle intuitsiooni eespool kirjeldatud võimatustulemusteks.

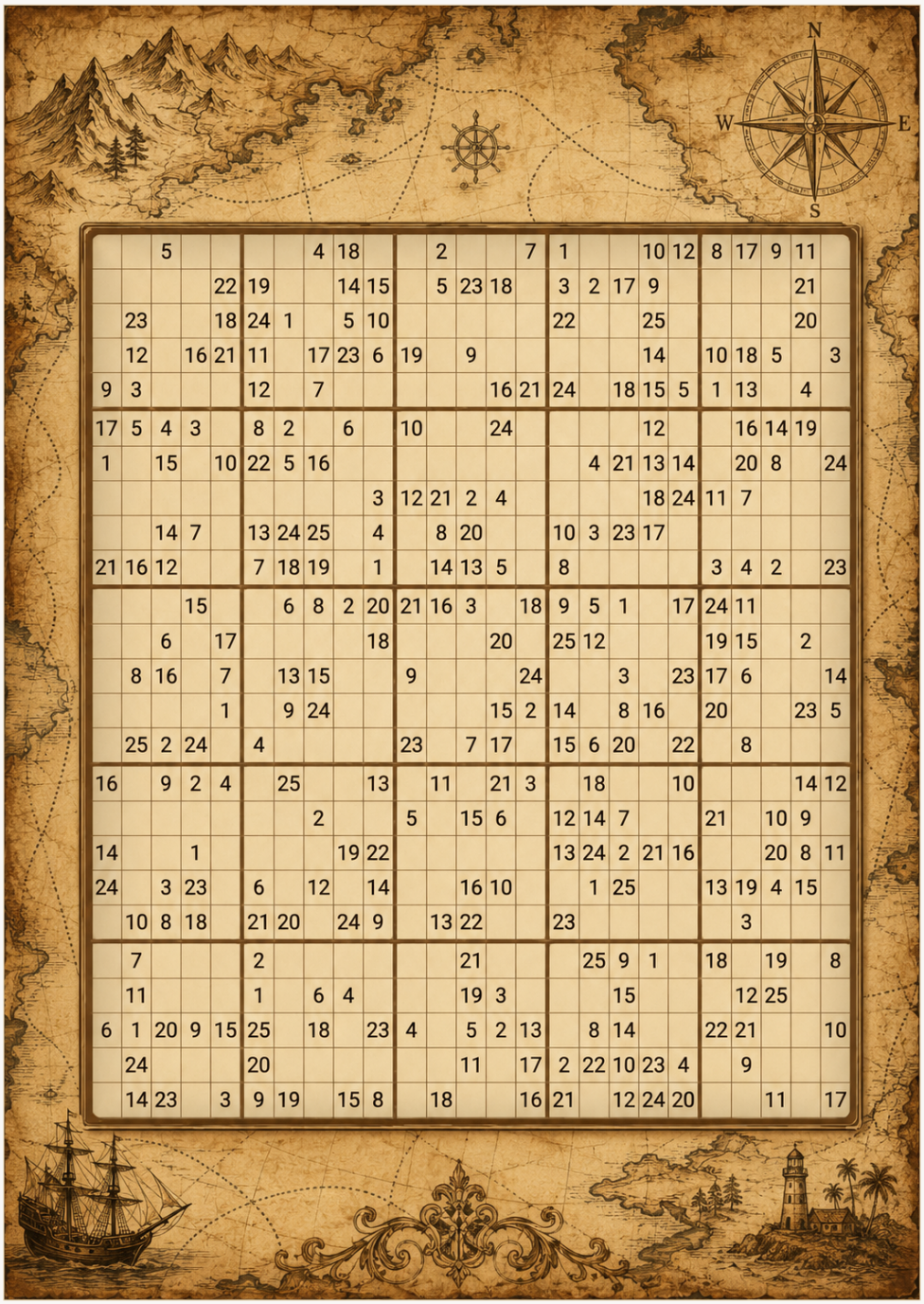
> **Kolm omadust, millest see artikkel ei loobu**
>
> Artikli pealkiri nimetab kolm piirangut:
> **Interaktsiooni pole:** Alice saadab ühe tõestussõne. Edasi-tagasi protokolli ei ole.
> **Seadistust pole:** Alice ja Bob ei tugine usaldatud ühisele viitesõnele ega muule varem kokku lepitud avalikule juhuslikkusele. Paljud süsteemid, mida nimetatakse „mitteinteraktiivseks nullteadmuseks", vajavad siiski seadistust; siin tähendab „seadistuseta" tõepoolest null seadistust.
> **Täiuslik korrektsus:** vääral väitel ei ole kehtivat tõestust. Mitte „seda peaaegu kunagi ei aktsepteerita", vaid kehtivat tõestust ei eksisteeri.
> Need kolm omadust on täpselt need, mis on tavalisel kirjalikul matemaatikal — ja nagu eespool selgitatud, ei saa klassikaline nullteadmus neid kõiki säilitada.

Erinevus mega-Sudoku näitel

Siin on tahtlikult lihtsustatud viis erinevuse tunnetamiseks.

