The Clean Paper

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

Kriptografski dokaz može sakriti tajnu tako da je teško dokazati odsutnost simulatora

Zero-knowledge dokazi omogućuju dokazivanje tvrdnje bez otkrivanja svedoka. Klasična teorija kaže da to, u punom smislu, ne možete imati s jednom porukom, bez pouzdanog setupa i sa savršenom zvučnošću. Rad Rahula Ilanga ne čini tu nemogućnost nestalom. Menja cilj: umesto zahteva da simulator stvarno postoji, traži da nijedan odabrani dokazni sistem ne može efikasno dokazati da simulator ne postoji. Pod velikim pretpostavkama iz složenosti dokaza i kriptografije to je dovoljno za vraćanje falsificabilnih, na bezbednosnim igrama zasnovanih posledica zero-knowledgea, svojstvo po svojstvo. Poenta nije gotov internetski primitiv. To je dokazno-teorijski način pretvaranja matematičke nedokazivosti u kriptografski zaklon.

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 nije u tome da dokažete da je tajna skrivena

Počnimo od najjednostavnije verzije zero-knowledge dokaza.

Alice želi uveriti Boba da Sudoku ima rešenje. Ako mu pošalje rešenje, Bob će biti uveren, ali slagalica je uništena. Ona želi nešto neobičnije: dokaz da rešenje postoji, bez otkrivanja samog rešenja.

To je obećanje zero-knowledge dokaza. Dokazivač (Alice) uverava proveravača (Boba) da je tvrdnja istinita, a pritom ne otkriva ništa osim same istinitosti tvrdnje.

Problem je što to obećanje nešto košta. Običan matematički dokaz ima dve ugodne funkcije. On je **jedna poruka**: napišete ga, predate i odete. I **savršeno je zvučan** (*perfectly sound*): lažna tvrdnja nema nijedan valjan dokaz. Klasični rezultati nemogućnosti kažu da se zero-knowledge mora odreći obe karakteristike — i ne samo njihove kombinacije; svaka je pojedinačno zabranjena.

Prvo, zero-knowledge dokaz treba razgovor. Ako Alice pošalje samo jednu poruku, bez pouzdanog setupa dogovorenog unapred, garancija zero-knowledgea se ruši — bez obzira koliko ste zvučnosti spremni žrtvovati zauzvrat.

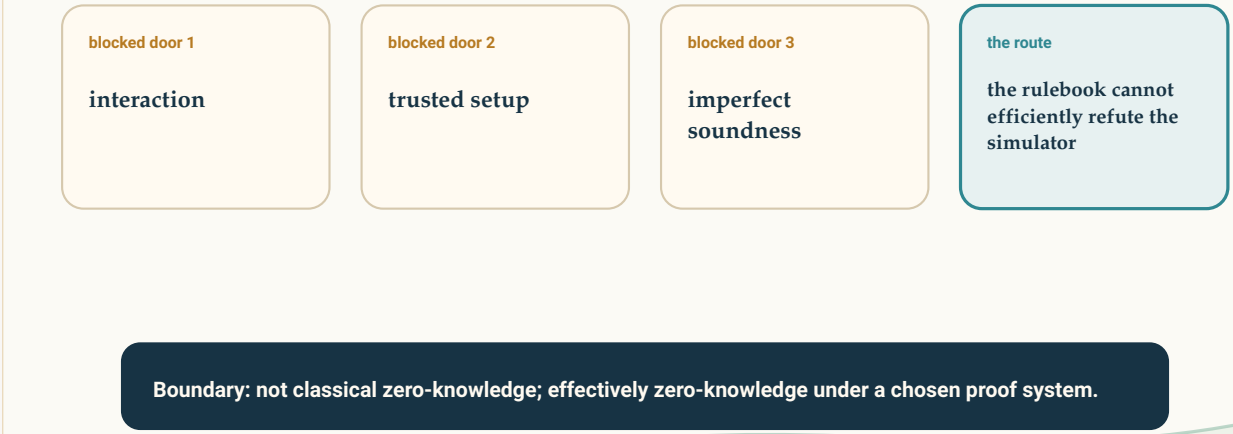
Drugo, zero-knowledge dokaz treba malu toleranciju na grešku. Zahtev za savršenom zvučnošću pokazuje se kao način da se tiho uništi i interakcija: proveravač koji nikada ne može biti prevaren, bez obzira na svoje slučajne izbore, mogao bi te izbore jednako dobro fiksirati unapred — a kad postane predvidljiv, Alice može odgovoriti na sve u jednoj poruci, upravo u slučaju za koji već znamo da ne funkcionira.

Rad Rahula Ilanga govori o putu oko tog dvostrukog zida. Ne tako da se pravi da zid ne postoji i ne tako da proizvede klasični zero-knowledge u nemogućem okruženju. Potez je suptilniji: oslabiti značenje „ne otkriva ništa”, ali na način koji čuva bezbednosna svojstva koja kriptografi stvarno mogu testirati.

Rezultat se zove **effectively zero-knowledge** — efikasno zero-knowledge.

