The Clean Paper

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

Kriptografski dokaz lahko skrije svojo skrivnost tako, da je odsotnost simulatorja težko dokazati

Dokazi brez razkritja omogočajo, da nekdo dokaže trditev, ne da bi razkril pričo. Klasična teorija pravi, da tega v polnem pomenu ni mogoče doseči z enim samim sporočilom, brez zaupanja vredne priprave in ob popolni zanesljivosti. Članek Rahula Ilanga te nemogočnosti ne odpravlja. Spremeni cilj: namesto zahteve, da simulator res obstaja, zahteva, da izbrani formalni dokazovalni sistem ne more učinkovito dokazati, da simulator ne obstaja. Ob pomembnih predpostavkah iz teorije dokazov in kriptografije to zadošča, da se lastnost za lastnostjo povrnejo preverljive, na igrah temelječe posledice znanja brez razkritja. Ne gre za kriptografski gradnik, ki bi ga lahko jutri vključili v internetni protokol. Gre za dokaznoteoretičen način, kako matematično nedokazljivost spremeniti v kriptografsko kritje.

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

Trik ni v tem, da dokažemo, da je skrivnost skrita

Začnimo z najpreprostejšo različico dokaza brez razkritja.

Alice želi Boba prepričati, da ima sudoku rešitev. Če mu rešitev pošlje, bo Bob prepričan, vendar je uganka s tem pokvarjena. Alice želi nekaj bolj nenavadnega: dokaz, da rešitev obstaja, ne da bi jo razkrila.

To je obljuba dokaza brez razkritja (*zero-knowledge proof*). Dokazovalec (Alice) prepriča preverjevalca (Boba), da je neka trditev resnična, pri tem pa ne razkrije ničesar razen same resničnosti trditve.

Težava je, da ta obljuba nekaj stane. Običajen matematični dokaz ima dve prijetni lastnosti. Je **eno samo sporočilo**: zapišete ga, ga izročite in odidete. In je **popolnoma zanesljiv**: za napačno trditev veljaven dokaz sploh ne obstaja. Klasični izreki o nemogočnosti pravijo, da se mora znanje brez razkritja odpovedati obema lastnostma — in ne le njuni kombinaciji; vsaka zase je že nedosegljiva.

Prvič, dokaz brez razkritja potrebuje pogovor. Če Alice pošlje eno samo sporočilo in pred tem ni bilo zaupanja vredne priprave, jamstvo o ničelnem razkritju razpade — ne glede na to, koliko zanesljivosti ste pripravljeni žrtvovati v zameno.

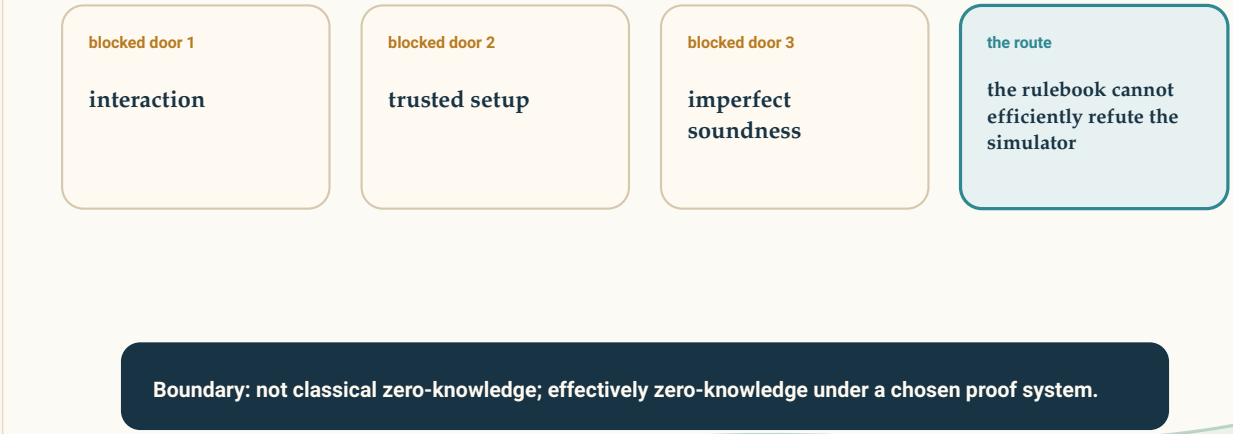
Drugič, dokaz brez razkritja potrebuje majhno toleranco do napake. Zahteva po popolni zanesljivosti neopazno uniči tudi interakcijo: preverjevalec, ki ga ni mogoče preslepiti ne glede na njegove naključne izbire, bi lahko te izbire določil že vnaprej. Ko je preverjevalec predvidljiv, lahko Alice na vse odgovori v enem samem sporočilu — in prav ta primer je že odpovedal.

Članek Rahula Ilanga govori o poti okoli tega dvojnega zidu. Ne tako, da bi se pretvarjal, da zid ne obstaja, in ne tako, da bi v nemogočem okolju izdelal klasično znanje brez razkritja. Poteza je bolj subtilna: oslabiti pomen izraza »ničesar ne razkrije«, vendar tako, da ostanejo ohranjene varnostne lastnosti, ki jih kriptografi dejansko lahko preizkusijo.

Rezultat se imenuje **učinkovito znanje brez razkritja** (*effectively zero-knowledge*).

