The Clean Paper

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

Крыптаграфічны доказ можа хаваць сакрэт, робячы адсутнасць сімулятара цяжкай для доказу

Доказы з нулявым разгалошваннем дазваляюць даказаць сцвярджэнне, не раскрываючы witness. Класічная тэорыя кажа, што ў поўным сэнсе гэта немагчыма адначасова з адным паведамленнем, адсутнасцю даверанага setup і perfect soundness. Артыкул Рахула Іланга не адмяняе гэтую немагчымасць. Ён змяняе мэту: замест патрабавання, каб сімулятар сапраўды існаваў, дастаткова, каб ніякая выбраная сістэма доказаў не магла эфектыўна даказаць, што сімулятара не існуе. Пры моцных дапушчэннях з тэорыі складанасці доказаў і крыптаграфіі гэтага хапае, каб па адной уласцівасці за раз аднавіць фальсіфікаваныя, гульнявыя наступствы zero-knowledge. Гэта не гатовы інтэрнэт-прымітыў, а тэарэтыка-доказавы спосаб ператварыць матэматычную недаказальнасць у крыптаграфічнае прыкрыццё.

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

Фокус не ў тым, каб даказаць, што сакрэт схаваны

Пачнём з самай простай версіі нулявога разгалошвання.

Аліса хоча пераканаць Боба, што судоку мае рашэнне. Калі яна дашле само рашэнне, Боб пераканаецца — але галаваломка будзе сапсавана. Ёй трэба нешта больш дзіўнае: доказ таго, што рашэнне існуе, без раскрыцця самога рашэння.

Менавіта гэта абяцае **доказ з нулявым разгалошваннем (zero-knowledge proof)**. Той, хто даказвае (Аліса), пераконвае таго, хто правярае (Боба), што сцвярджэнне праўдзівае, не раскрываючы нічога, акрамя самога факта яго праўдзівасці.

Праблема ў тым, што ў гэтага абяцання ёсць цана. Звычайны матэматычны доказ мае дзве зручныя ўласцівасці. Ён складаецца з **аднаго паведамлення**: вы запісваеце яго, перадаеце і сыходзіце. І ён мае **perfect soundness — дасканалую надзейнасць супраць ілжывых сцвярджэнняў**: для ілжывага сцвярджэння наогул не існуе карэктнага доказу. Класічныя тэарэмы немагчымасці кажуць, што zero-knowledge мусіць адмовіцца ад абедзвюх характарыстык — і не толькі ад іх спалучэння: кожная паасобку таксама недаступная.

Па-першае, доказ з нулявым разгалошваннем патрабуе ўзаемадзеяння. Калі Аліса пасылае адно паведамленне і няма загадзя арганізаванай даверанай наладкі, гарантыя zero-knowledge разбураецца — незалежна ад таго, наколькі вы гатовыя аслабіць soundness узамен.

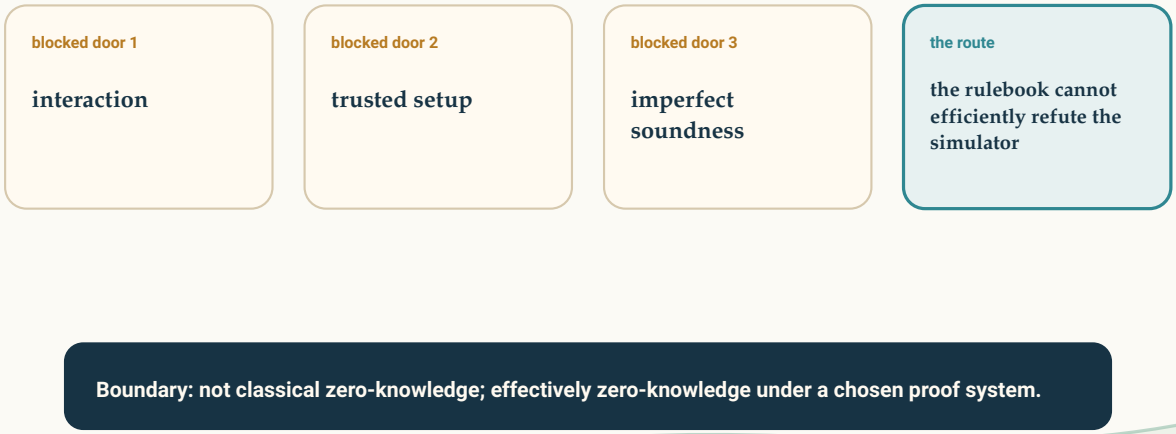
Па-другое, zero-knowledge патрабуе невялікай дапушчальнай імавернасці памылкі. Патрабаванне perfect soundness незаўважна знішчае і ўзаемадзеянне: калі таго, хто правярае, немагчыма падмануць ні пры якім наборы яго выпадковых выбараў, ён мог бы проста зафіксаваць гэтыя выбары загадзя. А як толькі правяральнік становіцца прадказальным, Аліса можа адказаць на ўсё адным паведамленнем — гэта значыць мы вяртаемся менавіта да выпадку, які ўжо немагчымы.

Артыкул Рахула Іланга прапануе шлях вакол гэтай падвойнай сцяны. Не адмаўляючы яе існавання і не ствараючы класічнае zero-knowledge там, дзе яно немагчыма. Ход больш тонкі: аслабіць значэнне фразы «нічога не раскрывае», але так, каб захаваць тыя ўласцівасці бяспекі, якія крыптографы сапраўды могуць правяраць.

Вынік называецца **эфектыўным нулявым разгалошваннем (effectively zero-knowledge)**.