A proof without leaking the witness

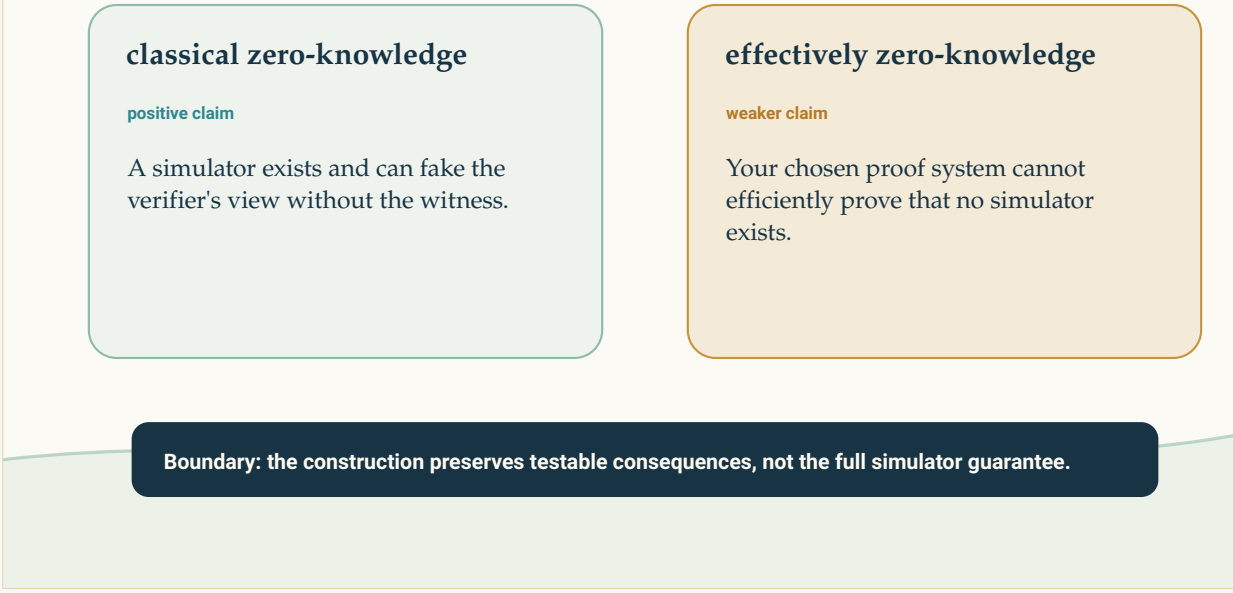
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Zero-knowledge je blokiran na troja vrata — interakciji, pouzdanom setupu i nesavršenoj zvučnosti. Ilangova konstrukcija prolazi kroz drugačija vrata: formalni sistem ne može efikasno opovrgnuti simulator.

Classical privacy vs effective privacy

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



Klasični zero-knowledge pita postoji li simulator; „effectively zero-knowledge" pita samo može li vaš odabrani formalni sistem efikasno dokazati da simulator ne može postojati. Slabije pitanje omogućuje konstrukciji da

zadrži jednu poruku, bez setupa i sa savršenom zvučnošću.

Stari test: simulator postoji

Klasična formalizacija zero-knowledgea koristi izmišljenog pomagača koji se zove **simulator**.

Ideja je ova: zamislite Jane, koja **ne zna** Alicinu tajnu. Ako Jane može potpuno sama generisati dokaze koji izgledaju jednako kao dokazi koje bi Bob primio od Alice, tada Alicini dokazi Boba nisu naučili ništa novo. Jane je već mogla lažirati celo iskustvo bez Alicine tajne.

Klasični zero-knowledge zato zahteva stvarni simulator. Mora postojati efikasan algoritam koji može proizvesti dokaze nalik pravima bez poznavanja tajne — *svedoka* (*witness*), u stručnom jeziku; za Sudoku je svedok jednostavno rešena mreža.

Ta je definicija snažna, ali upravo je na tom mestu pogađa stara nemogućnost. Intuicija je sledeća. Zaista neinteraktivni dokaz samo je niz znakova. Kada Bob dobije taj niz, može ga pokazati nekome drugome: stekao je sposobnost dokazati tvrdnju drugima, što već zvuči kao više od „ničega". Klasični teoremi tu intuiciju zaoštravaju u gore navedene rezultate nemogućnosti.

