The
CLEAN PAPER

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

چال یہ نہیں کہ راز کے چھپے ہونے کو ثابت کیا جائے

زیرو نالج ثبوت ثبوت پیش کرنے والا کو تصدیق کنندہ کو بیان درست ہونے پر قائل کرنے دیتی ہیں، گواہ *reveal* کیے بغیر۔ کلاسیکی *impossibility* نتائج کہتے ہیں کہ زیرو نالج کو بغیر سیٹ اپ ایک پیغام والا *form* میں *squeeze* نہیں کیا جا سکتا اور کامل صحتِ ثبوت بھی نہیں رکھی جا سکتی۔ *Ilango Rahul* کا مقالہ ان *impossibilities* کو *refute* نہیں کرتا۔ یہ *effectively notion weaker** زیرو نالج** *define* کرتا ہے: سیمیولیٹر کے واقعی *exist* کرنے کی *requirement* کے بجائے *chosen* ثبوت نظام — مثلاً *ZFC* جیسے صوری قاعدہ نامہ — کو مؤثر طور پر یہ ثابت کرنا کرنے سے عاجز ہونا چاہیے کہ سیمیولیٹر *exist* نہیں کرتا۔ کرپٹوگرافی کی *major* مفروضے (غیر تفاعلی گواہ *indistinguishable* ثبوت) اور ثبوت پیچیدگی مفروضہ (نہیں *optimal* ثبوت نظام (*exists* کے تحت مقالہ *NP/SAT* کے ایک پیغام والا، بغیر سیٹ اپ، *construct provers sound perfectly* کرتا ہے جو کلاسیکی زیرو نالج کی *property- consequences game-based falsfiiable* *by-property* حاصل کرتے ہیں۔ ایک واحد ثبوت پیش کرنے والا جو تمام "قدرتی" *cover properties such* کرے، مزید *extension conjectural partly* ہے؛ *property falsfiiable every literally* بیک وقت *cover* کرنا ممکنہ طور پر *impossible* ہے کیونکہ ثبوت *reusable* رہتی ہیں۔ نتیجہ نظری اور *conditional* ہے، *primitive deployed* نہیں، مگر ثبوت-*theoretic* *unprovability* کو کرپٹوگرافک *resource* بنانے کا نیا راستہ دکھاتا ہے۔

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: 00058.2025.FOCS63196/1109.10

چال یہ نہیں کہ راز کے چھپے ہونے کو ثابت کیا جائے

زیرو نالج کی سب سے سادہ شکل سے شروع کریں۔

Bob Alice، کو قائل کرنا چاہتی ہے کہ ایک Sudoku معما حل پذیر ہے۔ اگر وہ پورا حل بھیج دے تو Bob فوراً قائل ہو جائے گا، مگر راز بھی ختم ہو جائے گا۔ Alice اس سے زیادہ عجیب چیز چاہتی ہے: حل دکھائے بغیر یہ ثابت کرنا کہ حل **موجود** ہے۔

زیرو نالج ثبوت کا وعدہ یہی ہے۔ ثبوت پیش کرنے والا (Alice) تصدیق کنندہ (Bob) کو قائل کرتا ہے کہ بیان درست ہے، مگر بیان کے درست ہونے کے سوا کوئی اضافی معلومات ظاہر نہیں کرتا۔

مسئلہ یہ ہے کہ اس وعدے کی قیمت ہے۔ عام ریاضیاتی ثبوت میں دو آرام دہ خصوصیات ہوتی ہیں۔ پہلی، وہ **ایک پیغام** ہو سکتا ہے: اسے لکھیں، کسی کو دیں، اور بات ختم۔ دوسری، وہ **بالکل صحیح** ہو سکتا ہے: غلط بیان کے لیے کوئی درست ثبوت موجود ہی نہیں۔ کلاسیکی ناممکنیت کے نتائج کہتے ہیں کہ زیرو نالج میں یہ دونوں سہولتیں قربان کرنا پڑتی ہیں—اور مسئلہ صرف دونوں کو ایک ساتھ رکھنے کا نہیں؛ ہر ایک الگ بھی کلاسیکی زیرو نالج کے لیے رکاوٹ بنتی ہے۔

پہلی رکاوٹ یہ ہے کہ زیرو نالج عموماً باہمی گفتگو مانگتا ہے۔ اگر Alice صرف ایک پیغام بھیجے اور پہلے سے کوئی قابلِ اعتماد سیٹ اپ نہ ہو، تو کلاسیکی زیرو نالج کی ضمانت قائم نہیں رہتی—چاہے صحتِ ثبوت میں تھوڑی غلطی کی گنجائش قبول کر لی جائے۔

دوسری رکاوٹ صحتِ ثبوت سے متعلق ہے۔ اگر صحتِ ثبوت بالکل کامل ہو تو باہمی گفتگو بھی بے معنی ہو سکتی ہے: اگر تصدیق کنندہ کسی بھی تصادفی انتخاب کے باوجود غلط بیان سے کبھی دھوکا نہیں کھا سکتا، تو وہ اپنے تصادفی انتخاب پہلے ہی طے کر سکتا ہے۔ تصدیق کنندہ قابلِ پیش گوئی ہو جائے تو Alice تمام جواب ایک ہی پیغام میں دے سکتی ہے—اور ہم پھر اسی ناممکن صورت میں واپس پہنچ جاتے ہیں۔

Ilango Rahul کا مقالہ ان دونوں رکاوٹوں کے بیچ ایک راستہ تلاش کرتا ہے۔ وہ ناممکنیت کو رد نہیں کرتا اور نہ اسی ناممکن ترتیب میں کلاسیکی زیرو نالج بنانے کا دعویٰ کرتا ہے۔ چال زیادہ باریک ہے: “کچھ بھی ظاہر نہ کرنا” کی شرط کو کمزور کیا جاتا ہے، مگر اس طرح کہ وہ حفاظتی خصوصیات باقی رہیں جنہیں کرپٹوگرافر عملی طور پر آزمائشی کھیلوں میں جانچتے ہیں۔

اس تصور کو **مؤثر طور پر زیرو نالج** کہا گیا ہے۔

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.

زیرو نالج تین دروازوں پر رکتا ہے—باہمی گفتگو، قابلِ اعتماد سیٹ اپ، اور صحتِ ثبوت میں معمولی غلطی کی گنجائش۔ Ilango کی ساخت ایک مختلف راستہ لیتی ہے: منتخب رسمی قاعدہ نامہ مؤثر طور پر یہ ثابت نہیں کر سکتا کہ سیمیولیٹر موجود نہیں۔

Original diagram — The Clean Paper CC BY 0.4

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.