A proof without leaking the witness

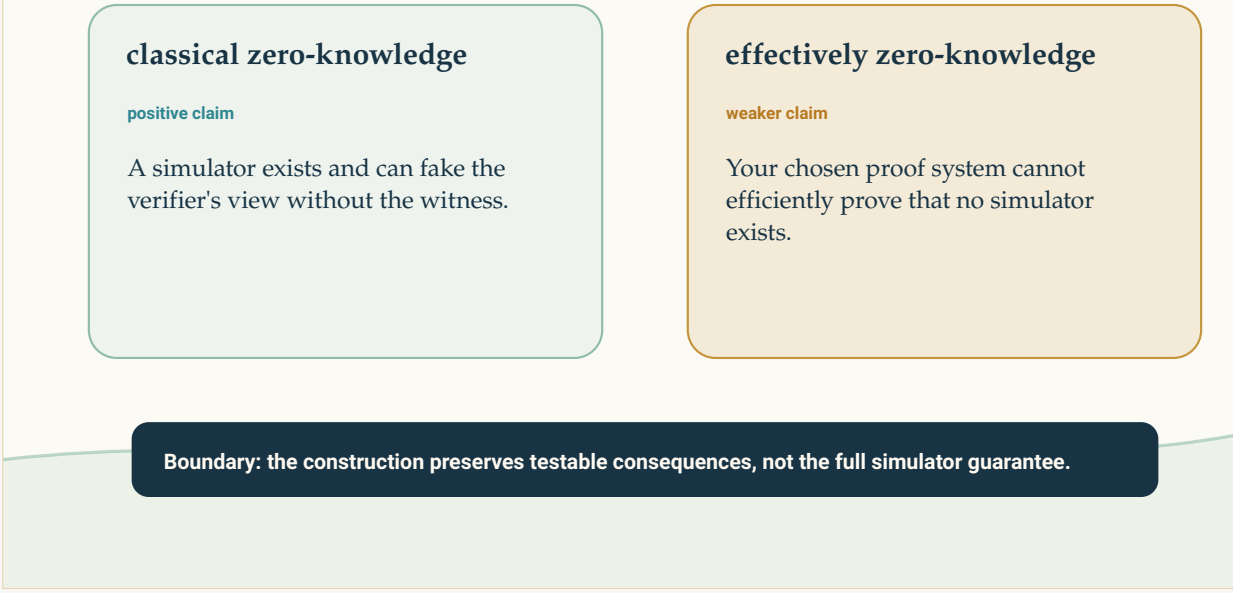
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Znanje brez razkritja je ustavljeno pri treh vratih — interakciji, zaupanja vredni pripravi in nepopolni zanesljivosti. Ilangova konstrukcija gre skozi druga vrata: formalni pravilnik ne more učinkovito ovreči simulatorja.

Classical privacy vs effective privacy

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



Klasično znanje brez razkritja sprašuje, ali simulator obstaja; »učinkovito znanje brez razkritja« sprašuje le, ali lahko izbrani formalni pravilnik učinkovito dokaže, da simulator ne more obstajati. Šibkejše vprašanje je tisto, ki

konstrukciji omogoči eno sporočilo, nič priprave in popolno zanesljivost.

Stari preizkus: simulator obstaja

Klasična formalizacija znanja brez razkritja uporablja izmišljenega pomočnika, imenovanega **simulator**.

Zamisel je naslednja: predstavljajte si Jane, ki **ne** pozna Alicine skrivnosti. Če lahko Jane povsem sama ustvari dokaze, ki so videti prav tako kot dokazi, ki bi jih Bob prejel od Alice, potem Alicini dokazi Boba niso naučili ničesar novega. Jane bi lahko isto izkušnjo ponaredila že brez Alicine skrivnosti.

Klasično znanje brez razkritja zato zahteva dejanski simulator. Obstajati mora učinkovit algoritem, ki lahko brez poznavanja skrivnosti ustvari verodostojno videti lažne dokaze — v žargonu brez **priče** (*witness*); pri sudokuju je priča preprosto izpolnjena mreža.

Ta definicija je močna, vendar je prav tu stara nemogočnost najbolj boleča. Intuicija je naslednja. Resnično neinteraktiven dokaz je samo niz znakov. Ko Bob ta niz prejme, ga lahko pokaže nekomu drugemu: pridobil je zmožnost, da trditev dokazuje drugim, kar že zveni kot nekaj več kot »nič«. Klasični izreki to intuicijo izostrijo v zgornji nemogočnosti.

