The Clean Paper

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

Kriptografski dokaz može sakriti svoju tajnu tako što je teško dokazati da simulator nedostaje

Dokazi nultog znanja omogućavaju nekome da dokaže tvrdnju bez otkrivanja svjedoka. Klasična teorija kaže da to, u punom smislu, nije moguće uz jednu poruku, bez pouzdane početne postavke i sa savršenom pouzdanošću. Rad Rahula Ilanga ne uklanja tu nemogućnost. On mijenja cilj: umjesto zahtjeva da simulator zaista postoji, traži se da nijedan odabrani dokazni sistem ne može efikasno dokazati da simulator ne postoji. Uz snažne pretpostavke o složenosti dokaza i kriptografiji, to je dovoljno da se, svojstvo po svojstvo, povrate opovrgljive posljedice nultog znanja zasnovane na igrama. Cilj nije gotova internetska primitiva. To je pristup iz teorije dokaza kojim se matematička nedokazivost pretvara 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 uvjeriti Boba da Sudoku ima rješenje. Ako mu pošalje rješenje, Bob će biti uvjeren, ali slagalica je uništena. Ona želi nešto neobičnije: dokaz da rješenje postoji, bez otkrivanja samog rješenja.

To je obećanje zero-knowledge dokaza. Dokazivač (Alice) uvjerava provjeravatelja (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 dvije ugodne karakteristike. 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 obje 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 unaprijed, jamstvo zero-knowledgea se ruši — bez obzira koliko ste zvučnosti spremni žrtvovati zauzvrat.

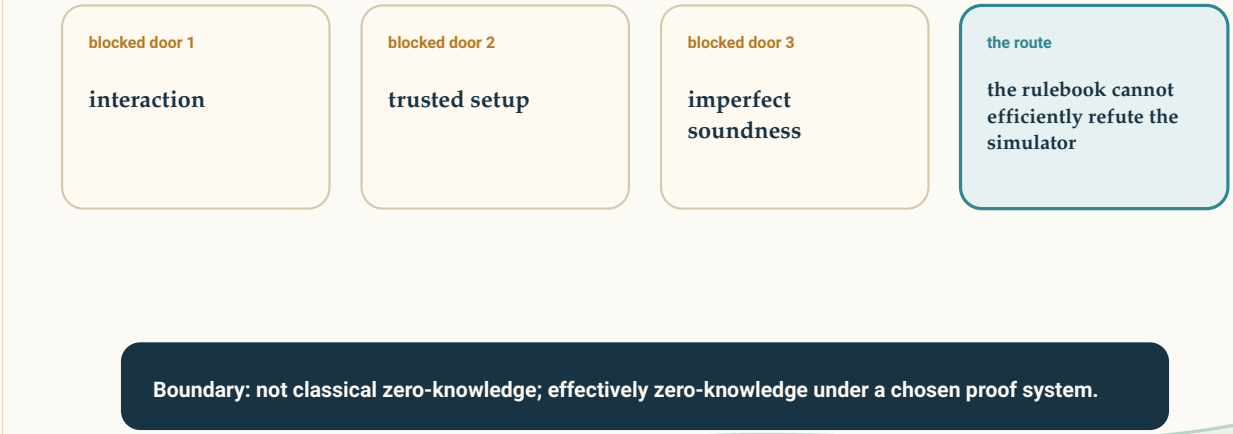
Drugo, zero-knowledge dokaz treba malu toleranciju na grešku. Zahtjev za savršenom zvučnošću pokazuje se kao način da se tiho uništi i interakcija: provjeravatelj koji nikada ne može biti prevaren, bez obzira na svoje slučajne izbore, mogao bi te izbore jednako dobro fiksirati unaprijed — a kad postane 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 sigurnosna svojstva koja kriptografi stvarno mogu testirati.