کلاسیکی زیرو نالج پوچھتا ہے کہ سیمیولیٹر حقیقت میں موجود ہے یا نہیں؛ "مؤثر طور پر زیرو نالج" صرف یہ پوچھتا ہے کہ منتخب رسمی قاعدہ

نامہ مؤثر طور پر یہ ثابت کر سکتا ہے یا نہیں کہ سیمیولیٹر **موجود نہیں**۔ یہی کمزور شرط ایک پیغام، بغیر سیٹ اپ، اور کامل صحتِ ثبوت کو ایک ساتھ ممکن بناتی ہے۔

Original diagram — The Clean Paper CC BY 0.4

پرانا ٹیسٹ: سیمیولیٹر واقعی موجود ہو

کلاسیکی زیرو نالج کو رسمی شکل دینے کا عام طریقہ ایک خیالی مددگار استعمال کرتا ہے جسے **سیمیولیٹر** کہتے ہیں۔

تصور کریں، Alice Jane کا راز **نہیں** جانتی۔ اگر Jane خود ایسے ثبوت بنا سکے جو Bob کو Alice سے ملنے والے ثبوتوں سے ناقابلِ تمیز ہوں، تو Alice کے ثبوت نے Bob کو کوئی نئی معلومات نہیں دیں۔ Jane راز کے بغیر ہی Bob کے تجربے جیسی نقل پیدا کر سکتی تھی۔

اس لیے کلاسیکی زیرو نالج ایک **حقیقی سیمیولیٹر** مانگتا ہے: ایسا مؤثر الگورتھم جو راز جانے بغیر اسی طرح کے ثبوت پیدا کر سکے۔ اصطلاحی زبان میں خفیہ حل کو گواہ کہتے ہیں؛ Sudoku میں گواہ بس مکمل حل شدہ گرڈ ہے۔

یہ تعریف طاقتور ہے، مگر پرانی ناممکنیت بھی یہی آ کر کاٹتی ہے۔ وجدان یہ ہے کہ واقعی غیر تفاعلی ثبوت محض ایک تحریری شے ہوتی ہے۔ Bob کے پاس وہ آ جائے تو وہ اسے کسی تیسرے شخص کو بھی دکھا سکتا ہے؛ یوں Bob خود بیان کو دوسروں کے سامنے ثابت کرنے کی صلاحیت حاصل کر لیتا ہے، جو "کوئی نئی معلومات نہیں" سے زیادہ محسوس ہوتی ہے۔ کلاسیکی قضیے اسی وجدان کو باقاعدہ ناممکنیت کے نتائج میں بدلتے ہیں۔

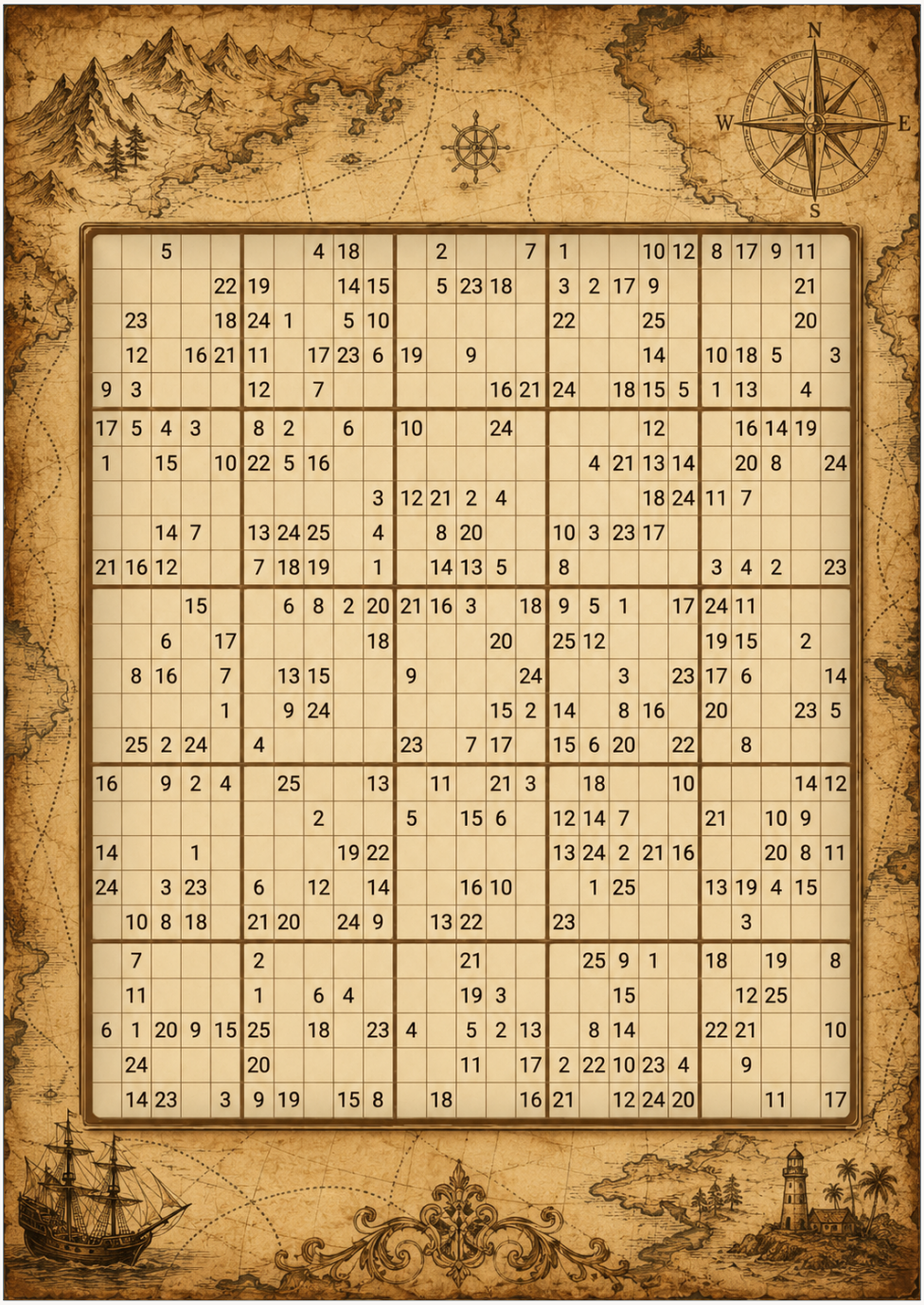
> **وہ تین خصوصیات جن پر مقالہ اصرار کرتا ہے**
>
> ہیں: شامل پابندیاں تین میں عنوان کے مقالے
>
> **باہمی گفتگو نہیں:** Alice ایک ثبوت بھیجتی ہے؛ آگے پیچھے کوئی مکالمہ نہیں ہوتا۔
> **سیٹ اپ نہیں:** Alice اور Bob کسی قابلِ اعتماد مشترک حوالہ، پہلے سے طے شدہ عوامی تصادف یا دوسری ابتدائی ترتیب پر انحصار نہیں کرتے۔ بہت سے نظام جنہیں "غیر تفاعلی زیرو نالج" کہا جاتا ہے کسی نہ کسی سیٹ اپ کے محتاج ہوتے ہیں؛ یہاں مراد واقعی صفر سیٹ اپ ہے۔
> **کامل صحتِ ثبوت:** غلط بیان کے لیے درست ثبوت موجود نہیں۔ صرف "تقریباً کبھی قبول نہیں ہوگا" نہیں؛ **کوئی** درست ثبوت نہیں۔
> یہ تینوں خصوصیات عام تحریری ریاضیاتی ثبوت میں ملتی ہیں—اور کلاسیکی زیرو نالج انہیں ایک ساتھ برقرار نہیں رکھ سکتا۔

فرق کو سمجھنے کے لیے MegaSudoku

فرق کا ایک جان بوجھ کر سادہ کیا گیا ذہنی ماڈل لیتے ہیں۔

سنجیدہ تشبیہ کے لیے معمول کا 9×9 Sudoku کافی نہیں۔ وہ بہت چھوٹا اور محدود ہے: کمپیوٹر اسے حل کر سکتا ہے یا ثابت کر سکتا ہے کہ حل موجود نہیں۔ اس کے بجائے **MegaSudoku(n)** نامی معما خاندان تصور کریں۔ قاعدے کو پیمانے کے ساتھ بڑھائیں: خانوں کا حجم n چنیں، $N = n^2$ رکھیں، پھر $N \times N$ گرڈ بنائیں جسے $n \times n$ بڑے خانوں میں تقسیم کیا گیا ہو اور جس میں N مختلف علامتیں استعمال ہوں۔ معمول کا Sudoku صرف چھوٹا سا کیس $n = 3$, $N = 9$ ہے: 9×9 گرڈ، 3×3 خانے اور