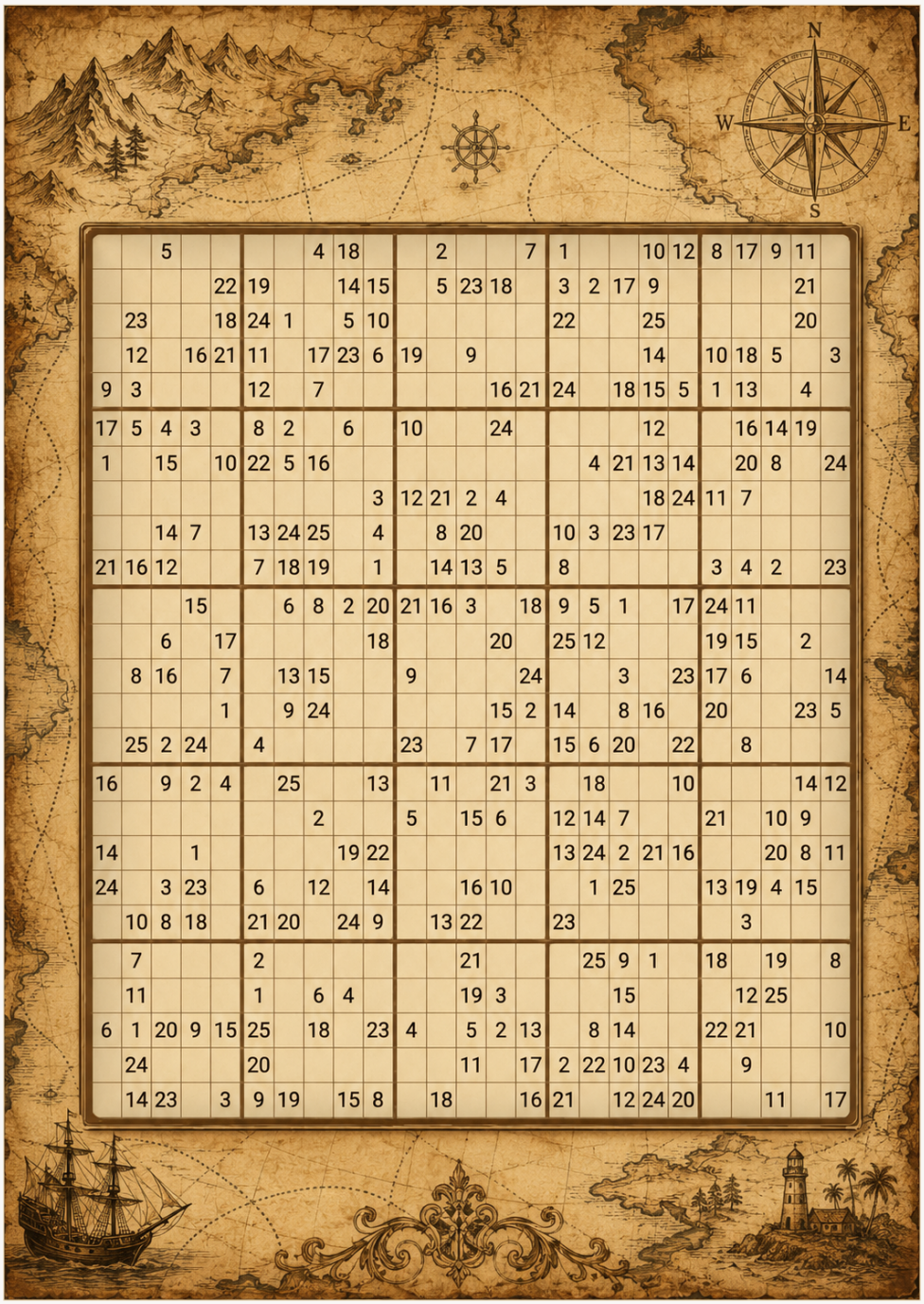
> **Tri lastnosti, pri katerih članek vztraja**
>
> Naslov članka navaja tri omejitve:
> **Brez interakcije:** Alice pošlje en dokazni niz. Ni protokola z izmenjavo sporočil.
> **Brez priprave:** Alice in Bob se ne zanašata na zaupanja vreden skupni referenčni niz ali drugo vnaprej dogovorjeno javno naključnost. Mnogi sistemi, imenovani »neinteraktivno znanje brez razkritja«, se še vedno zanašajo na pripravo; ta članek pomeni resnično nič priprave.
> **Popolna zanesljivost:** napačna trditev nima veljavnega dokaza. Ne »skoraj nikoli ni sprejeta«; veljaven dokaz sploh ne obstaja.
> To so natanko tri lastnosti običajne pisne matematike — in kot je pojasnjeno zgoraj, jih klasično znanje brez razkritja ne more ohraniti.

Razlika skozi mega-sudoku

Spodaj je namenoma poenostavljen način, kako začutiti razliko.

Za resni del analogije ne uporabljajmo običajnega sudokua 9×9. Premajhen je in preveč končen: računalnik ga lahko preprosto reši ali dokaže, da rešitve nima. Namesto tega si predstavljajmo družino ugank **MegaSudoku(n)**. Običajno pravilo povečajmo: izberimo velikost bloka n, naj bo $N = n^2$, nato pa zgradimo mrežo $N \times N$, razdeljeno na bloke $n \times n$, z N simboli. Običajni sudoku je le majhen primer $n = 3$, $N = 9$: mreža 9×9, bloki 3×3 in devet simbolov. Zgodba o kompleksnosti

dokazov se začne šele, ko lahko n raste in ko lahko mreža vsebuje dodatne gradnike, zaradi katerih se obnaša kot formula SAT, preoblečena v sudoku. Formula SAT je zgolj seznam omejitev z odgovorom da/ne: ali lahko spremenljivkam dodelimo vrednosti resnično/napačno tako, da so izpolnjene vse omejitve?



Sudoku 25 × 25: njegova pravila je mogoče preveriti, ne da bi razkrili končno mrežo — vizualna ponazoritev dokaza, ki preveri skrito rešitev, torej pričo.

Sudoku in SAT: ista uganka v dveh preoblekah

Trditev, da se lahko sudoku »obnaša kot formula SAT«, ni prispodoba. Pretvorba deluje v obe smeri, lažjo smer pa lahko zapišemo v celoti.

Iz sudokua v SAT. SAT govori samo resnično/napačno, zato mu dodelimo po eno Boolovo spremenljivko za vsako trojico (vrstica, stolpec, vrednost): *x(r,c,v)* pomeni »celica v vrstici *r* in stolpcu *c* vsebuje vrednost *v*.« Sudoku 4 × 4 (bloki 2 × 2, vrednosti 1–4) potrebuje 4·4·4 = 64 spremenljivk; klasični 9 × 9 jih potrebuje 729. Vsako pravilo sudokua se nato spremeni v skupino klavzul. (Klavzula je ALI spremenljivk oziroma njihovih negacij; celotna formula je IN vseh klavzul.)

Vsaka celica vsebuje vsaj eno vrednost — po ena klavzula za vsako celico:

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

Vsaka celica vsebuje največ eno vrednost — klavzula »ne obe hkrati« za vsak par vrednosti:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \text{... in tako naprej za vseh šest parov.}$$

Vsaka vrstica vsebuje vsako vrednost — za vrstico 1 in vrednost 3: vsaj enkrat,

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

in največ enkrat: $\neg x(1,1,3) \vee \neg x(1,2,3)$, nato enako za vsak par celic v vrstici.

Stolpci in bloki — enake skupine; spremeni se le skupina celic. Za zgornji levi blok in vrednost 2:

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

poleg tega pa še parne klavzule »ne obe hkrati«.

