



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

एक cryptographic proof अपने रहस्य को इस तरह छपासकता है कि “गैम्बल simulator” की अनुपस्थिति सप्रति करना कठिन हो जाए

Zero-knowledge proofs किसी कथन को बिना witness उजागर किए सप्रति करने देते हैं। Classical theory के अनुसार पूर्ण अर्थ में यह एक message, बिना trusted setup और perfect soundness के संभव नहीं है। Rahul Ilango का शोधपत्र उस असंभवता को मद्तिमान ही वह लक्ष्य बदलता है। वास्तविक simulator मौजूद होने की मंजा के बावजूद वह यह मंजाता है कि चुनी गई proof system यह कुशलतम पूर्वक सप्रति न कर सके कि simulator मौजूद नहीं है। Proof complexity और cryptography से जुड़ी बीबीएमयताओं के तहत यह zero-knowledge के falsifiable, game-based परिणामों को गुण-दर-गुण वमस पमे के लिए पर्याप्त है। यह इंटरनेट में सीधे लगा देने वाला primitive नहीं बल्कि proof theory का एक तरीका है जिसमें गणतीय अप्रमण्यता cryptographic cover बनती है।

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

चल यह सिद्ध करना नहीं है कि रहस्य छपा हुआ है

शून्य-जुझ के सबसे सरल रूप से शुरू करें।

Alice Bob को यह विश्वास दिलाना चाहती है कि सुडेक् puzzle का समझ है। यदि वह समझ भेज दे, तो Bob मना जाएगा लेकिन puzzle खत्म हो जाएगा। उसे कुछ अजीब चाहिए: यह प्रमाण कि समझ मौजूद है, समझ बताए बना।

यही शून्य-जुझ प्रमाण कावद्दा है। प्रूवर (Alice) वेरिफायर (Bob) को विश्वास दिलाना है कि कथन सत्य है, लेकिन कथन के सत्य होने के अलावा कुछ reveal नहीं करता।

समस्या यह है कि इस वजह की कीमत है। समझ गणति प्रमाण में दो सुविधाजनक विशेषताएँ होती हैं। पहला वह एक संदेश हो सकता है: आप प्रमाण लिखते हैं, देते हैं और बात खत्म। दूसरा उसमें पूर्ण soundness हो सकती है: असत्य कथन का कोई वैध प्रमाण होता ही नहीं। शस्त्रीय impossibility परणित बताते हैं कि शून्य-जुझ में इन दोनों सुविधाओं को इस रूप में बनाए रखना संभव नहीं— न दोनों को एक साथ, और कुछ परिस्थितियों में न हर एक को अलग से।

पहला शून्य-जुझ प्रमाण को बतचित चाहिए। यदि Alice एक ही संदेश भेजती है, और पहले से कई trusted सेटअप arranged नहीं है, तो शून्य-जुझ गारंटी collapse हो जाती है—चहे बदले में आप सड्डनेस जतिनी भी कम करने को तैयार हो।

दूसरा शून्य-जुझ प्रमाण को टर्न के लिए थोड़ी tolerance चाहिए। पूर्ण सड्डनेस माँगना इंटरैक्शन को भी चुपचाप खत्म कर देता है: ऐसा वेरिफायर जिसे उसके यह चूँकि वकिल्प कुछ भी हो कभी fool नहीं किया जा सकता वे वकिल्प पहले से सुधार ही कर सकता है—और वेरिफायर predictable होते ही Alice सारे उत्तर एक संदेश में दे सकती है, वही ममला जो पहले ही टूट चुका था।

Rahul Ilango का शेषपत्र इस double दीक्षा के आसपास रस्ता खोजता है। दीक्षा को नकार नहीं और असंभव परिस्थिति में शस्त्रीय शून्य-जुझ पैदा करने का दिखाकर के नहीं। कदम अधिक subtle है: “reveals nothing” का अर्थ कमजोर करना लेकिन इस तरह कि cryptographers जिन्हें सुरक्षा गुण को वास्तव में परीक्षण कर सकते हैं वे बची रहें।

परणित कानन है व्यक्त हर कि रूप से शून्य-जुझ।

A proof without leaking the witness

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

blocked door 1

interaction

blocked door 2

trusted setup

blocked door 3

imperfect
soundness

the route

the rulebook cannot
efficiently refute the
simulator

Boundary: not classical zero-knowledge; effectively zero-knowledge under a chosen proof system.

शून्य-ज्ञान तम दरवाजों पर blocked है — इंटरैक्शन, trusted सेटअप और अपूर्ण सप्रुडनेस। Ilango की निर्माण एक अलग दरवाजे से निकलती है: नियम-पुस्तक सिम्युलेटर को कुशलतपूर्वक खंडन करना नहीं कर सकता।

Original diagram — The Clean Paper CC BY 4.0

Classical privacy vs effective privacy

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

classical zero-knowledge

positive claim

A simulator exists and can fake the verifier's view without the witness.

effectively zero-knowledge

weaker claim

Your chosen proof system cannot efficiently prove that no simulator exists.

Boundary: the construction preserves testable consequences, not the full simulator guarantee.

शास्त्रीय शून्य-ज्ञान पूछता है कि सिम्युलेटर मौजूद है या नहीं। “व्यवहारिक रूप से शून्य-ज्ञान” केवल यह पूछता है कि चुना हुआ नियम-पुस्तक कुशलतपूर्वक सप्रुडनेस कर सकता है या नहीं। कि सिम्युलेटर मौजूद नहीं हो सकता। यही कमजोर सवाल निर्माण को एक

संदेश, no सेटअप और पूर्ण सफ़ंडनेस रखने देता है।

Original diagram — The Clean Paper CC BY 4.0

पुरमापरीक्षण: समियुलेटर मौजूद है

शून्य-ज्जम को formalize करने का शस्त्रीय तरीका एक fictional helper इस्तेमाल करता है जिसे **समियुलेटर** कहते हैं।

वचन यह है: Jane की कल्पना करें, जिसे Alice का रहस्य नहीं पता। यदि Jane पूरी तरह अपने दम पर ऐसे प्रमाण उत्पन्न कर सकती है जो Bob को Alice से मिलने वाले प्रमाण जैसे ही दिखें, तो Alice के प्रमाण ने Bob को कुछ नया नहीं सिखाया। Jane Alice के रहस्य के बिना ही वही experience fake कर सकती थी।