Analoogia tõsisema osa jaoks ei tasu kasutada tavalist 9×9 Sudokut. See on liiga väike ja liiga lõplik: arvuti võib selle lihtsalt ära lahendada või tõestada, et lahendust pole. Kujutleme selle asemel

ülesannete perekonda **MegaSudoku(n)**. Suurendame tavareeglit: valime ploki suuruseks n, paneme $N = n^2$ ja ehitame $N \times N$ ruudustiku, mis on jagatud $n \times n$ plokkideks ning kasutab N sümbolit. Tavaline Sudoku on vaid tilluke juhtum $n = 3$, $N = 9$: 9×9 ruudustik, 3×3 plokid ja üheksa sümbolit. Tõestuskeerukuse lugu algab alles siis, kui n võib kasvada ja ruudustikku saab lisada vidinaid, mis panevad selle käituma nagu Sudoku kujule maskeeritud SAT-valem. SAT-valem on lihtsalt jah/ei-tüüpi piirangute loend: kas muutujatele saab määrata tõene/väär väärtused nii, et kõik piirangud oleksid täidetud?



25 × 25 Sudoku: selle reeglite täitmist saab kontrollida valmis ruudustikku paljastamata — visuaalne vaste tõestusele, mis kinnitab peidetud lahenduse ehk tunnistaja olemasolu.

AI-generated editorial thumbnail — The Clean Paper CC BY 4.0

Sudoku ja SAT: sama mõistatus kahes kostüümis

Väide, et Sudoku võib „käituda nagu SAT-valem“, ei ole metafoor. Teisendus töötab mõlemas suunas ja lihtsama suuna saab täielikult kirja panna.

Sudokust SAT-iks. SAT räägib ainult tõene/väär keeles, seega anname talle iga kolmiku (rida, veerg, väärtus) kohta ühe Boole'i muutuja: *x(r,c,v)* tähendab „rea *r* ja veeru *c* lahtris on väärtus *v*“. 4 × 4 Sudoku (2 × 2 plokid, väärtused 1–4) vajab 4·4·4 = 64 muutujat; klassikaline 9 × 9 Sudoku vajab neid 729. Iga Sudoku reegel muutub seejärel klauslite kogumiks. (Klausel on muutujate või nende eituste OR ehk VÕI; kogu valem on kõigi klauslite AND ehk JA.)

Igas lahtris on vähemalt üks väärtus — üks klausel lahtri kohta:

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

Igas lahtris on kõige rohkem üks väärtus — iga väärtusepaari kohta „mitte mõlemad“ klausel:

$\neg x(1,1,1) \lor \neg x(1,1,2)$ $\neg x(1,1,1) \lor \neg x(1,1,3)$ … ja nii edasi kõigi kuue paari jaoks.

Iga rida sisaldab iga väärtust — rea 1 ja väärtuse 3 jaoks vähemalt üks kord:

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

ja kõige rohkem üks kord: $\neg x(1,1,3) \lor \neg x(1,2,3)$, ning samamoodi iga lahtripaari jaoks selles reas.

Veerud ja plokid — samasugused klauslikogumid; muutub ainult lahtrite rühm. Vasaku ülemise ploki ja väärtuse 2 korral:

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

ning lisaks paarikaupa „mitte mõlemad“ klauslid.

Etteantud vihjed — kõige lihtsam osa: iga vihje on ühe muutujaga klausel. Vasakusse ülanurka trükitud 3 muutub klausliks

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

Kõigi nende tingimuste JA on rahuldatav täpselt siis, kui Sudokul on lahendus — ja rahuldav väärtustus *ongi* lahendus: vaatame, millised x(r,c,v) on tõesed, ja täidame ruudustiku. 9 × 9 Sudoku puhul tähendab see 729 muutujat ja mõnda tuhandet klauslit, millega tänapäevane SAT-lahendaja saab hakkama millisekunditega. Pange tähele vihjeklauslit x(1,1,3): see ütleb „see lahter võrdub täpselt 3-ga“, mitte „need lahtrid on kõik erinevad“ — sama asümmeetria sunnib allpool protokolli märkuses vihjelahtrite jaoks kasutama lisavõtet.

SAT-ist Sudokuks. Artiklis on vaja vastupidist ja raskemat suunda: võtta *suvaline* SAT-valem ning ehitada mega-Sudoku, millel on lahendus täpselt siis, kui valem on rahuldatav. Sudoku loomulikud reeglid oskavad öelda ainult „need lahtrid on kõik erinevad“, seega tuleb suvalised loogilised piirangud *ehitada* — just selleks ongi vidinad. Vidin on väike ette valmistatud lahtrikogum, üks valemi iga klausli kohta, kus kindlad lahtrid täidavad muutujate rolli (neis olev sümbol kodeerib tõest või väärat) ning kogumi sisemised piirangud on kujundatud nii, et

selle ainsad lubatud täitmised vastavad seda klauslit rahuldavatele väärtustustele. See on NP-täielikkuse tõestustes tavapärane konstruktsioonitöö; üldistatud Sudoku jaoks tegid selle 2003. aastal Yato ja Seta.
Need kaks suunda koos ütlevad, et N × N Sudoku ja SAT on sama probleem kahes eri kostüümis. Just see lubab nii sellel artiklil kui ka käsitletaval teadustööl jutustada ruudustike ja sümbolite abil kogu NP-st.