Natisnjene začetne številke — najpreprostejši del: vsaka začetna številka je klavzula z eno samo spremenljivko. Natisnjena 3 v zgornjem levem kotu postane klavzula

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

IN vsega naštetega je izpolnljiv natanko takrat, ko ima sudoku rešitev — in izpolnjujoča prireditev *je* rešitev: preberemo, kateri x(r,c,v) so resnični, in izpolnimo mrežo. Za sudoku 9 × 9 dobimo 729 spremenljivk in nekaj tisoč klavzul, kar sodoben reševalnik SAT opravi v milisekundah. Opazimo klavzulo začetnega podatka x(1,1,3): pravi »ta celica je natanko 3«, ne pa »te celice so vse različne« — prav ta asimetrija bo zahtevala dodatni trik za začetne celice v spodnji opombi o protokolu.

Iz SAT v sudoku. Članek potrebuje nasprotno, težjo smer: iz *poljubne* formule SAT zgraditi mega-sudoku, ki ima rešitev natanko takrat, ko jo ima formula. Naravna pravila sudokua znajo povedati le »te celice so vse različne«, zato je treba poljubne logične omejitve *zgraditi* — in prav temu služijo gradniki. Gradnik je majhna vnaprej zasnovana skupina celic, po ena za vsako klavzulo formule, v kateri imajo določene celice vlogo spremenljivk (simbol v njih kodira resnično ali napačno), notranje omejitve skupine pa so zasnovane tako, da njena dovoljena izpolnjevanja natančno ustrezajo prireditvam, ki zadovoljijo to klavzulo. To je standardna tehnika dokazov NP-polnosti; za posplošeni sudoku sta jo leta 2003 izvedla Yato in Seta.

> Obe smeri skupaj pomenita, da sta sudoku N × N in SAT isti problem v dveh različnih preoblekah. Prav to dovoljuje temu članku — in izvirnemu članku — da zgodbo o celotnem razredu NP pripoveduje z mrežami in simboli.

Pričo si je še vedno lahko predstavljati. Alice pozna popolno veljavno izpolnitev mega-sudokua. Bob se želi prepričati, da taka izpolnitev obstaja, Alice pa je noče razkriti. Če pošlje celotno izpolnitev, je Bob prepričan, vendar skrivnosti ni več.

V klasični različici znanja brez razkritja Alice in Bob sodelujeta interaktivno. Stari miselni model uporablja prekrite ploščice. Alice skrije rešeno mrežo, pred vsakim krogom na skrivaj preimenuje simbole in Bobu dovoli pregled ene naključno izbrane lokalne omejitve: vrstice, stolpca, bloka ali gradnika. Če odkrite celice pokažejo med seboj različne simbole, Bob pridobi nekaj zaupanja. Nato se vse znova pokrije in simboli se na novo naključno preimenujejo. (Obstaja zaplet: začetne številke uganke potrebujejo dodaten trik, ker jih preimenovanje simbolov prav tako skrije. Spodnja opomba pojasni, kako klasični protokoli rešijo to težavo; za nadaljevanje zadostuje ta poenostavljena slika.)

> **Kako klasični protokoli v resnici obravnavajo začetne celice**
>
> Trik s preimenovanjem ima slepo pego. Pravila za vrstice, stolpce in bloke vsa pravijo »te celice so vse različne«, lastnost *vse različne* pa preživi poljubno preimenovanje simbolov. Začetna številka pa pravi »ta celica vsebuje natanko 5«; po preimenovanju Bob vidi le $\sigma(5)$ — nek zamaskiran simbol — ne da bi poznal preimenovanje σ. Ničesar ne more preveriti. Če tega ne popravimo, bi Alice lahko dokazala, da *neka* veljavna mreža obstaja, pri tem pa povsem prezrla natisnjene začetne številke, kar ne dokazuje ničesar o *tej* uganki. Klasična literatura ima dve standardni rešitvi.
>
> **Paleta.** Skriti mreži dodamo dodatno vrstico z N celicami — paleto, ki jo Alice v javno določenem vrstnem redu napolni s simboli 1…N in nato preimenuje skupaj z vsem drugim, tako da vsebuje $\sigma(1)…\sigma(N)$. Bobov naključni izziv ima zdaj še eno možnost. Poleg vrstice, stolpca, bloka ali gradnika lahko izbere **paleto in eno začetno celico**. Alice odkrije oboje; paleta razkrije preimenovanje v tem krogu, Bob pa preveri, ali začetna celica kaže natanko preimenovano različico natisnjenega podatka. Protokol ostane brez razkritja, ker Bob izve samo σ — ki je za vsak krog sveže naključno izbran in sam zase neuporaben — ter vrednost celice, ki jo je že poznal iz uganke. O skrivnih celicah ne izve ničesar, simulator pa lahko pogled ponaredi tako, da izbere naključen σ. Protokol je zanesljiv, ker je verjetnost, da bo goljufiva Alice razkrita, v vsakem krogu nespremenjena; krogi se ponavljajo, dokler dvom ne postane zanemarljiv.
>
> **Odprava začetnih podatkov z gradniki.** Bolj strukturna različica namesto dodatnega izziva odpravi posebno obravnavo. Namesto da vrednost začetne celice *preveri*, jo prisili z omejitvami neenakosti: začetno celico poveže z vsemi celicami palete razen s tisto, ki nosi njeno vrednost — »različna od $\sigma(1)$, različna od $\sigma(2)$, …, različna od vsega razen $\sigma(5)$.« Edini simbol, ki ga lahko celica zakonito vsebuje, je njen začetni podatek. Vse omejitve so spet oblike »ti dve sta različni« — nespremenljive pri preimenovanju in preverljive enako kot vrstica. To je isti prijem kot pri vnaprej obarvanih vozliščih v klasičnem protokolu za barvanje grafov in ponazarja pomen

besede *gradniki* zgoraj: v sliki MegaSudoku-kot-SAT se začetni podatki prevedujejo v gradnike neenakosti tako kot vse druge omejitve.
Fizični protokol. Resnični protokol s kartami za sudoku (Gradwohl, Naor, Pinkas in Rothblum, 2007) preimenovanja sploh ne uporablja in začetne podatke uredi še pred začetkom skrivanja. Alice za vsako celico položi tri enake karte z vrednostjo celice — za skrivne celice obrnjene navzdol, za **začetne celice pa navzgor**, tako da Bob na lastne oči vidi, da so začetni podatki upoštevani, še preden se karte obrnejo. Nato gre po ena karta iz vsake celice v paket svoje vrstice, ena v paket stolpca in ena v paket bloka; vsak paket se premeša in razkrije, Bob pa preveri, da vsebuje vseh N simbolov. Mešanje uniči informacijo o položaju (to je del brez razkritja), začetni podatki pa so bili potrjeni že ob razdeljevanju kart.
V vseh različicah je nauk isti, h kateremu se članek vedno znova vrača: protokol brez razkritja je natančno knjigovodstvo tega, *katera* dejstva preživijo skrivanje. Preimenovanje ohrani »vse različne« in izbriše »enako 5« — zato je treba »enako 5« vrniti v protokol po drugi poti.

