The CLEAN PAPER

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

يمكن لبرهان تشفيري أن يخفي سره بجعل إثبات غياب المُحاكي صعبًا

تسمح إثباتات انعدام المعرفة لشخص بإثبات عبارة من دون كشف الشاهد. وتقول النظرية الكلاسيكية إنك لا تستطيع الحصول على ذلك بالمعنى الكامل مع رسالة واحدة، ومن دون إعداد موثوق، ومع سلامة تامة. لا تجعل ورقة *Ilango Rahul* هذه الاستحالة تختفي. بل تغيّر الهدف: بدل اشتراط وجود مُحاكٍ فعلًا، تسأل ألا يستطيع نظام الإثبات المختار بكفاءة إثبات أن المُحاكي غير موجود. وتحت افتراضات كبيرة من تعقيد البراهين والتشفير، يكفي ذلك لاستعادة النتائج القابلة للتكذيب والمبنية على ألعاب لانعدام المعرفة، خاصية بعد خاصية. ليست الفكرة بدائية إنترنت جاهزة للاستخدام، بل طريقة من نظرية البراهين لتحويل عدم القابلية الرياضية للإثبات إلى غطاء تشفيري.

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

الحيلة ليست في إثبات أن السر مخفي

لنبدأ بأبسط صورة لإثباتات انعدام المعرفة (zero-knowledge).

تريد أليس إقناع بوب بأن لغز سودوكو له حل. إذا أرسلت إليه الحل، سيقتنع بوب، لكن اللغز سيكون قد فسد. ما تريده أغرب: إثبات أن هناك حلًا، من دون كشف الحل نفسه.

هذا هو وعد **إثبات انعدام المعرفة**. يقنع المُثبِت (أليس) المُتحقِّق (بوب) بأن عبارة ما صحيحة، من دون أن يكشف شيئًا يتجاوز حقيقة العبارة.

المشكلة أن لهذا الوعد ثمنًا. يملك البرهان الرياضي العادي ميزتين مريحتين. فهو **رسالة واحدة**: تكتبه، وتسلمه، ثم تنصرف. وهو أيضًا **تام السلامة** (perfectly sound): إذا كانت العبارة كاذبة فلا يوجد لها برهان صالح أصلًا. وتقول نتائج الاستحالة الكلاسيكية إن انعدام المعرفة لا يستطيع الاحتفاظ بكلتا الميزتين — بل إن المشكلة لا تقتصر على جمعهما معًا؛ كل واحدة منهما محظورة بمفردها أيضًا.

أولًا، يحتاج إثبات انعدام المعرفة إلى حوار. إذا أرسلت أليس رسالة واحدة فقط، من دون إعداد موثوق جرى ترتيبه مسبقًا، تنهار ضمانة انعدام المعرفة — ويظل هذا صحيحًا مهما كان مقدار السلامة الذي تقبل بالتخلي عنه في المقابل.