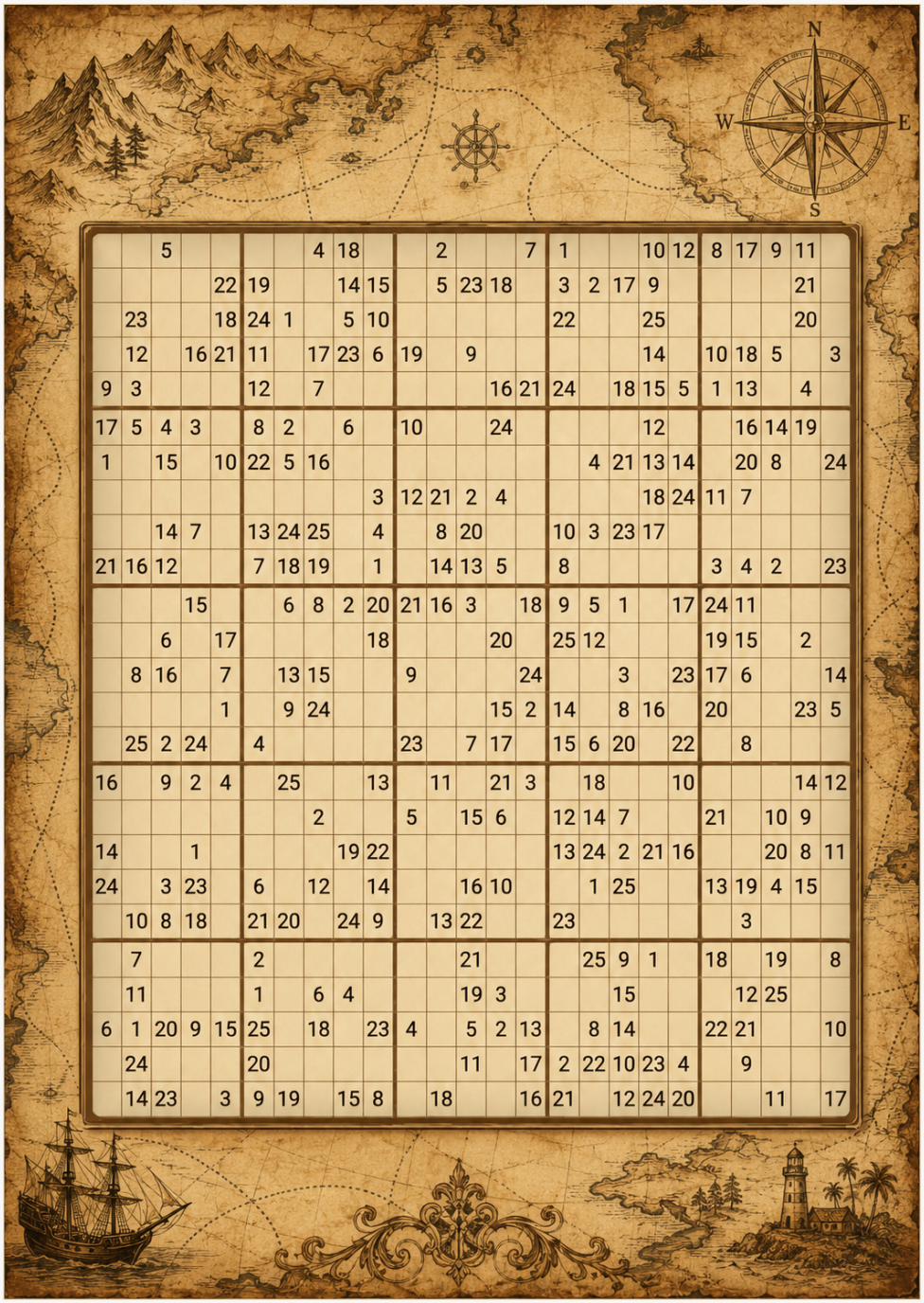
> **Tri svojstva na kojima ovaj rad inzistira**
>
> Naslov rada navodi tri ograničenja:
> **Bez interakcije:** Alice šalje jedan niz koji predstavlja dokaz. Nema protokola napred-natrag.
> **Bez setupa:** Alice i Bob ne oslanjaju se na pouzdan zajednički referentni niz ni na unapred dogovorenu javnu slučajnost. Mnogi sistemi nazvani „neinteraktivni zero-knowledge" ipak zavise o setupu; ovaj rad podrazumeva nulti setup.
> **Savršena zvučnost:** lažna tvrdnja nema valjan dokaz. Ne „gotovo se nikada ne prihvati"; valjan dokaz jednostavno ne postoji.
> To su upravo tri svojstva koja ima obična pisana matematika — a, kao što smo gore objasnili, klasični zero-knowledge ih ne može zadržati.

Mega-Sudoku verzija razlike

Evo namerno pojednostavljenog načina da se razlika oseti.

Za ozbiljni deo analogije nemojte uzeti običan Sudoku 9-na-9. Premalen je i previše konačan: računar ga jednostavno može rešiti ili dokazati da nema rešenja. Umesto toga zamislite porodica zagonetki **MegaSudoku(n)**. Uvećajte uobičajeno pravilo: odaberite veličinu bloka n, neka je $N = n^2$, i napravite mrežu N puta N podeljenu u blokove n puta n, s N simbola. Obični Sudoku samo je maleni slučaj $n = 3$, $N = 9$: mreža 9-na-9, blokovi 3-na-3 i devet simbola. Priča iz teorije složenosti dokaza počinje tek kada n sme rasti i kada mreža može nositi dodatne gadgete zbog kojih se ponaša kao SAT formula

prerušena u Sudoku. SAT formula samo je popis da/ne ograničenja: možete li varijablama dodeliti true/false vrednosti tako da su sva ograničenja zadovoljena?



Sudoku 25x25: njegova pravila mogu se proveravati bez otkrivanja dovršene mreže — vizuelna zamena za dokaz koji potvrđuje skriveno rešenje, odnosno svedoka.

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

Sudoku i SAT: ista zagonetka u dva kostima

Tvrdnja da se Sudoku može „ponašati kao SAT formula” nije metafora. prevod ide u oba smera,

a lakši smer možemo ispisati u celosti.

Od Sudokua prema SAT-u. SAT govori samo true/false, pa uvedite jednu Booleovu varijablu za svaku trojku (red, kolona, vrednost): *x(r,c,v)* znači „polje u retku *r*, stupcu *c* sadrži vrednost *v*". Sudoku 4-na-4 (blokovi 2-na-2, vrednosti 1–4) treba 4·4·4 = 64 varijable; klasični 9-na-9 treba 729. Svako pravilo Sudokua tada postaje skup klauzula. (Klauzula je OR varijabli ili njihovih negacija; cela formula je AND svih klauzula.)

Svako polje sadrži barem jednu vrednost — jedna klauzula po polju:

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

Svako polje sadrži najviše jednu vrednost — klauzula „ne oboje" za svaki par vrednosti:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \text{... i tako za svih šest parova.}$$

Svaki red sadrži svaku vrednost — za red 1 i vrednost 3: barem jednom,

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

a najviše jednom: $\neg x(1,1,3) \vee \neg x(1,2,3)$, i tako za svaki par polja u retku.

Kolone i blokovi — isti skupovi klauzula; menja se samo skup polja. Za gornji levi blok i vrednost 2:

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

uz parne klauzule „ne oboje".