To ni protokol iz članka. Je miselni model za klasično znanje brez razkritja:

- Alice in Bob si izmenjujeta sporočila.
- Bob izbira naključne preizkuse.
- Alice razkrije le lokalno skladnost, ne celotne rešitve.
- Dokaz zasebnosti temelji na tem, da bi bilo mogoče Bobov pogled ustvariti tudi brez Alicine skrivne rešitve.

Klasično znanje brez razkritja torej temelji na pozitivnem dejstvu:

> Simulator res obstaja.

Zdaj odstranimo udobne dele. Alice pošlje en dokazni niz in odide. Ni zaupanja vredne priprave, ni skupnega naključnega niza, pripravljenega vnaprej, in Bob nikoli ne sme sprejeti napačne uganke. To je okolje, v katerem klasično znanje brez razkritja ne more preživeti.

Pred trikom potrebujemo še enega igralca. Določimo **formalni pravilnik**: formalni dokazovalni sistem v logičnem smislu — določen nabor aksiomov in mehanskih pravil za preverjanje zapisanih matematičnih dokazov. ZFC, standardni aksiomi matematike, je kanonični primer. Od tod naprej so vse trditve relativne glede na vnaprej izbran pravilnik, izbira pa je poljubna: konstrukcija deluje za vsak pravilnik, ki ga določimo, tudi za ZFC.

(Opomba o izrazju, povzeta po članku: »proof system« tukaj vedno pomeni ta pravilnik — formalni sistem, ki preverja matematične dokaze — in nikoli sporočil, ki jih pošilja Alice. Mehanizem Alice in Boba se imenuje »dokazovalec in preverjevalec«.)

Gödelovska različica ohrani zgodbo z mega-sudokujem, vendar spremeni dokaz.

Izberimo drugi sistem omejitev enake prikazane velikosti in ga poimenujmo **D**. V zgodbi sta S in D dve uganki MegaSudoku(n) v istem formatu. V ozadju je D lahko nastal kot težka logična formula druge velikosti; po potrebi ga lahko dopolnimo z neškodljivimi navideznimi omejitvami, da se prilega isti

mreži. D je zgrajen iz logične formule, ki je v resnici **neizpolnljiva**: ni mogoče dodeliti vrednosti tako, da bi bile vse njene omejitve resnične, kakor pokvarjena uganka nima nobene dovoljene dokončane mreže. Igračni primer bi bila formula, ki hkrati zahteva »X je resničen« in »X je neresničen«. D torej nima veljavne izpolnitve.

Toda D ne sme biti pokvarjena uganka, ki jo je *lahko razkrinkati*. Zgornji igračni primer ne ustreza: vsak formalni pravilnik v eni vrstici ovrže »X in ne-X«. D mora biti napačen tako, da izbrani pravilnik tega ne more potrditi s kratkim argumentom. Če bi pravilnik lahko D ovrgel s kratkim dokazom, bi se spodnja zgodba sesula: alternativno pot, po kateri bi bilo mogoče ustvarjati dokaze brez Alicine skrivnosti, bi bilo mogoče formalno izključiti, s tem pa tudi jamstvo zasebnosti. D je zato izbran iz družine, ki je določeni pravilnik ne more učinkovito ovreči: znotraj tega pravilnika ni kratkega dokaza, da D nima rešitve.

Alicin dokaz z enim samim sporočilom se nato nanaša na disjunkcijo:

> bodisi ima pravi mega-sudoku S rešitev bodisi ima rešitev vaba D.

To je logična povezava. D **ni** ustvarjen na nek čaroben način, ki bi naredil S resničen. Dokaz ne trdi »D nima rešitve, zato ima S rešitev«. Dokazuje disjunkcijo **S ali D**. Popolna zanesljivost pomeni, da napačna disjunkcija ne more imeti veljavnega dokaza. Ker je D v resnici napačen — nima rešitve — je lahko disjunkcija resnična le, če je resničen S. Če je dokaz sprejet, mora imeti S rešitev. Vaba ne more napačnega S spremeniti v resničnega.

Za del, podoben znanju brez razkritja, pa vprašajmo, kaj bi se zgodilo, *če bi* D imel rešitev. Ta rešitev vabe bi bila alternativna priča. Omogočila bi ustvarjanje dokazov brez poznavanja Alicine prave rešitve mega-sudokua — z drugimi besedami, delovala bi kot simulator. V resnici D nima rešitve, zato je ta pot do simulatorja zaprta. Ključ pa je, da formalni pravilnik ne more učinkovito dokazati, da je zaprta.

D ima torej dve nalogi. Za **zanesljivost** je D napačen, zato veljaven dokaz »S ali D« prisili S. Za **učinkovito znanje brez razkritja** pa je D težko ovreči, zato pravilnik ne more hitro izključiti poti prek vabe, ki bi omogočila simulacijo.

Varnostni preizkus zato ni več:

> Ali lahko dokažemo, da simulator res obstaja?

Temveč:

> Ali lahko vaš formalni pravilnik učinkovito dokaže, da je simulator nemogoč?