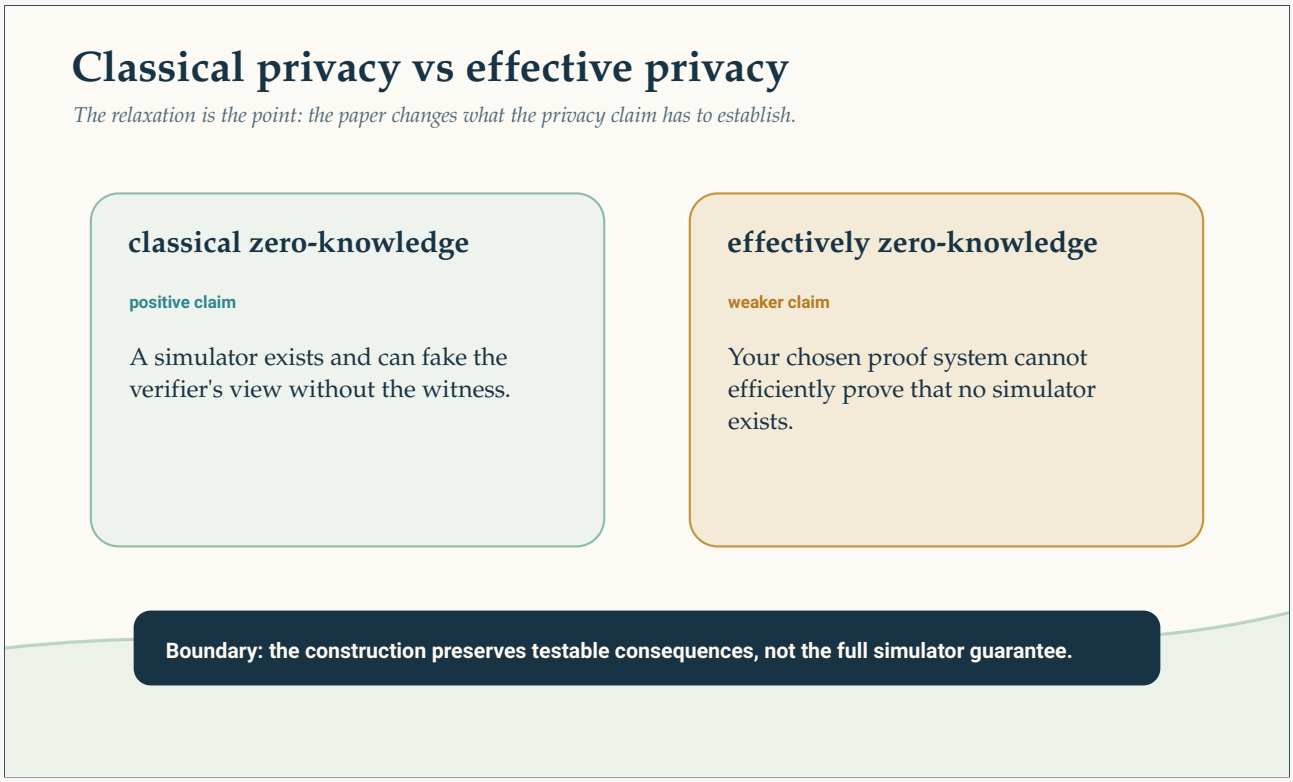
ثانيًا، يحتاج إثبات انعدام المعرفة إلى قدر صغير من احتمال الخطأ. يتبين أن المطالبة بالسلامة التامة تدمر التفاعل بهدوء أيضًا: فالمتحقق الذي لا يمكن خداعه مطلقًا، مهما كانت اختياراته العشوائية، يستطيع ببساطة تثبيت تلك الاختيارات مقدمًا — وبمجرد أن يصبح سلوك المتحقق قابلًا للتنبؤ، يمكن لأليس أن تجيب عن كل شيء في رسالة واحدة، فنعود بالضبط إلى الحالة التي ثبت أنها لا تعمل.

تتناول ورقة Ilango Rahul طريقةً للالتفاف حول هذا الجدار المزدوج. ليس بالتظاهر بأن الجدار غير موجود، ولا بإنتاج انعدام معرفة كلاسيكي في بيئة يستحيل فيها ذلك. الحركة أدق: إضعاف معنى «لا يكشف شيئًا»، لكن بطريقة تحافظ على خصائص الأمان التي يستطيع علماء التشفير اختبارها فعليًا.

يسمى الناتج **انعدام المعرفة الفعّال** (effectively zero-knowledge).

يصطدم انعدام المعرفة بثلاثة أبواب مغلقة — التفاعل، والإعداد الموثوق، وعدم السلامة التامة. يتسلل بناء Ilango من باب مختلف: كتاب القواعد لا يستطيع بكفاءة أن يدحض وجود المُحاكي.