Tunnistajat on endiselt lihtne ette kujutada. Alice teab mega-Sudoku täielikku ja korrektset täidetud ruudustikku. Bob tahab veenduda, et selline täitmine on olemas, kuid Alice ei taha seda paljastada. Kui ta saadab kogu lahenduse, on Bob veendunud, aga saladus on kadunud.

Klassikalises nullteadmuse variandis Alice ja Bob suhtlevad. Ühes vanas mõttemudelis kasutatakse kaetud klotse. Alice peidab lahendatud ruudustiku, nimetab sümbolid enne iga vooru salaja ümber ning laseb Bobil kontrollida üht juhuslikult valitud lokaalset piirangut: rida, veergu, plokki või vidinat. Kui avatud lahtrites on kõik sümbolid erinevad, kasvab Bobi kindlus. Seejärel kaetakse kõik uuesti kinni ja sümbolid nimetatakse värskelt ümber. (Üks nüanss: etteantud vihjed vajavad lisavõtet, sest sümbolite ümbernimetamine peidab ka need. Allolev märkus selgitab, kuidas klassikalised protokollid selle lahendavad; järgnevaks piisab sellest lihtsustatud pildist.)

Kuidas klassikalised protokollid vihjelahtritega tegelikult toime tulevad

Ümbernimetamise võttel on pime koht. Rea-, veeru- ja plokireegel ütlevad kõik „need lahtrid on kõik erinevad“ ning *kõik erinevad* jääb õigeks iga sümbolite ümbernimetamise korral. Kuid vihje ütleb „selles lahtris on täpselt 5“ ning pärast ümbernimetamist näeb Bob ainult $\sigma(5)$ — mingit maskeeritud sümbolit — teadmata ümbernimetust σ. Ta ei saa midagi kontrollida. Kui seda ei parandata, võiks Alice tõestada, et *mingisugune* korrektne ruudustik on olemas, eirates täielikult trükitud vihjeid, mis ei tõestaks midagi *selle* konkreetse ülesande kohta. Klassikalises kirjanduses on kaks tavapärast parandust.
Palett. Peidetud ruudustikule lisatakse üks N lahtriga lisarida — palett, mille Alice täidab sümbolitega 1…N kindlas avalikus järjekorras ja nimetab seejärel koos kõige muuga ümber, nii et reas on $\sigma(1)$…$\sigma(N)$. Bobi juhuslikul väljakutsel on nüüd üks lisavõimalus. Lisaks rea, veeru, ploki või vidina avamisele võib ta valida **paleti koos ühe vihjelahtriga**. Alice avab mõlemad; palett paljastab selle vooru ümbernimetuse ning Bob kontrollib, et vihjelahtris on täpselt trükitud vihje ümbernimetatud väärtus. Nullteadmus säilib, sest Bob saab teada ainult σ — mis valitakse igas voorus uuesti ja on iseenesest kasutu — ning ühe lahtri väärtuse, mida ta ülesandest niigi teadis. Salajaste lahtrite kohta midagi ei leki ning simulaator saab vaate võltsida, valides juhusliku σ. Protokoll on korrektne, sest petlik Alice tabatakse igas voorus kindla tõenäosusega ning voorusid korratakse, kuni kahtlus on tühiselt väike.
Vihjete kompileerimine piiranguteks. Struktuursem variant eemaldab eriväljakutse selle asemel, et seda lisada. Vihje väärtuse *kontrollimise* asemel sunnitakse see paika erinevustingimustega: vihjelahter seotakse iga paletilahtriga peale selle, mis kannab tema enda väärtust — „erineb $\sigma(1)$-st, erineb $\sigma(2)$-st, …, erineb kõigest peale $\sigma(5)$“. Ainus sümbol, mida lahter võib seaduslikult sisaldada, ongi vihje väärtus. Nüüd on kõik piirangud taas kujul

> „need kaks on erinevad“ — ümbernimetamise suhtes invariantne ja kontrollitav täpselt nagu rida. Sama võtet kasutatakse klassikalises graafivärvimise protokollis ette värvitud tippude jaoks ning see on ka eespool kasutatud sõna *vidinad* mõte: MegaSudoku-kui-SAT pildis kompileeritakse vihjed ebavõrdsusvidinateks nagu kõik muudki piirangud.
> **Füüsiline protokoll.** Sudoku pärismaailma kaardiprotokoll (Gradwohl, Naor, Pinkas ja Rothblum, 2007) ei kasuta üldse ümbernimetamist ja lahendab vihjed enne, kui peitmine algab. Iga lahtri jaoks asetab Alice kolm ühesugust kaarti selle lahtri väärtusega — salajaste lahtrite puhul pildiga allapoole, kuid **vihjelahtrite puhul pildiga ülespoole**, nii et Bob näeb oma silmaga juba enne kaartide ümberpööramist, et vihjeid järgitakse. Seejärel läheb igast lahtrist üks kaart selle rea pakki, üks veeru pakki ja üks ploki pakki; iga pakk segatakse ja avatakse ning Bob kontrollib, et selles oleksid kõik N sümbolit. Segamine hävitab asukohainfo (see tagab nullteadmuse), kuid vihjed olid juba jagamise hetkel kindlaks määratud.
> Mõlemal juhul on õppetund sama, mille juurde see artikkel ikka tagasi pöördub: nullteadmusprotokoll on hoolikas arvestus selle üle, *millised* faktid peitmise üle elavad. Ümbernimetamine säilitab omaduse „kõik erinevad“ ja kustutab „võrdub 5-ga“ — seega tuleb „võrdub 5-ga“ mõnel muul viisil tagasi tuua.