Če je odgovor ne, sledi nekaj presenetljivo močnega: vsako varnostno jamstvo, ki ga (a) lahko opazujemo z izvedbo preizkusa in (b) za katerega je znotraj tega pravilnika dokazano, da sledi iz obstoja simulatorja, dejansko velja. Uspešen napad na katero koli takšno jamstvo bi sam pomenil manjkajočo kratko ovržbo — te kratke ovržbe pa ni. To je »učinkoviti« del učinkovitega znanja brez razkritja.

Kontrast v učilnici je torej:

Klasično znanje brez razkritja: dokazi so varni, ker simulator obstaja.

Gödelovsko učinkovito znanje brez razkritja: dokazi se pri opazljivih varnostnih preizkusih obravnavajo kot varni, ker formalni pravilnik ne more učinkovito dokazati, da je simulator nemogoč.

Druga trditev je šibkejša. Prav zato lahko članek ohrani tri lastnosti, ki so zlomile klasično različico: eno sporočilo, nič priprave in popolno zanesljivost.

Novi preizkus: ne morete dokazati, da simulatorja ni

Ilangova sprostitev spremeni vprašanje.

Klasično znanje brez razkritja sprašuje:

> Ali simulator obstaja?

Učinkovito znanje brez razkritja postavlja šibkejše vprašanje:

> Ali lahko vaš izbrani formalni pravilnik učinkovito dokaže, da simulator ne obstaja?

To zveni kot tehničen ovinek, vendar je bistvo ideje. Konstrukcija obstaja v nenavadnem stanju: simulator dejansko ne obstaja — članek to izrecno pove — vendar izbrani pravilnik ne more učinkovito dokazati, da ga ni. Če bi vsaka slaba posledica, ki nas zanima, zahtevala prav takšno ovržbo, se sistem glede teh posledic še vedno obnaša kot znanje brez razkritja.

Tu vstopi Gödel. Ne kot okras in ne v smislu »Gödel naredi kriptografijo varno«. Povezava je dokaznoteoretična. Formalni pravilnik je **optimalen**, če je v natančnem smislu najboljši možni: kadar lahko katerikoli pravilnik neko formulo ustrezne vrste ovrže s kratkim dokazom, jo lahko tudi optimalni pravilnik ovrže z dokazom, ki je največ polinomsko daljši. Krajíček in Pudlák sta leta 1989 domnevala, da **optimalen dokazovalni sistem ne obstaja**: kateri koli pravilnik določimo, bo neki drug pravilnik določeno družino resničnih trditev dokazoval mnogo krajše. To je ena osrednjih odprtih domnev teorije kompleksnosti dokazov in končni, kompleksnostnoteoretični sorodnik Gödlovega izreka o nepopolnosti: nekatere resnične trditve v izbranem pravilniku nimajo kratkega dokaza — ne zato, ker jih načeloma ni mogoče dokazati, temveč zato, ker vsak fiksni pravilnik nekatere kratko zapisane resnice pusti brez kratkih dokazov.

Članek to domnevo predpostavi (v nekoliko močnejši obliki »neskončno pogosto«, ki je standardna pri kriptografski uporabi domnev). Korist je po izreku Krajíčka in Pudláka konkretna: za vsak pravilnik obstaja zaporedje formul, ki so resnično neizpolnljive, vendar jih pravilnik ne more ovreči s kratkimi dokazi — in kar je ključno, učinkovit algoritem jih lahko *ustvari*. Prav ta lastnost, uniformnost, spremeni idejo iz gole trditve o obstoju v dejanski algoritem, ki ga lahko Alice izvede: njene vabe D prihajajo iz proizvodne linije, ne iz nič.

Kriptografska poteza je, da to pomanjkanje dokazovalne moči uporabimo kot prednost.

Kaj konstrukcija počne

Takšna je konstrukcija iz članka, če jo skrčimo na njeno osnovno obliko.

Določimo formalni pravilnik — recimo ZFC. Ob predpostavki iz teorije kompleksnosti dokazov obstaja učinkovito ustvarljivo zaporedje formul, ki so dejansko neizpolnljive, pravilnik pa nima kratkega dokaza njihove neizpolnljivosti.

Nato zgradimo dokaz z enim samim sporočilom naslednje oblike:

> bodisi je prava trditev izpolnljiva bodisi je izpolnljiva ta posebna težka formula.

Posebna težka formula ni izpolnljiva. Če je osnovni dokazovalni mehanizem popolnoma zanesljiv, sprejeto sporočilo zato še vedno pomeni, da je prava trditev resnična. Tako dobimo popolno zanesljivost.

Za varnost, podobno znanju brez razkritja, pa si predstavljajmo, da bi bila posebna težka formula *izpolnljiva*. Njeno pričo bi bilo tedaj mogoče uporabiti za simulacijo dokazov brez poznavanja prave priče. V resnici formula ni izpolnljiva — vendar formalni pravilnik tega ne more učinkovito dokazati. Zato tudi ne more učinkovito dokazati, da je simulator nemogoč.

To je tečaj celotne ideje. Sistem skrivnosti ne skrije tako, da bi izdelal klasični simulator. Za širok razred opazljivih varnostnih preizkusov jo skrije za nezmožnostjo formalnega pravilnika, da potrdi odsotnost simulatorja.

Kaj članek trdi

Glavni izrek ima več plasti. Osrednji rezultat je naslednji:

Ob standardni kriptografski predpostavki — obstoju **neinteraktivnih dokazov z nerazločljivostjo prič** (*non-interactive witness indistinguishable proofs*), dobro raziskanih objektov, ki sledijo iz več uveljavljenih sklopov predpostavk — in ob domnevi iz teorije kompleksnosti dokazov, da **(neskončno pogosto) optimalen dokazovalni sistem ne obstaja**, članek za vsak izbrani formalni pravilnik zgradi dokazovalca in preverjevalca z enim sporočilom za NP/SAT, brez priprave in s **popolno zanesljivostjo**, ki sta glede na ta pravilnik učinkovito brez razkritja. (NP/SAT je standardni »najtrši skupni imenovalec« ugankam podobnih problemov; mega-sudoku je le ena od njegovih preoblek.)

