The Clean Paper

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

Криптографско доказателство може да скрие тайната си, като направи липсващия симулатор труден за опровергаване

Доказателствата с нулево знание позволяват да се докаже твърдение, без да се разкрива свидетелят. Класическата теория казва, че в пълния смисъл това не може да стане с едно съобщение, без доверена настройка и със съвършена коректност. Статията на Рахул Иланго не премахва тази невъзможност. Тя променя целта: вместо да изисква симулатор наистина да съществува, пита дали избрана доказателствена система може ефективно да докаже, че симулаторът не съществува. При големи допускания от сложността на доказателствата и криптографията това е достатъчно, за да се възстановят фалсифицируеми, основани на игри последствия на нулевото знание, свойство по свойство. Това не е готов за включване интернет примитив. То е доказателствено-теоретичен начин математическата недоказуемост да се превърне в криптографско прикритие.

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

Номерът не е да докажеш, че тайната е скрита

Да започнем с най-простата версия на доказателството с нулево знание.

Алис иска да убеди Боб, че една задача судоку има решение. Ако му изпрати решението, Боб ще бъде убеден, но загадката ще бъде развалена. Това, което тя иска, е по-странно: доказателство, че решение съществува, без самото решение да бъде разкрито.

Това е обещанието на доказателството с нулево знание. Доказващият (Алис) убеждава проверяващия (Боб), че дадено твърдение е вярно, без да разкрива нищо отвъд самия факт, че твърдението е вярно.

Проблемът е, че това обещание има цена. Обикновеното математическо доказателство има две удобни свойства. То е **едно съобщение**: записваш го, предаваш го и си тръгваш. И има **съвършена коректност**: за невярно твърдение изобщо не съществува валидно доказателство. Класическите резултати за невъзможност казват, че нулевото знание трябва да се откаже и от двете свойства — и не само от комбинацията им; всяко от тях поотделно също е недостижимо.

Първо, доказателството с нулево знание се нуждае от разговор. Ако Алис изпрати само едно съобщение, без предварително уговорена доверена настройка, гаранцията за нулево знание се срива — и това важи независимо колко от коректността сте готови да пожертвате в замяна.

Второ, доказателството с нулево знание се нуждае от малък толеранс към грешка. Изискването за съвършена коректност се оказва, че тихомълком унищожава и интерактивността: проверяващ, който никога не може да бъде измамен, независимо какви случайни избори прави, би могъл просто да фиксира тези избори предварително — а щом проверяващият стане предвидим, Алис може да отговори на всичко с едно съобщение, което е точно случаят, който вече се провали.

Статията на Рахул Иланго е за начин да се заобиколи тази двойна стена. Не като се преструваме, че стената я няма, и не като се произведе класическо нулево знание в среда, в която това е невъзможно. Ходът е по-фин: да се отслаби смисълът на „не разкрива нищо“, но по начин, който запазва свойствата за сигурност, които криптографите реално могат да проверяват.

Резултатът се нарича **ефективно нулево знание**.

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.

Нулевото знание е блокирано на три врати — интерактивност, доверена настройка и несъвършена коректност. Конструкцията на Иланго минава през друга: правилникът не може ефективно да опровергае симулатора.

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.

Класическото нулево знание пита дали съществува симулатор; „ефективното нулево знание“ пита само

дали избраният от вас правилник може ефективно да докаже, че такъв не може да съществува. Именно този по-слаб въпрос позволява на конструкцията да запази едно съобщение, липса на настройка и съвършена коректност.

Original diagram — The Clean Paper CC BY 4.0

Старият тест: съществува симулатор

Класическият начин да се формализира нулевото знание използва измислен помощник, наречен **симулатор**.

Идеята е следната: представете си Джейн, която **не** знае тайната на Алис. Ако Джейн може напълно самостоятелно да генерира доказателства, които изглеждат точно като тези, които Боб би получил от Алис, тогава доказателствата на Алис не са научили Боб на нищо ново. Джейн вече е можела да имитира преживяването без тайната на Алис.

Затова класическото нулево знание изисква реален симулатор. Трябва да съществува ефективен алгоритъм, който може да създава привидно истински доказателства, без да знае тайната — **свидетеля**, както се казва на жаргон; при судоку свидетелят е просто попълнената решетка.

Тази дефиниция е мощна, но точно тук хапе старият резултат за невъзможност. Интуицията е следната. Истински неинтерактивното доказателство е просто низ от символи. След като Боб го има, може да го покаже на друг човек: той вече е придобил способност да доказва твърдението пред други, което само по себе си звучи като повече от „нищо“. Класическите теореми превръщат тази интуиция в точните невъзможности, описани по-горе.