See ei ole artiklis kasutatav protokoll. See on mõttemudel klassikalise nullteadmuse jaoks:

- Alice ja Bob suhtlevad edasi-tagasi.
- Bob valib juhuslikke kontrolle.
- Alice paljastab ainult lokaalse kooskõla, mitte kogu lahendust.
- Privaatsuse tõestus näitab, et Bobi vaate oleks saanud tekitada ka ilma Alice’i salajase lahenduseta.

Seega toetub klassikaline nullteadmus positiivsele faktile:

> Simulaator on päriselt olemas.

Nüüd eemaldame mugavad osad. Alice saadab ühe tõestussõne ja lahkub. Usaldatud seadistust pole, varem ette valmistatud ühist juhuslikku sõnet pole ning Bob ei tohi kunagi aktsepteerida vale ülesannet. Sellises keskkonnas ei saa klassikaline nullteadmus püsima jääda.

Enne nippi on vaja veel üht tegelast. Fikseerime **reeglistiku**: loogiku mõttes formaalse tõestussüsteemi — kindla aksioomide kogumi koos mehaaniliste reeglitega kirjalike matemaatiliste tõestuste kontrollimiseks. ZFC, matemaatika standardne aksioomisüsteem, on kanooniline näide. Kõik järgnev sõnastatakse ette valitud reeglistiku suhtes ning valik ise on paindlik: konstruktsioon töötab iga fikseeritud reeglistiku korral, sealhulgas ZFC puhul.

(Sõnakasutuse märkus, mis pärineb ka artiklist endast: „tõestussüsteem“ tähendab siin alati seda reeglistikku — formaalset süsteemi, mis kontrollib matemaatilisi tõestusi — mitte Alice’i saadetud sõnumeid. Alice’i ja Bobi mehhanisme nimetatakse **tõestajaks** ja **kontrollijaks**.)

Gödeli-laadne versioon jätab mega-Sudoku loo alles, kuid muudab tõestust.

Valime teise, sama kuvatava suurusega piirangusüsteemi ja nimetame selle **D**-ks. Loos on S ja D kaks samas vormingus MegaSudoku(n) ülesannet. Taustal võis D alata teistsuguse suurusega raskest loogikavalemist; vajaduse korral saab sellele lisada kahjutuid näivpiiranguid, et see mahuks samasse ruudustikku. D ehitatakse loogikavalemist, mis on tegelikult **mitterahuldatav**: puudub väärtustus, mis teeks kõik selle piirangud korraga tõeseks, täpselt nagu katkisel mõistatusel puudub lubatud valmis ruudustik. Lihtne mängunäide oleks valem, mis nõuab korraga nii „X on tõene“ kui ka „X on väär“. Seega ei ole D-l kehtivat täitmist.

Kuid D ei tohi olla katkine ülesanne, mille katkisust on *lihtne paljastada*. Eelnev mängunäide siin ei sobi: iga reeglistik lükkab „X ja mitte-X“ ühe reaga ümber. D peab olema väär viisil, mida valitud reeglistik ei suuda lühikese argumendiga kinnitada. Kui reeglistik suudaks D lühikese tõestusega ümber lükata, variseks allolev lugu kokku: alternatiivne tee, mis oleks võinud toota tõestusi ilma Alice'i saladuseta, saaks formaalselt välistatud ning koos sellega kaoks privaatsusgarantii. Seepärast valitakse D perekonnast, mida fikseeritud reeglistik ei suuda tõhusalt ümber lükata: selles reeglistikus ei ole lühikest tõestust, et D-l pole lahendust.

Alice'i ühesõnumiline tõestus puudutab nüüd kas-või-väidet:

> kas tegelikul mega-Sudokul S on lahendus või peibutusel D on lahendus.

See on loogiline seos. D-d **ei** tekitata mingil võluviisil, mis muudaks S-i tõeseks. Tõestus ei väida „D-l pole lahendust, järelikult S-il on lahendus“. See tõestab disjunktsiooni **S või D**. Täiuslik korrektsus ütleb, et vääral disjunktsioonil ei saa olla kehtivat tõestust. Kuna D on tegelikkuses väär — sellel pole lahendust — saab disjunktsioon olla tõene ainult siis, kui S on tõene. Kui tõestus vastu võetakse, peab S-il seega lahendus olema. Peibutus ei saa muuta väärat S-i tõeseks.