A proof without leaking the witness

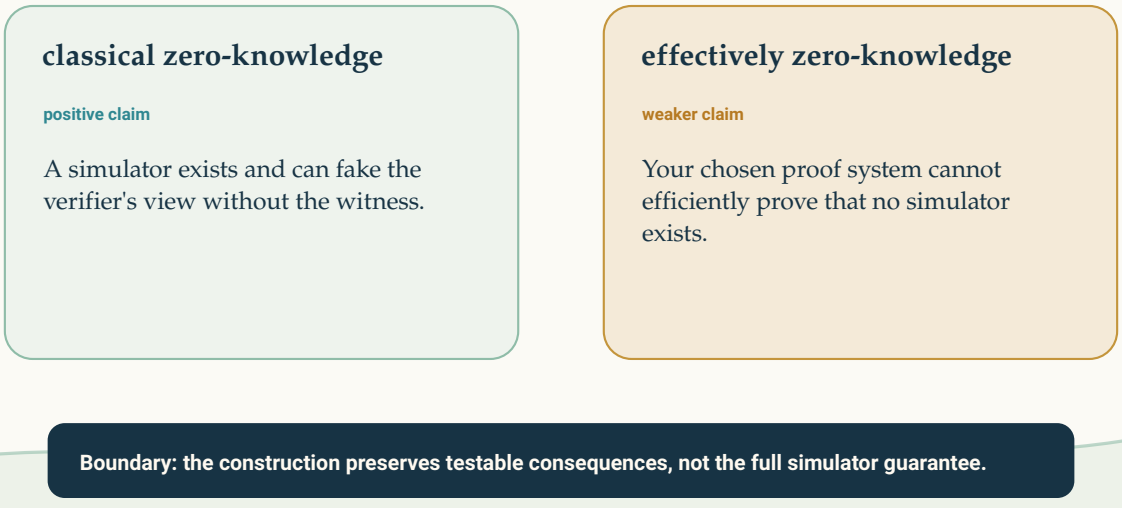
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Zero-knowledge заблакавана трыма дзвярыма — узаемадзеяннем, даверанай наладкай і недасканалай soundness. Канструкцыя Іланга ідзе іншым шляхам: выбраная фармальная сістэма не можа эфектыўна абвергнуць існаванне сімулятара.

Classical privacy vs effective privacy

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



Класічнае zero-knowledge пытаецца, ці існуе сімулятар; «effectively zero-knowledge» пытаецца толькі, ці

можа выбраная фармальная сістэма эфектыўна даказаць, што сімулятара не існуе. Менавіта больш слабае пытанне дазваляе канструкцыі захаваць адно паведамленне, адсутнасць setup і perfect soundness.

Стары крытэрый: сімулятар існуе

Класічнае фармальнае вызначэнне zero-knowledge выкарыстоўвае ўяўнага памочніка — **сімулятар**.

Ідэя такая. Уявім Джэйн, якая **не** ведае сакрэту Алісы. Калі Джэйн можа самастойна генераваць доказы, што выглядаюць гэтак жа, як доказы, якія Боб атрымаў бы ад Алісы, то доказы Алісы не навучылі Боба нічому новаму. Джэйн ужо магла падрабіць увесь досвед без сакрэту Алісы.

Таму класічнае zero-knowledge патрабуе рэальнага сімулятара. Павінен існаваць эфектыўны алгарытм, здольны генераваць праўдападобныя «фальшывыя» доказы без ведання сакрэту — **сведкі (witness)** у тэрміналогіі гэтай галіны; для судоку witness — гэта проста цалкам і правільна запоўненая сетка.

Гэта моцнае вызначэнне, але менавіта тут спрацоўвае старая немагчымасць. Інтуіцыя такая. Сапраўдны неінтэрактыўны доказ — проста радок. Як толькі Боб атрымаў гэты радок, ён можа паказаць яго камусьці яшчэ: ён набыў здольнасць пераконваць іншых у сцвярджэнні, а гэта ўжо гучыць як нешта большае за «нічога». Класічныя тэарэмы ператвараюць гэтую інтуіцыю ў вынікі немагчымасці, апісаныя вышэй.

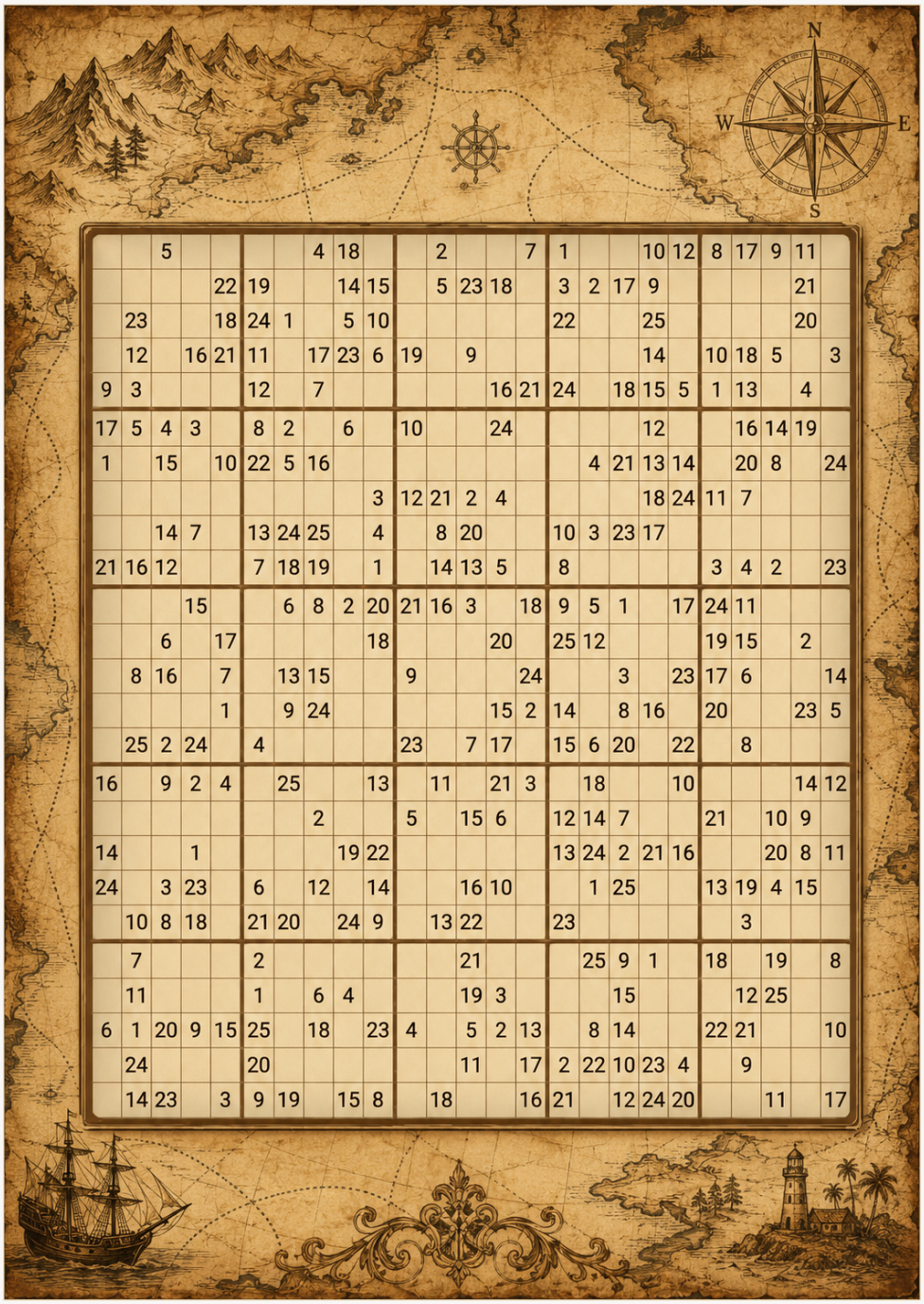
Тры ўласцівасці, ад якіх гэты артыкул не адмаўляецца

