The Clean Paper

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

'n Kriptografiese bewys kan sy geheim verberg deur die ontbrekende simulator moeilik bewysbaar te maak

Nulkennisbewyse laat iemand 'n stelling bewys sonder om die getuie te onthul. Klassieke teorie sê dat jy dit, in die volle sin, nie met een boodskap, geen vertroude opstelling en perfekte geldigheid kan hê nie. Rahul Ilango se artikel laat dié onmoontlikheid nie verdwyn nie. Dit verander die teiken: in plaas daarvan om te vereis dat 'n simulator werklik bestaan, vereis dit dat geen gekose bewysstelsel doeltreffend kan bewys dat die simulator nie bestaan nie. Onder groot aannames uit bewyskompleksiteit en kriptografie is dit genoeg om falsifiseerbare, spelgebaseerde gevolge van nulkennis eienskap vir eienskap terug te kry. Die punt is nie 'n inpropbare internetprimitief nie. Dit is 'n bewysteoretiese manier om wiskundige onbewysbaarheid in kriptografiese dekking te verander.

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

Die truuk is nie om te bewys dat die geheim verborge is nie

Begin by die eenvoudigste weergawe van nulkennis.

Alice wil Bob oortuig dat ’n Sudoku-raaisel ’n oplossing het. As sy die oplossing stuur, is Bob oortuig, maar die raaisel is verwoes. Wat sy wil hê, is vreemder: ’n bewys dat ’n oplossing bestaan, sonder om die oplossing te onthul.

Dit is die belofte van ’n **nulkennisbewys** (*zero-knowledge proof*). Die bewyser (Alice) oortuig die verifieerder (Bob) dat ’n stelling waar is, terwyl niks buiten die waarheid van die stelling onthul word nie.

Die probleem is dat dié belofte iets kos. ’n Gewone wiskundige bewys het twee gemaklike eienskappe. Dit is **een boodskap**: jy skryf dit neer, gee dit oor en stap weg. En dit het **perfekte geldigheid (soundness)**: ’n vals stelling het glad geen geldige bewys nie. Klassieke onmoontlikheidsresultate sê dat nulkennis albei eienskappe moet prysgee — en nie net die twee saam nie; elkeen op sy eie is buite bereik.

Eerstens het ’n nulkennisbewys ’n gesprek nodig. As Alice ’n enkele boodskap stuur, sonder ’n vertroude opstelling wat vooraf gereël is, stort die nulkenniswaarborg in — ongeag hoeveel geldigheid jy bereid is om in ruil daarvoor prys te gee.

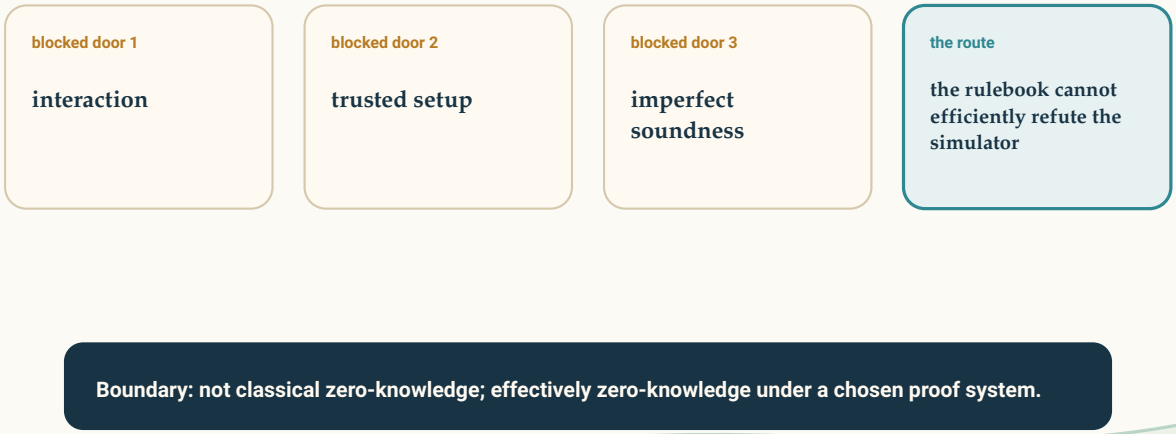
Tweedens het ’n nulkennisbewys ’n klein verdraagsaamheid vir fout nodig. Om perfekte geldigheid te eis, vernietig stilweg ook interaksie: ’n verifieerder wat nooit mislei kan word nie, ongeag watter ewekansige keuses hy maak, kan daardie keuses net so goed vooraf vasstel — en sodra die verifieerder voorspelbaar is, kan Alice alles in een boodskap beantwoord, presies die geval wat reeds gebreek het.

Rahul Ilango se artikel gaan oor ’n manier om om dié dubbele muur te beweeg. Nie deur voor te gee die muur bestaan nie, en nie deur klassieke nulkennis in die onmoontlike omgewing te produseer nie. Die skuif is subtieler: verswak wat “onthul niks” beteken, maar doen dit op ’n manier wat die sekuriteitseienskappe behou wat kriptograwe werklik kan toets.

Die resultaat word **effektief nulkennis** (*effectively zero-knowledge*) genoem.