इसलिए शस्त्रीय शून्य-ज्जम actual समियुलेटर माँगा है। एक कुशल एल्गोरिथम सब में मौजूद होना चाहिए जो रहस्य — jargon में *वटिनेस* — जमे बिना fake-looking प्रमाण बना सके। सुडोकू में वटिनेस बस solved ग्रिड है।

यह definition शक्तिशाली है, लेकिन old impossibility ठीक यही कहती है। Intuition यह है: सचमुच non-interactive प्रमाण सिर्फ एक string है। Bob के पास string आने के बाद वह उसे किसी और को दिखा सकता है; उसे कখন दूसरो को सिद्ध करने की ability मल गई, जो पहले ही “nothing” से अधिक लगती है। शस्त्रीय theorems इसी intuition को ऊपर की impossibilities में sharpen करती हैं।

इस paper के लिए तीन अनविद्य properties

शोधपत्र के title में तीन बघाएँ हैं:

No इंटरैक्शन: Alice एक प्रमाण string भेजती है। Back-और-forth प्रोटोकॉल नहीं।

No सेटअप: Alice और Bob किसी trusted समग्र संदर्भ string या पहले से arranged सार्वजनिक randomness पर निर्भर नहीं। “Non-interactive शून्य-ज्जम” कहलमे वाले कई प्रणालियाँ फिर भी सेटअप इस्तेमाल करते हैं; यहाँ मतलब शून्य सेटअप है।

पूर्ण सफ़ंडनेस: असत्य कथन का कोई वैध प्रमाण नहीं। “लगभग कभी accept नहीं होगा” नहीं वैध प्रमाण अस्तित्व में हीन है।

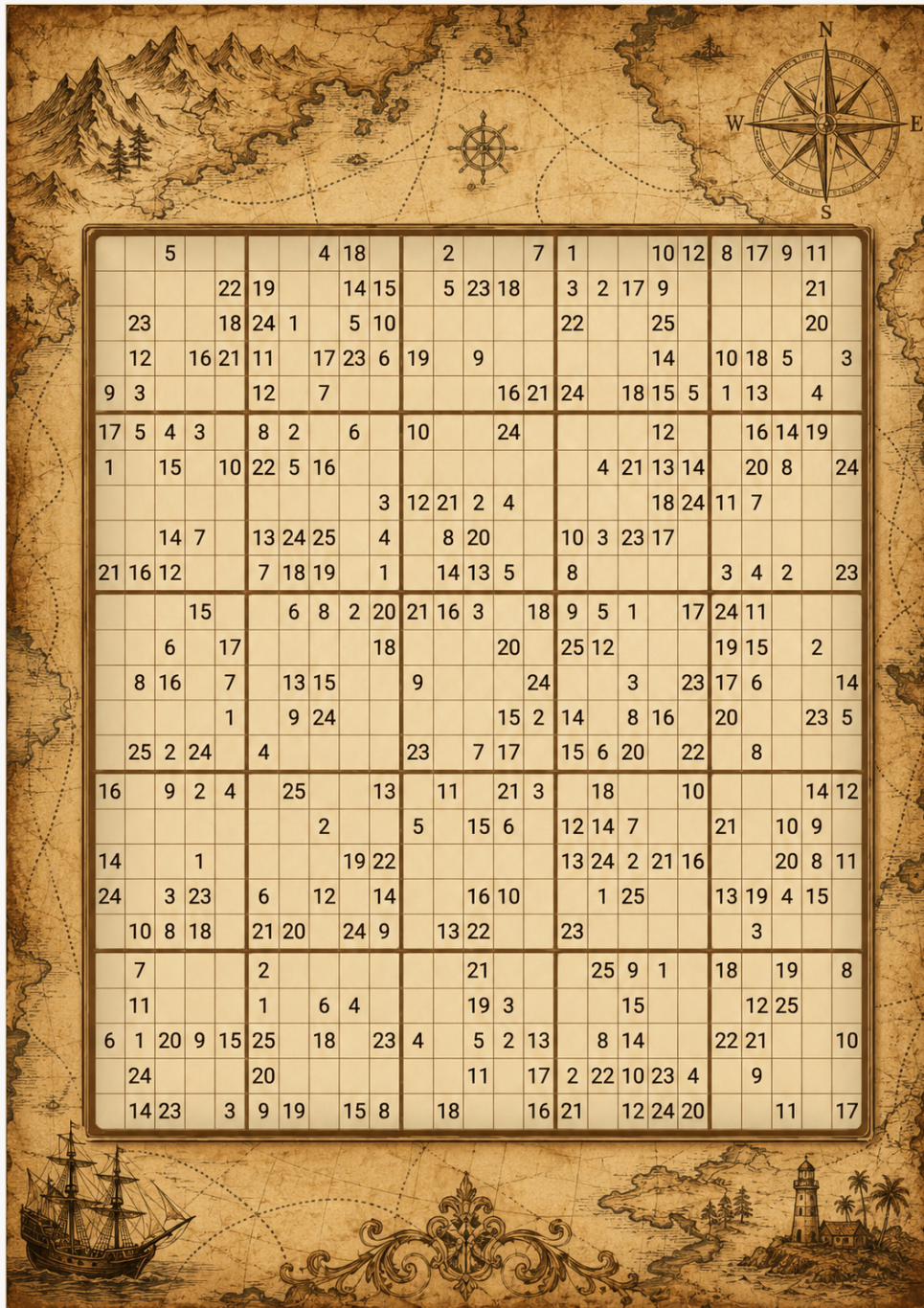
समग्र written mathematics में यही तीन गुण होती हैं — और ऊपर जैसा समझाया शस्त्रीय शून्य-ज्जम इन्हें सघ नहीं रख सकता।

फर्क को MegaSudoku से महसूस करें

यह फर्क समझने का ज़रूरी बूझकर simplified तरीका है।

उपमा के गंभीर हिससे में समग्र 9-by-9 सुडोकू न लें। वह बहुत छोटा और finite है: computer उसे हल कर सकता है या सिद्ध कर सकता है कि समग्र नहीं है। इसके बजाय **MegaSudoku(n)** puzzles की परीक्षा से। Usual नियम को पैमाना करें: रकना आकर n चुनें, $N = n^2$ रखें, फिर N by N ग्रिड बनाएँ जिसे n by n blocks में बाँटा गया हो और जिसमें N चहिन हों। समग्र सुडोकू सिर्फ tiny $n = 3$, $N = 9$ मसला है: 9-by-9 ग्रिड, 3-by-3 blocks और नौ चहिन। Proof-जटिलता कहनी तभी शुरू होती है जब n बढ़ सकता है, और ग्रिड अतिरिक्त गैजेट्स ले सकता है जो उसे सुडोकू के वेश में SAT सूत्र जैसा व्यवहार कराएँ। SAT सूत्र बस yes/no बघाएँ की list है: क्या variables को सत्य/असत्य assign किया जा सकता है तर्क हर

बन्नाSatisfied हो?