Original diagram — The Clean Paper CC BY 0.4



يسأل انعدام المعرفة الكلاسيكي هل يوجد مُحاكٍ فعلًا؛ أما «انعدام المعرفة الفعّال» فيسأل فقط هل يستطيع كتاب القواعد الذي اخترته أن يثبت بكفاءة أن

مُحاكيًا كهذا لا يمكن أن يوجد. هذا السؤال الأضعف هو ما يسمح للبناء بالاحتفاظ برسالة واحدة، ومن دون إعداد، ومع سلامة تامة.

Original diagram — The Clean Paper CC BY 0.4

الاختبار القديم: يوجد مُحاكٍ

تصوغ النظرية الكلاسيكية لانعدام المعرفة الفكرة باستخدام مساعد خيالي يسمى **المُحاكي** (simulator).

الفكرة هي الآتية: تخيل جين، التي **لا تعرف** سر أليس. إذا استطاعت جين أن تولّد بنفسها تمامًا براهين تبدو مثل البراهين التي كان بوب سيحصل عليها من أليس، فهذا يعني أن براهين أليس لم تعلّم بوب شيئًا جديدًا. كان بوسع جين تزييف التجربة أصلًا من دون معرفة سر أليس.

لذلك يطلب انعدام المعرفة الكلاسيكي مُحاكيًا حقيقيًا. يجب أن توجد خوارزمية كفؤة تستطيع إنتاج براهين تبدو حقيقية من دون معرفة السر — أي **الشاهد** (witness) بالمصطلح التقني؛ وفي السودوكو يكون الشاهد ببساطة الشبكة المحلولة.

هذا التعريف قوي، لكنه أيضًا النقطة التي تضرب عندها الاستحالة القديمة. والحدس هو التالي: البرهان غير التفاعلي حقًا مجرد سلسلة من الرموز. بعد أن يحصل بوب على هذه السلسلة يمكنه عرضها على شخص آخر؛ فقد اكتسب القدرة على إثبات العبارة للآخرين، وهذا يبدو أصلًا أكثر من «لا شيء». وتحول المبرهنات الكلاسيكية هذا الحدس إلى نتائج الاستحالة المذكورة أعلاه.

الخصائص الثلاث التي تصر عليها هذه الورقة

قيود: ثلاثة الورقة عنوان يذكر

لا تفاعل: ترسل أليس سلسلة إثبات واحدة. لا يوجد بروتوكول ذهاب وإياب.

لا إعداد: لا تعتمد أليس وبوب على سلسلة مرجعية مشتركة موثوقة أو على عشوائية عامة مرتبة مسبقًا. كثير من الأنظمة المسماة «إثباتات انعدام معرفة غير تفاعلية» ما زالت تعتمد على إعداد مسبق؛ أما هذه الورقة فتعني صفر إعداد.

سلامة تامة: لا توجد للعبارة الكاذبة أي حجة مقبولة. ليس «تكاد لا تُقبل أبدًا»؛ بل لا يوجد برهان صالح أصلًا.