Назва працы проста паказвае на тры абмежаванні:
Без узаемадзеяння: Аліса пасылае адзін радок-доказ. Няма пратакола з абменам паведамленнямі туды і назад.
Без наладкі: Аліса і Боб не абапіраюцца на даверaны агульны рэферэнтны радок або іншую загадзя падрыхтаваную публічную выпадковасць. Многія сістэмы, якія называюць «неінтэрактыўным zero-knowledge», усё роўна патрабуюць setup; тут setup няма наогул.
Perfect soundness: ілжывае сцвярджэнне не мае ніводнага карэктнага доказу. Не «амаль ніколі не прымаецца», а «карэктнага доказу не існуе».
Менавіта гэтыя тры ўласцівасці мае звычайная пісьмовая матэматыка — і, як тлумачылася вышэй, класічнае zero-knowledge не можа захаваць іх разам.

MegaSudoku як спосаб адчуць розніцу

Вось наўмысна спрошчаная аналогія.

Для сур'ёзнай часткі аналогіі не варта браць звычайнае судоку 9×9. Яно занадта малое і канечнае: камп'ютар можа проста вырашыць яго або даказаць, што рашэння няма. Замест гэтага ўявім сямейства галаваломак **MegaSudoku(n)**. Маштабуем звычайнае правіла: выбіраем памер блока n, задаём $N = n^2$ і будуем сетку $N \times N$, падзеленую на блокі $n \times n$, з N сімваламі. Звычайнае судоку — толькі малюсенькі выпадак $n = 3$, $N = 9$: сетка 9×9, блокі 3×3 і дзевяць сімвалаў. Гісторыя пра складанасць доказаў пачынаецца толькі тады, калі n можа расці, а сетка атрымлівае дадатковыя гаджэты, якія прымушаюць яе паводзіць сябе як формула SAT, пераапранутая ў судоку. Формула SAT — гэта проста набор абмежаванняў «так/не»: ці можна прысвоіць зменным значэнні ісціна/няпраўда так, каб усе абмежаванні выконваліся?



Судоку 25×25: яго правілы можна правяраць, не раскрываючы завершаную сетку — візуальная метафара доказу, які пацвярджае існаванне схаванага рашэння, гэта значыць witness.

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

Судоку і SAT: адна галаваломка ў двух строях

Сцвярджэнне, што судоку можа «паводзіць сябе як формула SAT», — не метафара. Пераклад працуе ў абодва бакі, і больш просты кірунак можна запісаць цалкам. **Ад судоку да SAT.** SAT аперуе толькі ісцінасцю/няпраўдай, таму ўвядзём адну булеву зменную для кожнай тройкі (радок, слупок, значэнне): *x(r,c,v)* азначае

«клетка ў радку *r*, слупку *c* змяшчае значэнне *v*». Судоку 4×4 (блокі 2×2, значэнні 1–4) патрабуе 4·4·4 = 64 зменныя; класічнае 9×9 — 729. Кожнае правіла судоку ператвараецца ў набор клаўз. (Клаўза — гэта OR зменных або іх адмаўленняў; уся формула з'яўляецца AND усіх клаўз.)
Кожная клетка змяшчае як мінімум адно значэнне — адна клаўза на клетку:

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

Кожная клетка змяшчае не больш за адно значэнне — клаўза «не абодва» для кожнай пары значэнняў:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \text{… і гэтак далей для ўсіх шасці пар.}$$

Кожны радок змяшчае кожнае значэнне — для радка 1 і значэння 3: як мінімум адзін раз,

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

і не больш за адзін раз: $\neg x(1,1,3) \vee \neg x(1,2,3)$, і гэтак далей для кожнай пары клетак у радку.
Слупкі і блокі — тыя ж наборы; змяняецца толькі група клетак. Для верхняга левага блока і значэння 2:

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

плюс папарныя клаўзы «не абодва».
Надрукаваныя падказкі — самая простая частка: кожная падказка з'яўляецца клаўзай з адной зменнай. Надрукаваная 3 у верхнім левым куце становіцца клаўзай

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

Кан'юнкцыя (AND) усяго гэтага выканальная тады і толькі тады, калі судоку мае рашэнне, а задавальняльнае прысваенне *і ёсць* рашэнне: глядзім, якія x(r,c,v) праўдзівыя, і запаўняем сетку. Для 9×9 гэта 729 зменных і некалькі тысяч клаўз — сучасны SAT-solver спраўляецца з імі за мілісекунды. Звярніце ўвагу на клаўзу падказкі x(1,1,3): яна азначае «гэтая клетка роўная менавіта 3», а не «ўсе гэтыя клеткі розныя». Тая ж асіметрыя ніжэй прымусіць нас выкарыстаць дадатковы трук для клетак-падказак.
Ад SAT да судоку. Артыкулу патрэбны супрацьлеглы і больш складаны кірунак: па *адвольнай* формуле SAT пабудаваць mega-Sudoku, якое мае рашэнне тады і толькі тады, калі формула выканальная. Уласныя правілы судоку ўмеюць казаць толькі «гэтыя клеткі ўсе розныя», таму адвольныя лагічныя абмежаванні трэба *сканструяваць* — менавіта для гэтага патрэбныя гаджэты. Гаджэт — невялікі загадзя спраектаваны кластар клетак, па адным на кожную клаўзу формулы, у якім вылучаныя клеткі адыгрываюць ролю зменных (сімвал у іх кадуе

ісціну або няпраўду), а ўнутраныя абмежаванні спраектаваныя так, каб адзіныя дапушчальныя запаўненні адпавядалі прысваенням, якія задавальняюць гэтую клаўзу. Гэта стандартная інжынерыя з доказаў NP-паўнаты; для абагульненага судоку яе рэалізавалі Yato і Seta ў 2003 годзе.
Разам абодва кірункі кажуць, што судоку N×N і SAT — адна і тая ж задача ў двух строях. Менавіта гэта дазваляе гэтаму артыкулу — і самой працы — гаварыць пра ўвесь NP на мове сетак і сімвалаў.