Nullteadmuse-laadse osa jaoks küsime aga, mis juhtuks siis, kui D-l *oleks* lahendus. See peibutuslahendus toimiks alternatiivse tunnistajana. Selle abil saaks keegi tekitada tõestusi Alice'i tegelikku mega-Sudoku lahendust teadmata — teisisõnu oleks olemas simulaator. Tegelikult D-l lahendust pole, nii et see simulatsioonitee on suletud. Võtmekoht on selles, et reeglistik ei suuda tõhusalt tõestada, et see tee on suletud.

Seega on D-l kaks ülesannet. **Korrektsuse** jaoks on D väär, mistõttu kehtiv tõestus väitele „S või D“ sunnib S-i olema tõene. **Efektiivse nullteadmuse** jaoks on D raskesti ümberlükatav, mistõttu reeglistik ei suuda kiiresti välistada peibutusteed, mis oleks simulatsiooni võimalikuks teinud.

Turvatest ei ole seega enam:

> Kas me suudame tõestada, et simulaator on päriselt olemas?

Selle asemel küsitakse:

> Kas sinu reeglistik suudab tõhusalt tõestada, et simulaator on võimatu?

Kui vastus on ei, järgneb midagi üllatavalt tugevat: iga turvagarantii, mida (a) saab testi käivitades vaadelda ja mis (b) reeglistiku sees tõestatavalt järeldub simulaatori olemasolust, kehtib tegelikult.

Edukas rünnak ükskõik millise sellise garantii vastu annaks ise puuduva lühikese ümberlükkamise — ning seda lühikest ümberlükkamist ei ole. See ongi „efektiivne“ osa efektiivsest nullteadmusest.

Seega on klassiruumiversiooni kontrast järgmine:

Klassikaline nullteadmus: tõestused on turvalised, sest simulaator on olemas.

Gödeli-laadne efektiivne nullteadmus: vaadeldavate turvatestide mõttes käsitletakse tõestusi turvalisena, sest reeglistik ei suuda tõhusalt tõestada, et simulaator on võimatu.

Teine väide on nõrgem. Just seetõttu saab artikkel säilitada kolm omadust, mis klassikalise versiooni katki tegid: ühe sõnumi, seadistuse puudumise ja täiusliku korrektsuse.

Uus test: sa ei suuda tõestada, et simulaator puudub

Ilango leevendus muudab küsimust.

Klassikaline nullteadmus küsib:

> Kas simulaator on olemas?

Efektiivne nullteadmus küsib midagi nõrgemat:

> Kas sinu valitud reeglistik suudab tõhusalt tõestada, et simulaatorit ei ole olemas?

See võib kõlada tehnilise möödahiilimisena, kuid on idee tuum. Konstruktsioon asub kummalises seisundis: simulaatorit tegelikult **ei eksisteeri** — artikkel ütleb seda otsesõnu — kuid fikseeritud reeglistik ei suuda tõhusalt tõestada, et seda pole. Kui iga halb tagajärg, millest hoolime, eeldaks just sellist ümberlükkamist, käitub süsteem nende tagajärgede suhtes ikkagi nagu nullteadmus.

Siin tuleb mängu Gödel. Mitte kaunistusena ega loosungina „Gödel teeb krüptograafia turvaliseks“. Seos on tõestusteoreetiline. Reeglistikku nimetatakse **optimaalseks**, kui see on täpses mõttes parim võimalik: kui mõni reeglistik suudab vastavat tüüpi valemi lühikese tõestusega ümber lükata, suudab optimaalne reeglistik seda samuti, kusjuures tema tõestus on kõige rohkem polünomiaalselt pikem. Krajíček ja Pudlák oletasid 1989. aastal, et **optimaalset tõestussüsteemi ei eksisteeri**: ükskõik millise reeglistiku me fikseerime, leidub mõni teine reeglistik, mis tõestab mõne tõeste väidete perekonna palju lühemalt. See on tõestuskeerukuse üks keskseid lahtisi oletusi ning Gödeli mittetäielikkuse teoreemi lõplik, keerukusteoreetiline sugulane: mõnel tõesel väitel pole fikseeritud reeglistikus lühikest tõestust — mitte seepärast, et seda ei saaks põhimõtteliselt tõestada, vaid seepärast, et iga fikseeritud reeglistik jätab osa lühidalt sõnastatavaid tõdesid ilma lühikese tõestuseta.

Artikkel eeldab seda oletust (veidi tugevamas „lõpmata sageli“ vormis, mida kasutatakse krüptograafilistes oletustes tavapäraselt). Krajíčeki ja Pudláki teoreemi järgi on tasu konkreetne: iga reeglistiku jaoks leidub valemite jada, mis on tõepoolest mitterahuldatavad, kuid mida see reeglistik ei suuda lühikeste tõestustega ümber lükata — ja mis veel olulisem, tõhus algoritm

suudab neid valemeid *genereerida*. Viimane omadus, ühtlus ehk **uniformity**, muudab idee pelgast olemasoluväitest algoritmiks, mida Alice saab tegelikult käivitada: tema peibutised D tulevad justkui tootmisliinilt, mitte tühjast õhust.