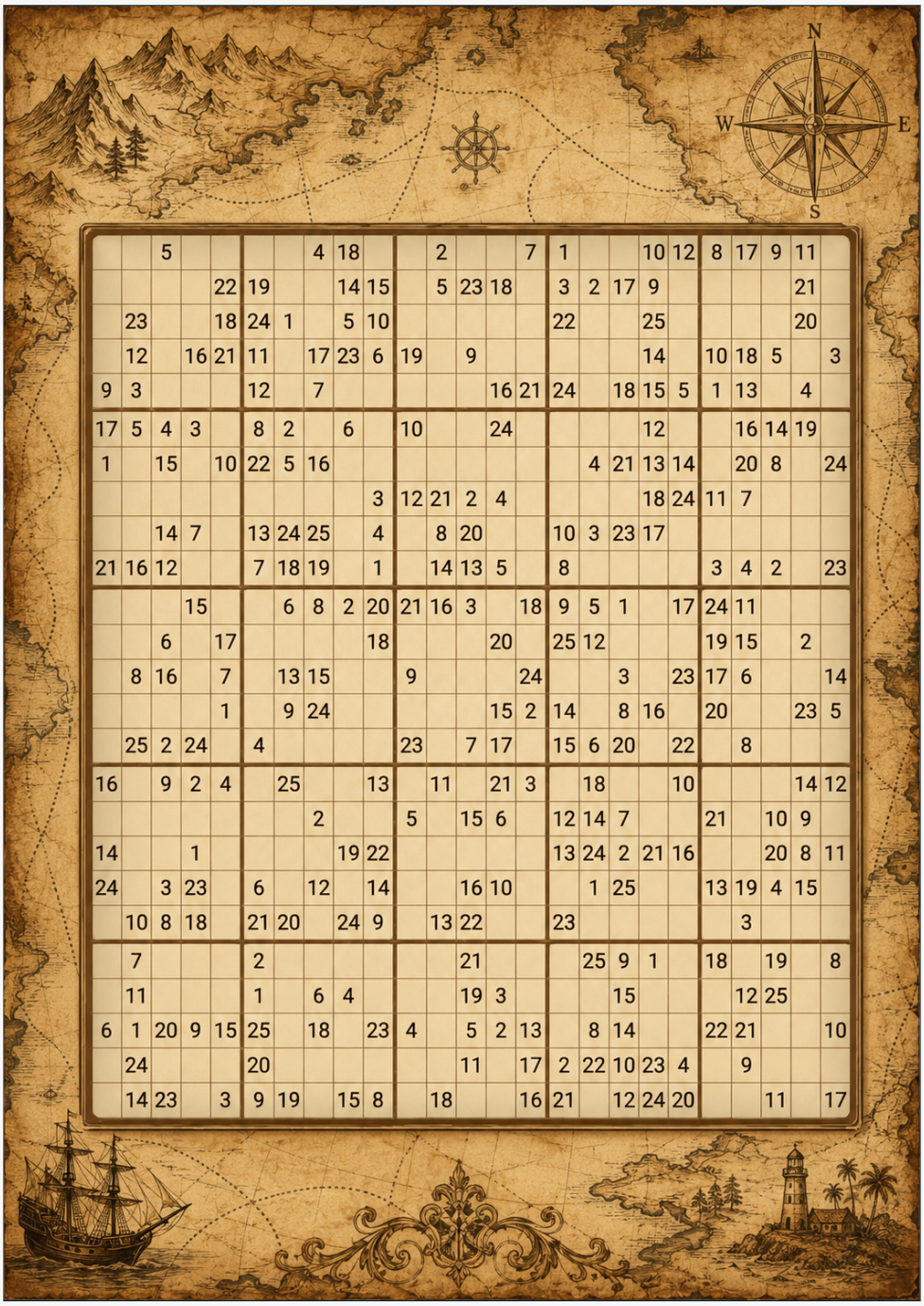
وهذه الخصائص الثلاث هي بالضبط ما يملكه البرهان الرياضي المكتوب العادي — وكما شرحنا أعلاه، لا يستطيع انعدام المعرفة الكلاسيكي الاحتفاظ بها.

نسخة «سودوكو عملاقة» لشرح الفرق

إليك طريقة مبسطة عمدًا للشعور بالفرق.

لا تستخدم سودوكو عادية 9×9 في الجزء الجاد من التشبيه. إنها صغيرة ومحدودة أكثر من اللازم: يستطيع الحاسوب ببساطة حلها، أو إثبات أنه لا حل لها. بدلًا من ذلك، تخيل عائلة من ألغاز **MegaSudoku(n)**. كبّر القاعدة المعتادة: اختر حجم كتلة n، واجعل $N = n^2$، ثم ابنِ شبكة $N\times N$ مقسمة إلى كتل $n\times n$ وبها N رمزًا. السودوكو العادية ليست سوى الحالة الصغيرة $n = 3$ و$N = 9$: شبكة 9×9، وكتل 3×3، وتسعة رموز. تبدأ قصة تعقيد البراهين فقط عندما يُسمح لـn بالنمو، وعندما تستطيع الشبكة حمل أدوات إضافية (gadgets) تجعلها تتصرف مثل صيغة SAT متنكرة في شكل سودوكو. وصيغة SAT ليست سوى قائمة من قيود نعم/لا: هل تستطيع إسناد قيم true/false