Ispisani tragovi — najjednostavniji deo: svaki trag je klauzula s jednom varijablom. Broj 3 ispisan u gornjem levom kutu postaje klauzula

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

AND svega toga zadovoljiv je tačno onda kada Sudoku ima rešenje — a zadovoljavajuća dodela *je* rešenje: pročitajte koje su x(r,c,v) istinite i ispunite mrežu. Za 9-na-9 dobijate 729 varijabli i nekoliko hiljada klauzula, što savremeni SAT solver reši u milisekundama. Primetite klauzulu traga x(1,1,3): ona kaže „ovo polje jednako je tačno 3", ne „sva su ova polja različita" — ista asimetrija koja će kasnije zahtevati dodatni trik za polja s tragovima.

Od SAT-a prema Sudokuu. Radu treba suprotan, teži smer: za *proizvoljnu* SAT formulu izgraditi mega-Sudoku koji ima rešenje tačno onda kada ga ima formula. Prirodna pravila Sudokua mogu reći samo „sva su ova polja različita", pa se proizvoljna logička ograničenja moraju *izgraditi* — upravo tome služe gadgeti. Gadget je mali unapred dizajniran skup polja, po jedan za svaku klauzulu formule, u kojem određena polja predstavljaju varijable (simbol koji nose kodira true ili false), a unutrašnja ograničenja nameštena su tako da jedina dozvoljena popunjavanja odgovaraju dodelama koje zadovoljavaju klauzulu. To je standardno umeće iz dokaza NP-potpunosti; za generalizirani Sudoku izveli su ga Yato i Seta 2003.

Ta dva smera zajedno znače da su N-na-N Sudoku i SAT isti problem u različitim kostimima. Zato ovaj članak — i rad — sme pričati priču o celom NP-u pomoću mreža i simbola.

Svedoka je i dalje lako zamisliti. Alice zna potpuno valjano popunjavanje mega-Sudokua. Bob želi biti uveren da takvo popunjavanje postoji, ali Alice ga ne želi otkriti. Ako pošalje celu mrežu, Bob je uveren, ali tajna je nestala.

U klasičnoj zero-knowledge verziji Alice i Bob komuniciraju. Jedan stari mentalni model koristi pokrivene pločice. Alice skriva rešenu mrežu, potajno preimenuje simbole pre svakog kruga i Bobu dozvolja proveru jednog nasumično odabranog lokalnog ograničenja: retka, kolone, bloka ili gadgeta. Ako otvorena polja sadrže sve različite simbole, Bobovo poverenje raste. Zatim se sve ponovo pokrije, a simboli sveže preimenuju. (Postoji jedna kvaka: zadani tragovi trebaju dodatni trik jer preimenovanje skriva i njih. Beleška ispod objašnjava kako klasični protokoli to rešavaju; pojednostavljena slika dovoljna je za ono što sledi.)

Kako klasični protokoli stvarno rešavaju polja s tragovima

Trik preimenovanja ima slepu tačku. Pravila redaka, kolona i blokova sva kažu „sva su ova polja različita", a svojstvo *sve različito* preživljava svako preimenovanje simbola. Ali trag kaže „ovo polje sadrži tačno 5", a nakon preimenovanja Bob vidi samo $\sigma(5)$ — neki maskirani simbol — bez poznavanja preimenovanja σ. Ne može ništa proveriti. Bez popravka Alice bi mogla dokazati da *neka* valjana mreža postoji potpuno zanemarujući ispisane tragove, što ne dokazuje ništa o *ovoj* zagonetki. Klasična literatura ima dva standardna popravka.

Paleta. Skrivenoj mreži dodajte jedan dodatni red od N polje — paletu koju Alice ispuni simbolima 1…N u fiksnom javnom redosledu, a zatim preimenuje zajedno sa svime ostalim, tako da sadrži $\sigma(1)$…σ(N). Bobov nasumični izazov sada ima još jednu mogućnost. Osim retka, kolone, bloka ili gadgeta može odabrati **paletu plus jedno polje s tragom**. Alice otkrije oboje; paleta otkriva preimenovanje u tom krugu, a Bob proveri da polje s tragom prikazuje tačno preimenovanu verziju ispisanog traga. Protokol ostaje zero-knowledge jer Bob saznaje samo σ — koji se u svakom krugu bira iznova i sam po sebi je bezvredan — i vrednost polja koju je već znao iz zagonetke. Ništa o tajnim poljima ne curi, a simulator može lažirati pogled odabirom nasumičnog σ. Protokol je zvučan jer Alice koja vara ima fiksnu verovatnoća da bude uhvaćena u svakom krugu, a krugovi se ponavljaju dok sumnja ne postane zanemariva.

Kompiliranje tragova. Strukturnija varijanta uklanja poseban izazov umesto da ga dodaje. Umesto *proveravanja* vrednosti traga, ona se prisilno zada ograničenjima različitosti: povežite polje s tragom sa svakim poljem palete osim one koja nosi njenu vrednost — „različito od $\sigma(1)$, različito od $\sigma(2)$, …, različito od svega osim $\sigma(5)$". Jedini simbol koji polje tada legalno može imati je onaj iz traga. Sva ograničenja opet su oblika „ove dve vrednosti su različite" — nepromenljiva pod preimenovanjem i proverljiva poput retka. To je isti manevar koji se koristi za unapred obojene vrhove u klasičnom protokolu bojenja grafova i smisao reči *gadget* iznad: u slici MegaSudoku-kao-SAT tragovi se kompiliraju u gadgete nejednakosti poput svih ostalih ograničenja.