25x25 सुडोकू: उसके नियम finished ग्रिड reveal किए बनिजॉब किए जा सकते हैं—छुपिसमन्त्र, यमीवटिनेस, कोverify करने वाले प्रमण कादृश्य stand-in।

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

Sudoku और SAT: एक ही puzzle दो costumes में

यह दन्नाक सुडोकू “SAT सूत्र जैसाव्यवहार करना” कर सकता है metaphor नहीं। Translation देमो directions में जती है, और आसम दशापूरीलखी जा सकती है।

सुडोकू से SAT। SAT केवल सत्य/असत्य बोलता है, इसलिए हर (पंक्ति, स्तंभ, मम) triple के लिए एक boolean variable दें: $x(r,c,v)$ का अर्थ “पंक्ति r , स्तंभ c की कोशिका में मम v है।” 4-by-4 सुडोकू (2-by-2 blocks, मम 1-4) को $4 \cdot 4 \cdot 4 = 64$ variables चाहिए; शस्त्रीय 9-by-9 को 729। हर सुडोकू नियम फिर clauses के batch में बदलता है। (Clause variables याउनकी negations का OR है; पूरी सूत्र सभी clauses का और है।)
हर कोशिका में कम से कम एक मम—हर कोशिका के लिए एक clause:

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

हर कोशिका में अधिकतम एक मम—हर value-pair के लिए “दोनों ही” clause:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \dots \text{और इसी तरह सभी छह जोड़ियों के लिए।}$$

हर पंक्ति में हर मम—पंक्ति 1 और मम 3 के लिए: कम से कम एक बार,

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

और अधिकतम एक बार: $\neg x(1,1,3) \vee \neg x(1,2,3)$, और इसी तरह पंक्ति की हर जोड़ी of कोशिकाएँ के लिए।
Columns और blocks—वैसे ही batches; केवल कोशिकाएँ का समूह बदलता है। शीर्ष-left रेकना और मम 2 के लिए:

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

सम में pairwise “नहीं both” clauses।

Printed सुराग—सबसे सरल हिसा हर सुराग एकल variable वाला clause है। शीर्ष-left corner में छपे हुए 3 clause बनता है

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

इन सब का और तभी satisfiable है जब सुडोकू का समझ हो—और satisfying निर्धारण ही समझ है: जो $x(r,c,v)$ सत्य है उन्हें पढ़ें और ग्रिड भरें। 9-by-9 के लिए 729 variables और कुछ हजार clauses होते हैं, जिन्हें आधुनिक SAT solver milliseconds में हल कर देता है। सुराग clause $x(1,1,3)$ पर ध्यान दें: यह कहता है “यह कोशिका ठीक 3 है,” न कि “ये कोशिकाएँ सभी अलग हैं”—यही असमझता आगे प्रेक्लेट टपिणी में सुराग कोशिकाएँ के लिए अतिरिक्त तरकीब की जरूरत पैदा करेगी।

SAT से सुडोकू। शेषपत्र को opposite, कठिन दिखा चाहिए: मनमंता SAT सूत्र से mega-Sudoku बनाएँ जिसका समझ तभी हो जब सूत्र satisfiable हो। सुडोकू के native नियम केवल “ये कोशिकाएँ सभी अलग हैं” कह सकते हैं, इसलिए मनमंता तक कि बघाएँ को build करना पड़ता है—और यही गैजेट्स हैं। Gadget कोशिकाएँ काछोटो pre-fabricated समूहति होना है, सूत्र के हर clause के लिए एक, जिसमें designated कोशिकाएँ variables का भूमिका नभित्ती हैं (उनका symbol सत्य/असत्य encode करता है) और समूहति होना की आंतरिक बघाएँ ऐसी इंजिनियर्ड होती हैं कि legal fillings ठीक वे assignments हो जो clause satisfy करती हैं। यह NP-completeness प्रमाण की मजक craftsmanship है; समर्थकृत सुडोकू के लिए Yato और Seta ने 2003 में इसे किया था।
दोनों directions मलिकर कहते हैं कि N-by-N सुडोकू और SAT एक ही समस्या हैं, अलग costumes में। इसीसे यह लेख—और शेषपत्र—grids और चहिन के जरिए पूरे NP की कहानी कह सकते हैं।

वटिनेस अभी भी easy to तस्वीर है। Alice को mega-Sudoku का पूर्ण वैध filling पता है। Bob को विश्वास करना है कि filling मौजूद है, लेकिन Alice उसे reveal नहीं करना चाहती। Whole filling भेजने पर Bob convinced होगा रहस्य खत्म।

शस्त्रीय शून्य-ज्जम संस्करण में Alice और Bob आपस में संबद्ध करते हैं। पुराने ढंग का एक सरल मजसकि मॉडल ढकी

हुई टाइलोकाइस्तेमल करता है। Alice हल किए हुए ग्रडि कोछपिती है, हर दौर से पहले प्रतीको के नम गुप्त रूप से बदलती है और Bob कोकसीयद्दृच्छिक स्थानीय बन्ना—पंक्ति, स्तंभ, खंड याकसीछोटे गैजेट—कीजँच करने देती है। खेलीगई कोशकियों में सभीप्रतीक अलग-अलग होतोBob कावश्विप्त बढता है। फिर सब कुछ दोहरादक दियाजता है और अगले दौर के लिए प्रतीको के नम फिर बदल दिए जते हैं। (एक पेच यह है कि पहले से छपे संकेतो के लिए अतिरिक्त तरीके चहिए, क्येकि नम बदलने से वे भीछपि जते हैं। नीचे टपिपणीमें शस्त्रीय प्रटेक्ल कावस्त्वकि समझन दियागया है; आगे की चर्चाके लिए यह सरल तस्वीर पर्यप्त है।)