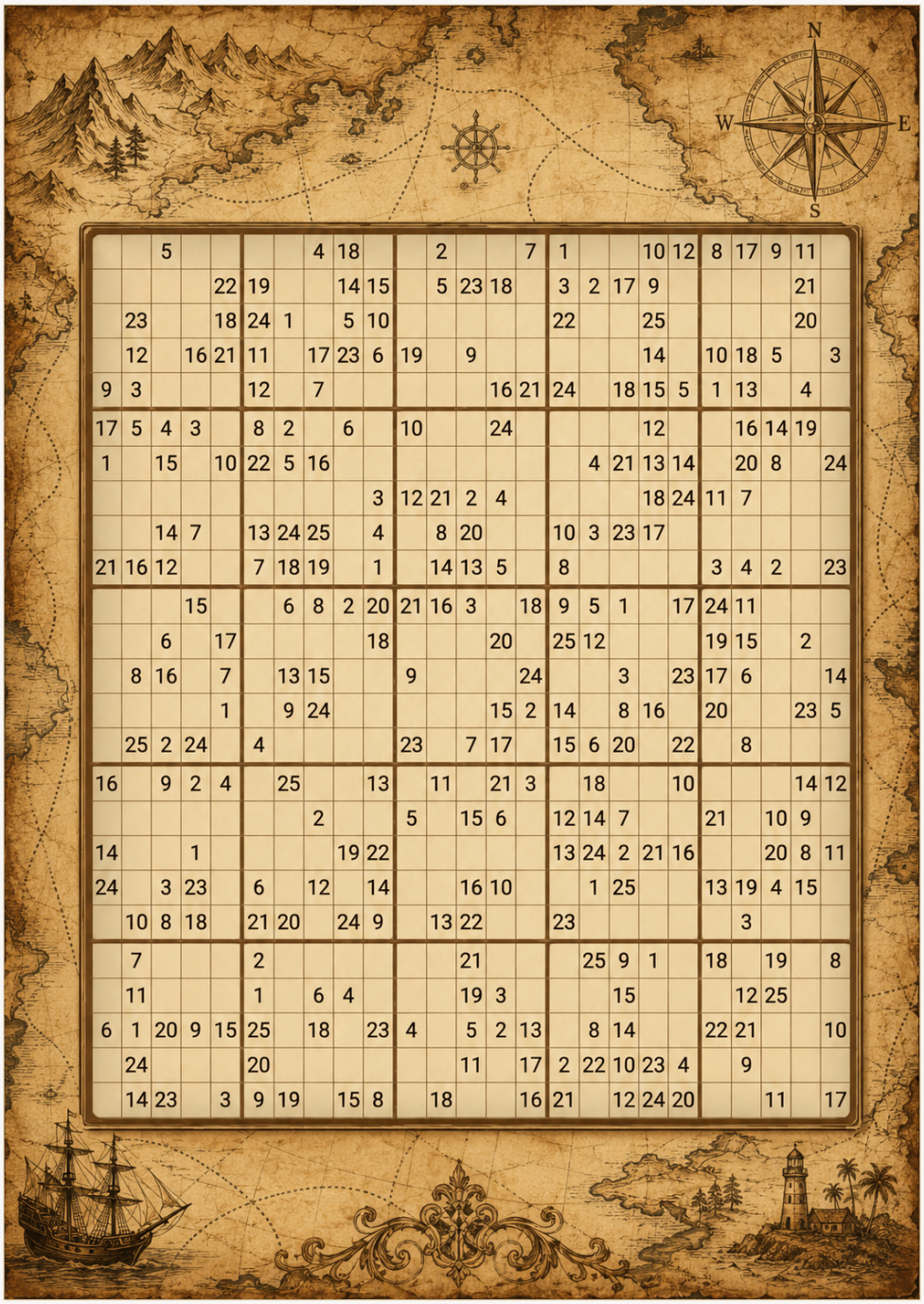
Трите свойства, на които тази статия държи

Заглавието на научната статия посочва три ограничения:
Без интерактивност: Алис изпраща един низ-доказателство. Няма протокол с размяна на съобщения напред-назад.
Без настройка: Алис и Боб не разчитат на доверен общ референтен низ или друга предварително уговорена публична случайност. Много системи, наричани „неинтерактивно нулево знание“, все пак разчитат на настройка; тук се има предвид нулева настройка.
Съвършена коректност: невярно твърдение няма валидно доказателство. Не „почти никога не се приема“; валидно доказателство изобщо не съществува.
Тези три свойства са точно това, което има обикновената писмена математика — и, както беше обяснено по-горе, класическото нулево знание не може да ги запази.

Разликата чрез мега-судоку

Ето един нарочно опростен начин да се усети разликата.