Witness па-ранейшаму лёгка ўявіць. Аліса ведае поўнае карэктнае запаўненне mega-Sudoku. Боб хоча пераканацца, што такое запаўненне існуе, але Аліса не хоча яго раскрываць. Калі яна дашле ўсю сетку, Боб пераканаецца, але сакрэт знікне.

У класічнай zero-knowledge-версіі Аліса і Боб узаемадзейнічаюць. Стары наглядны вобраз выкарыстоўвае закрытыя пліткі. Аліса хавае вырашаную сетку, перад кожным раўндам таемна пераймяноўвае сімвалы і дазваляе Бобу праверыць адно выпадкова выбранае лакальнае абмежаванне: радок, слупок, блок або гаджэт. Калі адкрытыя клеткі змяшчаюць усе розныя сімвалы, давер Боба расце. Затым усё зноў закрываюць, а сімвалы нанова пераймяноўваюць. (Ёсць адна тонкасць: зададзеныя падказкі галаваломкі патрабуюць асобнага трука, бо перайменаванне хавае і іх. Заўвага ніжэй тлумачыць, як класічныя пратаколы гэта вырашаюць.)

Як класічныя пратаколы насамрэч працуюць з клеткамі-падказкамі

У трука з перайменаваннем ёсць сляпая зона. Правілы радка, слупка і блока ўсе кажуць «гэтыя клеткі папарна розныя», а ўласцівасць *усе розныя* захоўваецца пры любым перайменаванні сімвалаў. Але падказка кажа: «гэтая клетка змяшчае менавіта 5». Пасля перайменавання Боб бачыць толькі $\sigma(5)$ — нейкі замаскіраваны сімвал — і не ведае перастаноўку σ. Праверыць нічога нельга. Калі гэта не выправіць, Аліса магла б даказаць існаванне *нейкай* правільнай сеткі, цалкам ігнаруючы надрукаваныя падказкі, а гэта нічога не даказвае пра *дадзеную* галаваломку. У класічнай літаратуры ёсць два стандартныя спосабы выпраўлення.
Палітра. Да схаванай сеткі дадаюць адзін дадатковы радок з N клетак — палітру, якую Аліса запаўняе сімваламі 1…N у фіксаваным публічным парадку, а затым пераймяноўвае разам з усім астатнім, так што там аказваюцца $\sigma(1)$…$\sigma(N)$. Цяпер у выпадковага выкліку Боба з'яўляецца яшчэ адзін варыянт. Акрамя радка, слупка, блока або гаджэта ён можа выбраць **палітру плюс адну клетку-падказку**. Аліса адкрывае абедзве; палітра паказвае перайменаванне гэтага раўнда, а Боб правярае, што клетка-падказка змяшчае менавіта перайменаваную версію надрукаванай падказкі. Zero-knowledge захоўваецца, бо Боб даведваецца толькі σ — новую выпадковую перастаноўку для гэтага раўнда, якая сама па сабе нічога не дае, — і значэнне клеткі, якое ён ужо ведаў з галаваломкі. Нічога пра сакрэтныя клеткі не ўцякае, а сімулятар можа падрабіць такую карціну, проста выбраўшы

выпадковую σ. Soundness захоўваецца, бо махлярскую Алісу ў кожным раўндзе ловяць з фіксаванай імавернасцю, а раўнды паўтараюць, пакуль імавернасць памылкі не стане нязначнай.

Кампіляцыя падказак у абмежаванні. Больш структурны варыянт не дадае спецыяльную праверку, а ліквідуе патрэбу ў ёй. Замест таго каб *правяраць* значэнне падказкі, яго прымушаюць выконвацца праз абмежаванні няроўнасці: клетку-падказку злучаюць з усімі клеткамі палітры, акрамя той, якая нясе яе ўласнае значэнне — «не роўная $\sigma(1)$, не роўная $\sigma(2)$, …, не роўная ўсяму, акрамя $\sigma(5)$». Адзіным сімвалам, які гэтая клетка можа законна змяшчаць, застаецца патрэбны. Усе абмежаванні зноў маюць форму «гэтыя дзве клеткі розныя» — яны інварыянтныя да перайменавання і правяраюцца гэтак жа, як радок. Менавіта такі прыём выкарыстоўваюць для загадзя афарбаваных вяршынь у класічным пратаколе афарбоўкі графа; ён перадае і сэнс слова *гаджэты* вышэй: у карціне MegaSudoku-як-SAT падказкі кампілююцца ў гаджэты няроўнасці гэтак жа, як усе астатнія абмежаванні.

Фізічны пратакол. Рэальны картачны пратакол для судоку (Gradwohl, Naor, Pinkas і Rothblum, 2007) наогул не выкарыстоўвае перайменаванне і фіксуе падказкі яшчэ да пачатку ўтойвання. Для кожнай клеткі Аліса выкладае тры аднолькавыя карты са значэннем клеткі — кашуляй уверх для сакрэтных клетак, але **тварам уверх для клетак-падказак**, каб Боб на ўласныя вочы бачыў выкананне падказак да таго, як карты перавернуць. Затым адна карта з кожнай клеткі ідзе ў пакет яе радка, адна — у пакет слупка, адна — у пакет блока; кожны пакет перамешваюць і адкрываюць, а Боб правярае, што ён змяшчае ўсе N сімвалаў. Перамешванне знішчае інфармацыю пра пазіцыі — гэта і дае zero-knowledge, — але падказкі ўжо былі зафіксаваныя пры раскладцы.

У любым варыянце ўрок той самы, да якога гэты артыкул пастаянна вяртаецца: пратакол zero-knowledge — гэта дбайны ўлік таго, *якія менавіта* факты пераканаўчыя. Перайменаванне захоўвае «ўсе розныя» і сцірае «роўна 5», таму «роўна 5» трэба вярнуць іншым спосабам.