Classical protocols clue cells कोवस्त्व में कैसे संभलते हैं

नम बदलनातरीके कीबलइंड spot है। पंक्ति, स्तंभ और खंड नियम कहते हैं “ये कोशकिएँ सभीअलग हैं,” और सभीअलग चहिन के कसीभीनम बदलनाके बढ भीसत्य रहता है। लेकिन सुरा कहता है “इस कोशकामें ठीक 5 है,” और नम बदलनाके बढ Bob केवल $\sigma(5)$ —कुछ masked symbol—देखता है, नम बदलना σ जमे बना। वह जँच नहींकर सकता यदि इसे ठीक न करे तो Alice छपे हुए सुरा ignore करके some वैध ग्रडि काप्रमाण दे सकती है, जोइस puzzle के बारे में कुछ सद्धि करनानहीकरता। शस्त्रीय literature में दोममक repairs हैं।

Palette। छपिग्रडि में N कोशकिएँ कीअतिरिक्त पंक्तिजोड़ें—palette—जसि Alice सवजनकि स्थिर ऑर्डर में चहिन $1 \dots N$ से भरती है और फिर बक्कीसबके सग rename करती है, इसलिए उसमें $\sigma(1) \dots \sigma(N)$ होते हैं। Bob के यद्दृच्छिक चुनैतीमें अब अतिरिक्त option है। पंक्ति, स्तंभ, खंड यागैजेट चुनने के अलमावह **palette plus** एक सुरा कोशकाचुन सकता है। Alice दोमोखेलती है; palette उस दौर कीनम बदलनाबतती है और Bob जँच करता है कि सुरा कोशकाछपे हुए सुरा काठीक renamed संस्करण दखिती है। यह शून्य-ज्जम रहता है क्येकि Bob केवल σ सीखता है—हर दौर fresh draw, अकेले बेकर—और उस कोशकाकीमम जसि puzzle से पहले हीजमताथा। रहस्य कोशकिएँ के बारे में कुछ रसिग नहींहोता और समियुलेटर यद्दृच्छिक σ draw करके view fake कर सकता है। सडंडनेस इसलिए है कि cheating Alice स्थिर संभननासे हर दौर पकड़ीजती है, और rounds तब तक repeat होते हैं जब तक doubt negligible न हो।

सुरा कोcompile away करना। अधिक संरचनत्मक variant विशेष चुनैतीजोड़ने कीबजय उसे हटादेता है। सुरा मम कोverify करने कीबजय अंतर बन्नाएँ से force करें: सुरा कोशकाकोpalette कीहर कोशकासे जोड़ें सविग उसकी अपनीमम वालीकोशकाके—“ $\sigma(1)$ से अलग, $\sigma(2)$ से अलग, ..., $\sigma(5)$ कोछोड़कर बक्कीसबसे अलग।” तब legally वहीsymbol बचता है जोसुरा का है। अब हर बन्नाफिर “ये दोअलग हैं” type की है—नम बदलनाinvariant, पंक्ति की तरह checkable। शस्त्रीय graph-coloring प्रटेक्ल में pre-colored vertices के लिए यहीmanoeuvre इस्तेमल होता है, और ऊपर गैजेटs काspirit यही है: MegaSudoku-as-SAT तस्वीर में सुरा भीबक्कीबन्नाएँ कीतरह inequality गैजेटs में compile होते हैं।

भौतिक प्रटेक्ल। सुडोका कावस्त्वकि दुनियाcard प्रटेक्ल (Gradwohl, Naor, Pinkas और Rothblum, 2007) नम बदलनाइस्तेमल नहींकरताऔर hiding शुरू हमे से पहले सुरा settle कर देता है। हर कोशकाके लिए Alice समम मम वाले तीम identical cards रखती है—रहस्य कोशकिएँ के लिए face-down, लेकिन सुरा कोशकिएँ के लिए face-up, तक्कि Bob अपनीआँखोसे देख सके कि cards flip हमे से पहले सुरा respected हैं। फिर हर कोशकाकाएक card पंक्ति packet में, एक स्तंभ packet में और एक खंड packet में जता है; हर packet shuffle और reveal होता है, और Bob जँच करता है कि उसमें सभीN चहिन हैं। Shuffling position जमकरीdestroy करती है—यहीशून्य-ज्जम है—लेकिन सुरा dealing समय में पहले ही nail down होचुके थे।

कसीभीतरके में सबक वही है जिस पर यह लेख बार-बार लैटता है: शून्य-ज्जम प्रटेक्ल इस बात कीसन्नधन bookkeeping है कि hiding के बढ कँम-सेतथ्य survive करते हैं। नम बदलना“सभीअलग” बचती है और “equals 5” मटिती है—इसलिए “equals 5” कोदूसरे तरके से वप्त लमापड़ता है।

यह शेषपत्र काactual प्रटेक्ल नहीं है। यह शस्त्रीय शून्य-ज्जम काममसकि मॉडल है:

- Alice और Bob back-और-forth करते हैं।

- Bob यह चूँकि जाँच चुनता है।
- Alice केवल स्थानीय consistency reveal करती है, whole समझ नहीं।
- गोपनीयता का प्रमाण दिखाता है कि Bob का view Alice के रहस्य समझ के बिना उत्पन्न किया जा सकता था।

इसलिए शास्त्रीय शून्य-ज्ञान positive fact पर built है:

सम्युलेटर वास्तव में मौजूद है।

अब comfortable हिससे हटा दें। Alice एक प्रमाण string भेजती है और चली जाती है। Trusted सेटअप नहीं पहले से shared यह चूँकि string नहीं और Bob को असत्य puzzle कभी accept नहीं करना। यही पर स्थिति शास्त्रीय शून्य-ज्ञान survive नहीं कर सकता।

तरकीब से पहले एक और character चाहिए। एक नियम-पुस्तक सुधार करें: logician के अर्थ में औपचारिक प्रमाण-प्रणाली—स्थिर axioms और written गणितिय प्रमाण जाँच करने के यंत्रिक नियम। ZFC, mathematics के मूल axioms, canonical उदाहरण है। आगे सब कुछ पहले से चुने नियम-पुस्तक के समेक है, और विकल्प flexible है: निर्माण आपके सुधार किए किसी भी नियम-पुस्तक के लिए कम करती है, ZFC सहित।

(शेषपत्र से borrowed शब्दों की टिप्पणी यहाँ “प्रमाण-प्रणाली” हमेशा इसी नियम-पुस्तक—गणितिय प्रमाण जाँच करने वाले औपचारिक प्रणाली—का अर्थ है, Alice के भेजे messages कानूनी। Alice और Bob की मशीनों को “पूर्वर और वेरिफायर” कहा जाता है।)