За сериозната част от аналогията не използвайте обикновено судоку 9 на 9. То е твърде малко и твърде крайно: компютърът може просто да го реши или да докаже, че няма решение. Вместо това си представете семейство задачи **MegaSudoku(n)**. Уголемете обичайното правило: изберете размер на блока n, нека $N = n^2$, и построете решетка N на N, разделена на блокове n на n, с N символа. Обикновеното судоку е само малкият случай $n = 3$, $N = 9$: решетка 9 на 9, блокове 3 на 3 и девет символа. Историята за сложността на доказателствата започва едва когато n може да расте и когато решетката може да съдържа допълнителни конструкции, които я карат да се държи като SAT формула, преоблечена като судоку. SAT формулата е просто списък от ограничения с отговор да/не: можете ли да присвоите стойности истина/лъжа на променливите така, че всяко ограничение да бъде удовлетворено?



Судоку 25 на 25: правилата му могат да бъдат проверени, без да се разкрива завършената решетка — визуален заместител на доказателство, което проверява скрито решение, свидетеля.

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

Судоку и SAT: една и съща задача в два костюма

Твърдението, че едно судоку може „да се държи като SAT формула“, не е метафора. Преводът работи и в двете посоки, а лесната посока може да бъде изписана изцяло.

От судоку към SAT. SAT говори само на езика истина/лъжа, затова му дайте по

една булева променлива за всяка тройка (ред, колона, стойност): *x(r,c,v)* означава „клетката на ред *r*, колона *c* съдържа стойността *v*“. Судоку 4 на 4 (блокове 2 на 2, стойности 1–4) се нуждае от 4·4·4 = 64 променливи; класическото 9 на 9 — от 729. След това всяко правило на судоку се превръща в група клаузи. (Клауза е OR на променливи или техните отрицания; цялата формула е AND на всички клаузи.)
Всяка клетка съдържа поне една стойност — по една клауза за клетка:

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

Всяка клетка съдържа най-много една стойност — клауза „не и двете“ за всяка двойка стойности:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … и така нататък за всичките шест двойки.

Всеки ред съдържа всяка стойност — за ред 1 и стойност 3: поне веднъж,

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

и най-много веднъж: ¬x(1,1,3) ∨ ¬x(1,2,3), и така нататък за всяка двойка клетки в реда.
Колони и блокове — същите групи; променя се само групата клетки. За горния ляв блок и стойност 2:

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

плюс двойковите клаузи „не и двете“.
Отпечатаните подсказки — най-простата част: всяка подсказка е клауза само с една променлива. Отпечатана 3 в горния ляв ъгъл става клаузата

x(1,1,3)

AND на всичко това е удовлетворима точно когато судокуто има решение — а едно удовлетворяващо присвояване *е* решението: прочетете кои x(r,c,v) са истина и попълнете решетката. За судоку 9 на 9 това означава 729 променливи и няколко хиляди клаузи, с които съвременен SAT решавач се справя за милисекунди. Забележете клаузата за подсказката x(1,1,3): тя казва „тази клетка е точно 3“, а не „тези клетки са различни една от друга“ — същата асиметрия, която ще наложи допълнителния трик за клетките с подсказки в бележката за протокола по-долу.
От SAT към судоку. На статията ѝ е нужна обратната, по-трудна посока: при *произволна* SAT формула да се построи мега-судоку, което има решение точно когато формулата има. Естествените правила на судоку могат да казват само „тези клетки са различни една от друга“, затова произволни логически ограничения трябва да бъдат *конструирани* — и точно това са гаджетите. Гаджетът е малък, предварително изграден клъстер от клетки, по един за всяка клауза на формулата, в който определени клетки играят ролята на променливи (символът в тях кодира истина или лъжа), а вътрешните ограничения на

клъстера са проектирани така, че единствените му допустими попълвания да съответстват на присвоявания, удовлетворяващи тази клауза. Това е стандартен занаят от доказателствата за NP-пълнота; за обобщеното судоку е направено от Ято и Сета през 2003 г.
Заедно двете посоки казват, че судоку N на N и SAT са един и същ проблем в различни костюми. Именно това позволява на този текст — и на научната статия — да разказва история за целия клас NP чрез решетки и символи.

Свидетелят все още е лесен за представяне. Алис знае пълно валидно попълване на мега-судокуто. Боб иска да бъде убеден, че такова попълване съществува, но Алис не иска да го разкрива. Ако тя изпрати цялото попълване, Боб е убеден, но тайната е изгубена.