9 علامتیں۔ ثبوتی پیچیدگی کی کہانی تب شروع ہوتی ہے جب n بڑھ سکتا ہو اور گرڈ میں اضافی آلات شامل کیے جا سکیں جو اسے Sudoku کے لباس میں SAT فارمولا بناتے ہیں۔ SAT فارمولا بنیادی طور پر درست/غلط قیود کی فہرست ہے: کیا متغیرات کو ایسی درست یا غلط قدریں دی جا سکتی ہیں کہ ہر قید پوری ہو؟



		5					4	18			2			7	1			10	12	8	17	9	11	
				22	19			14	15		5	23	18		3	2	17	9					21	
	23			18	24	1		5	10						22			25					20	
	12		16	21	11		17	23	6	19		9						14		10	18	5		3
9	3				12		7						16	21	24		18	15	5	1	13		4	
17	5	4	3		8	2		6		10			24					12			16	14	19	
1		15		10	22	5	16									4	21	13	14		20	8		24
									3	12	21	2	4					18	24	11	7			
		14	7		13	24	25		4		8	20			10	3	23	17						
21	16	12			7	18	19		1		14	13	5		8					3	4	2		23
			15			6	8	2	20	21	16	3		18	9	5	1		17	24	11			
		6		17					18				20		25	12				19	15		2	
	8	16		7		13	15			9				24			3		23	17	6			14
				1		9	24						15	2	14		8	16		20			23	5
	25	2	24		4					23		7	17		15	6	20		22		8			
16		9	2	4		25			13		11		21	3		18			10				14	12
							2			5		15	6		12	14	7			21		10	9	
14			1					19	22						13	24	2	21	16			20	8	11
24		3	23		6		12		14			16	10			1	25			13	19	4	15	
	10	8	18		21	20		24	9		13	22			23						3			
	7				2							21				25	9	1		18		19		8
	11				1		6	4				19	3				15				12	25		
6	1	20	9	15	25		18		23	4		5	2	13		8	14			22	21			10
	24				20							11		17	2	22	10	23	4		9			
	14	23		3	9	19		15	8		18			16	21		12	24	20			11		17

Sudoku: 25×25 اس کے قواعد مکمل گرڈ ظاہر کیے بغیر جانچے جا سکتے ہیں؛ چھپا ہوا حل، یعنی گواہ، اس چیز کی بصری مثال ہے جس کے وجود کا ثبوت دینا ہے۔

AI-generated editorial thumbnail — The Clean Paper CC BY 0.4

Sudoku اور SAT: ایک ہی مسئلہ، دو مختلف لباس

اور ہے، ممکن میں سمتوں دونوں تبدیلی نہیں۔ تشبیہ محض ہے سکتا جا برتا طرح کی فارمولا SAT کو Sudoku کہ کہنا یہ ہے۔ سکتی جا لکھی پر طور مکمل سمت آسان

Sudoku سے SAT۔ SAT میں متغیرات درست یا غلط ہوتے ہیں، اس لیے ہر (قطار، ستون، قدر) کے تین رکن کے لیے ایک Boolean متغیر رکھیں: $x(r,c,v)$ کا مطلب ہے "قطار r اور ستون c کے خلیے میں قدر v ہے۔" 4×4 Sudoku (2×2 خانے، قدریں 1–4) کے لیے 4·4·4 = 64 متغیرات درکار ہیں؛ کلاسیکی 9×9 کے لیے 729۔ پھر ہر Sudoku قاعدہ منطقی clauses کے ایک مجموعے میں بدل جاتا ہے۔ Clause) متغیرات یا ان کی نفی کا OR ہوتا ہے؛ پورا فارمولا تمام clauses کا AND۔)

ہر خلیہ میں کم از کم ایک قدر ہو — ہر خلیہ کے لیے ایک clause:

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

ہر خلیہ میں زیادہ سے زیادہ ایک قدر ہو — ہر جوڑا کے لیے "دونوں نہیں" clause:

$$\neg x(1,1,3) \vee \neg x(1,1,1) \quad \neg x(1,1,2) \vee \neg x(1,1,1)$$ ... اور اسی طرح تمام چھ جوڑے۔

ہر قطار میں ہر قدر ہو — قطار 1 اور قدر 3 کے لیے کم از کم ایک بار:

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

اور زیادہ سے زیادہ ایک بار: $\neg x(1,2,3)$، $\vee \neg x(1,1,3)$ پھر قطار کے ہر خلیہ-جوڑا کے لیے یہی قاعدہ۔
ستون اور خانے—یہی قاعدے، صرف خلیوں کا گروہ بدل جاتا ہے۔ بالائی بائیں خانے اور قدر 2 کے لیے:

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

اور ساتھ ہر جوڑے کے لیے "دونوں ایک ساتھ نہیں" والی clauses۔
پہلے سے دیے گئے اشارے—سب سے آسان حصہ: ہر اشارہ ایک واحد متغیر والی clause ہے۔ بالائی بائیں کونے میں پہلے سے لکھا 3 یوں بنے گا:

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

تمام clauses کا AND تب اور صرف تب satisfiable ہے جب Sudoku حل پذیر ہو—اور satisfying تعیین ہی حل دیتی ہے: دیکھیں کون سے x(r,c,v) درست ہیں اور انہی سے گرڈ بھریں۔ 9×9 صورت میں 729 متغیرات اور چند ہزار clauses بنتی ہیں، جنہیں جدید solver SAT بہت تیزی سے سنبھال سکتے ہیں۔ اشارہ clause $x(1,1,3)$ پر غور کریں: یہ کہتی ہے "یہ خلیہ **بالکل 3** ہے"، نہ کہ "یہ خلیے سب مختلف ہیں"۔ یہی فرق آگے اشارہ والے خلیوں کے لیے اضافی چال کی ضرورت پیدا کرتا ہے۔

SAT سے Sudoku۔ مقالے کو الٹی اور مشکل سمت چاہیے: کسی من مانے SAT فارمولے سے ایسا mega-Sudoku بنائیں جس کا حل تب اور صرف تب ہو جب فارمولا satisfiable ہو۔ Sudoku کے بنیادی قواعد صرف "یہ خلیے سب مختلف ہیں" جیسی بات کہہ سکتے ہیں، اس لیے من مانے منطقی قیود کو چھوٹے **gadgets** کے ذریعے بنانا پڑتا ہے۔ Gadget خلیوں کا پہلے سے تیار کیا گیا چھوٹا مجموعہ ہوتا ہے، مثلاً کسی clause کے لیے، جس میں مخصوص خلیے متغیرات کا کردار ادا کرتے ہیں اور اندرونی قیود یوں ترتیب دی جاتی ہیں کہ قانونی بھرائیاں صرف وہی ہوں جو clause کو پورا کریں۔ تکمیل-NP کے ثبوتوں میں یہ معیاری تکنیک ہے؛ Sudoku generalized کے لیے Yato اور Seta نے 2003 میں ایسی ساخت دی۔
دونوں سمتیں مل کر بتاتی ہیں کہ Sudoku N×N اور SAT پیچیدگی کے لحاظ سے ایک ہی مسئلے کے دو مختلف لباس ہیں۔
اسی لیے مضمون—اور مقالہ—گرڈ اور علامتوں کے ذریعے پورے NP کی کہانی بیان کر سکتے ہیں۔