A proof without leaking the witness

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

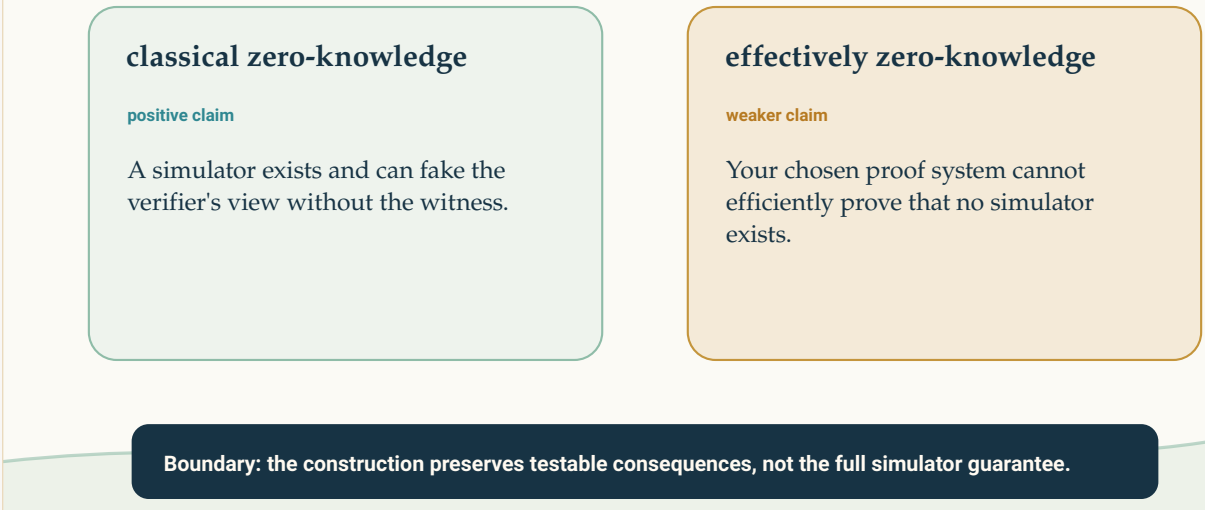


Nulkennis word by drie deure geblokkeer — interaksie, vertroude opstelling en onperfekte geldigheid. Ilango se konstruksie glip deur ’n ander deur: die reëlboek kan nie die simulator doeltreffend weerlê nie.

Original diagram — The Clean Paper CC BY 4.0

Classical privacy vs effective privacy

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



Klassieke nulkennis vra of ’n simulator bestaan; “effektief nulkennis” vra net of jou gekose reëlboek doeltreffend kan bewys dat een nie kan bestaan nie. Dit is dié swakker vraag wat die konstruksie toelaat om

een boodskap, geen opstelling en perfekte geldigheid te behou.

Die ou toets: ’n simulator bestaan

Die klassieke manier om nulkennis formeel te maak gebruik ’n denkbeeldige helper wat ’n **simulator** genoem word.

Die idee is hierdie: stel jou Jane voor, wat **nie** Alice se geheim ken nie. As Jane heeltemal op haar eie bewyse kan genereer wat net soos die bewyse lyk wat Bob van Alice sou ontvang het, dan het Alice se bewyse Bob niks nuuts geleer nie. Jane kon reeds die ervaring namaak sonder Alice se geheim.

Klassieke nulkennis vereis dus ’n werklike simulator. Daar moet ’n doeltreffende algoritme wees wat geloofwaardige vals bewyse kan produseer sonder om die geheim te ken — die **getuie** (*witness*) in die vaktaal; vir Sudoku is die getuie eenvoudig die voltooide rooster.

Daardie definisie is kragtig, maar dit is ook presies waar die ou onmoontlikheid byt. Hier is die intuïsie. ’n Werklik nie-interaktiewe bewys is net ’n string. Sodra Bob daardie string het, kan hy dit vir iemand anders wys: hy het die vermoë gekry om die stelling aan ander te bewys, wat reeds klink na meer as “niks”. Die klassieke stellings verskerp dié intuïsie tot die onmoontlikhede hierbo.

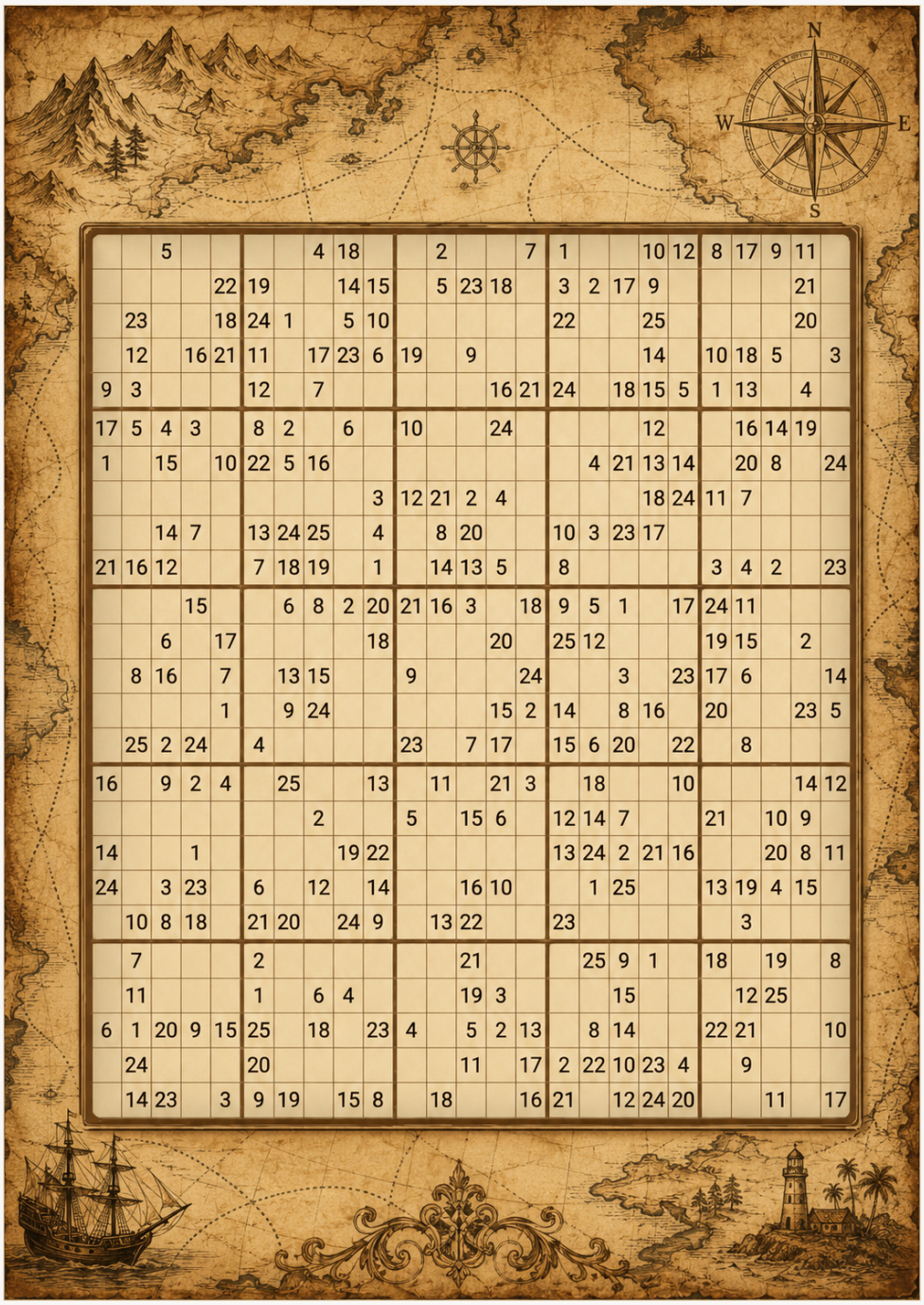
> **Die drie eienskappe waarop hierdie artikel aandring**
>
> Die titel van die artikel noem drie beperkings:
> **Geen interaksie:** Alice stuur een bewysstring. Daar is geen heen-en-weer-protokol nie.
> **Geen opstelling:** Alice en Bob steun nie op ’n vertroude gemeenskaplike verwysingsstring of ander voorafgereëlde openbare ewekansigheid nie. Baie stelsels wat “nie-interaktiewe nulkennis” genoem word, steun steeds op ’n opstelling; hierdie artikel bedoel nul opstelling.
> **Perfekte geldigheid:** ’n vals stelling het geen geldige bewys nie. Nie “word byna nooit aanvaar nie”; geen geldige bewys bestaan nie.
> Daardie drie eienskappe is presies wat gewone geskrewe wiskunde het — en, soos hierbo verduidelik, klassieke nulkennis kan hulle nie behou nie.