В класическата версия с нулево знание Алис и Боб взаимодействат. Един старомоден мисловен модел използва покрити плочки. Алис скрива решената решетка, тайно преименува символите преди всеки рунд и позволява на Боб да провери едно случайно избрано локално ограничение: ред, колона, блок или гаджет. Ако откритите клетки съдържат различни символи, Боб придобива увереност. После всичко отново се покрива и символите се преименуват наново. (Има една подробност: дадените подсказки в задачата изискват допълнителен трик, защото преименуването скрива и тях. Бележката по-долу обяснява как класическите протоколи решават това; опростената картина е достатъчна за следващото.)

Как класическите протоколи всъщност обработват клетките с подсказки

Трикът с преименуването има сляпо петно. Правилата за редове, колони и блокове казват „тези клетки са различни една от друга“, а свойството *всички са различни* оцелява при всяко преименуване на символите. Но една подсказка казва „тази клетка съдържа точно 5“, а след преименуването Боб вижда само $\sigma(5)$ — някакъв маскиран символ — без да знае самото преименуване σ. Той не може да провери нищо. Ако това не се поправи, Алис би могла да докаже, че *някаква* валидна решетка съществува, като напълно пренебрегне отпечатаните подсказки, което не доказва нищо за *тази* конкретна задача. В класическата литература има две стандартни поправки.
Палитрата. Добавете към скритата решетка още един ред от N клетки — палитра, която Алис запълва със символите 1…N във фиксиран публичен ред и после преименува заедно с всичко останало, така че тя съдържа $\sigma(1)\ldots\sigma(N)$. Случайното предизвикателство на Боб вече има още една възможност. Освен да избере ред, колона, блок или гаджет за отваряне, той може да избере **палитрата плюс една клетка с подсказка**. Алис разкрива и двете; палитрата показва преименуването за този рунд, а Боб проверява дали клетката с подсказката показва точно преименуваната версия на отпечатаната стойност. Това остава с нулево знание, защото Боб научава само σ — което се избира наново на всеки рунд и само по себе си не струва нищо — и стойността на клетка, която той вече е знаел от

задачата. Нищо за тайните клетки не изтича, а симулатор може да имитира гледката, като избере случайно σ. Протоколът е коректен, защото измамна Алис бива хваната с фиксирана вероятност във всеки рунд, а рундовете се повтарят, докато съмнението стане пренебрежимо.

Компилиране на подсказките. По-структурен вариант премахва специалното предизвикателство, вместо да го добавя. Вместо да *проверяваме* стойността на подсказката, я налагаме чрез ограничения за различност: свързваме клетката с подсказката с всяка клетка от палитрата освен тази, която носи собствената ѝ стойност — „различна от $\sigma(1)$, различна от $\sigma(2)$, …, различна от всичко освен $\sigma(5)$“. Единственият символ, който клетката може законно да съдържа, е стойността от подсказката. Така всяко ограничение отново е от вида „тези две са различни“ — инвариантно спрямо преименуването и проверимо точно като ред. Това е същият ход, използван за предварително оцветени върхове в класическия протокол за оцветяване на граф, и е в духа на думата *гаджети* по-горе: в картината MegaSudoku-като-SAT подсказките се компилират в гаджети за неравенство като всяко друго ограничение.

Физическият протокол. Реалният протокол с карти за судоку (Gradwohl, Naor, Pinkas и Rothblum, 2007) изобщо не използва преименуване и урежда подсказките още преди скриването да започне. За всяка клетка Алис поставя три еднакви карти със стойността на клетката — с лице надолу за тайните клетки, но **с лице нагоре за клетките с подсказки**, така че Боб със собствените си очи вижда, че подсказките са спазени, преди картите да бъдат обърнати. След това по една карта от всяка клетка отива в пакета на нейния ред, една — в пакета на колоната, една — в пакета на блока; всеки пакет се разбърква и разкрива, а Боб проверява, че съдържа всичките N символа. Разбъркването унищожава информацията за позицията (това е нулевото знание), но подсказките вече са били фиксирани при раздаването.

И в двата случая урокът е един и същ, към който този текст постоянно се връща: протоколът с нулево знание внимателно проследява *кои* факти се запазват след скриването. Преименуването запазва „всички са различни“ и изтрива „равно е на 5“ — затова „равно е на 5“ трябва да бъде вкарано обратно по друг начин.

Това не е протоколът в научната статия. Това е мисловният модел за класическо нулево знание:

- Алис и Боб си разменят съобщения.
- Боб избира случайни проверки.
- Алис разкрива само локална съгласуваност, не цялото решение.
- Доказателството за поверителност работи, като се показва, че това, което Боб вижда, би могло да бъде генерирано без тайното решение на Алис.

Следователно класическото нулево знание се гради около положителен факт:

> Симулатор наистина съществува.

Сега махнете удобните части. Алис изпраща един низ-доказателство и си тръгва. Няма доверена настройка, няма предварително подготвен общ случаен низ и Боб никога не трябва да приема невярна задача. Това е средата, в която класическото нулево знание не може да оцелее.