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

A proof without leaking the witness

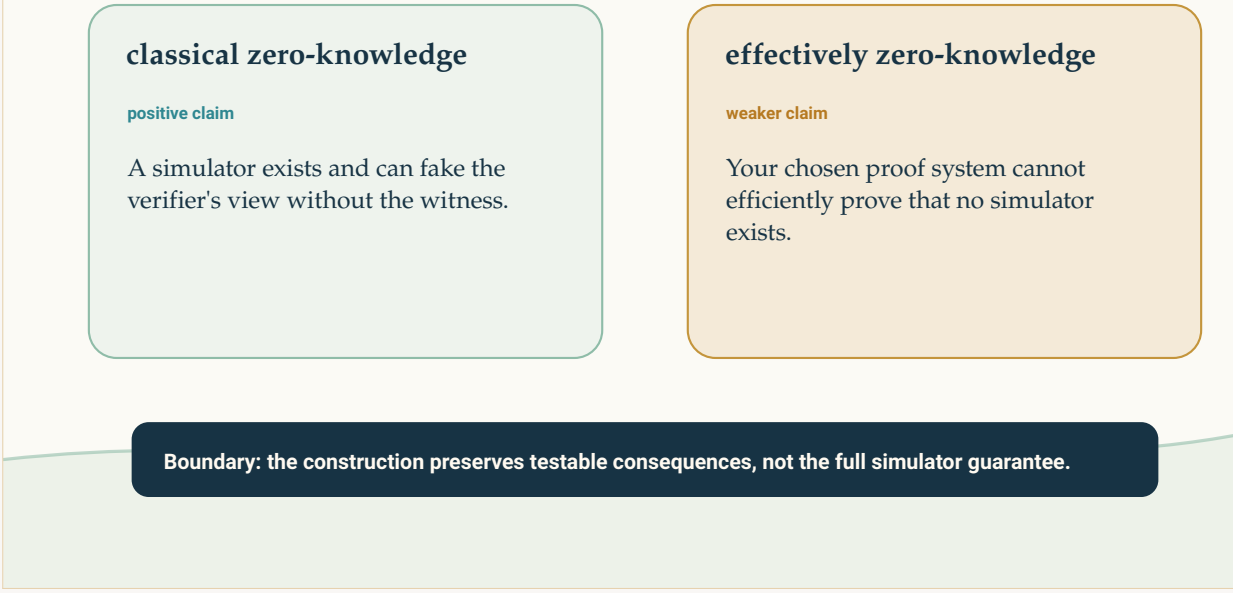
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Zero-knowledge je blokiran na troja vrata — interakciji, pouzdanom setupu i nesavršenoj zvučnosti. Ilangova konstrukcija prolazi kroz drukčija vrata: pravilnik 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 pravilnik efikasno dokazati da simulator ne može postojati. Slabije pitanje omogućava 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 generirati 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 cijelo iskustvo bez Alicine tajne.

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

Ta je definicija snažna, ali upravo je na tom mjestu pogađa stara nemogućnost. Intuicija je sljedeća. 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.