گواہ کا تصور اب بھی سادہ ہے۔ Alice mega-Sudoku کی مکمل درست بھرائی جانتی ہے۔ Bob قائل ہونا چاہتا ہے کہ ایسی بھرائی موجود ہے، مگر Alice اسے ظاہر نہیں کرنا چاہتی۔ پوری بھرائی بھیج دے تو Bob قائل ہو جائے گا، مگر راز ختم ہو جائے گا۔

کلاسیکی زیرو نالج میں Alice اور Bob باہم گفتگو کرتے ہیں۔ ایک پرانا ذہنی نمونہ ڈھکی ہوئی ٹائلیں استعمال کرتا ہے۔ Alice حل شدہ گرڈ چھپا دیتی ہے، ہر مرحلے سے پہلے علامتوں کے نام خفیہ طور پر بدلتی ہے، اور Bob کو کوئی تصادفی مقامی قید دیکھنے دیتی ہے: قطار، ستون، خانہ یا gadget۔ کھولے گئے خلیے اگر سب مختلف علامتیں دکھائیں تو Bob کا اعتماد بڑھتا ہے۔ پھر سب کچھ دوبارہ ڈھک دیا جاتا ہے اور علامتوں کے نام نئے سرے سے بدلے جاتے ہیں۔ ایک پیچیدگی باقی رہتی ہے: پہلے سے دیے گئے اشاروں کے لیے اضافی چال چاہیے، کیونکہ نام بدلنے سے وہ بھی چھپ جاتے ہیں۔ اگلا نوٹ بتاتا ہے کہ کلاسیکی پروٹوکول اسے کیسے سنبھالتے ہیں۔

کلاسیکی پروٹوکول اشارہ والے خلیوں کو کیسے سنبھالتے ہیں

مختلف سب خلیے "یہ ہیں کہتے قواعد کے خانے اور ستون قطار، ہے۔ نقطہ اندھا ایک کا چال کی بدلنے نام کے علامتوں ہے"۔ 5 بالکل خلیہ "یہ ہے کہتا اشارہ مگر ہے۔ رہتی برقرار بھی بعد کے بدلنے نام خاصیت کی ہونے مختلف سب اور ہیں"، درست اسے اگر سکتا۔ کر نہیں تصدیق کی اشارے لیے اس جانتا، نہیں σ اور ہے دیکھتا $\sigma(5)$ صرف Bob بعد کے بدلنے نام موجود گرڈ درست **کوئی** کہ ہے سکتی کر ثابت یہ صرف کے کر انداز نظر اشارے گئے دیے سے پہلے Alice تو جائے کیا نہ ہے۔ دیتا حل معیاری دو لٹریچر کلاسیکی ہوگا۔ نہیں ثابت کچھ میں بارے کے معما خاص اس ہے؛

علامتی قطار۔ چھپے ہوئے گرڈ میں N خلیوں کی ایک اضافی قطار شامل کریں، جسے ایک palette سمجھا جا سکتا ہے۔ Alice اسے معلوم ترتیب میں علامتوں 1…N سے بھرتی ہے اور پھر باقی گرڈ کی طرح ان کے نام بدل دیتی ہے، اس لیے قطار میں $\sigma(1)$…$\sigma(N)$ آتے ہیں۔ Bob کے تصادفی چیلنج میں اب ایک اضافی انتخاب ہوتا ہے: قطار، ستون، بڑے خانے یا gadget کے بجائے وہ **علامتی قطار اور ایک اشارہ والا خلیہ** کھولنے کو کہہ سکتا ہے۔ پھر وہ دیکھ سکتا ہے کہ اشارہ والا خلیہ اسی بدلی ہوئی علامت کے برابر ہے جو مطلوبہ عدد کے سامنے ہے، خود σ جانے بغیر۔

اشارے کو قیود میں بدل دینا۔ ایک زیادہ ساختی متبادل یہ ہے کہ اشارے کے لیے الگ چیلنج شامل کرنے کے بجائے اس شرط کو عدم مساوات کی قیود میں تبدیل کر دیا جائے۔ اشارہ والے خلیے کو علامتی قطار کے ہر خلیے سے مختلف قرار دیں، سوائے اپنی مطلوبہ قدر والے خلیے کے۔ مثلاً 5 کے لیے: "$\sigma(1)$ سے مختلف، $\sigma(2)$ سے مختلف، …، مگر $\sigma(5)$ سے مختلف ہونے کی شرط نہیں۔" تب قانونی طور پر صرف مطلوبہ علامت بچتی ہے۔

طبعی طریقۂ کار۔ حقیقی کارڈوں والے Sudoku پروٹوکول (Gradwohl, Naor, Pinkas, and Rothblum 2007) میں نام بدلنے کا مرحلہ سرے سے موجود نہیں۔ چھپانے سے پہلے اشاروں کی درستگی مقرر کر دی جاتی ہے۔ ہر خلیے کے لیے Alice اسی قدر کے تین یکساں کارڈ رکھتی ہے — راز والے خلیوں کے لیے اوندھے، مگر **اشارہ والے خلیوں کے لیے کھلے رخ** — تاکہ Bob اپنی آنکھوں سے دیکھ سکے کہ اشارے درست ہیں۔ پھر ہر خلیے کا ایک کارڈ قطار کے پیکٹ، ایک ستون کے پیکٹ اور ایک بڑے خانے کے پیکٹ میں جاتا ہے؛ پیکٹوں کو خلط کر کے ظاہر کیا جاتا ہے اور Bob دیکھتا ہے کہ ہر پیکٹ میں تمام N علامتیں موجود ہیں۔ خلط سے مقام کی معلومات مٹ جاتی ہے، اس لیے زیرو نالج برقرار رہتا ہے، جبکہ اشارے کارڈ بانٹتے وقت ہی مقفل ہو چکے ہوتے ہیں۔

ہر صورت میں سبق ایک ہی ہے: زیرو نالج پروٹوکول کو بہت احتیاط سے حساب رکھنا پڑتا ہے کہ چھپانے کے بعد **کون سے حقائق محفوظ رہتے ہیں۔** نام بدلنا "سب مختلف" کو محفوظ رکھتا ہے، مگر "5 کے برابر" کو مٹا دیتا ہے؛ اس لیے مؤخر الذکر حقیقت کو کسی دوسرے طریقے سے واپس لانا پڑتا ہے۔

یہ مقالے کا طریقۂ کار نہیں۔ یہ کلاسیکی زیرو نالج کا ذہنی ماڈل ہے:

- Alice اور Bob باری باری پیغامات کا تبادلہ کرتے ہیں۔
- Bob تصادفی جانچیں چنتا ہے۔
- Alice صرف مقامی consistency ظاہر کرتی ہے، پورا حل نہیں۔

- پرائیویسی کی ثبوت دکھاتی ہے کہ Bob کا منظر Alice کے راز حل کے بغیر بھی generate ہو سکتا تھا۔

اس لیے کلاسیکی زیرو نالج ایک مثبت حقیقت پر کھڑی ہے:

> سیمیولیٹر واقعی موجود ہے۔

اب سہولتیں ہٹا دیں۔ Alice ایک ثبوت بھیجتی ہے اور چلی جاتی ہے۔ کوئی قابلِ اعتماد سیٹ اپ نہیں، پہلے سے مشترک تصادفی string نہیں، اور Bob کو غلط معما کبھی قبول نہیں کرنا چاہیے۔ یہی وہ صورت ہے جس میں کلاسیکی زیرو نالج قائم نہیں رہ سکتا۔