’n Mega-Sudoku-weergawe van die verskil

Hier is ’n doelbewus vereenvoudigde manier om die verskil aan te voel.

Gebruik nie ’n gewone 9-by-9-Sudoku vir die ernstige deel van die analogie nie. Dit is te klein en te eindig: ’n rekenaar kan dit eenvoudig oplos, of bewys dat dit geen oplossing het nie. Stel jou eerder ’n familie **MegaSudoku(n)**-raaisels voor. Skaal die gewone reël op: kies ’n blokgrootte n, laat $N = n^2$, en bou ’n N by N-rooster wat in n by n-blokke verdeel is, met N simbole. Gewone Sudoku is net die klein $n = 3$, $N = 9$-geval: ’n 9-by-9-rooster, 3-by-3-blokke en nege simbole. Die bewyskompleksiteitsverhaal

begin eers wanneer n toegelaat word om te groei, en wanneer die rooster ekstra gadgets kan dra wat dit laat optree soos ’n SAT-formule vermom as ’n Sudoku. ’n SAT-formule is bloot ’n lys ja/nee-beperkings: kan jy waar/onwaar-waardes aan die veranderlikes toeken sodat elke beperking bevredig word?



’n 25x25-Sudoku: die reëls daarvan kan nagegaan word sonder om die voltooide rooster te onthul — ’n visuele plaasvervanger vir ’n bewys wat ’n versteekte oplossing, die getuie, verifieer.

Sudoku en SAT: dieselfde raaisel in twee kostuums

Die bewering dat ’n Sudoku “soos ’n SAT-formule kan optree” is nie ’n metafoor nie. Die vertaling loop in albei rigtings, en die maklike rigting kan volledig neergeskryf word.

Van Sudoku na SAT. SAT praat net waar/onwaar, dus gee dit een Booleaanse veranderlike vir elke (ry, kolom, waarde)-drietal: *x(r,c,v)* beteken “die sel in ry *r*, kolom *c* bevat die waarde *v*.” ’n 4-by-4-Sudoku (2-by-2-blokke, waardes 1–4) benodig 4·4·4 = 64 veranderlikes; die klassieke 9-by-9 benodig 729. Elke Sudoku-reël word dan ’n groep klousules. (’n Klousule is ’n OF van veranderlikes of hul ontkennings; die hele formule is die EN van al sy klousules.)

Elke sel bevat minstens een waarde — een klousule per sel:

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

Elke sel bevat hoogstens een waarde — ’n “nie albei nie”-klousule vir elke paar waardes:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \text{... en so aan vir al ses pare.}$$

Elke ry bevat elke waarde — vir ry 1 en die waarde 3: minstens een keer,

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

en hoogstens een keer: $\neg x(1,1,3) \vee \neg x(1,2,3)$, en so aan vir elke paar selle in die ry.

Kolomme en blokke — identiese groepe; net die groep selle verander. Vir die boonste linkerblok en die waarde 2:

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

plus die paarsgewyse “nie albei nie”-klousules.

Die gedrukte leidrade — die eenvoudigste deel: elke leidraad is ’n klousule met ’n enkele veranderlike. ’n Gedrukte 3 in die boonste linkerhoek word die klousule

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

Die EN van dit alles is bevredigbaar presies wanneer die Sudoku ’n oplossing het — en ’n bevredigende toekenning *is* die oplossing: lees af watter x(r,c,v) waar is en vul die rooster in. Vir ’n 9-by-9 kom dit neer op 729 veranderlikes en ’n paar duisend klousules, wat ’n moderne SAT-oplosser binne millisekondes afhandel. Let op die leidraadklousule x(1,1,3): dit sê “hierdie sel is presies 3”, nie “hierdie selle verskil almal” nie — dieselfde asimmetrie wat die ekstra truuk vir leidraadselle in die protokolnota verder ondertoe nodig maak.