Krüptograafiline võte seisneb selle tõestusjõu puudujäägi ärakasutamises.

Mida konstruktsioon teeb

Siin on artikli konstruktsioon kõige põhilisemal kujul.

Fikseerime reeglistiku — näiteks ZFC. Tõestuskeerukuse eelduse kohaselt leidub tõhusalt genereeritav valemite jada, mis on tegelikult mitterahuldatavad, kuid mille mitterahuldatavuse kohta pole selles reeglistikus lühikest tõestust.

Nüüd ehitame ühe sõnumiga tõestuse kujul:

> kas tegelik väide on rahuldatav või see eriline raske valem on rahuldatav.

Eriline raske valem ei ole rahuldatav. Kui aluseks olev tõestusmehhanism on täiuslikult korrektne, tähendab sõnumi aktsepteerimine seega endiselt, et tegelik väide on tõene. Nii saadakse täiuslik korrektsus.

Nullteadmuse-laadse turvalisuse jaoks kujutleme aga, et eriline raske valem *oleks* rahuldatav. Siis saaks selle tunnistaja abil simuleerida tõestusi tegelikku tunnistajat teadmata. Tegelikult valem ei ole rahuldatav — kuid reeglistik ei suuda seda tõhusalt tõestada. Seega ei suuda reeglistik tõhusalt tõestada, et simulaator on võimatu.

See on pöördepunkt. Süsteem ei peida saladust klassikalist simulaatorit luues. Suure hulga vaadeldavate turvatestide suhtes peidab ta saladuse reeglistiku suutmatuse taha kinnitada, et simulaator puudub.

Mida artikkel väidab

Põhiteoreem on mitmekihiline. Tuumtulemus on järgmine.

Ühe standardse krüptograafilise eelduse — **mitteinteraktiivsete tunnistajaid eristamatute tõestuste (non-interactive witness indistinguishable proofs)** olemasolu, mis on hästi uuritud objektid ja tulenevad mitmest väljakujunenud eelduste paketist — ning tõestuskeerukuse oletuse **„(lõpmata sageli) optimaalset tõestussüsteemi ei eksisteeri“** korral konstrueerib artikkel iga reeglistiku valiku jaoks NP/SAT-i tõestaja ja kontrollija, kus tõestus on üks sõnum, puudub seadistus, kehtib **täiuslik korrektsus** ning süsteem on selle reeglistiku suhtes efektiivselt nullteadmuslik. (NP/SAT on mõistatuselaadsete probleemide tavapärane „kõige raskem ühine nimetaja“; mega-Sudoku on üks selle kostüüme.)

Laiema väite jaoks, mis puudutab falsifitseeritavate turvaomaduste säilitamist, lisab artikkel veel ühe standardse eelduse: derandomiseerimise uskumuse **P = BPP** (jämedalt öeldes: juhuslikkus ei anna algoritmidele olulist lisavõimsust).

Teoreemikeelest tavakeelde tõlgituna:

- Tõestus on üks sõnum.
- Usaldatud seadistust pole.
- Vääraid väiteid ei saa tõestada.
- Tõestaja ei ole klassikaliselt nullteadmuslik — tal pole simulaatorit.
- Kuid selles keskkonnas saab saavutada klassikalise nullteadmuse iga falsifitseeritava, mängupõhise turvatagajärje.

„Falsifitseeritav“ on siin oluline. See tähendab, et turvariket saab testida, lastes vastasel mõnes mängus tegutseda. Paljud krüptograafilised turvadefinitsioonid on sellised: kas vastane suudab eristada kahte krüpteeringut, pöörata funktsiooni tagasi, taastada tunnistaja või võita mingi kindla eksperimendi? Teoreem annab iga falsifitseeritava omaduse jaoks oma tõestaja, ühe omaduse korraga. Üksainus tõestaja, millel oleks *kõik* falsifitseeritavad omadused korraga, on tõenäoliselt võimatu — vana taaskasutusrünnak („Bob võib tõestust teistele näidata“) on ise falsifitseeritav omadus ning siin see tõepoolest ei kehti. Artikli ettepanek on, et üks tõestaja võiks usutavalt katta kõik *loomulikud* falsifitseeritavad omadused — need, mis krüptograafilises praktikas päriselt esinevad —, kuid see osa on tingimuslik teoreem, mis tugineb „loomuliku“ mitteametlikule mõistele ja lisaks ühele sõnaselgele oletusele. Garantii sihib vaadeldavaid läbikukkumisi, mitte saladuse iga filosoofilist või simulatsioonipõhist tähendust.

Üht konkreetset järeldust tasub eraldi nimetada: konstruktsioon annab esimesed mitteinteraktiivsed **tunnistajat varjavad (witness hiding)** tõestused ühtse tõestajaga — „mõistatuse tõestus ei aita sul selle lahendust leida“, ilma interaktsiooni ja seadistuseta — tagasihoidlikult kõlava objekti, mida polnud aastakümneid suudetud konstrueerida.