اگلی چال سے پہلے ایک اور کردار درکار ہے: ایک **قاعدہ نامہ** طے کریں۔ یہاں مراد منطق کے معنی میں رسمی ثبوتی نظام ہے—مقرر اصولِ موضوعہ اور تحریری ریاضیاتی ثبوتوں کی مشینی جانچ کے قواعد۔ ZFC، ریاضی کے معیاری اصولِ موضوعہ، ایک معروف مثال ہے۔ آگے ہر بیان پہلے سے منتخب قاعدہ نامے کے لحاظ سے سمجھا جائے گا۔ انتخاب لچکدار ہے: ساخت کسی بھی مقرر قاعدہ نامے کے لیے کام کرتی ہے، نہ صرف ZFC کے لیے۔

(مقالے کی اصطلاح پر ایک نوٹ: یہاں "ثبوتی نظام" سے مراد یہی **قاعدہ نامہ** ہے—ریاضیاتی ثبوت جانچنے والا رسمی نظام—نہ کہ Alice کا پیغام۔ Alice/Bob کی مشینری کو "ثبوت پیش کرنے والا اور تصدیق کنندہ" کہا جاتا ہے۔)

Gödel-style ورژن MegaSudoku کہانی رکھتا ہے مگر ثبوت بدل دیتا ہے۔

اسی displayed حجم کا دوسرا قید نظام چنیں، اسے **D** کہیں۔ کہانی میں S اور D دونوں ایک ہی format کے MegaSudoku(n) معمے ہیں۔ the Behind مناظر D کسی مختلف-حجم مشکل منطقی فارمولا سے آیا ہو سکتا ہے؛ ضرورت ہو تو dummy harmless قیود سے pad کیا جا سکتا ہے تاکہ گرڈ حجم مطابقت کرے۔ D ایسی منطقی فارمولا سے بنا ہے جو حقیقت میں **unsatisfiable** ہے: کوئی تعیین تمام قیود کو درست نہیں کر سکتا، جیسے broken معما کی کوئی filling legal نہیں۔ Toy مثال وہ فارمولا ہے جو ایک ساتھ "X درست ہے" اور "X غلط ہے" demand کرے۔ اس لیے D کا درست filling نہیں۔

لیکن D ایسا ٹوٹا ہوا معما نہیں ہونا چاہیے جس کی خرابی **آسانی سے ثابت** ہو سکے۔ کوئی کھلونا مثال کام نہیں کرے گی، کیونکہ قاعدہ نامہ "X" اور "not-X" کو فوراً رد کر دے گا۔ D ایسا غلط معما ہونا چاہیے جس کے غلط ہونے کا مختصر ثبوت منتخب قاعدہ نامہ نہ دے سکے۔ اگر قاعدہ نامہ D کو مختصر دلیل سے رد کر دے تو نیچے والی کہانی بکھر جاتی ہے: وہ متبادل راستہ، جس سے Alice کے راز کے بغیر ثبوت بن سکتا تھا، باقاعدہ طور پر بند ثابت ہو جاتا ہے۔

Alice کی ایک پیغام والا ثبوت پھر either/or بیان کے بارے میں ہے:

> یا حقیقی S mega-Sudoku کا حل ہے، یا D decoy کا حل ہے۔

منطقی ربط یہی ہے۔ D کوئی جادوئی شے نہیں جو S کو درست بنا دے۔ ثبوت یہ دلیل نہیں دیتا کہ "D حل نہیں ہو سکتا، لہٰذا S کا حل ہے"۔ وہ صرف disjunction **S یا D** ثابت کرتا ہے۔ کامل صحتِ ثبوت کا مطلب ہے کہ غلط disjunction کے لیے درست ثبوت موجود نہیں۔ حقیقی دنیا میں D غلط ہے—اس کا حل نہیں—اس لیے disjunction درست ہونے کا واحد راستہ S کا درست ہونا ہے۔ ثبوت قبول ہو تو S کا حل ضرور موجود ہے۔

لیکن زیرو نالج والے پہلو سے سوال بدل جاتا ہے: اگر D کا حل **ہوتا** تو؟ وہ فرضی حل متبادل گواہ بن جاتا۔ Alice کے حقیقی Sudoku حل کے بغیر بھی کوئی ثبوت پیدا کر سکتا—یعنی سیمیولیٹر بن سکتا تھا۔ حقیقت میں D unsatisfiable ہے، اس لیے یہ راستہ واقعی بند ہے۔ نکتہ یہ ہے کہ منتخب قاعدہ نامہ مؤثر طور پر یہ **ثابت نہیں کر سکتا** کہ راستہ بند ہے۔

D کے دو الگ کام ہیں۔ **صحتِ ثبوت** کے لیے D غلط ہے، اس لیے "S یا "D کا درست ثبوت S کو لازم بناتا ہے۔ **مؤثر زیرو نالج** کے لیے D کو رد کرنا قاعدہ نامے کے لیے مشکل ہے، اس لیے قاعدہ نامہ اس فرضی متبادل راستے کو جلد ختم نہیں کر سکتا۔

اب حفاظتی ٹیسٹ یہ نہیں رہا:

> کیا ہم ثابت کر سکتے ہیں کہ سیمیولیٹر واقعی موجود ہے؟

بلکہ:

> کیا آپ کا قاعدہ نامہ مؤثر طور پر ثابت کر سکتا ہے کہ سیمیولیٹر ناممکن ہے؟

اگر جواب نہیں ہو تو surprisingly مضبوط consequence ملتا ہے: ہر حفاظتی ضمانت جو (a) چلانے کی ٹیسٹ کے ذریعے قابلِ مشاہدہ ہو، اور (b) قاعدہ نامہ کے اندر سیمیولیٹر وجود سے provably پیروی کرے، actually قائم رہتی ہے۔ ان guarantees پر successful حملہ خود وہ غائب مختصر refutation بن جائے گا — اور مفروضہ یہی ہے کہ ایسی مختصر refutation موجود نہیں۔ یہی مؤثر طور پر زیرو نالج کا "مؤثر" حصہ ہے۔

contrast: Classroom

کلاسیکی زیرو نالج: ثبوت محفوظ ہیں کیونکہ سیمیولیٹر موجود ہے۔

Gödel طرز کا مؤثر زیرو نالج: قابلِ مشاہدہ حفاظتی آزمائشوں کے لحاظ سے ثبوت محفوظ سمجھا جاتا ہے، کیونکہ منتخب قاعدہ نامہ مؤثر طور پر یہ ثابت نہیں کر سکتا کہ سیمیولیٹر ناممکن ہے۔

دوسرا دعویٰ کمزور ہے۔ اسی weakening کی وجہ سے مقالہ وہ تین خصوصیات رکھ سکتا ہے جو کلاسیکی ورژن میں break ہوتی تھیں: ایک پیغام، نہیں سیٹ اپ، کامل صحتِ ثبوت۔

نیا ٹیسٹ: سیمیولیٹر کی عدم موجودگی ثابت کرنا نہ کر پانا

Ilango کی relaxation سوال بدلتی ہے۔

کلاسیکی زیرو نالج پوچھتی ہے:

> کیا سیمیولیٹر موجود ہے؟

مؤثر طور پر زیرو نالج کمزور سوال پوچھتی ہے:

> کیا منتخب قاعدہ نامہ مؤثر طور پر ثابت کر سکتا ہے کہ کوئی سیمیولیٹر موجود نہیں؟

یہ محض تکنیکی بچاؤ معلوم ہو سکتا ہے، مگر یہی بنیادی خیال ہے۔ ساخت ایک عجیب حالت میں ہے: سیمیولیٹر حقیقت میں موجود **نہیں**—مقالہ اس بارے میں واضح ہے—مگر مقرر قاعدہ نامہ مؤثر طور پر یہ ثابت نہیں کر سکتا کہ وہ موجود نہیں۔ اگر آپ جن خراب نتائج سے بچنا چاہتے ہیں انہیں ثابت کرنے کے لیے یہی رد درکار ہو، تو انہی نتائج کے لحاظ سے نظام زیرو نالج جیسا برتاؤ کرتا ہے۔