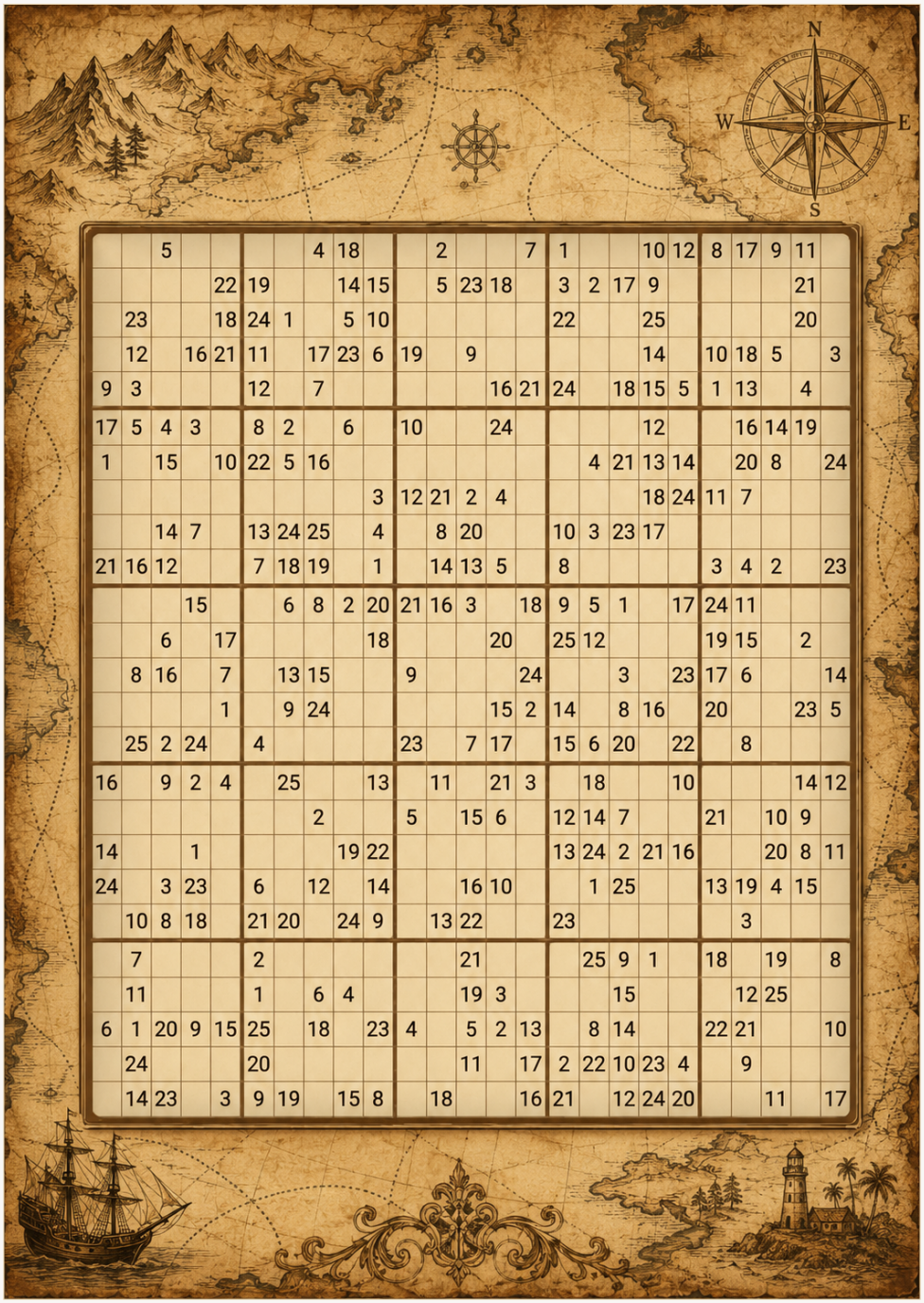
> **Tri svojstva na kojima ovaj rad inzistira**
>
> Naslov rada navodi tri ograničenja:
> **Bez interakcije:** Alice šalje jedan niz koji predstavlja dokaz. Nema protokola naprijed-natrag.
> **Bez setupa:** Alice i Bob ne oslanjaju se na pouzdan zajednički referentni niz ni na unaprijed dogovorenu javnu slučajnost. Mnogi sistemi nazvani „neinteraktivni zero-knowledge" ipak zavise o setupu; ovaj rad podrazumijeva 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 namjerno pojednostavljenog načina da se razlika osjeti.

Za ozbiljni dio analogije nemojte uzeti običan Sudoku 9-na-9. Premalen je i previše konačan: računar ga jednostavno može riješiti ili dokazati da nema rješenja. Umjesto toga zamislite porodicu zagonetki **MegaSudoku(n)**. Uvećajte uobičajeno pravilo: odaberite veličinu bloka n, neka je $N = n^2$, i napravite mrežu N puta N podijeljenu 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 smije 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 dodijeliti true/false vrijednosti tako da su sva ograničenja zadovoljena?



Sudoku 25x25: njegova pravila mogu se provjeravati bez otkrivanja dovršene mreže — vizualna zamjena za dokaz koji potvrđuje skriveno rješenje, odnosno svjedoka.

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. Prijevod ide u oba

smjera, a lakši smjer možemo ispisati u cijelosti.

Od Sudokua prema SAT-u. SAT govori samo true/false, pa uvedite jednu Booleovu varijablu za svaku trojku (red, kolona, vrijednost): *x(r,c,v)* znači „polje u retku *r*, stupcu *c* sadrži vrijednost *v*". Sudoku 4-na-4 (blokovi 2-na-2, vrijednosti 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; cijela formula je AND svih klauzula.)