Za širšo trditev o ohranitvi preverljivih varnostnih lastnosti članek doda še eno standardno predpostavko, derandomizacijsko domnevo **P = BPP** (približno: naključnost algoritmom ne daje bistvene dodatne moči).

Če izrek prevedemo v običajen jezik:

- Dokaz je eno sporočilo.
- Ni zaupanja vredne priprave.

- Napačnih trditev ni mogoče dokazati.
- Dokazovalec ni klasično brez razkritja — nima simulatorja.
- Kljub temu je mogoče v tem okolju doseči vsako preverljivo, na varnostnih igrah temelječo posledico klasičnega znanja brez razkritja.

Beseda »preverljivo« je pomembna. Pomeni, da lahko varnostni neuspeh preizkusimo tako, da nasprotnika zaženemo v igri. Mnogo kriptografskih varnostnih definicij ima to obliko: ali lahko nasprotnik razlikuje med dvema šifratoma, invertira funkcijo, pridobi pričo ali zmaga v natančno določenem poskusu? Izrek poda dokazovalca za vsako takšno preverljivo lastnost posebej. En sam dokazovalec, ki bi imel *vse* preverljive lastnosti hkrati, je verjetno nemogoč — stari napad s ponovno uporabo (»Bob lahko dokaz pokaže drugim«) je tudi sam preverljiva lastnost in tukaj dejansko odpove. Predlog članka je, da bi en sam dokazovalec lahko verjetno pokrival vse *naravne* preverljive lastnosti — tiste, ki se dejansko pojavljajo v kriptografski praksi — vendar je ta del pogojni izrek, ki sloni na neformalnem pojmu »naravno« in dodatni izrecni domnevi. Jamstvo meri na opazljive varnostne zlome, ne na vsak filozofski ali simulacijski pomen tajnosti.

Vredno je izpostaviti eno konkretno posledico: konstrukcija daje prve neinteraktivne dokaze, ki **skrivajo pričo**, z uniformnim dokazovalcem — »dokaz, da ima uganka rešitev, vam ne pomaga najti rešitve«, brez interakcije in brez priprave. To zveni skromno, vendar se je tak objekt konstrukciji izmikal desetletja.

Česa to ne pomeni

Ta del ohranja članek pošten.

Rezultat **ne** pravi, da so bili stari izreki o nemogočnosti napačni. Konstrukcija se jim izogne tako, da spremeni definicijo.

Ne daje običajnega, klasičnega znanja brez razkritja brez interakcije, brez priprave in s popolno zanesljivostjo. Članek izrecno pove, da skonstruirani dokazovalec nima simulatorja.

Ne pomeni, da dokaza ni mogoče ponovno uporabiti. Dokaz z enim sporočilom je še vedno mogoče pokazati nekomu drugemu; članek ne ohrani lastnosti, podobnih zanikanju avtorstva oziroma neprenosljivosti. (Enako omejitev ima neinteraktivno znanje brez razkritja z zaupanja vredno pripravo.)

Ne pomeni, da je to praktičen protokol, pripravljen za uporabo. Gre za teorijo kompleksnosti in temelje kriptografije. Rezultat je odvisen od pomembnih predpostavk iz teorije dokazov in kriptografije, konstrukcija pa govori o tem, kaj je načeloma mogoče.

Prav tako **ne** spreminja »Gödla« v čarobni varnostni gradnik. Povezava z Gödlom poteka prek dokazovalnih sistemov, optimalnih dokazovalnih sistemov in končnih analogov nepopolnosti. Uporabna intuicija ni »nepopolnost varuje vaše geslo«. Je naslednja: če formalni pravilnik ne more učinkovito dokazati, da je simulator nemogoč, je mogoče na ravni varnostnih definicij blokirati napade, ki bi tak dokaz zahtevali.

Zakaj je kljub temu zanimivo

Kriptografija pogosto spremeni računsko težavnost v varnost. Faktorizacija je težka, zato postanejo uporabne predpostavke v slogu RSA. Problemi na mrežah so težki, zato postane uporabna mrežna kriptografija. Tukaj je težavnost bolj nenavadna: ne »težko je izračunati skrivnost«, temveč »težko je dokazati, da določen dokazni objekt ne more obstajati«.

Prav zato je članek nenavaden. Aksiome in formalne pravilnike obravnava skoraj kot kriptografske vire. Običajna nemogočnost pravi, da obstaja napetost med zanesljivostjo in simulacijo. Ilangova poteza to napetost postavi za dokaznoteoretično zaveso: simulatorja ni, formalni sistem pa njegove odsotnosti ne more učinkovito razkriti.

Za bralca ni presenetljivo predvsem to, da bi ta pristop nadomestil današnje sisteme znanja brez razkritja. Vsaj neposredno jih verjetno ne bo. Presenetljivo je, da je mogoče omejitev matematične logike uporabiti konstruktivno: ne le kot zid, temveč kot nekakšno kritje.

Kako trdna je utemeljitev?

To je članek z izreki, zato »dokazi« tukaj pomenijo nekaj drugega kot v biologiji ali astronomiji. Ne sprašujemo, ali je bil poskus ponovljen. Sprašujemo, ali definicije, predpostavke in veriga dokazov podpirajo trditev.

Dokaz je formalen, članek pa svoje predpostavke navaja izrecno. Te niso priložnostne. Neinteraktivni dokazi z nerazločljivostjo prič so standardni objekti v kriptografiji in sledijo iz več uveljavljenih sklopov predpostavk. Domneva o neobstoju optimalnega dokazovalnega sistema je osrednja domneva teorije kompleksnosti dokazov. **P = BPP** je standardna derandomizacijska domneva, potrebna samo za širši izrek o preverljivih lastnostih.