یہاں Gödel آتا ہے — decoration کے طور پر نہیں، اور نہ Gödel" crypto محفوظ بناتا ہے" کے طور پر۔ Connection ثبوت-نظریاتی ہے۔ قاعدہ نامہ کو **بہترین** کہیں اگر درست معنی میں وہ بہترین ممکن ہو: جب بھی کوئی قاعدہ نامہ متعلقہ فارمولا کو مختصر ثبوت

سے رد کر سکے، بہترین قاعدہ نامہ بھی اسے at سب سے زیادہ کثیر رقمی طور پر زیادہ طویل ثبوت سے رد کر سکے۔ Krajíček اور Pudlák نے 1989 میں قیاس کیا کہ **نہیں بہترین ثبوت نظام exists**: آپ جو بھی قاعدہ نامہ درست کریں، کوئی دوسرا قاعدہ نامہ درست statements کی کچھ خاندان کو کہیں زیادہ مختصر طور پر ثابت کرے گا۔ یہ ثبوت پیچیدگی کی مرکزی کھلا قیاسات میں سے ایک ہے، اور incompleteness Gödel کا محدود، پیچیدگی-نظریاتی قریبی ہم شکل ہے: مقرر قاعدہ نامہ کچھ مختصر درست بیانات کو مختصر ثبوت نہیں دے پاتا — اس لیے نہیں کہ وہ اصول میں ناقابلِ اثبات ہیں، بلکہ اس لیے کہ ہر مقرر قاعدہ نامہ کہیں نہ کہیں succinct ثبوت طاقت کھوتا ہے۔

مقالہ اس قیاس کو mildly زیادہ مضبوط "infinitely often" شکل میں assume کرتا ہے، جو کرپٹوگرافک uses میں معیاری ہے۔ Krajíček–Pudlák قضیہ کا فائدہ واضح ہے: ہر قاعدہ نامہ کے لیے formulas unsatisfiable کی ایسی سلسلہ موجود ہے جسے قاعدہ نامہ مختصر ثبوت سے رد کرنا نہیں کر سکتا — اور اہم بات یہ کہ مؤثر الگورتھم انہیں **generate** بھی کر سکتا ہے۔ یہی unfiormity وجود دعویٰ کو حقیقی الگورتھم بناتی ہے جسے Alice چلا سکتی ہے: assembly D decoys لائن سے آتے ہیں، پتلا air سے نہیں۔

کرپٹوگرافک حرکت اسی of shortage ثبوت طاقت کو وسیلہ بنانا ہے۔

یہ ساخت حقیقت میں کیا کر رہی ہے

شکل میں ساخت یوں ہے۔

ایک قاعدہ نامہ درست کریں — مثلاً ZFC۔ ثبوت-پیچیدگی مفروضہ کے تحت مؤثر طور پر formulas generatable کی سلسلہ ملتی ہے جو حقیقت میں unsatisfiable ہیں، مگر قاعدہ نامہ کے پاس ان کی unsatisfiability کی مختصر ثبوت نہیں۔

اب ایک پیغام والا ثبوت اس شکل میں بنائیں:

> یا حقیقی بیان satisfiable ہے، یا یہ خاص مشکل فارمولا satisfiable ہے۔

خاص مشکل فارمولا satisfiable actually نہیں۔ اس لیے underlying ثبوت مشینری perfectly صحیح ہو تو پیغام قبول ہونا پھر بھی حقیقی بیان کے درست ہونے کو imply کرتا ہے۔ یہی کامل صحتِ ثبوت ہے۔

زیرو نالج جیسی حفاظت کو سمجھنے کے لیے فرض کریں کہ مخصوص مشکل فارمولا satisfiable **ہوتا**۔ تب اس کا گواہ حقیقی گواہ جانے بغیر ثبوت کی نقل بنانے دیتا۔ حقیقت میں فارمولا satisfiable نہیں، مگر قاعدہ نامہ مؤثر طور پر یہ ثابت نہیں کر سکتا۔ اسی لیے وہ سیمیولیٹر کی ناممکنیت بھی مؤثر طور پر ثابت نہیں کر پاتا۔

یہ hinge ہے۔ نظام راز کو کلاسیکی سیمیولیٹر produce کر کے hide نہیں کرتا۔ قابلِ مشاہدہ حفاظتی ٹیسٹ کی ایک بڑی class کے لیے راز قاعدہ نامہ کی اس inability کے پیچھے چھپتا ہے کہ وہ سیمیولیٹر عدم موجودگی certfiy نہیں کر سکتا۔

مقالہ کیا دعویٰ کرتا ہے

اہم قضیہ کئی تہوں میں آتا ہے۔ بنیادی نتیجہ یہ ہے:

ایک معیاری کرپٹوگرافک مفروضے—**proofs witness-indistinguishable non-interactive** کے وجود—اور ثبوتی پیچیدگی کے اس قیاس کہ **کوئی بہترین ثبوتی نظام often infinitely موجود نہیں**، کے تحت مقالہ ہر منتخب قاعدہ نامے کے لیے NP/SAT کا

ایک پیغام والا ثبوتی طریقہ بناتا ہے جس میں **کامل صحتِ ثبوت**، صفر سیٹ اپ، اور اسی قاعدہ نامے کے لحاظ سے مؤثر زیرو نالج موجود ہے۔ NP/SAT معما نما مسائل کے لیے ایک معیاری "مشکل ترین مشترک قالب" ہے؛ MegaSudoku اسی کا ایک لباس ہے۔

قابلِ ابطال حفاظتی خصوصیات کو وسیع طور پر محفوظ رکھنے والے قضیے کے لیے مقالہ ایک اور معیاری مفروضہ شامل کرتا ہے: derandomization کا مفروضہ **BPP = P**، یعنی تقریباً یہ خیال کہ تصادفی الگورتھم لازماً اضافی بنیادی حسابی طاقت نہیں دیتے۔

قضیہ زبان سے باہر:

- ثبوت ایک ہی پیغام ہے۔
- کوئی قابلِ اعتماد سیٹ اپ نہیں۔
- غلط بیان کا درست ثبوت نہیں بنایا جا سکتا۔
- ثبوت پیش کرنے والا کلاسیکی زیرو نالج نہیں؛ اس کے پاس حقیقی سیمیولیٹر نہیں۔
- مگر کلاسیکی زیرو نالج کی ہر قابلِ ابطال، کھیل پر مبنی حفاظتی خاصیت کو اس ترتیب میں ایک ایک کر کے حاصل کیا جا سکتا ہے۔

"قابلِ ابطال" اہم لفظ ہے۔ اس سے مراد ایسی حفاظتی ناکامی ہے جسے کسی adversary کے ساتھ باقاعدہ تجرباتی کھیل چلا کر جانچا جا سکے۔ کرپٹوگرافی کی بہت سی تعریفیں ایسی ہیں: کیا adversary دو encryptions میں فرق کر سکتا ہے؟ کسی فنکشن کو الٹ سکتا ہے؟ گواہ بازیافت کر سکتا ہے؟ مخصوص کھیل جیت سکتا ہے؟ قضیہ ہر قابلِ ابطال خاصیت کے لیے الگ ثبوت پیش کرنے والا دیتا ہے۔ ایک ہی ثبوت پیش کرنے والا جو **تمام** قابلِ ابطال خصوصیات بیک وقت رکھے غالباً ناممکن ہے—پرانا دوبارہ استعمال والا حملہ Bob") ثبوت دوسروں کو دکھا سکتا ہے") خود ایک قابلِ ابطال خاصیت ہے، اور یہاں واقعی ناکام ہونا پڑتا ہے۔ مقالہ تجویز کرتا ہے کہ ایک ثبوت پیش کرنے والا شاید تمام **قدرتی** قابلِ ابطال خصوصیات سمیٹ سکے، یعنی وہ خصوصیات جو حقیقی کرپٹوگرافک عمل میں سامنے آتی ہیں؛ مگر یہ حصہ "قدرتی" کی غیر رسمی تعریف اور ایک واضح قیاس پر منحصر ہے۔ ضمانت قابلِ مشاہدہ ناکامیوں کے بارے میں ہے، رازداری کے ہر فلسفیانہ یا سیمولیشن-مبنی معنی کے بارے میں نہیں۔