Mida see ei väida

See osa hoiab loo ausana.

See **ei** ütle, et vanad võimatusteoreemid olid valed. Konstruktsioon väldib neid definitsiooni muutes.

See **ei** anna tavalist klassikalist nullteadmust ilma interaktsiooni ja seadistuseta ning täiusliku korrektsusega. Artikkel ütleb otsesõnu, et konstrueeritud tõestajal ei ole simulaatorit.

See **ei** tähenda, et tõestust ei saaks uuesti kasutada. Ühe sõnumiga tõestust saab endiselt kellelegi teisele näidata; artikkel ei säilita eitatavusega (deniability) seotud omadusi. (Sama piirang on ka usaldatud seadistusega mitteinteraktiivsel nullteadmusel.)

See **ei** tähenda, et tegemist oleks juurutusvalmis praktilise protokolliga. See on keerukusteooria ja krüptograafia aluste uurimus. Tulemus sõltub olulistest tõestuskeerukuse ja krüptograafia eeldustest

ning konstruktsioon käsitleb põhimõttelist võimalikkust.

Samuti ei muuda see „Gödelit“ maagiliseks turbeprimitiiviks. Seos Gödeliga kulgeb tõestussüsteemide, optimaalsete tõestussüsteemide ja mittetäielikkuse lõplike analoogide kaudu. Kasulik intuitsioon ei ole „mittetäielikkus kaitseb sinu parooli“. Mõte on hoopis selles: kui reeglistik ei suuda tõhusalt tõestada, et simulaator on võimatu, saab sellist tõestust vajavad ründed blokeerida juba turvadefinitsioonide tasandil.

Miks see ikkagi huvitav on

Krüptograafia muudab raskuse sageli turvalisuseks. Tegurdamine on raske, seega muutuvad RSA-laadsed eeldused kasulikuks. Võreprobleemid on rasked, seega muutub kasulikuks võrekrüptograafia. Siin on raskus kummalisem: mitte „saladust on raske arvutada“, vaid „on raske tõestada, et teatavat tõestusobjekti ei saa olemas olla“.

Just seepärast tundub artikkel ebatavaline. See kohtleb aksioome ja reeglistikke peaaegu nagu krüptograafilisi ressursse. Tavaline võimatus ütleb, et korrektsuse ja simulatsiooni vahel on pinge. Ilango võte on paigutada see pinge tõestusteoreetilise kardina taha: simulaator puudub, kuid formaalne süsteem ei suuda seda puudumist tõhusalt nähtavale tuua.

Lugeja jaoks pole üllatav osa see, et see võiks asendada tänapäevased nullteadmussüsteemid. Tõenäoliselt ei asenda, vähemalt mitte otseselt. Üllatav on hoopis see, et matemaatilise loogika piirangut saab kasutada konstruktiivselt: mitte üksnes müürina, vaid omamoodi kattena.

Kui tugevad on tõendid?

See on teoreemiartikkel, seega tähendab „tõendusmaterjal“ siin midagi muud kui bioloogia- või astronoomiaartiklis. Küsimus pole selles, kas katset korrati. Küsimus on selles, kas definitsioonid, eeldused ja tõestusahel toetavad väidet.

Tõestus on formaalne ja artikkel ütleb oma eeldused selgelt välja. Need pole juhuslikud eeldused. Mitteinteraktiivsed tunnistajaid eristamatud tõestused on krüptograafias standardsed objektid ja tulenevad mitmest väljakujunenud eelduste komplektist. Optimaalse tõestussüsteemi puudumise oletus on tõestuskeerukuse keskne oletus. P = BPP on standardne derandomiseerimise uskumus, mida kasutatakse ainult laiema falsifitseeritavate omaduste teoreemi jaoks.

Artikkel väidab ka, et need eeldused on õige hind, mitte suvaline tugikonstruktsioon: see tõestab pöördtulemuse, mille järgi on need sisuliselt vajalikud — kui sellised konstruktsioonid üldse eksisteerivad, peavad olemas olema mitteinteraktiivsed tunnistajaid eristamatud tõestused ning (eeldades standardseid ühesuunalisi funktsioone) optimaalset tõestussüsteemi ei saa olemas olla. Eeldused on ka „võit mõlemal juhul“ tüüpi: ükskõik millise neist ümberlükkamine oleks ise murranguline avastus tõestuskeerukuses, krüptograafias või keerukusteoorias.

Kuid kuna tulemus on tingimuslik, on ka kindlus selle suhtes tingimuslik. Kui need eeldused ei kehti, muutub teoreemi tõlgendus. Ja isegi kui eeldused kehtivad, ei ole garantii täielik klassikaline nullteadmus; see on artikli leevendatud, tõestusteoreetiline versioon.

Seega on põhjendatud suur kindlus, et artikkel tõestab sidusa tingimusliku võimalikkustulemuse; mõõdukas kindlus, et selle eeldused kirjeldavad krüptograafilist maailma, milles me tegelikult elame; ning väike kindlus mis tahes vahetu praktilise tagajärje suhtes.