Gödel-style संस्करण mega-Sudoku कहानी खता है लेकिन प्रमाण बदलता है।

Displayed आकार का दूसरा बधा प्रणाली चुनें, उसे D कहें। कहानी में S और D समान format के दो MegaSudoku(n) puzzles हैं। Behind scenes D अलग आकार की कठिनी तर्किक सूत्र से आया हो सकता है; जरूरत हो तो harmless dummy बधाएँ से pad करके समान ग्रिड में फिट किया जा सकता है। D ऐसी तर्किक सूत्र से बना जाता है जो वास्तव में unsatisfiable है: मूल की कोई निर्धारण सभी बधाएँ सत्य नहीं कर सकती जैसे broken puzzle का legal completed ग्रिड नहीं। Toy उदाहरण ऐसी सूत्र होगी जो एक साथ “X सत्य है” और “X असत्य है” माँगे। इसलिए D का वैध filling नहीं है।

लेकिन D ऐसा broken puzzle नहीं होना चाहिए जिसे उजागर करना आसान हो। Toy उदाहरण विफल होता है: कोई भी नियम-पुस्तक “X और नहीं X” को एक रेखा में खंडन कर देगा। D को ऐसी तरह असत्य होता है कि चुनानियम-पुस्तक छोटो तर्क से certify न कर सके। यदि नियम-पुस्तक D को छोटा प्रमाण से खंडन कर सके, नीचे की कहानी collapse होगी वैकल्पिक मार्ग जो Alice के रहस्य बना प्रमाण पैदा कर सकता था। formally नियम out हो जाएगा और गोपनीयता गारंटी उसके साथ। इसलिए D ऐसी परीक्षा से चुना जाता है जिसे स्थिर नियम-पुस्तक कुशलतम पूर्वक खंडन करना नहीं कर सकता नियम-पुस्तक के भीतर कोई छोटा प्रमाण नहीं कि D का समझ नहीं है।

Alice का एक-संदेश प्रमाण फिर either/or कथन के बारे में है:

वास्तविक mega-Sudoku S का समझ है, या decoy D का समझ है।

यही तर्किक कड़ी है। D किसी ज़ुई तरीके से S को सत्य नहीं बनाता। प्रमाण का तर्क यह नहीं है कि “D का समझ नहीं इसलिए S का है।” वह disjunction S or D को सदिध करता है। पूर्ण soundness कहती है कि असत्य disjunction का कोई वैध प्रमाण नहीं हो सकता। चूँकि D वास्तव में असत्य है — उसका कोई समझ नहीं — disjunction के सत्य होने का एक मात्र रस्ता S का सत्य होता है। इसलिए प्रमाण स्वीकार होता है तो S का समझ मौजूद होता चाहिए। Decoy, असत्य S को सत्य नहीं बना सकता।

लेकिन शून्य-ज्ञान वाले हिससे के लिए कल्पना करें कि यदि D का समझ होता तो क्या होता। वह decoy समझ वैकल्पिक witness बन सकता था। उससे simulator, Alice के वास्तविक mega-Sudoku समझ को जमे बना प्रमाण जैसी transcript

बनासकताथा। वास्तविकतामें D कासमझन नहींहै, इसलिए यह रस्तासचमुच उपलब्ध नहीं। महत्वपूर्ण बात यह है कि चुनीहुई नियम-पुस्तिकाकुशलतमपूर्वक यह सिद्ध नहींकर सकतीकि वह रस्ताबंद है।

इसलिए D के दोनैकरियाँहैं। सड्डनेस के लिए D असत्य है, इसलिए “S or D” कावैध प्रमाण S कोforce करताहै। Effective शून्य-ज्जम के लिए D कठिनी to खंडन करनाहै, इसलिए नियम-पुस्तिकाउस decoy मार्ग कोजल्दीनियम out नहींकर सकताजोसमिलेशन संभव बनता।

इसलिए सुरक्षापरिक्षण अब यह नहींहै:

क्याहम सिद्ध कर सकते हैं कि समियुलेटर सच में मौजूद है?

वह बनताहै:

क्याआपकानियम-पुस्तिकाकुशलतमपूर्वक सिद्ध कर सकताहै कि समियुलेटर असंभव है?

यदि उत्तर no है, तोsurprisingly मजबूत चीज अनुसरण करतीहै: हर सुरक्षागारंटीजो(a) परिक्षण चलाकर observe की जासकतीहै, और (b) नियम-पुस्तिकाके भीतर समियुलेटर के existence से provably अनुसरण करतीहै, वास्तव में hold करतीहै। उनमें से किसीपर successful हमलाखुद वहीअनुपस्थिति छोटाखंडन बन जाएगा और वह अनुपस्थिति छोटाखंडन मौजूद नहींहै। यहीव्यवहारकि रूप से शून्य-ज्जम का“effective” हिसाहै।

इसलिए classroom contrast:

शस्त्रीय शून्य-ज्जम: प्रमाण सुरक्षति हैं क्योंकि समियुलेटर exists।

Gödel-style effective शून्य-ज्जम: observable सुरक्षापरिक्षण के लिए प्रमाण सुरक्षति ममानाकि जते हैं क्योंकि नियम-पुस्तिकाकुशलतमपूर्वक सिद्ध करनानहींकर सकताकि समियुलेटर असंभव है।

दूसरादस्ताऔर कमजोर है। यहीवजह है कि शोधपत्र शस्त्रीय संस्करण में टूटने वालीतीन विशेषताएँ रख सकताहै: एक संदेश, no सेटअप और पूर्ण सड्डनेस।

नयापरिक्षण: आप समियुलेटर कीअनुपस्थिति सिद्ध करना नहींकर सकते

Ilango कीrelaxation सबसे बदलतीहै।

शस्त्रीय शून्य-ज्जम पूछताहै:

क्यासमियुलेटर मौजूद है?

व्यवहारकि रूप से शून्य-ज्जम कुछ और कमजोर पूछताहै:

क्याआपकाचुनानियम-पुस्तिकाकुशलतमपूर्वक सिद्ध कर सकताहै कि कोई समियुलेटर मौजूद नहींहै?