ایک واضح ضمنی نتیجہ بھی اہم ہے: ساخت ایک یکساں ثبوت پیش کرنے والے کے ساتھ پہلا غیر تفاعلی **witness-hiding** ثبوت دیتی ہے—یعنی "معما کا ثبوت آپ کو اس کا حل تلاش کرنے میں مدد نہیں دیتا"—وہ بھی بغیر باہمی گفتگو اور بغیر سیٹ اپ کے۔ یہ ایک محدود سنائی دینے والی خاصیت ہے جس کی تعمیر کئی دہائیوں سے مشکل رہی تھی۔

یہ کیا نہیں کہتا

یہ حصہ کہانی کو دیانت دار رکھتا ہے۔

یہ **نہیں** کہتا کہ پرانے ناممکنیت کے قضیے غلط تھے۔ ساخت تعریف بدل کر ان سے بچتی ہے۔

یہ باہمی گفتگو کے بغیر، سیٹ اپ کے بغیر، اور کامل صحتِ ثبوت کے ساتھ معمول کا کلاسیکی زیرو نالج **نہیں** دیتا۔ مقالہ صاف کہتا ہے کہ بنائے گئے ثبوت پیش کرنے والے کے پاس حقیقی سیمیولیٹر نہیں۔

یہ **نہیں** کہتا کہ ثبوت دوبارہ استعمال نہیں ہو سکتا۔ ایک پیغام والا ثبوت کسی اور کو دکھایا جا سکتا ہے؛ deniability جیسی خصوصیات محفوظ نہیں رہتیں۔ قابلِ اعتماد سیٹ اپ والے غیر تفاعلی زیرو نالج میں بھی یہ حد موجود ہو سکتی ہے۔

یہ عملی تعیناتی کے لیے تیار پروٹوکول **نہیں**۔ یہ پیچیدگی نظریہ اور کرپٹوگرافک بنیادوں کا نتیجہ ہے۔ یہ ثبوتی پیچیدگی اور کرپٹوگرافی کے بڑے مفروضوں پر منحصر ہے، اور سوال اصولی امکان کا ہے، فوری اطلاق کا نہیں۔

یہ Gödel کو کوئی جادوئی حفاظتی جزو نہیں بناتا۔ تعلق ثبوتی نظاموں، بہترین ثبوتی نظام کے مسئلے اور incompleteness کی محدود مثالوں سے ہے۔ درست وجدان یہ نہیں کہ incompleteness" آپ کا password محفوظ کرتی ہے"۔ بات یہ ہے کہ اگر قاعدہ نامہ مؤثر طور پر ثابت نہ کر سکے کہ سیمیولیٹر ناممکن ہے، تو وہ حملے جنہیں حفاظتی تعریف کے اندر اسی رد کی ضرورت ہو، روکے جا سکتے ہیں۔

پھر بھی یہ دلچسپ کیوں ہے

کرپٹوگرافی اکثر کسی مشکل حسابی مسئلے کو حفاظت میں بدلتی ہے۔ Factoring مشکل ہے، اس لیے RSA طرز کے مفروضے مفید بنتے ہیں۔ Lattice مسائل مشکل ہیں، اس لیے lattice کرپٹوگرافی بنتی ہے۔ یہاں مشکل زیادہ عجیب ہے: "راز نکالنا مشکل ہے" نہیں، بلکہ "یہ ثابت کرنا مشکل ہے کہ ایک خاص ثبوتی شے موجود نہیں ہو سکتی"۔

اسی لیے مقالہ غیر معمولی محسوس ہوتا ہے۔ یہ اصولِ موضوعہ اور رسمی قاعدہ ناموں کو تقریباً کرپٹوگرافک وسائل کی طرح برتتا ہے۔ معمول کی ناممکنیت صحتِ ثبوت اور سیمولیشن کے درمیان تناؤ دکھاتی ہے۔ Ilango اس تناؤ کو ثبوتی نظریے کے پردے کے پیچھے رکھتا ہے: سیمیولیٹر حقیقت میں غائب ہے، مگر رسمی نظام مؤثر طور پر اس عدم موجودگی کو ظاہر نہیں کر سکتا۔

قاری کے لیے حیرت یہ نہیں کہ یہ آج کے زیرو نالج نظاموں کی جگہ لے لے گا—کم از کم براہِ راست تو شاید نہیں۔ حیرت یہ ہے کہ ریاضیاتی منطق کی ایک حد کو تعمیری طور پر استعمال کیا جا سکتا ہے: صرف دیوار کے طور پر نہیں، پردے کے طور پر بھی۔

شواہد کتنے مضبوط ہیں؟

یہ قضیہ پر مبنی مقالہ ہے، اس لیے یہاں "شواہد" کا مطلب حیاتیات یا فلکیات سے مختلف ہے۔ سوال یہ نہیں کہ تجربہ دوبارہ ہوا یا نہیں؛ سوال یہ ہے کہ تعریفیں، مفروضے اور ثبوت کی زنجیر دعوے کو سہارا دیتی ہیں یا نہیں۔

ثبوت رسمی ہے اور مفروضے واضح ہیں۔ یہ مفروضے معمولی نہیں۔ proofs witness-indistinguishable non-interactive کرپٹوگرافی میں معروف اشیا ہیں اور کئی قائم شدہ مفروضاتی مجموعوں سے حاصل ہوتے ہیں۔ "کوئی بہترین ثبوتی نظام نہیں" کا قیاس ثبوتی پیچیدگی کا مرکزی سوال ہے۔ **BPP = P** ایک معیاری derandomization مفروضہ ہے، جو صرف وسیع تر قابلِ ابطال خصوصیات والے قضیے میں استعمال ہوتا ہے۔

مقالہ یہ بھی دلیل دیتا ہے کہ یہ مفروضے من مانا سہارا نہیں بلکہ تقریباً درست قیمت ہیں: الٹی سمت کا نتیجہ دکھاتا ہے کہ وہ بنیادی طور پر ضروری بھی ہیں—اگر ایسی ساختیں موجود ہوں تو proofs witness-indistinguishable non-interactive بھی موجود ہونے چاہییں، اور معیاری functions one-way ماننے پر کوئی بہترین ثبوتی نظام بھی نہیں ہونا چاہیے۔ مفروضوں کو رد کرنا خود ثبوتی پیچیدگی، کرپٹوگرافی یا پیچیدگی نظریے میں بڑی دریافت ہوگی۔

مگر نتیجہ مشروط ہے، اس لیے اعتماد بھی مشروط ہونا چاہیے۔ اگر مفروضے غلط نکلیں تو قضیے کی تعبیر بدل جائے گی۔ اور اگر مفروضے درست بھی ہوں، تب بھی ضمانت مکمل کلاسیکی زیرو نالج نہیں بلکہ مقالے کا نرم کیا ہوا، ثبوتی نظریے پر مبنی تصور ہے۔