للمتغيرات بحيث يتحقق كل قيد؟



سودوكو 25×25: يمكن التحقق من قواعدها من دون كشف الشبكة المكتملة — بديل بصري عن برهان يتحقق من حل مخفي، أي الشاهد.

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

السودوكو وSAT: اللغز نفسه بزيين مختلفين

السهل الاتجاه كتابة ويمكن الاتجاهين، في يعمل التحويل استعارة. ليس «SAT صيغة مثل «تتصرف أن تستطيع سودوكو إن القول كاملًا.

من السودوكو إلى SAT. لا تتحدث SAT إلا بلغة true/false، لذلك نعطيها متغيرًا بوليانيًا لكل ثلاثية (صف، عمود، قيمة): يعني $x(r,c,v)$ أن «الخلية في الصف r والعمود c تحتوي القيمة v». سودوكو 4×4 (كل 2×2، والقيم 1–4) تحتاج إلى 4·4·4 = 64 متغيرًا؛ أما 9×9 الكلاسيكية فتحتاج 729. ثم تتحول كل قاعدة من قواعد السودوكو إلى مجموعة من العبارات الشرطية (clauses). (الـclause هي OR لمتغيرات أو نفيها؛ والصيغة الكاملة هي AND لجميع الـclauses.)

كل خلية تحمل قيمة واحدة على الأقل — clause واحدة لكل خلية:

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

كل خلية تحمل قيمة واحدة على الأكثر — clause من نوع «ليس الاثنان معًا» لكل زوج من القيم:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \dots$$ وهكذا لكل الأزواج الستة.

كل صف يحتوي كل قيمة — للصف 1 والقيمة 3: مرة واحدة على الأقل،

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

ومرة واحدة على الأكثر: $\neg x(1,1,3) \vee \neg x(1,2,3)$، وهكذا لكل زوج من الخلايا في الصف.

الأعمدة والكتل — مجموعات مماثلة تمامًا، ويتغير فقط تجمع الخلايا. بالنسبة إلى الكتلة العليا اليسرى والقيمة 2:

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

مع clauses «ليس الاثنان معًا» لكل زوج.

الأرقام المطبوعة مسبقًا — وهي أبسط جزء: كل رقم معطى هو clause بمتغير واحد. فإذا كان الرقم 3 مطبوعًا في الزاوية العليا اليسرى تصبح العبارة

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

يكون AND لكل هذه العبارات قابلاً للإرضاء إذا وفقط إذا كان للسودوكو حل — وإسناد القيم الذي يرضي الصيغة هو الحل: اقرأ أي من $x(r,c,v)$ قيمته true واملأ الشبكة. في سودوكو 9×9 ينتج عن ذلك 729 متغيرًا وبضعة آلاف من الـclauses، وهي مهمة يحلها محلل SAT حديث في أجزاء من الألف من الثانية. لاحظ clause الرقم المعطى: $x(1,1,3)$ فهي تقول «هذه الخلية تساوي 3 بالضبط»، لا «هذه الخلايا كلها مختلفة» — وهذه هي اللامتماثلية نفسها التي ستجبرنا على إضافة حيلة خاصة لخلايا الأرقام المعطاة في ملاحظة البروتوكول أدناه.