Fizički protokol. Stvarni kartični protokol za Sudoku (Gradwohl, Naor, Pinkas i Rothblum, 2007.) uopšte ne koristi preimenovanje i tragove rešava pre nego što skrivanje počne. Za svaku polje Alice položi tri jednake karte s vrednošću polja — licem naniže za tajna polja, ali **licem naviše za polja s tragovima**, pa Bob sopstvenim očima vidi da su tragovi poštovani pre okretanja karata. Zatim jedna karta iz svakog polja ide u paket svog retka, jedna u paket svog kolone, jedna u paket svog bloka; svaki se paket promeša i otvori, a Bob proveri da sadrži svih

> N simbola. Mešanje uništava podatak o položaju — to daje zero-knowledge — ali tragovi su već bili fiksirani pri deljenju.
> U oba slučaja lekcija je ista ona kojoj se članak stalno vraća: zero-knowledge protokol pažljivo vodi knjigovodstvo o tome *koje* činjenice preživljavaju skrivanje. Preimenovanje čuva „sve različito" i briše „jednako 5" — zato se „jednako 5" mora vratiti drugim putem.

To nije protokol iz rada. To je mentalni model klasičnog zero-knowledgea:

- Alice i Bob komuniciraju napred-natrag.
- Bob bira nasumične provere.
- Alice otkriva samo lokalnu konzistentnost, ne celo rešenje.
- Dokaz privatnosti radi tako da se pokaže kako je Bobov pogled mogao biti generisan bez Alicina tajnog rešenja.

Klasični zero-knowledge zato se gradi oko pozitivne činjenice:

> Simulator stvarno postoji.

Sada uklonite ugodne delove. Alice pošalje jedan dokaz i ode. Nema pouzdanog setupa, nema zajedničkog nasumičnog niza pripremljenog unapred, a Bob nikada ne sme prihvatiti lažnu zagonetku. To je okruženje u kojem klasični zero-knowledge ne može preživeti.

Pre trika treba još jedan lik. Fiksirajte **formalni sistem**: formalni dokazni sistem u logičkom smislu — fiksni skup aksioma i mehaničkih pravila za proveru pisanih matematičkih dokaza. ZFC, standardni aksiomi matematike, kanonski je primer. Sve što sledi navodi se relativno prema unapred odabranom formalnom sistemu, a izbor je fleksibilan: konstrukcija radi za bilo koji formalni sistem koji fiksirate, uključujući ZFC.

(Napomena o terminima, prema samom radu: „proof system" ovde uvek znači taj formalni sistem — formalni sistem koji proverava matematičke dokaze — a nikada poruke koje Alice šalje. Alicin i Bobov mehanizam zovu se „prover" i „verifier".)

Gödelovska verzija zadržava priču o mega-Sudokuu, ali menja dokaz.

Odaberite drugi sistem ograničenja iste prikazane veličine i nazovite ga **D**. U priči su S i D dva Mega-Sudoku(n) problema u istom formatu. U pozadini je D možda nastao iz teške logičke formule druge veličine; po potrebi se može nadopuniti bezopasnim lažnim ograničenjima kako bi stao u istu mrežu. D je izgrađen iz logičke formule koja je stvarno **nezadovoljiva**: ne postoji dodela vrednosti koja zadovoljava sva njena ograničenja, kao što pokvarena zagonetka nema legalno popunjenu mrežu. Jednostavan primer bila bi formula koja zahteva i „X je istinit" i „X je neistinit". Dakle, D nema valjano rešenje.

Ali D ne sme biti pokvarena zagonetka koju je *lako razotkriti*. Gornji jednostavni primer ne valja: svaki formalni sistem opovrgava „X i ne-X" u jednom retku. D mora biti lažan na način koji odabrani formalni sistem ne može potvrditi kratkim argumentom. Kada bi formalni sistem mogao opovrgnuti D kratkim dokazom, priča ispod bi propala: alternativni put koji bi možda proizveo dokaze bez Alicine

tajne mogao bi se formalno isključiti, a s njim i garancija privatnosti. Zato se D bira iz porodici koju fiksni formalni sistem ne može efikasno opovrgnuti: u tom formalnom sistemu nema kratkog dokaza da D nema rešenje.

Alicin jednoporukovni dokaz tada govori o disjunkciji:

> ili stvarni mega-Sudoku S ima rešenje, ili mamac D ima rešenje.

To je logička veza. D **nije** generisan nekim čarobnim načinom koji čini S istinitim. Dokaz ne tvrdi „D nema rešenje, stoga S ima rešenje". Dokazuje disjunkciju **S ili D**. Savršena zvučnost kaže da lažna disjunkcija ne može imati valjan dokaz. Budući da je D u stvarnosti lažan — nema rešenje — jedini način da disjunkcija bude istinita je da je S istinit. Ako se dokaz prihvati, S mora imati rešenje. Mamak ne može lažni S pretvoriti u istiniti.

Ali za deo nalik zero-knowledgeu pitajte što bi se dogodilo da D *ima* rešenje. To rešenje mamca bilo bi alternativni svedok. Omogućilo bi nekome proizvesti dokaze bez poznavanja Alicina pravog rešenja mega-Sudokua — drugim rečima, simulator. U stvarnosti D nema rešenje, pa je taj put simulatora zatvoren. Poenta je da formalni sistem ne može efikasno dokazati da je zatvoren.

D dakle ima dva posla. Za **zvučnost**, D je lažan, pa valjan dokaz „S ili D" prisiljava S. Za **effectively zero-knowledge**, D je teško opovrgnuti, pa formalni sistem ne može brzo isključiti mamac koji bi simulaciju učinio mogućom.