यह तकनीकीचलन जैसा लग सकता है, लेकिन मुख्य वचन यही है। निर्माण एक अजीब अवस्थामें रहती है: सम्युलेटर वस्तु में मौजूद नहीं है—शोधपत्र इस पर स्पष्ट है—लेकिन आपने जोनियम-पुस्तकसुधार किया वह कुशलतमपूर्वक सिद्ध करना नहीं कर सकता कि वह मौजूद नहीं। यदि हर खरब परणम जसकी आपको परवह है ऐसी खंडन मॉड, तो उन नतीजों के लिए प्रणालीशून्य-जन्म जैसा व्यवहार करता है।

यही Gödel आता है। Decoration के रूप में नहीं और “Gödel crypto को सुरक्षित बनाता है” के रूप में नहीं। Connection proof-theoretic है। नियम-पुस्तकसर्वोत्तम कहलाता है यदि सटीक अर्थ में वह सर्वोत्तम संभव हो जब भी कोई नियम-पुस्तक प्रसंगिक kind की सूत्र को छोटा प्रमाण से खंडन कर सकता है, सर्वोत्तम नियम-पुस्तक भी कर सकता है, अधिकतम polynomially longer प्रमाण के साथ। Krajíček और Pudlák ने 1989 में conjecture किया कि कोई सर्वोत्तम प्रमाण-प्रणाली नहीं है: आप जोनियम-पुस्तकसुधार करें, कोई दूसरा नियम-पुस्तकसत्य कथन की किसी परवह को बहुत अधिक succinctly सिद्ध करेगा। यह प्रमाण जटिलता की केंद्रीय खुला conjectures में से है और Gödel incompleteness प्रमेय का finite, जटिलता theoretic cousin है: कुछ सत्य कथन आपके स्थिर नियम-पुस्तक में छोटा प्रमाण नहीं रखते—इसलिए नहीं कि वे सिद्धांत में unprovable हैं, बल्कि इसलिए कि हर स्थिर नियम-पुस्तक कुछ छोटे truths को छोटा प्रमाण के बिना छोड़ देता है।

शोधपत्र इस conjecture को mildly अधिक मजबूत “infinitely often” form में assume करता है, जो क्रिप्टोग्राफिक उपयोग में मजबूत है। Krajíček और Pudlák के प्रमेय से payoff concrete है: हर नियम-पुस्तक के लिए formulas की क्रम है जो वस्तु में unsatisfiable हैं, जिनकी छोटे खंडन नियम-पुस्तक नहीं दे सकता—और crucially, जिनमें कुशल एल्गोरिदम उत्पन्न करना कर सकता है। यही last गुण, uniformity, वचन को existence दवा से actual एल्गोरिदम बनाती है जस Alice चला सकती है: decoys D assembly रेखा से आते हैं, पतला वायु से नहीं।

क्रिप्टोग्राफिक कदम इसी shortage of प्रमाण शक्ति को कम में लगता है।

निर्माण क्या कर रही है

शोधपत्र की निर्माण को उसकी आकार तक पट्टी करे।

एक नियम-पुस्तकसुधार करें—मन लें ZFC। Proof-जटिलता मयता के तहत कुशलतमपूर्वक generatable formulas की क्रम है जो वस्तु में unsatisfiable हैं, लेकिन नियम-पुस्तक के पास उनकी unsatisfiability का छोटा प्रमाण नहीं।

अब इस form का एक-संदेश प्रमाण बनाएं:

या वस्तु कथन satisfiable है, या यह विशेष कठिन सूत्र satisfiable है।

विशेष कठिन सूत्र satisfiable नहीं है। इसलिए यदि मूल प्रमाण मशीनी perfectly ध्वनि है, संदेश स्वीकार हमें का अर्थ अभी भी वस्तु कथन सत्य होता है। इससे पूर्ण सण्डनेस मलित है।

लेकिन शून्य-जन्म-like सुरक्षा के लिए imagine करें कि विशेष कठिन सूत्र satisfiable होती। तब उसका वटिनेस वस्तु कथन वटिनेस जमे बना प्रमाण simulate करने में इस्तेमाल हो सकता था। Reality में सूत्र satisfiable नहीं—लेकिन नियम-पुस्तकसुधार कुशलतमपूर्वक सिद्ध करना नहीं कर सकता कि ऐसा है। इसलिए वह कुशलतमपूर्वक सिद्ध करना नहीं कर सकता कि सम्युलेटर असंभव है।

यही hinge है। प्रणालीशून्य सम्युलेटर उत्पन्न करके रहस्य hide नहीं करता। Observable सुरक्षा परीक्षण की बीड़ी class के लिए रहस्य को नियम-पुस्तक की इस inability के पीछे रखता है कि वह सम्युलेटर की absence certify नहीं कर सकता।

शोधपत्र क्यादवा करता है

मुख्य प्रमेय layers में आता है। मुख्य परिणाम यह है:

एक मजबूत क्रिप्टोग्राफिक मजबूती—non-interactive वटिनेस indistinguishable प्रमाण का existence, अच्छी तरह studied वस्तुएँ जो कई established मजबूती packages से अनुसरण करते हैं—और proof-जटिलता conjecture कि कोई (infinitely often) सर्वोत्तम प्रमाण-प्रणाली मौजूद नहीं के तहत, शोधपत्र हर chosen नियम-पुस्तिका के लिए NP/SAT का एक-संदेश प्रूवर और वेरिफायर construct करता है जिसमें पूर्ण सटंडनेस, no सेटअप और उस नियम-पुस्तिका के समेकित व्यवहार की रूप से शून्य-जजम है। (NP/SAT puzzle-like समस्याएँ कामजबूत “hardest समस्य denominator” हैं; mega-Sudoku उसका एक costume है।)

परिक्षण-योग्य सुरक्षागुण बचाए रखना करने के व्यापक दवा के लिए शोधपत्र एक और मजबूत मजबूती जोड़ता है, derandomization मजबूती $P = BPP$ —लगभग, randomness एल्गोरिदम को essential अतिरिक्त शक्ति नहीं देती।

प्रमेय भाषा के बहर:

- प्रमाण एक संदेश है।
- Trusted सेटअप नहीं है।
- असत्य कथन सिद्ध करना नहीं किया जा सकता।
- प्रूवर शास्त्रीय शून्य-जजम नहीं है—उसका समिप्लेटर नहीं है।
- लेकिन शास्त्रीय शून्य-जजम के हर परिक्षण-योग्य, game-based सुरक्षापरिणाम को इस परिस्थिति में achieve किया जा सकता है।