Преди трика е нужен още един персонаж. Фиксирайте **правилник**: формална доказателствена система в смисъла на математическата логика — фиксиран набор от аксиоми плюс механични правила за проверка на написани математически доказателства. ZFC, стандартните аксиоми на математиката, е каноничният пример. Всичко оттук нататък се формулира спрямо правилник, избран предварително, като изборът е гъвкав: конструкцията работи за всеки фиксиран правилник, включително ZFC.

(Бележка за термините, заета от самата статия: „proof system“ тук винаги означава този правилник — формалната система, която проверява математически доказателства — и никога съобщенията, които Алис изпраща. Механизмите на Алис и Боб се наричат „доказващ“ и „проверяващ“.)

Версията в духа на Гьодел запазва историята с мега-судоку, но променя доказателството.

Изберете втора система от ограничения със същия показан размер и я наречете **D**. В разказа S и D са две задачи MegaSudoku(n) в един и същ формат. Зад кулисите D може да е започнала като трудна логическа формула с друг размер; ако е необходимо, тя може да бъде допълнена с безвредни фиктивни ограничения, за да пасне на същата решетка. D е построена от логическа формула, която всъщност е **неудовлетворима**: няма възможно присвояване на стойности, което да направи всичките ѝ ограничения верни, точно както счупена задача няма допустима завършена решетка. Играчка-пример би била формула, която изисква едновременно „X е истина“ и „X е лъжа“. Следователно D няма валидно попълване.

Но D не трябва да е счупена задача, която е *лесно да бъде разобличена*. Играчка-примерът по-горе не става: всеки правилник опровергава „X и не-X“ с един ред. D трябва да е невярна по начин, който избраният правилник не може да удостовери с кратък аргумент. Ако правилникът можеше да опровергае D с кратко доказателство, историята по-долу щеше да се срине: алтернативният път, който би могъл да произведе доказателства без тайната на Алис, можеше формално да бъде изключен, а с него и гаранцията за поверителност. Затова D се избира от семейство, което фиксираният правилник не може ефективно да опровергава: вътре в този правилник няма кратко доказателство, че D няма решение.

Едносъобщителното доказателство на Алис тогава е за твърдение от типа „или/или“:

или реалното мега-судоку S има решение, или примамката D има решение.

Това е логическата връзка. D **не** се генерира по някакъв магически начин, който прави S вярно. Доказателството не твърди „D няма решение, следователно S има решение“. То доказва дизюнкцията **S или D**. Съвършената коректност казва, че за невярна дизюнкция не може да има валидно доказателство. Тъй като D е невярна в

действителност — няма решение — единственият начин дизюнкцията да е вярна е S да е вярно. Следователно, ако доказателството е прието, S трябва да има решение. Примамката не може да превърне невярно S във вярно.

Но за частта, подобна на нулево знание, попитайте какво би станало, ако D *имаше* решение. Това решение на примамката би действало като алтернативен свидетел. То би позволило на някого да произвежда доказателства, без да знае реалното решение на мега-судокуто на Алис — с други думи, би дало симулатор. В действителност D няма решение, така че този път към симулатор е затворен. Същественото е, че правилникът не може ефективно да докаже, че е затворен.

Затова D има две задачи. За **коректността** D е невярна, така че валидно доказателство за „S или D“ налага S. За **ефективното нулево знание** D е трудна за опровергаване, така че правилникът не може бързо да изключи примамния път, който би направил симулацията възможна.

Следователно тестът за сигурност вече не е:

> Можем ли да докажем, че симулатор наистина съществува?

Той става:

> Може ли вашият правилник ефективно да докаже, че симулаторът е невъзможен?

Ако отговорът е „не“, следва нещо изненадващо силно: всяка гаранция за сигурност, която (а) може да бъде наблюдавана чрез изпълнение на тест и (б) доказуемо следва — вътре в този правилник — от съществуването на симулатор, действително е изпълнена. Успешна атака срещу която и да е от тях сама по себе си би дала липсващото кратко опровержение, а такова кратко опровержение не съществува. Това е „ефективното“ в ефективно нулево знание.

Така контрастът в учебна форма е:

Класическо нулево знание: доказателствата са безопасни, защото съществува симулатор.

Ефективно нулево знание в духа на Гьодел: доказателствата се третират като безопасни за наблюдаеми тестове за сигурност, защото правилникът не може ефективно да докаже, че симулаторът е невъзможен.

Второто твърдение е по-слабо. Именно затова статията може да запази трите свойства, които счупиха класическата версия: едно съобщение, без настройка и съвършена коректност.

Новият тест: не можете да докажете, че симулаторът отсъства

Отслабената дефиниция на Иланго променя въпроса.