Miks see oluline on

Artikkel avab tee, mis pidi olema suletud.

Klassikaline teooria ütleb: täielikku nullteadmust ei saa ilma seadistuseta suruda ühte sõnumisse ning sellel ei saa olla täiuslikku korrektsust. Ilango artikkel ütleb: kui küsime nullteadmuse tagajärgede kohta, mida saab turvamängudes testida, ning lubame turvadefinitsioonil sõltuda sellest, mida reeglistik suudab või ei suuda tõhusalt ümber lükata, saab suure osa kasulikust käitumisest tagasi — ühe sõnumi, seadistuse puudumise ja täiusliku korrektsusega.

See pole väike definitsioonimuudatus. See on teistsugune viis krüptograafilistest garantiidest mõelda. Selle asemel et küsida ainult, mis on olemas, küsime, mida meie reeglistik suudab välistada. Selle asemel et käsitleda tõestamatust filosoofilise tüütusena, kasutame seda struktuurina.

Praktiline maailm ei pruugi homme muutuda. Kuid mõisteline kaart muutub. Nüüd on olemas formaalne tähendus, milles „keegi ei suuda tõhusalt tõestada, et saladus lekkis“ võib olla piisavalt tugev, et taastada paljud mängupõhised kaitsed, mida tahtsime väitest „saladus ei lekkinud“.

Seepärast kuulub Gödel pealkirja.

Lühidalt

Nullteadmustõestused võimaldavad tõestajal veenda kontrollijat väite tõesuses tunnistajat paljastamata. Klassikalised võimatustulemused ütlevad, et nullteadmust ei saa ilma seadistuseta suruda ühte sõnumisse ja samal ajal ei saa sellel olla täiuslikku korrektsust. Rahul Ilango artikkel ei lükka neid võimatusi ümber. See defineerib nõrgema mõiste, efektiivse nullteadmuse: selle asemel et nõuda simulaatori tegelikku olemasolu, nõutakse, et valitud tõestussüsteem — formaalne reeglistik nagu ZFC — ei suudaks tõhusalt tõestada, et simulaatorit ei ole. Oluliste krüptograafiliste eelduste (mitteinteraktiivsed tunnistajaid eristamatud tõestused) ja tõestuskeerukuse eelduse (optimaalset tõestussüsteemi ei eksisteeri) korral konstrueerib artikkel NP/SAT-i jaoks ühe sõnumiga, seadistuseta ja täiuslikult korrektsed tõestajad, mis saavutavad nullteadmuse falsifitseeritavad mängupõhised tagajärjed omadus omaduse järel. Üksainus tõestaja, mis kataks kõiki selliseid „loomulikke“ omadusi, on järgmine, osaliselt oletuslik samm — ning sõna otseses mõttes kõigi falsifitseeritavate omaduste katmine on tõenäoliselt võimatu, sest tõestused jäävad taaskasutatavaks. Tulemus on teoreetiline ja tingimuslik, mitte juurutatud primitiiv, kuid see näitab uut viisi kasutada tõestusteoreetilist tõesta-

matust krüptograafilise ressursina.

Kaine hinnang

Mida artikkel näitab: Sõnastatud eeldustel saab NP/SAT-i jaoks ehitada ühe sõnumiga, seadistuseta ja täiuslikult korrektseid tõestajaid, mis on iga valitud tõestussüsteemi suhtes efektiivselt nullteadmuslikud ning saavutavad eraldi iga klassikalise nullteadmuse falsifitseeritava mängupõhise turvatagajärje.

Mis on usutav, kuid tingimusteta tõestamata: Et vajalikud tõestuskeerukuse ja krüptograafilised eeldused kehtivad. Need on tõsised ja põhjalikult uuritud eeldused — ning artikkel näitab, et need on sisuliselt nii vajalikud kui ka piisavad —, kuid siiski eeldused.

Mida see ei näita: Klassikalist nullteadmust ilma interaktsiooni ja seadistuseta ning täiusliku korrektsusega; juurutusvalmis praktilist süsteemi; tõestuste eitatavust või mittetaaskasutatavust; ega seda, et Gödeli mittetäielikkuse teoreem üksi muudaks krüptograafia turvaliseks.

Peamised piirangud: Garantii on nullteadmuse leevendus; kõige laiem versioon sõltub mitmest eeldusest; ühe universaalse tõestaja kohta käivad väited jäävad osaliselt oletuslikuks; ning tulemus on eeskätt fundamentaalne.

Kui kindel peaks tavalugeja olema? Suur kindlus selles, et definitsioonidega nõustudes on tegu olulise tingimusliku teooriatulemusega. Mõõdukas kindlus selles, et eeldused kirjeldavad tegelikkust. Väike kindlus vahetu praktilise rakendamise osas. Turvaline järeldus on: artikkel ei murra nullteadmuse võimatustulemusi; see leiab uue tõestusteoreetilise tee ümber nende osade, mis on paljude turvamängude jaoks olulised.

Allikad

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