“परिक्षण-योग्य” महत्वपूर्ण है। इसका अर्थ सुरक्षा failure adversary को खेल में run करके परिक्षण की जा सकती है। कई क्रिप्टोग्राफिक सुरक्षा definitions इसी form की हैं: क्या adversary दो encryptions अलग पहचान सकता है, कार्य invert कर सकता है, वटिनेस recover कर सकता है या specified प्रयोग जीत सकता है? प्रमेय हर परिक्षण-योग्य गुण के लिए एक प्रूवर देता है, एक at a समय। एक एकल प्रूवर जिसमें हर परिक्षण-योग्य गुण एक साथ होशियार असंभव है—old reusability हमला (“Bob प्रमाण दूसरो को दिखा सकता है”) खुद परिक्षण-योग्य गुण है, और यहाँ सच में विफल होती है। शोधपत्र का proposal है कि एकल प्रूवर संभवतः सभी प्रकृतिक परिक्षण-योग्य गुण शामिल कर सकता है—जो क्रिप्टोग्राफिक practice में वस्तु में आती हैं—लेकिन यह हिसाब informal “प्रकृतिक” notion और स्पष्ट conjecture पर टिका conditional प्रमेय है। गारंटी observable failures को लक्ष्य करती है, secrecy के हर philosophical या समिप्लेशन-based अर्थ को नहीं।

एक concrete corollary नम लेने लायक है: निर्माण uniform प्रूवर के साथ पहले non-interactive वटिनेस hiding प्रमाण देती है—“puzzle का प्रमाण आपको उसका समाधान खोजने में मदद नहीं करता” no इंटरैक्शन और no सेटअप के साथ—सुनने में मध्यम वस्तु जिसने दशकोतक निर्माण resist की।

यह क्या नहीं कहता

यही section piece कोई मजदूर रखता है।

यह नहीं कहता कि old impossibility theorems गलत थे। निर्माण definition बदलकर उनसे बचती है।

यह no इंटरैक्शन, no सेटअप और पूर्ण सटंडनेस के साथ समस्य शास्त्रीय शून्य-जजम नहीं देती। शोधपत्र स्पष्ट है

कॉन्स्ट्रक्टेड प्रूवर कासम्युलेटर नहीं है।

इसका अर्थ प्रमाण reuse नहीं हो सकता नहीं है। एक-संदेश प्रमाण किसी और को दिखाया जा सकता है; शोधपत्र deniability-style गुण बचाए रखना नहीं करता। (Trusted सेटअप वाले non-interactive शून्य-जुझ में भी यही सीमा है।)

इसका अर्थ यह व्यवहार कि प्रोटोकॉल तैयारी नहीं है। यह जटिलतासिद्ध और क्रिप्टोग्राफिक foundations है। परिणाम प्रमाण जटिलता और क्रिप्टोग्राफी की मुख्य मज्यताएँ पर निर्भर है और निर्माण सिद्ध में क्या संभव है, उस बारे में है।

यह “Gödel” को magic सुरक्षा primitive नहीं बनाता। Gödel connection प्रमाण-प्रणाली, सर्वोत्तम प्रमाण-प्रणाली और incompleteness के finite analogues से है। उपयोगी intuition “incompleteness आपका password सुरक्षा देती है” नहीं वह है: यदि नियम-पुस्तिका कुशलतम पूर्वक सिद्ध करना नहीं कर सकता कि सम्युलेटर असंभव है, तो ऐसी प्रमाण की जरूरत वाले हमले सुरक्षा definitions के level पर रकना किया जा सकते हैं।

फिर भी यह दलितचस्प क्यों है

क्रिप्टोग्राफी अक्सर hardness को सुरक्षामें बदलती है। Factoring कठिन है, इसलिए RSA-style मज्यताएँ उपयोगी बनते हैं। Lattice समस्याएँ कठिन हैं, इसलिए lattice क्रिप्टोग्राफी उपयोगी है। यहाँ hardness अर्जित है: “रहस्य compute करना कठिन” नहीं बल्कि “यह सिद्ध करना कठिन कि कोई खास प्रमाण वस्तु exist नहीं कर सकता”

इसलिए शोधपत्र unusual लगता है। वह axioms और नियम-पुस्तिकाएँ को लगभग क्रिप्टोग्राफिक resources की तरह मजना करता है। Usual impossibility सड्डनेस और समिलेशन के बीच tension कहती है। Ilango का कदम इस tension को proof-theoretic curtain के पीछे रखता है: सम्युलेटर absent है, लेकिन औपचारिक प्रणाली कुशलतम पूर्वक उसकी absence उजागर करना नहीं कर सकता।

पठक के लिए surprise यह नहीं कि यह आज के शून्य-जुझ प्रणालियाँ replace करेगा शायद सीधे नहीं करेगा। Surprise यह है कि गणितिय logic की सीमा constructively इस्तेमाल की जा सकती है: दीक्षा की तरह हीन ही शामिल की तरह भी।

सम्पूर्ण कतिनामजबूत है?

यह प्रमेय शोधपत्र है, इसलिए “सम्पूर्ण” जघनवज्जु या astronomy शोधपत्र से अलग अर्थ रखता है। सवाल प्रयोग प्रतिकृति बनीयानही नहीं। सवाल है definitions, मज्यताएँ और प्रमाण श्रृंखलाद्वारा समर्थन करते हैं यानही।

प्रमाण औपचारिक है और शोधपत्र मज्यताएँ सफ़ बतता है। मज्यताएँ casual नहीं। Non-interactive वटिनेस indistinguishable प्रमाण क्रिप्टोग्राफी के मजक वस्तुएँ हैं और कई established मज्यता packages से अनुसरण करते हैं। No-सर्वोत्तम-proof-system conjecture प्रमाण जटिलता की केंद्रीय conjecture है। $P = BPP$ मजक derandomization मज्यता है, केवल व्यापक परिक्षण-योग्य-property प्रमेय के लिए।

शोधपत्र यह भीतर देता है कि मज्यताएँ सही कीमत हैं, मनमसाद्वानही विपरीत दशा का कथन सिद्ध करता है कि वे मूलतः आवश्यक हैं—यदि ऐसी निर्माण मौजूद हैं, तो non-interactive वटिनेस indistinguishable प्रमाण exist करने ही चाहिए, और मजक एक-way कथ्य मजक कई सर्वोत्तम प्रमाण-प्रणाली exist नहीं कर सकता। मज्यताएँ “दो ओर लम वाली” भी हैं: इनमें से किसी को खंडन करना अपने आप प्रमाण जटिलता क्रिप्टोग्राफी या जटिलतासिद्ध की महत्वपूर्ण खोज होगा।