Класическото нулево знание пита:

> Съществува ли симулатор?

Ефективното нулево знание пита нещо по-слабо:

> Може ли избраният от вас правилник ефективно да докаже, че не съществува симулатор?

Това звучи като техническо заобикаляне, но е сърцевината на идеята. Конструкцията живее в странно състояние: симулатор в действителност не съществува — статията го казва изрично — но фиксираният от вас правилник не може ефективно да докаже, че той не съществува. Ако всяко лошо последствие, което ви интересува, би изисквало такова опровержение, системата все пак се държи като нулево знание по отношение на тези последствия.

Тук влиза Гьодел. Не като украса и не като „Гьодел прави криптографията сигурна“. Връзката е доказателствено-теоретична. Един правилник се нарича **оптимален**, ако в точен смисъл е най-добрият възможен: когато някой правилник може да опровергае формула от съответния вид с кратко доказателство, оптималният също може, с доказателство, което е най-много полиномиално по-дълго. Крайчек и Пудлак предполагат през 1989 г., че **не съществува оптимална доказателствена система**: който и правилник да фиксирате, някакъв друг правилник доказва някое семейство верни твърдения много по-кратко. Това е една от централните отворени хипотези в сложността на доказателствата и е крайният, сложностно-теоретичен родственик на теоремата на Гьодел за непълнота: някои верни твърдения нямат кратко доказателство в правилника, който сте фиксирали — не защото по принцип са недоказуеми, а защото всеки фиксиран правилник оставя някои кратки истини без кратки доказателства.

Статията приема тази хипотеза (в малко по-силна форма „безкрайно често“, стандартна когато хипотези се използват криптографски). Печалбата, благодарение на теорема на Крайчек и Пудлак, е конкретна: за всеки правилник има редица формули, които наистина са неудовлетворими, но които правилникът не може да опровергае с кратки доказателства — и, което е решаващо, един ефективен алгоритъм може да ги *генерира*. Последното свойство, еднообразността, превръща цялата идея от твърдение за съществуване в реален алгоритъм, който Алис може да изпълни: нейните примамки D излизат от поточна линия, а не от нищото.

Криптографският ход е този недостиг на доказателствена сила да бъде впрегнат в работа.

Какво прави конструкцията

Ето конструкцията от статията, сведена до формата си.

Фиксирайте правилник — например ZFC. При хипотезата от сложността на доказателствата съществува ефективно генерируема редица от формули, които в действителност са неудовлетворими, но за които правилникът няма кратко доказателство, че са неудовлетворими.

Сега построете едносъобщително доказателство с форма:

> или реалното твърдение е удовлетворимо, или тази специална трудна формула е удовлетворима.

Специалната трудна формула не е удовлетворима. Затова, ако основният доказателствен механизъм има съвършена коректност, приемането на съобщението все още означава, че реалното твърдение е вярно. Това дава съвършена коректност.

Но за сигурността, подобна на нулево знание, си представете, че специалната трудна формула *беше* удовлетворима. Тогава нейният свидетел би могъл да се използва за симулиране на доказателства, без да се знае реалният свидетел. Формулата в действителност не е удовлетворима — но правилникът не може ефективно да докаже това. Следователно той не може ефективно да докаже, че симулаторът е невъзможен.

Това е шарнирът. Системата не скрива тайната, като създава класически симулатор. Тя скрива тайната, за голям клас наблюдаеми тестове за сигурност, зад неспособността на правилника да удостовери, че симулаторът отсъства.

Какво твърди статията

Основната теорема идва на слоеве. Ядрото на резултата е следното:

При стандартно криптографско допускане — съществуването на **неинтерактивни доказателства с неразличимост на свидетеля**, добре изследвани обекти, които следват от няколко установени пакета допускания — и при хипотезата от сложността на доказателствата, че **не съществува (безкрайно често) оптимална доказателствена система**, статията конструира за всеки избор на правилник едносъобщителен доказващ и проверяващ за NP/SAT със **съвършена коректност** и без настройка, който е ефективно с нулево знание спрямо този правилник. (NP/SAT е стандартният „най-труден общ знаменател“ на задачи от типа на пъзелите; мега-судоку е един от костюмите му.)

За по-широкото твърдение за запазване на фалсифицируеми свойства за сигурност статията добавя още едно стандартно допускане — убеждението за дерандомизация **P**

= **BPP** (грубо казано: случайността не дава на алгоритмите съществена допълнителна сила).

Преведено от езика на теоремите:

- Доказателството е едно съобщение.
- Няма доверена настройка.
- Невярни твърдения не могат да бъдат доказани.
- Доказващият не е класически с нулево знание — той няма симулатор.
- Но всяко фалсифицируемо, основано на игра последствие за сигурността от класическото нулево знание може да бъде постигнато в тази среда.