Svako polje sadrži barem jednu vrijednost — 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 vrijednost — klauzula „ne oboje" za svaki par vrijednosti:

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

Svaki red sadrži svaku vrijednost — za red 1 i vrijednost 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.

Stupci i blokovi — isti skupovi klauzula; mijenja se samo skup polja. Za gornji lijevi blok i vrijednost 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 dio: svaki trag je klauzula s jednom varijablom. Broj 3 ispisan u gornjem lijevom kutu postaje klauzula

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

AND svega toga zadovoljiv je tačno onda kada Sudoku ima rješenje — a zadovoljavajuća dodjela *jest* rješenje: pročitajte koje su x(r,c,v) istinite i ispunite mrežu. Za 9-na-9 dobivate 729 varijabli i nekoliko hiljada klauzula, što savremeni SAT solver riješi u milisekundama. Primijetite 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 zahtijevati dodatni trik za polja s tragovima.

Od SAT-a prema Sudokuu. Radu treba suprotan, teži smjer: za *proizvoljnu* SAT formulu izgraditi mega-Sudoku koji ima rješenje 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 unaprijed 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 namještena su tako da jedina dopuštena popunjavanja odgovaraju dodjelama koje zadovoljavaju klauzulu. To je standardno umijeće iz dokaza NP-potpunosti; za generalizirani Sudoku izveli su ga Yato i Seta 2003.

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

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

U klasičnoj zero-knowledge verziji Alice i Bob komuniciraju. Jedan stari mentalni model koristi pokrivene pločice. Alice skriva riješenu mrežu, potajno preimenuje simbole prije svakog kruga i Bobu dopušta provjeru jednog nasumično odabranog lokalnog ograničenja: retka, stupca, bloka ili gadgeta. Ako otvorena polja sadrže sve različite simbole, Bobovo povjerenje raste. Zatim se sve ponovno pokrije, a simboli svježe preimenuju. (Postoji jedna kvaka: zadani tragovi trebaju dodatni trik jer preimenovanje skriva i njih. Bilješka ispod objašnjava kako klasični protokoli to rješavaju; pojednostavljena slika dovoljna je za ono što slijedi.)

Kako klasični protokoli stvarno rješavaju polja s tragovima

Trik preimenovanja ima slijepu tačku. Pravila redova, kolona i blokova sva kažu „sva su ova polja različita", a svojstvo *sve različito* preživljava svako preimenovanje simbola. Ali trag kaže „ova polje sadrži tačno 5", a nakon preimenovanja Bob vidi samo $\sigma(5)$ — neki maskirani simbol — bez poznavanja preimenovanja σ. Ne može ništa provjeriti. 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 redoslijedu, a zatim preimenuje zajedno sa svime ostalim, tako da sadrži $\sigma(1)…\sigma(N)$. Bobov nasumični izazov sada ima još jednu mogućnost. Osim retka, stupca, bloka ili gadgeta može odabrati **paletu plus jedno polje s tragom**. Alice otkrije oboje; paleta otkriva preimenovanje u tom krugu, a Bob provjeri 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 bezvrijedan — i vrijednost 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 vjerovatnoću da bude uhvaćena u svakom krugu, a krugovi se ponavljaju dok sumnja ne postane zanemariva.

Kompiliranje tragova. Strukturnija varijanta uklanja poseban izazov umjesto da ga dodaje. Umjesto *provjeravanja* vrijednosti traga, ona se prisilno zada ograničenjima različitosti: povežite polje s tragom sa svakim poljem palete osim one koja nosi njenu vrijednost — „različito od $\sigma(1)$, različito od $\sigma(2)$, …, različito od svega osim $\sigma(5)$". Jedini simbol koji polje tada legalno može imati jest onaj iz traga. Sva ograničenja opet su oblika „ove dvije vrijednosti su različite" — nepromjenjiva pod preimenovanjem i provjerljiva poput retka. To je isti manevar koji se koristi za unaprijed obojene vrhove u klasičnom protokolu bojenja grafova i smisao riječi *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.) uopće ne koristi preimenovanje i tragove rješava prije nego što skrivanje počne. Za svaku polje Alice položi tri jednake karte s vrijednošću polja — licem prema dolje za tajna polja, ali **licem prema gore za polja s tragovima**, pa Bob vlastitim očima vidi da su tragovi poštovani prije okretanja karata. Zatim jedna karta iz svakog polja ide u paket svog retka, jedna u paket svog stupca, jedna u paket svog bloka; svaki se paket promiješa i otvori, a Bob provjeri da sadrži