من SAT إلى السودوكو. تحتاج الورقة إلى الاتجاه المعاكس والأصعب: انطلاقًا من صيغة SAT اعتباطية، ابنِ سودوكو عملاقة لها حل إذا وفقط إذا كانت للصيغة قيمة مُرضية. قواعد السودوكو الأصلية لا تستطيع قول أكثر من «هذه الخلايا كلها مختلفة»، لذلك يجب بناء القيود المنطقية الاعتباطية — وهذه بالضبط وظيفة الـgadgets. الـgadget تجمع صغير جاهز من الخلايا، واحد لكل clause في الصيغة، تؤدي فيه خلايا معينة دور المتغيرات (فالرمز الذي تحمله يشفر true أو false)، وتُهندس القيود الداخلية للتجمع بحيث تكون تعبئاته القانونية الوحيدة هي الإسنادات التي ترضي تلك الـclause. وهذه حرفة معيارية من براهين NP-completeness؛ وقد نُفذت للسودوكو المعممة بواسطة Yato وSeta عام 2003.

ويعني الاتجاهان معًا أن سودوكو N×N وSAT هما المشكلة نفسها بزيين مختلفين. وهذا ما يسمح لهذا المقال — وللورقة — بأن يروي قصة عن كامل NP باستخدام شبكات ورموز.

ما زال من السهل تصور الشاهد. تعرف أليس تعبئة كاملة وصحيحة للسودوكو العملاقة. يريد بوب أن يقتنع بوجود تعبئة كهذه، لكن أليس

لا تريد كشفها. إذا أرسلت إليه التعبئة كاملة، يقتنع بوب، لكن السر يضيع.

في النسخة الكلاسيكية من انعدام المعرفة تتفاعل أليس وبوب. يستخدم نموذج ذهني قديم قطعًا مغطاة. تخفي أليس الشبكة المحلولة، وتعيد تسمية الرموز سرًا قبل كل جولة، ثم تسمح لبوب بفحص قيد محلي واحد اختير عشوائيًا: صف، أو عمود، أو كتلة، أو gadget. إذا أظهرت الخلايا المفتوحة رموزًا كلها مختلفة، تزداد ثقة بوب. ثم تُغطى كل الأشياء من جديد وتُعاد تسمية الرموز مرة أخرى. (هناك تفصيلة: الأرقام المعطاة أصلًا في اللغز تحتاج إلى حيلة إضافية، لأن إعادة تسمية الرموز تخفيها هي أيضًا. تشرح الملاحظة التالية كيف تعالج البروتوكولات الكلاسيكية ذلك؛ أما الصورة المبسطة فتكفي لما سيأتي.)

كيف تتعامل البروتوكولات الكلاسيكية فعلًا مع خلايا الأرقام المعطاة

وشرط بعض»، عن بعضها مختلفة الخلايا «هذه كلها تقول والكتلة والعمود الصف فقواعد عمياء. نقطة التسمية إعادة حيلة لدى إعادة وبعد بالضبط»، 5 تحتوي الخلية «هذه يقول المعطى الرقم لكن للرموز. تسمية إعادة أي تحت صحيحًا يبقى الكامل الاختلاف وإذا شيء. من التحقق يستطيع فلا σ. التسمية إعادة يعرف أن دون من — ما مقنع رمز — $\sigma(5)$ سوى بوب يرى لا التسمية هذا عن شيئًا يثبت لا وهذا أصلًا، المطبوعة الأرقام تجاهل مع ما صحيحة شبكة هناك أن إثبات لأليس يمكن إصلاح، بلا هذا تركنا معياريان. إصلاحان الكلاسيكية الأدبيات لدى اللغز.