„Фалсифицируемо“ е важно. Това означава, че пробив в сигурността може да бъде проверен, като се пусне противник в игра. Много криптографски дефиниции за сигурност имат тази форма: може ли противникът да различи две шифротекстове, да обърне функция, да възстанови свидетел или да спечели определен експеримент? Теоремата дава доказващ за всяко фалсифицируемо свойство поотделно. Един-единствен доказващ, който да притежава *всички* фалсифицируеми свойства едновременно, вероятно е невъзможен — старата атака чрез повторно използване („Боб може да покаже доказателството на други“) сама по себе си е фалсифицируемо свойство и тук действително се проваля. Предложението на статията е, че един доказващ вероятно може да покрие всички *естествени* фалсифицируеми свойства — онези, които реално се срещат в криптографската практика — но тази част е условна теорема, опираща се на неформално понятие за „естествено“, плюс изрично формулирана хипотеза. Гаранцията е насочена към наблюдаеми провали, не към всеки философски или симулационно-базиран смисъл на тайната.

Едно конкретно следствие си заслужава да бъде назовано: конструкцията дава първите неинтерактивни доказателства със *скриване на свидетеля* и еднообразен доказващ — „доказателството за една задача не ви помага да намерите нейното решение“, без интерактивност и без настройка — скромно звучащ обект, който десетилетия е устоявал на конструиране.

Какво не означава това

Това е разделът, който държи текста честен.

То **не** означава, че старите теореми за невъзможност са били грешни. Конструкцията ги заобикаля, като променя дефиницията.

То **не** дава обикновено, класическо нулево знание без интерактивност, без настройка и със съвършена коректност. Статията изрично казва, че конструираният доказващ няма симулатор.

То **не** означава, че доказателството не може да се използва повторно. Едносъобщително

доказателство все още може да бъде показано на друг човек; статията не запазва свойства от типа на отричаемостта. (Неинтерактивното нулево знание с доверена настройка има същото ограничение.)

То **не** означава, че това е практически протокол, готов за внедряване. Това е теория на сложността и фундаментална криптография. Резултатът зависи от големи допускания от сложността на доказателствата и криптографията, а конструкцията е за това какво е възможно по принцип.

То **не** превръща „Гьодел“ в магически примитив за сигурност. Връзката с Гьодел минава през доказателствени системи, оптимални доказателствени системи и крайни аналози на непълнотата. Полезната интуиция не е „непълнотата пази паролата ви“. Тя е: ако един правилник не може ефективно да докаже, че симулаторът е невъзможен, тогава атаки, които биха изисквали такова доказателство, могат да бъдат блокирани на нивото на дефинициите за сигурност.

Защо въпреки това е интересно

Криптографията често превръща трудността в безопасност. Факторизацията е трудна, затова допускания от типа на RSA стават полезни. Решетъчните задачи са трудни, затова решетъчната криптография става полезна. Тук трудността е по-странна: не „трудно е да се изчисли тайна“, а „трудно е да се докаже, че определен доказателствен обект не може да съществува“.

Затова статията се усеща необичайна. Тя третира аксиомите и правилниците почти като криптографски ресурси. Обичайният резултат за невъзможност казва, че има напрежение между коректност и симулация. Ходът на Иланго е да постави това напрежение зад доказателствено-теоретична завеса: симулаторът отсъства, но формалната система не може ефективно да разкрие това отсъствие.

За читателя изненадващото не е, че това ще замени днешните системи с нулево знание. Вероятно няма, поне не пряко. Изненадващото е, че ограничение от математическата логика може да се използва конструктивно: не само като стена, а като вид прикритие.

Колко силни са основанията?

Това е статия с теореми, затова „основания“ тук означава нещо различно от статия по биология или астрономия. Въпросът не е дали експеримент е бил възпроизведен. Въпросът е дали дефинициите, допусканията и веригата от доказателства подкрепят твърдението.

Доказателството е формално, а статията изрично посочва допусканията си. Те не са случайни. Неинтерактивните доказателства с неразличимост на свидетеля са

стандартни обекти в криптографията и следват от няколко утвърдени пакета допускания. Хипотезата, че няма оптимална доказателствена система, е централна хипотеза в сложността на доказателствата. P = BPP е стандартно убеждение за дерандомизация, използвано само за по-широката теорема за фалсифицируемите свойства.

Статията също така аргументира, че тези допускания са правилната цена, а не произволно скеле: доказва обратно твърдение, показващо, че по същество са необходими — ако изобщо съществуват конструкции като тази, тогава трябва да съществуват неинтерактивни доказателства с неразличимост на свидетеля и (приемайки стандартни еднопосочни функции) не може да съществува оптимална доказателствена система. А допусканията са „печеливши и в двата случая“: опровергаването на което и да е от тях само по себе си би било знаково откритие в сложността на доказателствата, криптографията или теорията на сложността.