> svih N simbola. Miješanje uništava podatak o položaju — to daje zero-knowledge — ali tragovi su već bili fiksirani pri dijeljenju.
> U oba slučaja lekcija je ista ona kojoj se članak stalno vraća: protokol bez otkrivanja znanja (zero-knowledge) pažljivo prati *koje* činjenice ostaju sačuvane nakon skrivanja. 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 naprijed-natrag.
- Bob bira nasumične provjere.
- Alice otkriva samo lokalnu konzistentnost, ne cijelo rješenje.
- Dokaz privatnosti radi tako da se pokaže kako je Bobov pogled mogao biti generiran bez Alicina tajnog rješenja.

Klasični zero-knowledge zato se gradi oko pozitivne činjenice:

> Simulator stvarno postoji.

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

Prije trika treba još jedan lik. Fiksirajte **pravilnik**: formalni dokazni sistem u logičkom smislu — fiksni skup aksioma i mehaničkih pravila za provjeru pisanih matematičkih dokaza. ZFC, standardni aksiomi matematike, kanonski je primjer. Sve što slijedi navodi se relativno prema unaprijed odabranom pravilniku, a izbor je fleksibilan: konstrukcija radi za bilo koji pravilnik koji fiksirate, uključujući ZFC.

(Napomena o terminima, prema samom radu: „proof system" ovdje uvijek znači taj pravilnik — formalni sistem koji provjerava 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 mijenja 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 dodjela vrijednosti koja zadovoljava sva njena ograničenja, kao što pokvarena zagonetka nema legalno popunjenu mrežu. Jednostavan primjer bila bi formula koja zahtijeva i „X je istinit" i „X je neistinit". Dakle, D nema valjano rješenje.

Ali D ne smije biti pokvarena zagonetka koju je *lako razotkriti*. Gornji jednostavni primjer ne valja: svaki pravilnik opovrgava „X i ne-X" u jednom retku. D mora biti lažan na način koji odabrani pravilnik ne može potvrditi kratkim argumentom. Kada bi pravilnik 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 jamstvo privatnosti. Zato se D bira iz porodice koju fiksni pravilnik ne može efikasno opovrgnuti: u tom pravilniku nema kratkog dokaza da D nema rješenje.

Alicin jednoporukovni dokaz tada govori o disjunkciji:

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

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

Ali za dio nalik zero-knowledgeu pitajte što bi se dogodilo da D *ima* rješenje. To rješenje mamca bilo bi alternativni svjedok. Omogućilo bi nekome proizvesti dokaze bez poznavanja Alicina pravog rješenja mega-Sudokua — drugim riječima, simulator. U stvarnosti D nema rješenje, pa je taj put simulatora zatvoren. Poenta je da pravilnik 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 pravilnik 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 pravilnik efikasno dokazati da je simulator nemoguć?

Ako je odgovor ne, slijedi nešto iznenađujuće snažno: svako sigurnosno jamstvo koje (a) možemo opažati izvođenjem testa i (b) unutar pravilnika dokazivo slijedi iz postojanja simulatora, zapravo vrijedi. Uspješan 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 sigurnosne testove tretiraju kao sigurni jer pravilnik ne može efikasno dokazati da je simulator nemoguć.

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

Novi test: ne možete dokazati da simulator nedostaje

Ilangovo slabljenje definicije mijenja pitanje.

Klasični zero-knowledge pita:

> Postoji li simulator?

Effectively zero-knowledge pita nešto slabije:

> Može li vaš odabrani pravilnik 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 pravilnik ne može efikasno dokazati da ne postoji. Ako bi svaka loša posljedica koja vas zanima zahtijevala upravo takvo opovrgavanje, sistem se za te posljedice i dalje ponaša kao zero-knowledge.