لوحة الرموز. أضف صفًا إضافيًا من N خلية إلى الشبكة المخفية — لوحة تملؤها أليس بالرموز 1...N بترتيب عام ثابت، ثم تعيد تسميتها مع كل شيء آخر، فتحتوي $\sigma(1)$...σ.(N) يصبح لاختبار بوب العشوائي خيار إضافي: إلى جانب اختيار صف أو عمود أو كتلة أو gadget لفتحه، يمكنه اختيار **لوحة الرموز مع خلية رقم معطى واحدة.** تكشف أليس الاثنين؛ فتُظهر اللوحة إعادة التسمية لتلك الجولة، ويتحقق بوب من أن خلية الرقم المعطى تعرض بالضبط النسخة المعاد تسميتها من الرقم المطبوع. يظل هذا عديم المعرفة لأن بوب لا يتعلم سوى σ — وهي تُختار من جديد كل جولة ولا قيمة لها بمفردها — وقيمة خلية كان يعرفها أصلًا من اللغز. لا يتسرب شيء عن الخلايا السرية، ويمكن للمُحاكي تزييف المشهد باختيار σ عشوائية. والبروتوكول سليم لأن أليس الغشاشة تُكتشف باحتمال ثابت في كل جولة، وتُكرر الجولات حتى يصبح الشك ضئيلًا جدًا.

ترجمة الأرقام المعطاة إلى قيود. هناك نسخة أكثر بنيوية تزيل الاختبار الخاص بدلًا من إضافته. بدل التحقق من قيمة الرقم المعطى، أجبِرها بقيود اختلاف: اربط خلية الرقم المعطى بكل خلية من لوحة الرموز ما عدا الخلية التي تحمل قيمته — «مختلفة عن $\sigma(1)$، ومختلفة عن $\sigma(2)$، ...، ومختلفة عن كل شيء ما عدا $\sigma(5)$». عندها يكون الرمز الوحيد الذي يمكن أن تحمله الخلية قانونيًا هو رمز الرقم المعطى. وهكذا تصبح كل القيود مرة أخرى من نوع «هاتان الخليتان مختلفتان» — ثابتة تحت إعادة التسمية وقابلة للتحقق تمامًا مثل الصف. وهذه هي الحيلة نفسها المستخدمة للرؤوس الملونة مسبقًا في بروتوكول تلوين الرسوم البيانية الكلاسيكي، وهي روح كلمة *gadgets* أعلاه: في صورة MegaSudoku-as-SAT تُحوّل الأرقام المعطاة إلى gadgets من قيود عدم المساواة مثل أي قيد آخر.

البروتوكول المادي. بروتوكول البطاقات الواقعي للسودوكو (Gradwohl وNaor وPinkas وRothblum، 2007) لا يستخدم إعادة تسمية أصلًا، ويحسم الأرقام المعطاة قبل أن يبدأ الإخفاء. لكل خلية تضع أليس ثلاث بطاقات متطابقة تحمل قيمة الخلية — مقلوبة الوجه في الخلايا السرية، لكن **مكشوفة الوجه في خلايا الأرقام المعطاة**، بحيث يرى بوب بعينيه أن الأرقام المعطاة محترمة قبل قلب البطاقات. ثم تدخل بطاقة من كل خلية إلى حزمة صفها، وأخرى إلى حزمة عمودها، وثالثة إلى حزمة كتلتها؛ تُخلط كل حزمة وتُكشف، ويتحقق بوب من أنها تحتوي جميع الرموز N. يدمّر الخلط معلومات الموضع (وهذا هو انعدام المعرفة)، لكن الأرقام المعطاة ثُبتت بالفعل لحظة توزيع البطاقات.

في كلتا الحالتين، الدرس هو نفسه الذي يعود إليه المقال مرارًا: بروتوكول انعدام المعرفة هو ضبط دقيق لما يبقى ظاهراً من الحقائق بعد الإخفاء. إعادة التسمية تحافظ على «كلها مختلفة» وتمحو «تساوي 5» — لذلك يجب إعادة إدخال «تساوي 5» بوسيلة أخرى.

هذا ليس البروتوكول الموجود في الورقة. إنه النموذج الذهني لانعدام المعرفة الكلاسيكي:

- تتبادل أليس وبوب الرسائل ذهابًا وإيابًا.
- يختار بوب اختبارات عشوائية.
- تكشف أليس الاتساق المحلي فقط، لا الحل الكامل.
- يعمل برهان الخصوصية بإظهار أن المشهد الذي يراه بوب كان يمكن توليده من دون حل أليس السري.