Но понеже резултатът е условен, увереността в него също е условна. Ако тези допускания се окажат неверни, тълкуването на теоремата се променя. И дори ако са верни, гаранцията не е пълно класическо нулево знание; тя е отслабената, доказателствено-теоретична версия на статията.

Затова правилната степен на увереност е висока, че статията установява съгласуван условен резултат за възможност; умерена, че допусканията ѝ описват криптографския свят, в който действително живеем; и ниска за каквито и да било непосредствени практически последствия.

Защо има значение

Статията отваря път, който би трябвало да е затворен.

Класическата теория казва: пълното нулево знание не може да бъде едно съобщение без настройка и не може да има съвършена коректност. Статията на Иланго казва: ако поискаме последствията от нулевото знание, които могат да се проверят в игри за сигурност, и ако позволим дефиницията за сигурност да зависи от това какво един правилник може или не може ефективно да опровергае, тогава голяма част от полезното поведение може да бъде възстановена — с едно съобщение, без настройка и със съвършена коректност.

Това не е дребна промяна в дефиницията. Това е различен начин да се мисли за криптографските гаранции. Вместо да питаме само какво съществува, да попитаме какво вашият правилник може да изключи. Вместо да третираме недоказуемостта като философско неудобство, да я използваме като структура.

Практическият свят може да не се промени утре. Но концептуалната карта се променя. Вече има формален смисъл, в който „никой не може ефективно да докаже, че тайната е изтекла“ може да бъде достатъчно силно, за да възстанови много от защитите, основани на игри, които искахме от „тайната не е изтекла“.

Затова Гьодел принадлежи в заглавието.

Накратко

Доказателствата с нулево знание позволяват на доказващ да убеди проверяващ, че дадено твърдение е вярно, без да разкрива свидетеля. Класическите резултати за невъзможност казват, че нулевото знание не може да бъде свито до едно съобщение без настройка и не може да има съвършена коректност. Статията на Рахул Иланго не опровергава тези невъзможности. Тя дефинира по-слабо понятие, ефективно нулево знание: вместо да изисква симулатор наистина да съществува, тя изисква избрана доказателствена система — формален правилник като ZFC — да не може ефективно да докаже, че симулатор не съществува. При големи допускания от криптографията (неинтерактивни доказателства с неразличимост на свидетеля) и сложността на доказателствата (не съществува оптимална доказателствена система), статията конструира едносъобщителни доказващи за NP/SAT без настройка и със съвършена коректност, които постигат фалсифицируемите, основани на игри последствия на нулевото знание едно свойство по едно. Един-единствен доказващ, покриващ всички „естествени“ такива свойства, е по-нататъшно, отчасти хипотетично разширение — а покриването буквално на всяко фалсифицируемо свойство вероятно е невъзможно, защото доказателствата остават многократно използваеми. Резултатът е теоретичен и условен, не внедрен примитив, но показва нов начин доказателствено-теоретичната недоказуемост да се използва като криптографски ресурс.

Проверка без украса

Какво показва статията: При заявените допускания могат да бъдат построени едносъобщителни, без настройка и със съвършена коректност доказващи за NP/SAT, които са ефективно с нулево знание спрямо всяка избрана доказателствена система и постигат всяко фалсифицируемо, основано на игра последствие на класическото нулево знание.

Какво е правдоподобно, но не е доказано безусловно: Че необходимите допускания от сложността на доказателствата и криптографията са верни. Те са сериозни, добре изследвани допускания — а статията показва, че по същество са както необходими, така и достатъчни — но все пак са допускания.

Какво не показва: Класическо нулево знание без интерактивност, без настройка и със съвършена коректност; практическа система, готова за внедряване; отричаемост или невъзможност за повторно използване на доказателствата; нито че теоремата на Гьодел за непълнота сама по себе си защитава криптографията.

Основни ограничения: Гаранцията е отслабване на нулевото знание; най-широката

версия зависи от множество допускания; твърденията за един универсален доказващ остават отчасти хипотетични; и резултатът е преди всичко фундаментален.

Колко уверен трябва да бъде един общ читател? Висока увереност, че това е важен условен теоретичен резултат, ако дефинициите бъдат приети. Умерена, че допусканията отразяват реалността. Ниска за незабавно практическо внедряване. Безопасният извод е: статията не разбива невъзможностите на нулевото знание; тя намира нов доказателствено-теоретичен начин да заобиколи онези части от тях, които имат значение за много игри за сигурност.

Източници

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