Van SAT na Sudoku. Die artikel het die teenoorgestelde, moeiliker rigting nodig: gegee ’n *willekeurige* SAT-formule, bou ’n mega-Sudoku wat ’n oplossing het presies wanneer die formule een het. Sudoku se natuurlike reëls kan net sê “hierdie selle verskil almal”, dus moet arbitrêre logiese beperkings *gebou* word — en dit is presies wat die gadgets doen. ’n Gadget is ’n klein voorafvervaardigde groep selle, een per klousule van die formule, waarin aangewese selle die rol van veranderlikes speel (die simbool wat hulle bevat kodeer waar of onwaar) en die interne beperkings so ontwerp is dat sy enigste wettige invullings ooreenstem met toekennings wat daardie klousule bevredig. Dit is standaardvakmanskap uit NP-volledigheidsbewyse; vir veralgemeende Sudoku is dit in 2003 deur Yato en Seta uitgewerk. Saam sê die twee rigtings dat N-by-N-Sudoku en SAT dieselfde probleem in verskillende kostuums is. Dit is wat hierdie artikel — en die bronartikel — toelaat om ’n verhaal oor die hele NP met roosters en simbole te vertel.

Die getuie bly maklik om voor te stel. Alice ken ’n volledige geldige invulling van die mega-Sudoku. Bob wil oortuig word dat so ’n invulling bestaan, maar Alice wil dit nie onthul nie. As sy die hele invulling stuur, is Bob oortuig, maar die geheim is weg.

In die klassieke nulkennisweergawe werk Alice en Bob interaktief. Een ou-styl denkmodel gebruik bedekte teëls. Alice versteek die opgeloste rooster, hernoem die simbole in elke ronde in die geheim en laat Bob een ewekansig gekose plaaslike beperking inspekteer: ’n ry, ’n kolom, ’n blok of ’n gadget. As die oopgemaakte selle almal verskillende simbole toon, kry Bob meer vertroue. Daarna word alles weer bedek en die simbole opnuut hernoem. (Een komplikasie: die gegewe leidrade van die raaisel vereis ’n ekstra truuk, omdat die hernoeming hulle ook versteek. Die nota hieronder verduidelik hoe klassieke protokolle dit oplos; die eenvoudige prentjie is genoeg vir wat volg.)

Hoe die klassieke protokolle die leidraadselle werklik hanteer

Die hernoemtruuk het ’n blindekol. Die ry-, kolom- en blokreëls sê almal “hierdie selle verskil almal”, en *almal verskillend* oorleef enige hernoeming van die simbole. Maar ’n leidraad sê “hierdie sel bevat presies 5”, en ná hernoeming sien Bob net $\sigma(5)$ — een gemaskerde simbool — sonder om die hernoeming σ te ken. Hy kan niks kontroleer nie. As dit nie herstel word nie, kan Alice bewys dat *een of ander* geldige rooster bestaan terwyl sy die gedrukte leidrade heeltemal ignoreer, wat niks oor *hierdie* raaisel bewys nie. Die klassieke literatuur het twee standaardherstelwerk.

Die palet. Voeg een ekstra ry van N selle by die versteekte rooster — ’n palet wat Alice met die simbole 1…N in ’n vaste openbare volgorde vul, en dan saam met alles anders hernoem, sodat dit $\sigma(1)…\sigma(N)$ bevat. Bob se ewekansige uitdaging het nou een ekstra opsie. Benewens ’n ry, kolom, blok of gadget om oop te maak, kan hy **die palet plus een leidraadsel** kies. Alice maak albei oop; die palet onthul daardie ronde se hernoeming, en Bob kontroleer dat die leidraadsel presies die hernoemde weergawe van die gedrukte leidraad toon. Dit bly nulkennis omdat Bob net σ leer — wat elke ronde vars gekies word en op sy eie waardeloos is — en die waarde van ’n sel wat hy reeds uit die raaisel geken het. Niks oor die geheime selle lek nie, en ’n simulator kan die aansig namaak deur ’n ewekansige σ te kies. Dit is geldig omdat ’n bedrieglike Alice met ’n vaste waarskynlikheid per ronde gevang word, en rondes herhaal word totdat die twyfel verwaarloosbaar is.

Kompileer die leidrade weg. ’n Meer strukturele variant verwyder die spesiale uitdaging in plaas daarvan om dit by te voeg. In plaas daarvan om die leidraadwaarde te *verifieer*, dwing dit met verskilbeperkings af: koppel die leidraadsel aan elke paletsel behalwe die een wat sy eie waarde dra — “verskillend van $\sigma(1)$, verskillend van $\sigma(2)$, …, verskillend van alles behalwe $\sigma(5)$.” Die enigste simbool wat die sel wettiglik kan bevat, is die leidraad s’n. Elke beperking is nou weer van die tipe “hierdie twee verskil” — invariant onder hernoeming en op presies dieselfde manier as ’n ry kontroleerbaar. Dit is dieselfde skuif wat vir voorafgekleurde hoekpunte in die klassieke grafiekkleurprotokol gebruik word, en dit is die gees van die woord *gadgets* hierbo: in die MegaSudoku-as-SAT-prentjie word die leidrade soos elke ander beperking in ongelykheidsgadgets gekompileer.

Die fisiese protokol. Die werklike kaartprotokol vir Sudoku (Gradwohl, Naor, Pinkas en Rothblum, 2007) gebruik glad geen hernoeming nie en hanteer die leidrade voordat die verberging selfs begin. Vir elke sel lê Alice drie identiese kaarte met die sel se waarde neer

> — gesig na onder vir geheime selle, maar **gesig na bo vir leidraadselle**, sodat Bob met sy eie oë sien dat die leidrade gerespekteer word voordat die kaarte omgedraai word. Daarna gaan een kaart uit elke sel in sy ry se pakkie, een in sy kolom s'n en een in sy blok s'n; elke pakkie word geskommel en oopgemaak, en Bob kontroleer dat dit al N simbole bevat. Die skommeling vernietig die posisie-inligting (dit is die nulkennis), maar die leidrade is reeds by die uitdeel vasgespyker.
> Hoe dit ook al gedoen word, die les is dieselfde een waarna hierdie artikel telkens terugkeer: 'n nulkennisprotokol vereis noukeurige rekenskap van *watter* feite die verberging oorleef. Hernoeming behou "almal verskillend" en wis "is gelyk aan 5" uit — dus moet "is gelyk aan 5" op 'n ander manier teruggesmokkel word.