Sigurnosni test više nije:

> Možemo li dokazati da simulator stvarno postoji?

Postaje:

> Može li vaš formalni sistem efikasno dokazati da je simulator nemoguć?

Ako je odgovor ne, sledi nešto iznenađujuće snažno: svaka bezbednosna garancija koje (a) možemo posmatrati izvođenjem testa i (b) unutar formalnog sistema dokazivo sledi iz postojanja simulatora, zapravo vredi. Uspešan napad na bilo koje od njih sam bi predstavljao nedostajuće kratko opovrgavanje, a takvog kratkog opovrgavanja nema. To je „effective" u effectively zero-knowledgeu.

Kontrast za učionicu glasi:

Klasični zero-knowledge: dokazi su sigurni jer simulator postoji.

Gödelovski effectively zero-knowledge: dokazi se za opažljive bezbednosne testove tretiraju kao sigurni jer formalni sistem ne može efikasno dokazati da je simulator nemoguć.

Druga tvrdnja je slabija. Upravo zato rad može zadržati tri funkcije koje su slomile klasičnu verziju: jednu poruku, bez setupa i savršenu zvučnost.

Novi test: ne možete dokazati da simulator nedostaje

Ilangovo slabljenje definicije menja pitanje.

Klasični zero-knowledge pita:

> Postoji li simulator?

Effectively zero-knowledge pita nešto slabije:

> Može li vaš odabrani formalni sistem efikasno dokazati da simulator ne postoji?

To zvuči kao tehničko izvlačenje, ali to je centralna ideja. Konstrukcija živi u čudnom stanju: simulator u stvarnosti ne postoji — rad je oko toga izričit — ali fiksirani formalni sistem ne može efikasno dokazati da ne postoji. Ako bi svaka loša posledica koja vas zanima zahtevala upravo takvo opovrgavanje, sistem se za te posledice i dalje ponaša kao zero-knowledge.

Tu ulazi Gödel. Ne kao ukras i ne kao „Gödel čini kriptografiju sigurnom". Veza je dokazno-teorijska. Dokazni sistem se naziva **optimalnim** ako je, u preciznom smislu, najbolji mogući: kad god neki formalni sistem može opovrgnuti formulu relevantne vrste kratkim dokazom, optimalni to može takođe, dokazom najviše polinomno dužim. Krajíček i Pudlák 1989. postavili su pretpostavku da **ne postoji optimalan dokazni sistem**: koji god formalni sistem fiksirate, neki drugi formalni sistem neke porodice istinitih tvrdnji dokazuje mnogo sažetije. To je jedna od centralnih otvorenih pretpostavki teorije složenosti dokaza i konačni, složenostni rođak Gödelove teoreme nepotpunosti: neke istinite tvrdnje nemaju kratak dokaz u formalnom sistemu koji ste fiksirali — ne zato što ih je načelno nemoguće dokazati, nego zato što svaki fiksni formalni sistem ostavlja neke kratke istine bez kratkih dokaza.

Rad pretpostavlja tu hipotezu, u malo jačem obliku „infinitely often", standardnom kada se pretpostavke koriste kriptografski. Dobitak, prema teoremu Krajíčeka i Pudláka, konkretan je: za svaki formalni sistem postoji niz formula koje su stvarno nezadovoljive, a koje formalni sistem ne može opovrgnuti kratkim dokazima — i, presudno, koje efikasan algoritam može *generisati*. To poslednje svojstvo, uniformnost, pretvara ideju iz tvrdnje o postojanju u stvarni algoritam koji Alice može pokrenuti: njeni mamci D izlaze s proizvodne trake, ne iz ničega.

Kriptografski potez je iskoristiti taj nedostatak dokazne moći.

Šta konstrukcija radi

Evo konstrukcije rada, svedene na oblik.

Fiksirajte formalni sistem — recimo ZFC. Pod pretpostavkom iz složenosti dokaza postoji efikasno generabilan niz formula koje su stvarno nezadovoljive, ali formalni sistem nema kratke dokaze njihove nezadovoljivosti.

Sada izgradite jednoporukovni dokaz oblika:

> ili je stvarna tvrdnja zadovoljiva, ili je ova posebna teška formula zadovoljiva.

Posebna teška formula nije zadovoljiva. Ako je osnovni dokazni mehanizam savršeno zvučan, prihvatanje poruke zato i dalje znači da je stvarna tvrdnja istinita. To daje savršenu zvučnost.

Ali za bezbednost nalik zero-knowledgeu zamislite da je posebna teška formula *zadovoljiva*. Tada bi se njen svedok mogao koristiti za simuliranje dokaza bez poznavanja pravog svedoka. Formula u stvarnosti nije zadovoljiva — ali formalni sistem to ne može efikasno dokazati. Zato ne može efikasno dokazati da je simulator nemoguć.

To je ključ. Sistem ne skriva tajnu proizvodnjom klasičnog simulatora. Za veliku klasu opažljivih bezbednosnih testova skriva je iza nesposobnosti formalnog sistema da potvrdi odsutnost simulatora.

Šta rad tvrdi

Glavni teorem dolazi u slojevima. Jezgra rezultata je ova:

Pod standardnom kriptografskom pretpostavkom — postojanjem **neinteraktivnih witness-indistinguishable dokaza**, dobro proučenih objekata koji slede iz više ustaljenih skupova pretpostavki — i pod pretpostavkom teorije složenosti dokaza da **ne postoji (infinitely often) optimalan dokazni sistem**, rad za svaki izbor formalnog sistema konstruiše jednoporukovni prover i verifier za NP/SAT s **perfect soundness**, bez setupa, koji je effectively zero-knowledge relativno prema tom formalnom sistemu. (NP/SAT je standardni „najteži zajednički nazivnik” problema nalik zagonetkama; mega-Sudoku samo je jedan kostim.)