लेकिन परिणाम conditional है, इसलिए विश्वास भी conditional। यदि मज्यताएँ वफिल होना प्रमेय की व्याख्या बदलती

है। और मस्यताएँ hold करने पर भीगारंटीपूराशस्त्रीय शून्य-ज्जम नहीं शेषपत्र का relaxed, proof-theoretic संस्करण है।

इसलिए सही विश्वास: उच्च क शेषपत्र सुसंगत conditional possibility परणिम establish करता है; मध्यम कम मस्यताएँ उस क्रिप्टोग्राफ़िक दुनिया को describe करती हैं जसमें हम वस्तुतः में रहते हैं; immediate व्यवहारिक परणिम पर कम।

यह क्यों मस्यने रखता है

शेषपत्र ऐसारस्ताखेतता है जसि बंद मसाजताथा।

शस्त्रीय सदिधंत कहती है: पूरा शून्य-ज्जम सेटअप बनाएक संदेश नहीं हो सकता और perfectly ध्वनि नहीं हो सकता। Ilango का शेषपत्र कहता है: यदि हम शून्य-ज्जम के उन नतीजों की माँग करें जनिहें सुरक्षा games में परिक्षण किया जा सकता है, और सुरक्षा definition को नियम-पुस्तिका का कुशलत पूर्वक खंडन कर सकता या नहीं कर सकता इस पर निर्भर होता करने दें, तो उपयोगी व्यवहार का बड़ा हिस्सा वापस पया जा सकता है—एक संदेश, no सेटअप और पूर्ण सडंडनेस के साथ।

यह छोटा definitional tweak नहीं क्रिप्टोग्राफ़िक guarantees सोचने का अलग तरीका है। केवल यह मत पूछें कि क्या exists करता है; पूछें नियम-पुस्तिका का नियम out कर सकता है। Unprovability को philosophical nuisance की बजाय संरचना की तरह इस्तेमाल करें।

व्यवहारिक दुनिया कल नहीं बदलेगी। Conceptual मसचित्र बदलती है। अब औपचारिक अर्थ है जसमें “कोई कुशलत पूर्वक सदिध करना नहीं कर सकता कि रहस्य रसिप्त हुआ” इतना मजबूत हो सकता है कि “रहस्य रसिप्त नहीं हुआ” से चही गई कई game-based protections वापस मिलें।

इसलिए title में Gödel है।

साफ सारांश

शून्य-ज्जम प्रमाण प्रवर को वटिनेस reveal किए बिना वेरिफायर को कथन सत्य होने का प्रमाण देने देते हैं। शस्त्रीय impossibility परणिम कहते हैं कि शून्य-ज्जम को सेटअप बनाएक संदेश में squeeze नहीं किया जा सकता और पूर्ण सडंडनेस नहीं रख सकता। Rahul Ilango का शेषपत्र इन impossibilities को खंडन नहीं करता। वह और कमजोर notion परभिषति करता है, व्यवहारिक रूप से शून्य-ज्जम: सम्युलेटर सच में मौजूद होता जरूरी नहीं requirement यह है कि chosen प्रमाण-प्रणाली—ZFC जैसा औपचारिक नियम-पुस्तिका—कुशलत पूर्वक सदिध न कर सके कि सम्युलेटर मौजूद नहीं। क्रिप्टोग्राफ़िकी मुख्य मस्यताएँ (non-interactive वटिनेस indistinguishable प्रमाण) और प्रमाण जटिलता (no सर्वोत्तम प्रमाण-प्रणाली exists) के तहत शेषपत्र NP/SAT के एक-संदेश provers construct करता है, no सेटअप और पूर्ण सडंडनेस के साथ, जो शून्य-ज्जम के परिक्षण-योग्य, game-based नतीजों गुण by गुण achieve करते हैं। सभी “प्रकृतिक” गुण शमलि करने वाला एकल प्रवर आगे का partly conjectural extension है—और literally हर परिक्षण-योग्य गुण शमलि करना शायद असंभव है क्योंकि प्रमाण reusable रहते हैं। परणिम सैद्धंतिक और conditional है, तैन्त primitive नहीं लेकिन proof-theoretic unprovability को क्रिप्टोग्राफ़िक resource की तरह इस्तेमाल करने का नया तरीका दिखाता है।

बनाबढ़ाचढ़कर जाँच

पेपर क्या दिखाता है: Stated मजबूती के तहत NP/SAT के एक-संदेश, no-व्यवस्था perfectly ध्वनि provers बनाए जा सकते हैं जो किसी भी chosen प्रमाण-प्रणाली के समक्ष व्यवहारिक रूप से शून्य-जुझ है और शास्त्रीय शून्य-जुझ के प्रत्येक परीक्षण-योग्य game-based परणाम को achieve करते हैं।

क्या संभव है लेकिन unconditionally सिद्ध नहीं कि ज़रूरी proof-जटिलता और क्रिप्टोग्राफ़िक मजबूती सही हैं। वे गंभीर, well-studied मजबूती हैं—और शोधपत्र दिखाता है कि वे मूलतः आवश्यक भी हैं और sufficient भी—लेकिन फिर भी मजबूती हैं।

यह क्या नहीं दिखाता No इंटरैक्शन, no सेटअप और पूर्ण सड़ने के साथ शास्त्रीय शून्य-जुझ; तैयारी व्यवहारिक प्रणाली प्रमाण की deniability या non-reusability; या Gödel incompleteness प्रमेय अपने आप क्रिप्टोग्राफ़ी सुरक्षा करता है।

मुख्य सीमाएँ: गारंटी शून्य-जुझ की relaxation है; broadest संस्करण multiple मजबूती पर निर्भर करती है; single-universal-prover दम partially conjectural है; और परणाम मुख्यतः foundational है।

समस्या पठक को कतिनाभरेसार खना चाहिए? Definitions स्वीकार करने पर यह महत्वपूर्ण conditional सिद्ध परणाम है—इस पर उच्च विश्वास। मजबूती वास्तव में capture करती है—मध्यम। Immediate व्यवहारिक तैयारी—कम। सुरक्षा takeaway: शोधपत्र शून्य-जुझ impossibilities को तोड़ता नहीं वह उन हिससों के आसपास नया proof-theoretic रस्ता खोजता है जो कई सुरक्षा games में मजबूती रखते हैं।

स्रोत

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>