Гэта не пратакол з самога артыкула. Гэта толькі мысленная мадэль класічнага zero-knowledge:

- Аліса і Боб абменьваюцца паведамленнямі.
- Боб выбірае выпадковыя праверкі.
- Аліса раскрывае толькі лакальную ўзгодненасць, а не ўсё рашэнне.
- Доказ прыватнасці ў тым, што карціну, якую бачыць Боб, можна было б згенераваць без ведання сакрэтнага рашэння Алісы.

Такім чынам, класічнае zero-knowledge пабудавана вакол станоўчага факта:

> Сімулятар сапраўды існуе.

Цяпер прыбяром зручныя часткі. Аліса пасылае адзін радок-доказ і сыходзіць. Няма

даверанага setup, няма агульнага выпадковага радка, падрыхтаванага загадзя, а Боб ніколі не павінен прымаць ілжывую галаваломку. Менавіта ў такім асяроддзі класічнае zero-knowledge не выжывае.

Перад самім трукам патрэбны яшчэ адзін персанаж. Зафіксуем **кнігу правілаў**: фармальную сістэму доказаў у лагічным сэнсе — фіксаваны набор аксіём плюс механічныя правілы праверкі пісьмовых матэматычных доказаў. Кананічны прыклад — ZFC, стандартная сістэма аксіём матэматыкі. Усё далейшае фармулюецца адносна загадзя выбранай кнігі правілаў, але выбар гнуткі: канструкцыя працуе для любой фіксаванай фармальнай сістэмы, уключаючы ZFC.

(Тэрміналагічная заўвага, узятая з самога артыкула: «proof system» тут заўсёды азначае менавіта такую кнігу правілаў — фармальную сістэму, якая правярае матэматычныя доказы, — а не паведамленні, якія пасылае Аліса. Механізмы Алісы і Боба называюцца «prover» і «verifier» — тым, хто даказвае, і тым, хто правярае.)

Версія ў стылі Гёдэля захоўвае гісторыю пра mega-Sudoku, але змяняе сам доказ.

Выберам другую сістэму абмежаванняў такога ж адлюстроўванага памеру і назавём яе **D**. У нашай гісторыі S і D — дзве галаваломкі MegaSudoku(n) аднаго фармату. За кулісамі D магла пачынацца як складаная лагічная формула іншага памеру; пры неабходнасці яе можна дапоўніць бяскрыўднымі фіктыўнымі абмежаваннямі, каб яна змясцілася ў такую ж сетку. D будуецца з лагічнай формулы, якая насамрэч **невыканальная**: не існуе прысваення значэнняў, што задавальняе ўсім яе абмежаванням, гэтак жа як зламаная галаваломка не мае законна запоўненай сеткі. Цацачны прыклад — формула, якая адначасова патрабуе «X праўдзівае» і «X ілжывае». Значыць, D не мае правільнага запаўнення.

Але D не павінна быць зламанай галаваломкай, якую *лёгка выкрыць*. Цацачны прыклад не падыходзіць: любая фармальная сістэма абвергне «X і не-X» адным радком. D павінна быць ілжывай такім чынам, каб выбраная кніга правілаў не магла сертыфікаваць гэта кароткім аргументам. Калі б яна магла каротка абвергнуць D, уся канструкцыя ніжэй развалілася б: альтэрнатыўны шлях, які мог бы дазволіць генераваць доказы без сакрэту Алісы, быў бы фармальна выключаны, а разам з ім знікла б гарантыя прыватнасці. Таму D бяруць з сямейства, якое фіксаваная кніга правілаў не можа эфектыўна абвергнуць: унутры гэтай сістэмы няма кароткага доказу таго, што D не мае рашэння.

Аднапаведамленчы доказ Алісы цяпер датычыцца дыз'юнкцыі:

альбо сапраўднае mega-Sudoku S мае рашэнне, альбо прынада D мае рашэнне.

Вось лагічная сувязь. D **не** генеруецца нейкім магічным спосабам, які робіць S праўдзівай. Доказ не сцвярджае «D не мае рашэння, значыць S мае рашэнне». Ён даказвае дыз'юнкцыю **S або D**. Perfect soundness кажа, што ілжывая дыз'юнкцыя не можа мець карэктнага доказу. Паколькі ў рэальнасці D ілжывая — рашэння няма, — адзіны спосаб, каб дыз'юнкцыя была праўдзівай, — гэта праўдзівасць S. Значыць, калі

доказ прыняты, S павінна мець рашэнне. Прынада не можа ператварыць ілжывую S у праўдзівую.

Але для часткі ў стылі zero-knowledge спытаем, што адбылося б, калі б D *мела* рашэнне. Такое рашэнне-прынада было б альтэрнатыўным witness. Яно дазволіла б генераваць доказы, не ведаючы сапраўднага рашэння mega-Sudoku Алісы — гэта значыць дало б сімулятар. У рэальнасці D рашэння не мае, таму гэты шлях сімуляцыі закрыты. Сутнасць у тым, што кніга правілаў не можа эфектыўна даказаць, што ён закрыты.

Такім чынам, D выконвае дзве працы. Для **soundness** D ілжывая, таму карэктны доказ «S або D» прымушае S быць праўдзівай. Для **effective zero-knowledge** D цяжка абвергнуць, таму кніга правілаў не можа хутка выключыць шлях праз прынаду, які зрабіў бы сімуляцыю магчымай.

Таму тэст бяспекі цяпер не такі:

> Ці можам мы даказаць, што сімулятар сапраўды існуе?

Замест гэтага ён становіцца такім:

> Ці можа ваша кніга правілаў эфектыўна даказаць, што сімулятар немагчымы?

Калі адказ «не», вынікае нешта нечакана моцнае: кожная гарантыя бяспекі, якая (а) назіраецца шляхам выканання тэсту і (б) унутры гэтай кнігі правілаў даказальна вынікае з існавання сімулятара, насамрэч выконваецца. Паспяховая атака на любую з іх сама стала б тым адсутным кароткім абвяржэннем — а такога кароткага абвяржэння няма. Менавіта гэта азначае «effective» у effectively zero-knowledge.

Такім чынам, вучэбнае супрацьпастаўленне выглядае так:

Класічнае zero-knowledge: доказы бяспечныя, таму што сімулятар існуе.