Za širu tvrdnju o očuvanju proverljivih bezbednosnih svojstava rad dodaje još jednu standardnu pretpostavku, derandomizacijsku hipotezu **P = BPP** — grubo, da slučajnost algoritmima ne daje bitnu dodatnu moć.

Prevedeno iz jezika teorema:

- Dokaz je jedna poruka.
- Nema pouzdanog setupa.
- Lažne tvrdnje ne mogu se dokazati.
- Prover nije klasični zero-knowledge — nema simulator.
- Ali svaka falsificabilna, na sigurnosnoj igri zasnovana posledica klasičnog zero-knowledgea može se postići u tom okruženju.

„Falsificabilno” je važno. To znači da se bezbednosni neuspeh može testirati pokretanjem protivnika u igri. Mnoge kriptografske definicije bezbednosti imaju taj oblik: može li protivnik razlikovati dve šifrirane poruke, invertirati funkciju, pronaći svedoka ili pobediti u određenom eksperimentu? Teorem daje prover za svako falsificabilno svojstvo, jedno po jedno. Jedan prover koji bi istovremeno

imao *svako* falsificabilno svojstvo verovatno je nemoguć — stari napad ponovne upotrebe („Bob može pokazati dokaz drugima”) i sam je falsificabilno svojstvo, a ovde zaista ne vredi. predlog rada je da jedan prover verovatno može pokriti sva *prirodna* falsificabilna svojstva — ona koja se stvarno pojavljuju u kriptografskoj praksi — ali taj je deo uslovni teorem koji se oslanja na neformalnu ideju „prirodnog”, uz izričitu dodatnu pretpostavku. Jamstvo cilja opažljive neuspehe, ne svako filozofsko ili simulacijsko značenje tajnosti.

Vredi imenovati jednu konkretnu posledicu: konstrukcija daje prve neinteraktivne *witness-hiding* dokaze s uniformnim proverom — „dokaz da zagonetka ima rešenje ne pomaže vam pronaći to rešenje”, bez interakcije i bez setupa — objekt skromnog zvuka koji je decenijama odolevao konstrukciji.

Šta ovo ne kaže

Ovo je deo koji čuva poštenje teksta.

Ne kaže da su stari teoremi nemogućnosti bili pogrešni. Konstrukcija ih zaobilazi promenom definicije.

Ne daje obični, klasični zero-knowledge bez interakcije, setupa i uz savršenu zvučnost. Rad izričito kaže da konstruisani prover nema simulator.

Ne znači da se dokaz ne može ponovo koristiti. Jednoporukovni dokaz i dalje se može pokazati drugome; rad ne čuva svojstva nalik poricanju. (I neinteraktivni zero-knowledge s pouzdanim setupom ima isto ograničenje.)

Ne znači da je ovo praktičan protokol spreman za primenu. Ovo su teorija složenosti i osnove kriptografije. Rezultat zavisi o velikim pretpostavkama iz složenosti dokaza i kriptografije, a konstrukcija govori o tome što je načelno moguće.

Ne čini „Gödela” čarobnim bezbednosnim primitivom. Veza s Gödelom ide kroz dokazne sisteme, optimalne dokazne sisteme i konačne analogije nepotpunosti. Korisna intuicija nije „nepotpunost štiti vašu lozinku”. Ona glasi: ako formalni sistem ne može efikasno dokazati da je simulator nemoguć, tada se napadi koji bi zahtevali takav dokaz mogu blokirati na nivou bezbednosnih definicija.

Zašto je ipak zanimljivo

Kriptografija često pretvara težinu problema u bezbednost. Faktorizacija je teška, pa pretpostavke nalik RSA-u postaju korisne. Problemi na rešetkama su teški, pa postaje korisna kriptografija na rešetkama. Ovde je težina čudnija: ne „teško je izračunati tajnu”, nego „teško je dokazati da određeni dokazni objekt ne može postojati”.

Zato rad deluje neobično. Aksiome i formalni sisteme tretira gotovo kao kriptografske resurse. Uo-

bičajena nemogućnost kaže da postoji napetost između zvučnosti i simulacije. Ilangov potez stavlja tu napetost iza dokazno-teorijske zavjese: simulator nedostaje, ali formalni sistem ne može efikasno razotkriti njegovu odsutnost.

Za čitalaca iznenađenje nije da će ovo zameniti današnje zero-knowledge sisteme. Verovatno neće, barem ne direktno. Iznenađenje je da se ograničenje iz matematičke logike može koristiti konstruktivno: ne samo kao zid nego kao svojevrsno zaklonjeno mesto.

Koliko su dokazi jaki?

Ovo je rad s teoremima, pa „dokazi" znače nešto drugo nego u biologiji ili astronomiji. Pitanje nije da li je eksperiment repliciran. Pitanje je podržavaju li definicije, pretpostavke i lanac dokaza tvrdnju.

Dokaz je formalan, a rad otvoreno navodi pretpostavke. One nisu usputne. Neinteraktivni witness-indistinguishable dokazi standardni su objekti u kriptografiji i slede iz više etabliranih skupova pretpostavki. Pretpostavka da ne postoji optimalan dokazni sistem centralna je pretpostavka složenosti dokaza. P = BPP standardna je derandomizacijska hipoteza koja se koristi samo za širi teorem o falsificabilnim svojstvima.