Dit is nie die protokol in die artikel nie. Dit is die denkmodel vir klassieke nulkennis:

- Alice en Bob gaan heen en weer.
- Bob kies ewekansige kontroles.
- Alice onthul net plaaslike konsekwentheid, nie die hele oplossing nie.
- Die privaatheidsbewys werk deur te wys dat Bob se aansig sonder Alice se geheime oplossing gegenereer kon gewees het.

Klassieke nulkennis is dus rondom 'n positiewe feit gebou:

'n Simulator bestaan werklik.

Verwyder nou die gemaklike dele. Alice stuur een bewysstring en stap weg. Daar is geen vertroude opstelling nie, geen gedeelde ewekansige string wat vooraf voorberei is nie, en Bob mag nooit 'n vals raaisel aanvaar nie. Dit is die omgewing waarin klassieke nulkennis nie kan oorleef nie.

Nog een karakter is nodig voor die truuk. Kies 'n **reëlboek**: 'n formele bewysstelsel, in die logikus se sin — 'n vaste stel aksiomas plus meganiese reëls om geskrewe wiskundige bewyse te kontroleer. ZFC, die standaardaksiomas van wiskunde, is die klassieke voorbeeld. Alles van hier af word relatief tot 'n voorafgekose reëlboek gestel, en die keuse is buigsaam: die konstruksie werk vir enige reëlboek wat jy vasstel, ZFC ingesluit.

('n Nota oor woorde, ontleen aan die artikel self: "bewysstelsel" beteken hier altyd dié reëlboek — die formele stelsel wat wiskundige bewyse kontroleer — nooit die boodskappe wat Alice stuur nie. Alice en Bob se masjinerie word "die bewyser en die verifieerder" genoem.)

Die Gödel-styl-weergawe behou die mega-Sudoku-verhaal maar verander die bewys.

Kies 'n tweede beperkingstelsel van dieselfde vertoonde grootte en noem dit **D**. Vir die verhaal is S en D twee MegaSudoku(n)-raaisels in dieselfde formaat. Agter die skerms kon D as 'n moeilike logiese formule van 'n ander grootte begin het; indien nodig kan dit met onskadelike dummy-beperkings opgevul word om dieselfde rooster te pas. D word gebou uit 'n logiese formule wat werklik **onbevredigbaar** is: daar is geen moontlike toekenning van waardes wat al sy beperkings waar maak nie, net soos 'n gebreekte raaisel geen wettige voltooide rooster het nie. 'n Speelgoedvoorbeeld sou

’n formule wees wat sowel “X is waar” as “X is onwaar” vereis. D het dus geen geldige invulling nie.

Maar D mag nie ’n gebreekte raaisel wees waarvan die fout *maklik blootgelê* kan word nie. Die speelgoedvoorbeeld hierbo faal: enige reëlboek weerlê “X en nie-X” in een reël. D moet vals wees op ’n manier wat die gekose reëlboek nie met ’n kort argument kan sertifiseer nie. As die reëlboek D met ’n kort bewys kon weerlê, sou die verhaal hieronder ineenstort: die alternatiewe roete wat moontlik bewyse sonder Alice se geheim kon produseer, sou formeel uitgesluit kon word, en daarmee saam die privaatheidswaarborg. D word dus gekies uit ’n familie wat die vaste reëlboek nie doeltreffend kan weerlê nie: daar is geen kort bewys, binne daardie reëlboek, dat D geen oplossing het nie.

Alice se eenboodskapbewys gaan dan oor ’n óf/óf-stelling:

> óf die werklike mega-Sudoku S het ’n oplossing, óf die lokmiddel D het ’n oplossing.

Dit is die logiese skakel. D word **nie** op ’n magiese manier gegenereer wat S waar maak nie. Die bewys redeneer nie “D het geen oplossing nie, dus het S ’n oplossing” nie. Dit bewys die disjunksie **S of D**. Perfekte geldigheid sê ’n vals disjunksie kan geen geldige bewys hê nie. Omdat D in werklikheid vals is — dit het geen oplossing nie — is die enigste manier waarop die disjunksie waar kan wees dat S waar is. As die bewys dus aanvaar word, moet S ’n oplossing hê. Die lokmiddel kan nie ’n vals S waar maak nie.

Maar vir die nulkennisagtige deel, vra wat sou gebeur as D *wel* ’n oplossing gehad het. Daardie lokmiddeloplossing sou as ’n alternatiewe getuie werk. Dit sou iemand toelaat om bewyse te produseer sonder om Alice se werklike mega-Sudoku-oplossing te ken — met ander woorde, ’n simulator. In werklikheid het D geen oplossing nie, dus is hierdie simulatorroete toe. Die punt is dat die reëlboek nie doeltreffend kan bewys dat dit toe is nie.

D het dus twee take. Vir **geldigheid** is D vals, sodat ’n geldige bewys van “S of D” S afdwing. Vir **effektiewe nulkennis** is D moeilik om te weerlê, sodat die reëlboek nie vinnig die lokmiddelroete kan uitsluit wat simulasie moontlik sou gemaak het nie.

Die sekuriteitstoets is dus nie meer:

> Kan ons bewys dat ’n simulator werklik bestaan?

Dit word:

> Kan jou reëlboek doeltreffend bewys dat die simulator onmoontlik is?

As die antwoord nee is, volg iets verrassend sterk: elke sekuriteitswaarborg wat (a) waargeneem kan word deur ’n toets uit te voer, en (b) binne daardie reëlboek bewysbaar uit die bestaan van ’n simulator volg, geld werklik. ’n Suksesvolle aanval op enigeen daarvan sou self neerkom op die ontbrekende kort weerlegging, en dié kort weerlegging bestaan nie. Dit is die “effektiewe” deel van effektief nulkennis.