Effective zero-knowledge ў стылі Гёдэля: для назіраных тэстаў бяспекі доказы паводзяць сябе як бяспечныя, таму што кніга правілаў не можа эфектыўна даказаць, што сімулятар немагчымы.

Другое сцвярджэнне слабейшае. Але менавіта таму артыкул можа захаваць тры ўласцівасці, якія разбуралі класічную версію: адно паведамленне, адсутнасць setup і perfect soundness.

Новы крытэрый: вы не можаце даказаць адсутнасць сімулятара

Аслабленне Іланга змяняе само пытанне.

Класічнае zero-knowledge пытаецца:

> Ці існуе сімулятар?

Effectively zero-knowledge пытаецца нешта слабейшае:

> Ці можа выбраная вамі кніга правілаў эфектыўна даказаць, што сімулятара не існуе?

Гэта можа гучаць як тэхнічная шчыліна, але менавіта тут цэнтральная ідэя. Канструкцыя знаходзіцца ў дзіўным стане: сімулятара насамрэч **не існуе** — артыкул кажа пра гэта проста, — але зафіксаваная вамі кніга правілаў не можа эфектыўна даказаць яго адсутнасць. Калі кожны непажаданы вынік, які вас цікавіць, патрабаваў бы такога абвяржэння, сістэма ўсё роўна паводзіць сябе як zero-knowledge адносна гэтых вынікаў.

Менавіта тут з'яўляецца Гёдэль. Не як упрыгожанне і не ў сэнсе «Гёдэль робіць крыптаграфію бяспечнай». Сувязь тэарэтыка-доказавая. Кнігу правілаў называюць **аптымальнай**, калі яна ў дакладным сэнсе з'яўляецца найлепшай магчымай: калі любая фармальная сістэма можа абвергнуць формулу патрэбнага тыпу кароткім доказам, аптымальная таксама можа гэта зрабіць, прычым яе доказ будзе не больш чым паліномна даўжэйшы. Krajíček і Pudlák у 1989 годзе вылучылі гіпотэзу, што **аптымальнай сістэмы доказаў не існуе**: якую кнігу правілаў ні зафіксуй, знойдзецца іншая, якая даказвае некаторае сямейства праўдзівых сцвярджэнняў значна карацей. Гэта адна з цэнтральных адкрытых гіпотэз тэорыі складанасці доказаў і канечны, тэарэтыка-складанасны сваяк тэарэмы Гёдэля пра непаўнату: некаторыя праўдзівыя сцвярджэнні не маюць кароткага доказу ў фіксаванай вамі сістэме — не таму, што іх у прынцыпе немагчыма даказаць, а таму, што кожная фіксаваная кніга правілаў пакідае некаторыя коратка сфармуляваныя ісціны без кароткіх доказаў.

Артыкул дапускае гэтую гіпотэзу — у крыху мацнейшай форме «бясконца часта», стандартнай для крыптаграфічнага выкарыстання гіпотэз. Паводле тэарэмы Krajíček і Pudlák выйгрыш канкрэтны: для кожнай кнігі правілаў існуе паслядоўнасць формул, якія сапраўды невыканальныя, але якія гэтая сістэма не можа абвергнуць кароткімі доказамі — і, што крытычна важна, эфектыўны алгарытм можа іх *генераваць*. Менавіта гэта апошняя ўласцівасць, аднароднасць (uniformity), ператварае ўсю ідэю са сцвярджэння пра існаванне ў сапраўдны алгарытм, які можа выконваць Аліса: яе прынады D сыходзяць з канвеера, а не ўзнікаюць з паветра.

Крыптаграфічны ход у тым, каб выкарыстаць гэты недахоп доказавай сілы.

Што робіць канструкцыя

Вось канструкцыя артыкула ў аголеным выглядзе.

Зафіксуйце кнігу правілаў — скажам, ZFC. Пры дапушчэнні з тэорыі складанасці доказаў існуе эфектыўна генераваная паслядоўнасць формул, якія насамрэч невыканальныя, але кніга правілаў не мае кароткага доказу іх невыканальнасці.

Цяпер пабудуйце аднапаведамленчы доказ такога тыпу:

> альбо сапраўднае сцвярджэнне выканальнае, альбо гэтая спецыяльная складаная формула выканальная.

Спецыяльная складаная формула невыканальная. Такім чынам, калі базавы механізм доказу мае perfect soundness, прыняцце паведамлення ўсё роўна азначае, што сапраўднае сцвярджэнне праўдзівае. Гэта дае perfect soundness.

Але для бяспекі ў стылі zero-knowledge ўявім, што спецыяльная складаная формула *была б* выканальнай. Тады яе witness можна было б выкарыстоўваць для сімуляцыі доказаў без ведання сапраўднага witness. У рэчаіснасці формула невыканальная — але кніга правілаў не можа эфектыўна гэта даказаць. Значыць, яна не можа эфектыўна даказаць, што сімулятар немагчымы.

Менавіта гэта — шарнір усёй канструкцыі. Сістэма не хавае сакрэт шляхам стварэння класічнага сімулятара. Для вялікага класа назіраных тэстаў бяспекі яна хавае сакрэт за няздольнасцю кнігі правілаў сертыфікаваць адсутнасць сімулятара.

Што сцвярджае артыкул

Галоўная тэарэма мае некалькі слаёў. Ядро выніку такое.

Пры стандартным крыптаграфічным дапушчэнні — існаванні **неінтэрактыўных доказаў з неадрознымі сведкамі (non-interactive witness indistinguishable proofs)**, добра вывучаных аб'ектаў, якія вынікаюць з некалькіх устояных набораў дапушчэнняў, — і пры гіпотэзе тэорыі складанасці доказаў, што **не існуе (бясконца часта) аптымальнай сістэмы доказаў**, артыкул для кожнай выбранай кнігі правілаў будуе аднапаведамленчыя prover і verifier для NP/SAT з **perfect soundness**, без setup, які з'яўляецца effectively zero-knowledge адносна гэтай кнігі правілаў. (NP/SAT — стандартны «найцяжэйшы агульны назоўнік» задач-галаваломак; mega-Sudoku — толькі адзін з яго строяў.)

Для больш шырокага сцвярджэння пра захаванне фальсіфікаваных уласцівасцей бяспекі артыкул дадае яшчэ адно стандартнае дапушчэнне — гіпотэзу дэранамізацыі **P = BPP** (груба кажучы: выпадковасць не дае алгарытмам прынцыпова дадатковай сілы).