مناسب اعتماد یہ ہے: زیادہ اعتماد کہ مقالہ ایک مربوط مشروط امکانی نتیجہ ثابت کرتا ہے؛ درمیانہ اعتماد کہ اس کے مفروضے ہماری حقیقی کرپٹوگرافک دنیا کو اچھی طرح بیان کرتے ہیں؛ اور فوری عملی نتائج پر کم اعتماد۔

یہ کیوں اہم ہے

مقالہ ایک ایسا راستہ کھولتا ہے جو کلاسیکی نظریہ میں بند سمجھا جاتا تھا۔

کلاسیکی نظریہ کہتا ہے کہ کامل زیرو نالج ایک پیغام، صفر سیٹ اپ اور کامل صحتِ ثبوت کے ساتھ حاصل نہیں کیا جا سکتا۔ Ilango کی تجویز یہ ہے کہ اگر ہم زیرو نالج کی ان نتائج پر توجہ دیں جنہیں حفاظتی کھیل میں جانچا جا سکتا ہے، اور تعریف کو اس بات پر منحصر ہونے دیں کہ رسمی قاعدہ نامہ مؤثر طور پر کیا رد کر سکتا ہے، تو مفید رویّے کا بڑا حصہ واپس حاصل کیا جا سکتا ہے—ایک پیغام، صفر سیٹ اپ اور کامل صحتِ ثبوت کے ساتھ۔

یہ معمولی تعریفاتی تبدیلی نہیں، بلکہ کرپٹوگرافک ضمانتوں کو دیکھنے کا ایک مختلف طریقہ ہے۔ صرف یہ نہ پوچھیں کہ کیا شے حقیقت میں موجود ہے؛ یہ بھی پوچھیں کہ آپ کا رسمی قاعدہ نامہ کس چیز کے عدم وجود کو ثابت کر سکتا ہے۔ ناقابلِ اثباتیت کو محض فلسفیانہ رکاوٹ کے بجائے ساختی وسیلے کے طور پر استعمال کریں۔

عملی دنیا کل نہیں بدلے گی، مگر تصوراتی نقشہ بدلتا ہے۔ اب ایک رسمی معنی موجود ہے جس میں "کوئی مؤثر طور پر ثابت نہیں کر سکتا کہ راز فاش ہوا" اتنا مضبوط ہو سکتا ہے کہ "راز فاش نہیں ہوا" سے مطلوب بہت سی کھیل پر مبنی حفاظتی خصوصیات واپس حاصل کی جا سکیں۔

اسی لیے title میں Gödel ہے۔

صاف خلاصہ

زیرو نالج ثبوت میں ثبوت پیش کرنے والا، گواہ ظاہر کیے بغیر، تصدیق کنندہ کو قائل کرتا ہے کہ بیان درست ہے۔ کلاسیکی ناممکنیت کے نتائج کہتے ہیں کہ بغیر کسی ابتدائی ترتیب کے زیرو نالج کو ایک ہی پیغام میں سمیٹتے ہوئے کامل صحتِ ثبوت برقرار نہیں رکھی جا سکتی۔ Ilango Rahul کا مقالہ ان نتائج کو رد نہیں کرتا۔ اس کے بجائے یہ ایک کمزور تصور، **مؤثر زیرو نالج**، متعین کرتا ہے: اس میں حقیقی سیمیولیٹر کے وجود کی شرط کے بجائے منتخب رسمی ثبوتی نظام — مثلاً ZFC — مؤثر طور پر یہ ثابت نہ کر سکے کہ ایسا سیمیولیٹر موجود نہیں۔ ایک بڑے کرپٹوگرافک مفروضے (غیر تفاعلی witness-indistinguishable proofs) اور ثبوتی پیچیدگی کے مفروضے (کہ کوئی بہترین ثبوتی نظام موجود نہیں) کے تحت، مقالہ NP/SAT کے لیے ایک پیغام والے، بغیر ابتدائی ترتیب کے، کامل صحتِ ثبوت رکھنے والے prover بناتا ہے جو کلاسیکی زیرو نالج کی قابلِ ابطال کھیل پر مبنی خصوصیات ایک ایک کر کے حاصل کرتے ہیں۔ ایسا ایک واحد prover جو تمام "قدرتی" خصوصیات کو سمیٹ لے، مزید قیاسی توسیع ہے؛ ہر قابلِ ابطال خصوصیت کو بیک وقت حاصل کرنا غالباً ناممکن ہے کیونکہ ثبوت دوبارہ استعمال کیے جا سکتے ہیں۔ نتیجہ نظریاتی اور مشروط ہے، عملی طور پر تعینات کرپٹوگرافک جز نہیں، مگر ثبوتی نظریے کی ناقابلِ اثباتیت کو کرپٹوگرافک وسیلہ بنانے کا نیا راستہ دکھاتا ہے۔

بلا مبالغہ جانچ

مقالہ کیا دکھاتا ہے: بیان کردہ مفروضوں کے تحت NP/SAT کے لیے ایک پیغام والے، بغیر سیٹ اپ، کامل صحتِ ثبوت رکھنے والے طریقے بنائے جا سکتے ہیں جو کسی منتخب ثبوتی نظام کے لحاظ سے مؤثر طور پر زیرو نالج ہوں، اور کلاسیکی زیرو نالج کی ہر قابلِ ابطال کھیل پر مبنی حفاظتی خاصیت کو الگ الگ حاصل کر سکیں۔

کیا قرینِ قیاس ہے مگر بلا شرط ثابت نہیں: درکار ثبوتی پیچیدگی اور کرپٹوگرافک مفروضے درست ہیں۔ یہ سنجیدہ اور خوب مطالعہ

شدہ مفروضے ہیں—اور مقالہ دکھاتا ہے کہ وہ بڑی حد تک ضروری بھی ہیں—مگر بہرحال مفروضے ہیں۔

یہ کیا نہیں دکھاتا: باہمی گفتگو کے بغیر، سیٹ اپ کے بغیر اور کامل صحتِ ثبوت کے ساتھ کلاسیکی زیرو نالج، عملی تعیناتی کے لیے تیار نظام، ثبوت کی deniability یا دوبارہ استعمال نہ ہو سکنے کی ضمانت، یا یہ کہ Gödel کا incompleteness قضیہ خود کرپٹوگرافی کو محفوظ بناتا ہے۔

اہم حدود: ضمانت زیرو نالج کی ایک نرم کی گئی تعریف ہے، سب سے وسیع ورژن کئی مفروضوں پر منحصر ہے، ایک ہی عالمگیر ثبوت پیش کرنے والے کے بارے میں کچھ دعوے قیاسی ہیں، اور نتیجہ بنیادی نظری تحقیق ہے۔

عام قاری کو کتنا اعتماد ہونا چاہیے؟ تعریفیں قبول ہوں تو اس مشروط نظری نتیجے کی اہمیت پر زیادہ اعتماد۔ مفروضے حقیقی دنیا کی حسابی مشکل کو اچھی طرح بیان کرتے ہیں، اس پر درمیانہ اعتماد۔ فوری عملی تعیناتی پر کم اعتماد۔ محفوظ خلاصہ یہ ہے: مقالہ زیرو نالج کے ناممکنیت کے قضیے نہیں توڑتا؛ وہ ثبوتی نظریے کا ایک راستہ دکھاتا ہے جس سے انہی قیود کے اندر بہت سی عملی، کھیل پر مبنی حفاظتی خصوصیات واپس حاصل کی جا سکتی ہیں۔

ماخذ

Ilango, 2025/1296 ePrint IACR
https://eprint.iacr.org/2025/1296

FOCS 2025, DOI 10.1109/FOCS63196.2025.00058
https://doi.org/10.1109/FOCS63196.2025.00058