Die klaskamerkontras is dus:

Klassieke nulkennis: die bewyse is veilig omdat ’n simulator bestaan.

Gödel-styl effektiewe nulkennis: die bewyse word vir waarneembare sekuriteitstoetse as veilig behandel omdat die reëlboek nie doeltreffend kan bewys dat die simulator onmoontlik is nie.

Die tweede aanspraak is swakker. Dit is ook waarom die artikel die drie eienskappe kan behou wat die klassieke weergawe gebreek het: een boodskap, geen opstelling en perfekte geldigheid.

Die nuwe toets: jy kan nie bewys dat die simulator afwesig is nie

Ilango se verslapping verander die vraag.

Klassieke nulkennis vra:

> Bestaan ’n simulator?

Effektief nulkennis vra iets swakker:

> Kan jou gekose reëlboek doeltreffend bewys dat geen simulator bestaan nie?

Dit klink soos ’n tegniese uitvlug, maar dit is die kernidee. Die konstruksie leef in ’n vreemde toestand: ’n simulator bestaan in werklikheid nie — die artikel is uitdruklik hieroor — maar die reëlboek wat jy vasgestel het kan nie doeltreffend bewys dat dit nie bestaan nie. As elke slegte gevolg waaroor jy omgee so ’n weerlegging sou vereis, gedra die stelsel hom vir daardie gevolge steeds soos nulkennis.

Dit is waar Gödel inkom. Nie as versiering nie, en nie as “Gödel maak kriptografie veilig” nie. Die skakel is bewysteoreties. ’n Reëlboek word **optimaal** genoem as dit, in ’n presiese sin, die beste moontlike een is: wanneer enige reëlboek ’n formule van die relevante soort met ’n kort bewys kan weerlê, kan die optimale reëlboek dit ook doen, met ’n bewys wat hoogstens polinomiaal langer is. Krajíček en Pudlák het in 1989 vermoed dat **geen optimale bewysstelsel bestaan nie**: watter reëlboek jy ook al vasstel, ’n ander reëlboek bewys ’n sekere familie ware stellings baie bondiger. Dit is een van die sentrale oop vermoedens in bewyskompleksiteit, en dit is die eindige, kompleksiteitsteoretiese neef van Gödel se onvolledigheidstelling: sommige ware stellings het geen kort bewys in die reëlboek wat jy vasgestel het nie — nie omdat hulle in beginsel onbewysbaar is nie, maar omdat elke vaste reëlboek sommige kort ware stellings sonder kort bewyse laat.

Die artikel neem dié vermoede aan (in ’n effens sterker “oneindig dikwels”-vorm, wat standaard is wanneer vermoedens kriptografies gebruik word). Deur ’n stelling van Krajíček en Pudlák is die opbrengs konkreet: vir elke reëlboek is daar ’n ry formules wat werklik onbevredigbaar is, maar wat die reëlboek nie met kort bewyse kan weerlê nie — en, belangrik, wat ’n doeltreffende algoritme kan *genereer*. Daardie laaste eienskap, uniformiteit, verander die hele idee van ’n bestaanstelling in ’n werklike algoritme wat Alice kan uitvoer: haar lokmiddels D kom van ’n monteerlyn af, nie uit die niet nie.

Die kriptografiese skuif is om dié tekort aan bewyskrag te benut.

Wat die konstruksie doen

Hier is die artikel se konstruksie, tot sy vorm gestroop.

Stel ’n reëlboek vas — byvoorbeeld ZFC. Onder die bewyskompleksiteitsaanname bestaan daar ’n doeltreffend genereerbare ry formules wat werklik onbevredigbaar is, maar waarvoor die reëlboek geen kort bewys het dat hulle onbevredigbaar is nie.

Bou nou ’n eenboodskapbewys van hierdie vorm:

> óf die werklike stelling is bevredigbaar, óf hierdie spesiale moeilike formule is bevredigbaar.

Die spesiale moeilike formule is nie bevredigbaar nie. As die onderliggende bewysmasjinerie dus perfek geldig is, beteken aanvaarding van die boodskap steeds dat die werklike stelling waar is. Dit gee perfekte geldigheid.

Maar vir die nulkennisagtige sekuriteit, stel jou voor die spesiale moeilike formule *was* bevredigbaar. Dan kon sy getuie gebruik word om bewyse te simuleer sonder om die werklike getuie te ken. Die formule is in werklikheid nie bevredigbaar nie — maar die reëlboek kan dit nie doeltreffend bewys nie. Dit kan dus nie doeltreffend bewys dat die simulator onmoontlik is nie.

Dit is die skarnier. Die stelsel versteek nie die geheim deur ’n klassieke simulator te produseer nie. Dit versteek die geheim, vir ’n groot klas waarneembare sekuriteitstoetse, agter die reëlboek se onvermoë om te sertifiseer dat die simulator afwesig is.

Wat die artikel beweer

Die hoofstelling kom in lae. Die kernresultaat is hierdie:

Onder ’n standaard-kriptografiese aanname — die bestaan van **nie-interaktiewe getuie-ononderskeibare bewyse** (*non-interactive witness indistinguishable proofs*), goed bestudeerde objekte wat uit verskeie gevestigde pakkette aannames volg — en onder die bewyskompleksiteitsvermoede dat **geen (oneindig-dikwels) optimale bewysstelsel bestaan nie**, konstrueer die artikel, vir elke keuse van reëlboek, ’n eenboodskap-bewyser en -verifieerder vir NP/SAT met **perfekte geldigheid** en geen opstelling, wat effektief nulkennis relatief tot daardie reëlboek is. (NP/SAT is die standaard-“moeilikste gemeenskaplike noemer” van raaiselagtige probleme; mega-Sudoku is een kostuum wat dit dra.)