Калі перакласці з мовы тэарэм:

- Доказ — адно паведамленне.
- Даверанага setup няма.
- Ілжывыя сцвярджэнні немагчыма даказаць.

- Prover не з’яўляецца класічным zero-knowledge — сімулятара ў яго няма.
- Але ў гэтым асяроддзі можна атрымаць кожнае фальсіфікаванае, гульнявое наступства бяспекі класічнага zero-knowledge.

Слова «фальсіфікаванае» важнае. Яно азначае, што правал бяспекі можна праверыць, запусціўшы праціўніка ў вызначанай гульні. Многія крыптаграфічныя вызначэнні бяспекі маюць менавіта такую форму: ці можа праціўнік адрозніць два шыфратэксты, інвертаваць функцыю, аднавіць witness або выйграць канкрэтны эксперымент? Тэарэма дае prover для кожнай такой уласцівасці асобна, па адной за раз. Адзін prover, які адначасова мае *ўсе* фальсіфікаваныя ўласцівасці, хутчэй за ўсё немагчымы: старая атака праз паўторнае выкарыстанне («Боб можа паказаць доказ іншым») сама з’яўляецца фальсіфікаванай уласцівасцю, і тут яна сапраўды не выконваецца. Прапанова артыкула ў тым, што адзін prover можа праўдападобна ахапіць усе *натуральныя* фальсіфікаваныя ўласцівасці — тыя, якія рэальна сустракаюцца ў крыптаграфічнай практыцы, — але гэтая частка з’яўляецца ўмоўнай тэарэмай, якая абапіраецца на нефармальнае паняцце «натуральнасці» плюс відавочную гіпотэзу. Гарантыя накіравана на назіраныя правалы, а не на кожнае філасофскае або сімуляцыйнае значэнне сакрэтнасці.

Адно канкрэтнае наступства варта назваць асобна: канструкцыя дае першыя неінтэрактыўныя доказы з **утойваннем witness (witness hiding)** і аднародным prover — «доказ існавання рашэння галаваломкі не дапамагае вам знайсці само рашэнне», без узаемадзеяння і без setup. Гучыць сціпла, але такі аб’ект не ўдавалася пабудаваць дзесяцігоддзямі.

Чаго гэта не азначае

Менавіта гэты раздзел не дае матэрыялу ператварыцца ў гіпербалу.

Гэта **не** азначае, што старыя тэарэмы немагчымасці былі няправільныя. Канструкцыя абыходзіць іх, змяніўшы вызначэнне.

Гэта **не** дае звычайнага класічнага zero-knowledge без узаемадзеяння, без setup і з perfect soundness. Артыкул проста кажа, што пабудаваны prover не мае сімулятара.

Гэта **не** азначае, што доказ немагчыма паўторна выкарыстоўваць. Аднапаведамленчы доказ усё яшчэ можна паказаць камусьці яшчэ; артыкул не захоўвае ўласцівасці кшталту адмаўляльнасці (deniability). (Неінтэрактыўнае zero-knowledge з даверaным setup мае тую ж мяжу.)

Гэта **не** практычны пратакол, гатовы да разгортвання. Гэта тэорыя складанасці і фундаментальная крыптаграфія. Вынік залежыць ад моцных дапушчэнняў з тэорыі складанасці доказаў і крыптаграфіі, а канструкцыя адказвае на пытанне пра тое, што ў прынцыпе магчыма.

І гэта **не** ператварае «Гёдэля» ў магічны прымітыў бяспекі. Сувязь з Гёдэлем праходзіць

праз сістэмы доказаў, аптымальныя сістэмы доказаў і канечныя аналагі непаўнаты. Карысная інтуіцыя тут не «непаўната абараняе ваш пароль», а такая: калі кніга правілаў не можа эфектыўна даказаць, што сімулятар немагчымы, то атакі, якія патрабавалі б такога доказу, можна блакаваць на ўзроўні вызначэнняў бяспекі.

Чаму гэта ўсё роўна цікава

Крыптаграфія часта ператварае складанасць у бяспеку. Фактарызацыя цяжкая — значыць, дапушчэнні ў стылі RSA становяцца карыснымі. Рашоткавыя задачы цяжкія — значыць, карыснай становіцца рашоткавая крыптаграфія. Тут складанасць больш дзіўная: не «цяжка вылічыць сакрэт», а «цяжка даказаць, што пэўны аб'ект доказу не можа існаваць».

Менавіта таму праца адчуваецца незвычайнай. Яна абыходзіцца з аксіёмамі і кнігамі правілаў амаль як з крыптаграфічнымі рэсурсамі. Звычайная немагчымасць кажа пра напружанне паміж soundness і сімуляцыяй. Ход Іланга змяшчае гэтае напружанне за тэарэтыка-доказавую заслону: сімулятара няма, але фармальная сістэма не можа эфектыўна выкрыць гэтую адсутнасць.

Для чытача нечакана не тое, што гэта заменіць сучасныя zero-knowledge-сістэмы. Хутчэй за ўсё, прынамсі непасрэдна, не заменіць. Нечакана тое, што абмежаванне з матэматычнай логікі можна выкарыстаць канструктыўна: не толькі як сцяну, але як свайго роду сховішча.

Наколькі пераканаўчыя падставы?

Гэта артыкул з тэарэмай, таму «доказы» тут азначаюць іншае, чым у біялогіі або астраноміі. Пытанне не ў тым, ці паўтарыўся эксперымент. Пытанне ў тым, ці падтрымліваюць вызначэнні, дапушчэнні і ланцужок матэматычнага доказу заяўлены вынік.

Доказ фармальны, а артыкул выразна пералічвае дапушчэнні. І яны не выпадковыя. Неінтэрактыўныя witness-indistinguishable proofs — стандартныя аб'екты крыптаграфіі, якія вынікаюць з некалькіх устояных набораў дапушчэнняў. Гіпотэза пра адсутнасць аптымальнай сістэмы доказаў з'яўляецца цэнтральнай гіпотэзай тэорыі складанасці доказаў. **P** = **BPP** — стандартнае дапушчэнне пра дэранамізацыю, патрэбнае толькі для больш шырокай тэарэмы пра фальсіфікаваныя ўласцівасці.