Rad takođe tvrdi da su pretpostavke prava cena, a ne proizvoljna skela: dokazuje obrat koji pokazuje da su u bitnom smislu nužne — ako konstrukcije poput ove uopšte postoje, moraju postojati neinteraktivni witness-indistinguishable dokazi i, uz standardne jednosmerne funkcije, ne može postojati optimalan dokazni sistem. Pretpostavke su i „win-win": njihovo opovrgavanje samo po sebi bilo bi veliko otkriće u složenosti dokaza, kriptografiji ili teoriji složenosti.

Ali budući da je rezultat uslovan, i poverenje je uslovno. Ako pretpostavke ne vrede, menja se interpretacija teorema. A čak i ako vrede, garancija nije potpuni klasični zero-knowledge; to je opuštena, dokazno-teorijska verzija iz rada.

Zato je ispravno imati visoko poverenje da rad uspostavlja koherentan uslovni rezultat mogućnosti; umereno da njegove pretpostavke opisuju kriptografski svet u kojem stvarno živimo; i nisko za neposredne praktične posledice.

Zašto je to važno

Rad otvara put koji je trebao biti zatvoren.

Klasična teorija kaže: puni zero-knowledge ne može biti jedna poruka bez setupa i ne može imati savršenu zvučnost. Ilangov rad kaže: ako tražimo posledice zero-knowledgea koje se mogu testirati u bezbednosnim igrama i ako dozvolimo da bezbednosna definicija zavisi od toga što formalni sistem može ili ne može efikasno opovrgnuti, tada se velik deo korisnog ponašanja može vratiti — s jednom porukom, bez setupa i sa savršenom zvučnošću.

To nije mala promena definicije. To je drugačiji način razmišljanja o kriptografskim jamstvima. Umesto da pitate samo što postoji, pitajte što vaš formalni sistem može isključiti. Umesto da nedokazivost tretirate kao filozofsku smetnju, upotrebite je kao strukturu.

Praktični se svet možda neće promeniti sutra. Ali konceptualna karta menja se. Sada postoji formalan smisao u kojem „niko ne može efikasno dokazati da je tajna procurila" može biti dovoljno snažno da vrati mnoge zaštite iz bezbednosnih igara koje smo željeli od „tajna nije procurila".

Zato Gödel pripada naslovu.

Kratak rezime

Zero-knowledge dokazi omogućuju dokazivaču da uveri proveravača da je tvrdnja istinita bez otkrivanja svedoka. Klasični rezultati nemogućnosti kažu da se zero-knowledge ne može stisnuti u jednu poruku bez setupa i ne može imati savršenu zvučnost. Rad Rahula Ilanga ne opovrgava te nemogućnosti. Definiše slabiji pojam, effectively zero-knowledge: umesto zahteva da simulator stvarno postoji, traži da odabrani dokazni sistem — formalni sistem poput ZFC-a — ne može efikasno dokazati da simulator ne postoji. Pod velikim pretpostavkama iz kriptografije (neinteraktivni witness-indistinguishable dokazi) i složenosti dokaza (ne postoji optimalan dokazni sistem), rad konstruiše jednoporukovne provere za NP/SAT bez setupa i sa savršenom zvučnošću koji ostvaruju falsificabilne, na bezbednosnim igrama zasnovane posledice zero-knowledgea, svojstvo po svojstvo. Jedan prover koji bi pokrivao sva „prirodna" takva svojstva dalje je, delimično konjekturalno proširenje — a pokriti doslovno svako falsificabilno svojstvo verovatno je nemoguće jer se dokazi i dalje mogu ponovo koristiti. Rezultat je teorijski i uslovan, ne gotov kriptografski primitiv, ali pokazuje novi način korišćenja dokazno-teorijske nedokazivosti kao kriptografskog resursa.

Provera bez ulepšavanja

Šta rad pokazuje: Pod navedenim pretpostavkama mogu se izgraditi jednoporukovni, bez-setup, savršeno zvučni proveri za NP/SAT koji su effectively zero-knowledge relativno prema bilo kojem odabranom dokaznom sistemu i koji ostvaruju svaku falsificabilnu posledicu klasičnog zero-knowledgea definisanu sigurnosnom igrom.

Šta je verovatno, ali nije bezuslovno dokazano: Da potrebne pretpostavke iz složenosti dokaza i kriptografije vrede. Ozbiljne su i dobro proučene — a rad pokazuje da su u bitnom smislu i nužne i dovoljne — ali i dalje su pretpostavke.

Šta ne pokazuje: Klasični zero-knowledge bez interakcije, setupa i uz savršenu zvučnost; praktičan sistem spreman za upotrebu; mogućnost poricanja ili nemogućnost ponovne upotrebe dokaza; niti da Gödelov teorem nepotpunosti sam po sebi čini kriptografiju sigurnom.

Glavna ograničenja: Jamstvo je slabljenje zero-knowledgea; najširа verzija zavisi o više pretpostavki; tvrdnje o jednom univerzalnom proveru ostaju delimično konjekturalne; rezultat je pre svega temel-

jan.

Koliko poverenja treba imati opšti čitalac? Visoko da je ovo važan uslovni teorijski rezultat ako se prihvate definicije. Umereno da pretpostavke odgovaraju stvarnosti. Nisko za neposrednu praktičnu upotrebu. Siguran zaključak glasi: rad ne ruši nemogućnosti zero-knowledgea; pronalazi novi dokazno-teorijski put oko njihovih delova koji su važni u mnogim bezbednosnim igrama.

Izvori

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`