Vir die breër aanspraak oor die behoud van falsifiseerbare sekuriteitseienskappe voeg die artikel nog een standaardaanname by, die derandomiseringsgeloof **P = BPP** (rofweg: ewekansigheid gee

algoritmes geen noodsaaklike ekstra krag nie).

Uit stellingstaal vertaal:

- Die bewys is een boodskap.
- Daar is geen vertroude opstelling nie.
- Vals stellings kan nie bewys word nie.
- Die bewyser is nie klassieke nulkennis nie — dit het geen simulator nie.
- Maar elke falsifiseerbare, spelgebaseerde sekuriteitsgevolg van klassieke nulkennis kan in hierdie omgewing bereik word.

"Falsifiseerbaar" maak saak. Dit beteken 'n sekuriteitsmislukking kan getoets word deur 'n teenstander in 'n spel te laat speel. Baie kriptografiese sekuriteitsdefinisies het dié vorm: kan die teenstander tussen twee enkripsies onderskei, 'n funksie omkeer, 'n getuie herwin of 'n bepaalde eksperiment wen? Die stelling gee vir elke falsifiseerbare eienskap, een op 'n slag, 'n bewyser. 'n Enkele bewyser wat *elke* falsifiseerbare eienskap gelyktydig geniet, is waarskynlik onmoontlik — die ou herbruikbaarheidsaanval ("Bob kan die bewys vir ander wys") is self 'n falsifiseerbare eienskap, en dit faal werklik hier. Die artikel stel voor dat 'n enkele bewyser moontlik al die *natuurlike* falsifiseerbare eienskappe kan dek — dié wat werklik in kriptografiese praktyk voorkom — maar daardie deel is 'n voorwaardelike stelling wat op 'n informele begrip van "natuurlik" plus 'n uitdruklike vermoede berus. Die waarborg mik na waarneembare mislukkings, nie elke filosofiese of simulasiegebaseerde betekenis van geheimhouding nie.

Een konkrete gevolgtrekking is die moeite werd om te noem: die konstruksie lewer die eerste nie-interaktiewe **getuie-verbergende** (*witness hiding*) bewyse met 'n uniforme bewyser — "'n bewys van 'n raaisel help jou nie om sy oplossing te vind nie", met geen interaksie en geen opstelling — 'n beskeie-klinkende objek wat dekades lank konstruksie weerstaan het.

Wat dit nie sê nie

Dit is die afdeling wat die stuk eerlik hou.

Dit sê **nie** die ou onmoontlikheidstellings was verkeerd nie. Die konstruksie vermy hulle deur die definisie te verander.

Dit gee **nie** gewone, klassieke nulkennis met geen interaksie, geen opstelling en perfekte geldigheid nie. Die artikel sê uitdruklik dat die gekonstrueerde bewyser geen simulator het nie.

Dit beteken **nie** dat die bewys nie hergebruik kan word nie. 'n Eenboodskapbewys kan steeds aan iemand anders gewys word; die artikel behou nie ontkenbaarheid-agtige eienskappe nie. (Nie-interaktiewe nulkennis met 'n vertroude opstelling het dieselfde beperking.)

Dit beteken **nie** dat dit 'n praktiese protokol gereed vir ontplooiing is nie. Dit is kompleksiteitsteorie en kriptografiese grondslagwerk. Die resultaat steun op groot aannames uit bewyskompleksiteit en kriptografie, en die konstruksie gaan oor wat in beginsel moontlik is.

Dit maak **nie "Gödel" 'n magiese sekuriteitsprimitief nie**. Die Gödel-skakel loop deur bewysstelsels, optimale bewysstelsels en eindige analoë van onvolledigheid. Die bruikbare intuïsie is nie "onvolledigheid beskerm jou wagwoord" nie. Dit is: as 'n reëlboek nie doeltreffend kan bewys dat 'n simulator onmoontlik is nie, kan aanvalle wat so 'n bewys sou vereis op die vlak van sekuriteitsdefinisies geblokkeer word.

Waarom dit tog interessant is

Kriptografie verander moeilikheid dikwels in veiligheid. Faktorisasie is moeilik, dus word RSA-agtige aannames nuttig. Roosterprobleme is moeilik, dus word roosterkriptografie nuttig. Hier is die moeilikheid vreemder: nie "dit is moeilik om 'n geheim te bereken" nie, maar "dit is moeilik om te bewys dat 'n bepaalde bewysobjek nie kan bestaan nie".

Dit is waarom die artikel ongewoon voel. Dit behandel aksiomas en reëlboeke amper soos kriptografiese hulpbronne. Die gewone onmoontlikheid sê daar is 'n spanning tussen geldigheid en simulasie. Ilango se skuif plaas dié spanning agter 'n bewysteoretiese gordyn: die simulator is afwesig, maar die formele stelsel kan daardie afwesigheid nie doeltreffend blootlê nie.

Vir 'n leser is die verrassende deel nie dat dit vandag se nulkennisstelsels gaan vervang nie. Dit sal waarskynlik nie, ten minste nie direk nie. Die verrassende deel is dat 'n beperking uit wiskundige logika konstruktief gebruik kan word: nie net as 'n muur nie, maar as 'n soort dekking.

Hoe sterk is die bewys?

Dit is 'n stellingartikel, dus beteken "bewys" iets anders as in 'n biologie- of sterrekundeartikel. Die vraag is nie of 'n eksperiment gerepliseer is nie. Die vraag is of die definisies, aannames en bewysketting die aanspraak dra.

Die bewys is formeel, en die artikel is uitdruklik oor sy aannames. Die aannames is nie terloops nie. Nie-interaktiewe getuie-ononderskeibare bewyse is standaardobjekte in kriptografie en volg uit verskeie gevestigde pakkette aannames. Die vermoede dat geen optimale bewysstelsel bestaan nie is 'n sentrale vermoede in bewyskompleksiteit. P = BPP is 'n standaard-derandomiseringsgeloof wat net vir die breër stelling oor falsifiseerbare eienskappe gebruik word.