Артыкул таксама аргументуе, што гэтыя дапушчэнні — не адвольныя будаўнічыя рыштаванні, а фактычна неабходная цана. Ён даказвае адваротны вынік: калі такія канструкцыі ўвогуле існуюць, павінны існаваць неінтэрактыўныя witness-indistinguishable proofs, а пры стандартным дапушчэнні пра існаванне аднабаковых функцый аптымальнай

сістэмы доказаў існаваць не можа. І дапушчэнні маюць характар «win-win»: абвяржэнне любога з іх само стала б знакавым адкрыццём у тэорыі складанасці доказаў, крыптаграфіі або тэорыі складанасці.

Але паколькі вынік умоўны, упэўненасць у яго інтэрпрэтацыі таксама ўмоўная. Калі дапушчэнні ілжывыя, змест тэарэмы змяняецца. І нават калі яны праўдзівыя, гарантыя не з'яўляецца поўным класічным zero-knowledge; гэта аслабленая, тэарэтыка-доказавая версія артыкула.

Таму правільная ацэнка такая: высокая ўпэўненасць, што артыкул усталёўвае цэльны ўмоўны вынік пра магчымасць; умераная — што дапушчэнні апісваюць крыптаграфічны свет, у якім мы сапраўды жывём; і нізкая — адносна любога неадкладнага практычнага наступства.

Чаму гэта важна

Артыкул адкрывае маршрут, які лічыўся закрытым.

Класічная тэорыя кажа: поўнае zero-knowledge не можа складацца з аднаго паведамлення без setup і не можа мець perfect soundness. Артыкул Іланга кажа: калі пытацца пра тыя наступствы zero-knowledge, якія можна правяраць у гульнях бяспекі, і дазволіць вызначэнню бяспекі залежаць ад таго, што кніга правілаў можа або не можа эфектыўна абвергнуць, то значную частку карысных паводзінаў можна вярнуць — з адным паведамленнем, без setup і з perfect soundness.

Гэта не невялікая падкрутка вызначэння. Гэта іншы спосаб думаць пра крыптаграфічныя гарантыі. Замест таго каб пытацца толькі, што існуе, спытайце, што ваша кніга правілаў здольная выключыць. Замест таго каб лічыць недаказальнасць філасофскай нязручнасцю, выкарыстоўвайце яе як структуру.

Практычны свет, магчыма, не зменіцца заўтра. Але канцэптуальная карта ўжо змянілася. Цяпер існуе фармальны сэнс, у якім «ніхто не можа эфектыўна даказаць, што сакрэт уцек» можа быць дастаткова моцным, каб аднавіць многія гульнявыя абароны, якіх мы хацелі ад сцвярджэння «сакрэт не ўцек».

Менавіта таму Гёдэль — у назве.

Коратка

Доказы з нулявым разгалошваннем дазваляюць prover пераканаць verifier у праўдзівасці сцвярджэння, не раскрываючы witness. Класічныя вынікі немагчымасці кажуць, што zero-knowledge нельга ўціснуць у адно паведамленне без setup і што яно не можа мець perfect soundness. Артыкул Рахула Іланга не абвяргае гэтыя тэарэмы. Ён

вызначае больш слабае паняцце — effectively zero-knowledge: замест патрабавання рэальнага існавання сімулятара трэба, каб выбраная сістэма доказаў — фармальная кніга правілаў кшталту ZFC — не магла эфектыўна даказаць, што сімулятара не існуе. Пры моцных дапушчэннях з крыптаграфіі (неінтэрактыўныя witness-indistinguishable proofs) і тэорыі складанасці доказаў (адсутнасць аптымальнай сістэмы доказаў) артыкул будуе аднапаведамленчыя prover для NP/SAT без setup і з perfect soundness, якія па адной уласцівасці за раз узнаўляюць фальсіфікаваныя, гульнявыя наступствы zero-knowledge. Адзін prover для ўсіх «натуральных» такіх уласцівасцей — далейшае, часткова гіпатэтычнае пашырэнне, а літаральна ўсе фальсіфікаваныя ўласцівасці адначасова, верагодна, немагчымыя, бо доказы застаюцца паўторна выкарыстоўвальнымі. Вынік тэарэтычны і ўмоўны, а не гатовы крыптаграфічны прымітыў, але ён паказвае новы спосаб ператварыць тэарэтыка-доказавую недаказальнасць у крыптаграфічны рэсурс.

Праверка без прыкрас

Што паказвае артыкул: Пры выразна сфармуляваных дапушчэннях можна пабудаваць аднапаведамленчыя prover для NP/SAT без setup і з perfect soundness, якія з’яўляюцца effectively zero-knowledge адносна любой выбранай сістэмы доказаў і рэалізуюць кожнае фальсіфікаванае, гульнявое наступства класічнага zero-knowledge.

Што праўдападобна, але не даказана безумоўна: Што неабходныя дапушчэнні з тэорыі складанасці доказаў і крыптаграфіі праўдзівыя. Гэта сур’ёзныя, добра вывучаныя дапушчэнні — і артыкул паказвае, што яны па сутнасці не толькі дастатковыя, але і неабходныя, — аднак яны ўсё роўна застаюцца дапушчэннямі.

Чаго ён не паказвае: Класічнага zero-knowledge без узаемадзеяння, без setup і з perfect soundness; практычнай сістэмы, гатовай да разгортвання; адмаўляльнасці або немагчымасці паўторнага выкарыстання доказаў; або таго, што сама па сабе тэарэма Гёдэля пра непаўнату забяспечвае крыптаграфічную бяспеку.

Галоўныя абмежаванні: Гарантыя з’яўляецца аслабленнем zero-knowledge; самая шырокая версія залежыць ад некалькіх дапушчэнняў; сцвярджэнні пра адзін універсальны prover часткова застаюцца гіпатэтычнымі; а вынік перадусім фундаментальны.

Якой упэўненасці заслугоўвае выснова для звычайнага чытача? Высокай у тым, што гэта важны ўмоўны тэарэтычны вынік, калі прыняць яго вызначэнне. Умеранай у тым, што дапушчэнні адпавядаюць рэальнасці. Нізкай адносна неадкладнага практычнага прымянення. Бяспечная выснова: артыкул не ламае тэарэмы немагчымасці для zero-knowledge; ён знаходзіць новы тэарэтыка-доказавы спосаб абысці тыя іх часткі, якія важныя для многіх гульняў бяспекі.

Крыніцы

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