Članek poleg tega utemeljuje, da so te predpostavke prava cena in ne poljubno postavljen oder: dokaže obratno smer, po kateri so v bistvenem smislu nujne — če takšne konstrukcije sploh obstajajo, morajo obstajati neinteraktivni dokazi z nerazločljivostjo prič in (ob standardni predpostavki o enosmernih funkcijah) optimalen dokazovalni sistem ne more obstajati. Predpostavke imajo tudi značaj »v vsakem primeru nekaj pridobimo«: ovržba katerekoli od njih bi bila sama po sebi prelomno odkritje v teoriji kompleksnosti dokazov, kriptografiji ali teoriji kompleksnosti.

Ker je rezultat pogojen, je pogojena tudi stopnja zaupanja vanj. Če predpostavke odpovejo, se spremeni pomen izreka. In tudi če držijo, jamstvo ni polno klasično znanje brez razkritja; gre za sproščeno, dokaznoteoretično različico iz članka.

Primerna ocena je zato: veliko zaupanje, da članek vzpostavi koherenten pogojni rezultat o možnosti; zmerno zaupanje, da njegove predpostavke opisujejo kriptografski svet, v katerem dejansko živimo; in malo zaupanja v kakršnekoli neposredne praktične posledice.

Zakaj je pomembno

Članek odpre pot, ki naj bi bila zaprta.

Klasična teorija pravi: polnega znanja brez razkritja brez priprave ni mogoče stisniti v eno sporočilo in ne more biti popolnoma zanesljivo. Ilangov članek pravi: če zahtevamo posledice znanja brez razkritja, ki jih je mogoče preizkusiti v varnostnih igrah, in dovolimo, da je varnostna definicija odvisna od tega, kaj lahko formalni pravilnik učinkovito ovrže oziroma česa ne more, lahko velik del uporabnega vedenja dobimo nazaj — z enim sporočilom, brez priprave in s popolno zanesljivostjo.

To ni majhen popravek definicije. Gre za drugačen način razmišljanja o kriptografskih jamstvih. Namesto da sprašujemo samo, kaj obstaja, vprašamo, kaj lahko vaš formalni pravilnik izključi. Namesto da nedokazljivost obravnavamo kot filozofsko nadlogo, jo uporabimo kot strukturo.

Praktični svet se jutri morda ne bo spremenil. Konceptualni zemljevid pa se je. Zdaj obstaja formalen smisel, v katerem je lahko trditev »nihče ne more učinkovito dokazati, da je skrivnost ušla« dovolj močna, da povrne številne zaščite iz varnostnih iger, ki smo jih želeli od trditve »skrivnost ni ušla«.

Zato Gödel sodi v naslov.

Kratek povzetek

Dokazi brez razkritja omogočajo dokazovalcu, da preverjevalca prepriča o resničnosti trditve, ne da bi razkril pričo. Klasični izreki o nemogočnosti pravijo, da znanja brez razkritja brez priprave ni mogoče stisniti v eno samo sporočilo in da ne more imeti popolne zanesljivosti. Članek Rahula Ilanga teh nemogočnosti ne ovrže. Definira šibkejši pojem, učinkovito znanje brez razkritja: namesto zahteve, da simulator res obstaja, zahteva, da izbrani dokazovalni sistem — formalni pravilnik, kot je ZFC — ne more učinkovito dokazati, da simulator ne obstaja. Ob pomembnih predpostavkah iz kriptografije (neinteraktivni dokazi z nerazločljivostjo prič) in teorije kompleksnosti dokazov (optimalen dokazovalni sistem ne obstaja) članek zgradi dokazovalce z enim sporočilom za NP/SAT, brez priprave in s popolno zanesljivostjo, ki lastnost za lastnostjo dosegajo preverljive, na varnostnih igrah temelječe posledice znanja brez razkritja. En sam dokazovalec, ki bi pokril vse »naravne« takšne lastnosti, je dodatna, deloma domnevna razširitev — pokriti dobesedno vsako preverljivo lastnost pa je verjetno nemogoče, ker dokazi ostanejo ponovno uporabni. Rezultat je teoretičen in pogojen, ne pa že uporaben kriptografski gradnik, vendar pokaže nov način, kako dokaznoteoretično nedokazljivost uporabiti kot kriptografski vir.

Preverjanje brez olepševanja

Kaj članek pokaže: ob navedenih predpostavkah je mogoče zgraditi dokazovalce z enim sporočilom, brez priprave in s popolno zanesljivostjo za NP/SAT, ki so glede na poljubno izbrani dokazovalni sistem učinkovito brez razkritja in dosegajo vsako posamezno preverljivo posledico klasičnega znanja

brez razkritja, definirano z varnostno igro.

Kaj je verjetno, vendar ni brezpogojno dokazano: da potrebne predpostavke iz teorije kompleksnosti dokazov in kriptografije držijo. Gre za resne, dobro raziskane predpostavke — članek pokaže tudi, da so v bistvenem smislu nujne in ne le zadostne — vendar so še vedno predpostavke.

Česa ne pokaže: klasičnega znanja brez razkritja brez interakcije, brez priprave in s popolno zanesljivostjo; praktičnega sistema, pripravljenega za uporabo; zanikanja avtorstva oziroma neprenosljivosti dokazov; ali tega, da Gödlov izrek o nepopolnosti sam po sebi varuje kriptografijo.

Glavne omejitve: jamstvo je sprostitev pojma znanja brez razkritja; najširša različica je odvisna od več predpostavk; trditve o enem univerzalnem dokazovalcu ostajajo deloma domnevne; rezultat pa je predvsem temeljne narave.

Koliko zaupanja naj ima splošni bralec? Veliko, da gre ob sprejetih definicijah za pomemben pogojni teoretični rezultat. Zmerno, da predpostavke opisujejo resničnost. Malo glede takojšnje praktične uporabe. Varna sklepna misel je: članek ne poruši izrekov o nemogočnosti znanja brez razkritja; najde nov dokaznoteoretičen način, kako obiti tiste njihove dele, ki so pomembni za številne varnostne igre.

Viri

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`