Die artikel voer ook aan dat die aannames die regte prys is, nie 'n arbitrêre steierwerk nie: dit bewys 'n omgekeerde resultaat wat wys dat hulle in wese noodsaaklik is — as konstruksies soos hierdie hoegenaamd bestaan, moet nie-interaktiewe getuie-ononderskeibare bewyse bestaan, en (gegewe standaard-eenrigtingfunksies) kan geen optimale bewysstelsel bestaan nie. En die aannames is "wenwen": om enigeen daarvan te weerlê sou self 'n grensverskuiwende ontdekking in bewyskompleksiteit, kriptografie of kompleksiteitsteorie wees.

Maar omdat die resultaat voorwaardelik is, is die sekerheid daarvan ook voorwaardelik. As dié aannames faal, verander die interpretasie van die stelling. En selfs as die aannames hou, is die waarborg

nie volle klassieke nulkennis nie; dit is die artikel se verslapte, bewysteoretiese weergawe.

Die regte vertrouensprofiel is dus hoog dat die artikel ’n samehangende voorwaardelike moontlikheidsresultaat vestig; matig dat sy aannames die kriptografiese wêreld waarin ons werklik leef beskryf; en laag vir enige onmiddellike praktiese gevolg.

Waarom dit saak maak

Die artikel maak ’n roete oop wat veronderstel was om gesluit te wees.

Klassieke teorie sê: volle nulkennis kan nie sonder opstelling in een boodskap ingedruk word nie, en kan nie perfekte geldigheid hê nie. Ilango se artikel sê: as ons vra vir die gevolge van nulkennis wat in sekuriteitspele getoets kan word, en as ons toelaat dat die sekuriteitsdefinisie afhang van wat ’n reëlboek wel of nie doeltreffend kan weerlê nie, kan baie van die nuttige gedrag herwin word — met een boodskap, geen opstelling en perfekte geldigheid.

Dit is nie ’n klein definisie-aanpassing nie. Dit is ’n ander manier om oor kriptografiese waarborge te dink. Vra nie net wat bestaan nie; vra wat jou reëlboek kan uitsluit. Behandel onbewysbaarheid nie net as ’n filosofiese irritasie nie; gebruik dit as struktuur.

Die praktiese wêreld verander dalk nie môre nie. Maar die konseptuele kaart verander wel. Daar is nou ’n formele sin waarin “niemand kan doeltreffend bewys dat die geheim gelek het nie” sterk genoeg kan wees om baie van die spelgebaseerde beskermings te herwin wat ons van “die geheim het nie gelek nie” wou hê.

Daarom hoort Gödel in die titel.

Kortliks

Nulkennisbewyse laat ’n bewyser ’n verifieerder oortuig dat ’n stelling waar is sonder om die getuie te onthul. Klassieke onmoontlikheidsresultate sê nulkennis kan nie sonder opstelling in een boodskap saamgepers word nie en kan nie perfekte geldigheid hê nie. Rahul Ilango se artikel weerlê dié onmoontlikhede nie. Dit definieer ’n swakker begrip, effektief nulkennis: in plaas daarvan om te vereis dat ’n simulator werklik bestaan, vereis dit dat ’n gekose bewysstelsel — ’n formele reëlboek soos ZFC — nie doeltreffend kan bewys dat geen simulator bestaan nie. Onder belangrike aannames uit kriptografie (nie-interaktiewe getuie-ononderskeibare bewyse) en bewyskompleksiteit (geen optimale bewysstelsel bestaan nie), konstrueer die artikel eenboodskap-bewysers vir NP/SAT met geen opstelling en perfekte geldigheid wat, eienskap vir eienskap, die falsifiseerbare, spelgebaseerde gevolge van nulkennis bereik. ’n Enkele bewyser wat al sulke “natuurlike” eienskappe dek is ’n verdere, gedeeltelik vermoedelike uitbreiding — en om letterlik elke falsifiseerbare eienskap te dek is waarskynlik onmoontlik omdat bewyse herbruikbaar bly. Die resultaat is teoreties en voorwaardelik, nie ’n ontplooide primitief nie, maar dit wys ’n nuwe manier om bewysteoretiese onbewysbaarheid as ’n kriptografiese hulpbron te gebruik.

Nugtere beoordeling

Wat die artikel wys: Onder die verklaarde aannames kan eenboodskap-, opstellinglose, perfek geldige bewysers vir NP/SAT gebou word wat effektief nulkennis relatief tot enige gekose bewysstelsel is, en wat elke falsifiseerbare, spelgebaseerde gevolg van klassieke nulkennis kan bereik.

Wat aannemelik is maar nie onvoorwaardelik bewys nie: Dat die nodige aannames uit bewyskompleksiteit en kriptografie waar is. Dit is ernstige, goed bestudeerde aannames — en die artikel wys dat hulle in wese noodsaaklik sowel as voldoende is — maar dit bly aannames.

Wat dit nie wys nie: Klassieke nulkennis met geen interaksie, geen opstelling en perfekte geldigheid; ’n praktiese stelsel gereed vir ontplooiing; ontkenbaarheid of nie-herbruikbaarheid van bewyse; of dat Gödel se onvolledigheidstelling op sigself kriptografie beveilig.

Belangrikste beperkings: Die waarborg is ’n verslapping van nulkennis; die breedste weergawe steun op verskeie aannames; die aansprake oor ’n enkele universele bewyser bly gedeeltelik vermoedeliks; en die resultaat is hoofsaaklik grondslagwerk.

Hoeveel vertroue behoort ’n algemene leser hierin te hê? Hoë vertroue dat dit ’n belangrike voorwaardelike teorieresultaat is as die definisies aanvaar word. Matige vertroue dat die aannames die werklikheid vasvang. Lae vertroue vir onmiddellike praktiese ontplooiing. Die veilige slotsom is: die artikel breek nie die nulkennis-onmoontlikhede nie; dit vind ’n nuwe bewysteoretiese manier om rondom die dele te werk wat vir baie sekuriteitspele saak maak.

Bronne

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`