Tu ulazi Gödel. Ne kao ukras i ne kao „Gödel čini kriptografiju sigurnom". Veza je dokazno-teorijska. Pravilnik se naziva **optimalnim** ako je, u preciznom smislu, najbolji mogući: kad god neki pravilnik može opovrgnuti formulu relevantne vrste kratkim dokazom, optimalni to može također, dokazom najviše polinomno dužim. Krajíček i Pudlák 1989. postavili su pretpostavku da **ne postoji optimalan dokazni sistem**: koji god pravilnik fiksirate, neki drugi pravilnik neke porodice istinitih tvrdnji dokazuje mnogo sažetije. To je jedna od centralnih otvorenih pretpostavki teorije složenosti dokaza i konačni, složenostni rođak Gödelova teorema nepotpunosti: neke istinite tvrdnje nemaju kratak dokaz u pravilniku koji ste fiksirali — ne zato što ih je načelno nemoguće dokazati, nego zato što svaki fiksni pravilnik 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 pravilnik postoji niz formula koje su stvarno nezadovoljive, a koje pravilnik ne može opovrgnuti kratkim dokazima — i, presudno, koje efikasan algoritam može *generirati*. To posljednje 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 pravilnik — recimo ZFC. Pod pretpostavkom iz složenosti dokaza postoji efikasno generabilan niz formula koje su stvarno nezadovoljive, ali pravilnik 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 temeljni dokazni mehanizam savršeno zvučan, prihvaćanje poruke zato i dalje znači da je stvarna tvrdnja istinita. To daje savršenu zvučnost.

Ali za sigurnost nalik zero-knowledgeu zamislite da je posebna teška formula *zadovoljiva*. Tada bi se njen svjedok mogao koristiti za simuliranje dokaza bez poznavanja pravog svjedoka. Formula u stvarnosti nije zadovoljiva — ali pravilnik 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 sigurnosnih testova skriva je iza nesposobnosti pravilnika 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 slijede iz više ustaljenih skupova pretpostavki — i pod pretpostavkom teorije složenosti dokaza da **ne postoji (infinitely often) optimalan dokazni sistem**, rad za svaki izbor pravilnika konstruira jednoporukovni prover i verifier za NP/SAT s **perfect soundness**, bez setupa, koji je effectively zero-knowledge relativno prema tom pravilniku. (NP/SAT je standardni „najteži zajednički nazivnik” problema nalik zagonetkama; mega-Sudoku samo je jedan kostim.)

Za širu tvrdnju o očuvanju provjerljivih sigurnosnih 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 utemeljena posljedica klasičnog zero-knowledgea može se postići u tom okruženju.

„Falsificabilno” je važno. To znači da se sigurnosni neuspjeh može testirati pokretanjem protivnika u igri. Mnoge kriptografske definicije sigurnosti imaju taj oblik: može li protivnik razlikovati dvije šifrirane poruke, invertirati funkciju, pronaći svjedoka ili pobijediti u određenom eksperimentu? Teorem daje prover za svako falsificabilno svojstvo, jedno po jedno. Jedan prover koji bi istovremeno imao *svako* falsificabilno svojstvo vjerovatno je nemoguć — stari napad ponovne upotrebe („Bob može

pokazati dokaz drugima") i sam je falsificabilno svojstvo, a ovdje zaista ne vrijedi. Prijedlog rada jest da jedan prover vjerovatno može pokriti sva *prirodna* falsificabilna svojstva — ona koja se stvarno pojavljuju u kriptografskoj praksi — ali taj je dio uslovni teorem koji se oslanja na neformalnu ideju „prirodnog", uz izričitu dodatnu pretpostavku. Jamstvo cilja opažljive neuspjehe, ne svako filozofsko ili simulacijsko značenje tajnosti.

Vrijedi imenovati jednu konkretnu posljedicu: konstrukcija daje prve neinteraktivne *witness-hiding* dokaze s uniformnim proverom — „dokaz da zagonetka ima rješenje ne pomaže vam pronaći to rješenje", bez interakcije i bez setupa — objekt skromnog zvuka koji je desetljećima odolijevao konstrukciji.

Šta ovo ne kaže

Ovo je dio koji čuva poštenje teksta.

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

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

Ne znači da se dokaz ne može ponovno 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 primjenu. Ovo su teorija složenosti i temelji kriptografije. Rezultat zavisi o velikim pretpostavkama iz složenosti dokaza i kriptografije, a konstrukcija govori o tome što je načelno moguće.

Ne čini „Gödela" čarobnim sigurnosnim 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 pravilnik ne može efikasno dokazati da je simulator nemoguć, tada se napadi koji bi zahtijevali takav dokaz mogu blokirati na razini sigurnosnih definicija.

Zašto je ipak zanimljivo

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

Zato rad djeluje neobično. Aksiome i pravilnike tretira gotovo kao kriptografske resurse. Uobičajena 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 čitaoca iznenađenje nije da će ovo zamijeniti današnje zero-knowledge sisteme. Vjerovatno neće, barem ne direktno. Iznenađenje je da se ograničenje iz matematičke logike može koristiti konstruktivno: ne samo kao zid nego kao svojevrsno zaklonjeno mjesto.

Koliko su dokazi jaki?

Ovo je rad s teoremima, pa „dokazi" znače nešto drugo nego u biologiji ili astronomiji. Pitanje nije je li 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 slijede 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 također tvrdi da su pretpostavke prava cijena, a ne proizvoljna skela: dokazuje obrat koji pokazuje da su u bitnom smislu nužne — ako konstrukcije poput ove uopće postoje, moraju postojati neinteraktivni witness-indistinguishable dokazi i, uz standardne jednosmjerne 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 povjerenje je uslovno. Ako pretpostavke ne vrijede, mijenja se interpretacija teorema. A čak i ako vrijede, jamstvo nije potpuni klasični zero-knowledge; to je opuštena, dokazno-teorijska verzija iz rada.

Zato je ispravno imati visoko povjerenje da rad uspostavlja koherentan uslovni rezultat mogućnosti; umjereno da njegove pretpostavke opisuju kriptografski svijet u kojem stvarno živimo; i nisko za neposredne praktične posljedice.

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 posljedice zero-knowledgea koje se mogu testirati u sigurnosnim igrama i ako dopustimo da sigurnosna definicija zavisi o tome što pravilnik može ili ne može efikasno opovrgnuti, tada se velik dio korisnog ponašanja može vratiti — s jednom porukom, bez setupa i sa savršenom zvučnošću.

To nije mala promjena definicije. To je drukčiji način razmišljanja o kriptografskim jamstvima. Um-

jesto da pitate samo što postoji, pitajte što vaš pravilnik može isključiti. Umjesto da nedokazivost tretirate kao filozofsku smetnju, upotrijebite je kao strukturu.

Praktični se svijet možda neće promijeniti sutra. Ali konceptualna karta mijenja 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 sigurnosnih igara koje smo željeli od „tajna nije procurila".

Zato Gödel pripada naslovu.

Kratak sažetak

Zero-knowledge dokazi omogućavaju dokazivaču da uvjeri provjeravatelja da je tvrdnja istinita bez otkrivanja svjedoka. 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. Definira slabiji pojam, effectively zero-knowledge: umjesto zahtjeva da simulator stvarno postoji, traži da odabrani dokazni sistem — formalni pravilnik 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 konstruira jednoporukovne provere za NP/SAT bez setupa i sa savršenom zvučnošću koji ostvaruju falsificabilne, na sigurnosnim igrama utemeljene posljedice zero-knowledgea, svojstvo po svojstvo. Jedan prover koji bi pokrivao sva „prirodna" takva svojstva dalje je, djelomično konjekturalno proširenje — a pokriti doslovno svako falsificabilno svojstvo vjerovatno je nemoguće jer se dokazi i dalje mogu ponovno koristiti. Rezultat je teorijski i uslovan, ne gotov kriptografski primitiv, ali pokazuje novi način korištenja dokazno-teorijske nedokazivosti kao kriptografskog resursa.

Provjera bez uljepšavanja

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 posljedicu klasičnog zero-knowledgea definiranu sigurnosnom igrom.

Šta je vjerovatno, ali nije bezuslovno dokazano: Da potrebne pretpostavke iz složenosti dokaza i kriptografije vrijede. 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 djelomično konjekturalne; rezultat je prije svega

temeljan.

Koliko povjerenja treba imati opći čitalac? Visoko da je ovo važan uslovni teorijski rezultat ako se prihvate definicije. Umjereno 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 dijelova koji su važni u mnogim sigurnosnim 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`