إذن يقوم انعدام المعرفة الكلاسيكي على حقيقة إيجابية:

يوجد مُحاكٍ فعلًا.

والآن أزل الأجزاء المريحة. ترسل أليس سلسلة إثبات واحدة ثم تنصرف. لا يوجد إعداد موثوق، ولا سلسلة عشوائية مشتركة أُعدت مسبقًا، ويجب ألا يقبل بوب لغزًا كاذبًا أبدًا. هذه هي البيئة التي لا يستطيع انعدام المعرفة الكلاسيكي البقاء فيها.

نحتاج إلى شخصية أخرى قبل الحيلة. ثبّت **كتاب قواعد**: أي نظام إثبات رسمي بالمعنى المنطقي — مجموعة ثابتة من البديهيات مع قواعد ميكانيكية للتحقق من البراهين الرياضية المكتوبة. وZFC، مجموعة البديهيات القياسية في الرياضيات، هي المثال الأشهر. كل ما يأتي من هنا يُصاغ بالنسبة إلى كتاب قواعد مختار مسبقًا، والاختيار مرن: يعمل البناء مع أي كتاب قواعد تثبته، بما في ذلك ZFC.

(ملاحظة اصطلاحية مأخوذة من الورقة نفسها: عبارة «نظام إثبات» (proof system) هنا تعني دائمًا كتاب القواعد هذا — أي النظام الرسمي الذي يتحقق من البراهين الرياضية — ولا تعني الرسائل التي ترسلها أليس. أما آليتا أليس وبوب فتسميان «المُثبِت» و«المتحقق».)

تحتفظ النسخة ذات الطابع الغودلي بقصة السودوكو العملاقة، لكنها تغير البرهان.

اختر نظام قيود ثانيًا بالحجم الظاهر نفسه، وسمّه **D**. في القصة، S وD لغزان من MegaSudoku(n) بالتنسيق نفسه. خلف الكواليس ربما بدأ D كصيغة منطقية صعبة بحجم مختلف؛ وإذا لزم الأمر يمكن حشوها بقيود وهمية غير مؤذية كي تلائم الشبكة نفسها. يُبنى D من صيغة منطقية **غير قابلة للإرضاء فعلًا** :(unsatisfiable) لا يوجد إسناد للقيم يجعل جميع قيودها صحيحة، مثل لغز مكسور لا توجد له أي تعبئة قانونية كاملة. مثال بسيط سيكون صيغة تطالب في الوقت نفسه بأن X» صحيحة» وأن X» خاطئة». إذن لا توجد لD تعبئة صحيحة.

لكن يجب ألا يكون D لغزًا مكسورًا يسهل فضحه. المثال البسيط أعلاه يفشل لهذا السبب: يستطيع أي كتاب قواعد دحض X» وnot-X» في سطر واحد. يجب أن تكون D كاذبة بطريقة لا يستطيع كتاب القواعد المختار إثباتها بحجة قصيرة. فإذا استطاع كتاب القواعد دحض D ببرهان قصير، انهارت القصة التالية: يمكن عندها استبعاد الطريق البديل الذي ربما كان يسمح بإنتاج البراهين من دون سر أليس، ومعه ينهار ضمان الخصوصية. لذلك تُختار D من عائلة لا يستطيع كتاب القواعد الثابت دحضها بكفاءة: لا يوجد داخل ذلك النظام برهان قصير على أن D بلا حل.

يصبح برهان أليس ذو الرسالة الواحدة عن عبارة «إما/أو»:

إما أن السودوكو العملاقة الحقيقية S لها حل، أو أن الطُّعم D له حل.

هذه هي الوصلة المنطقية. لا تُولَّد D بطريقة سحرية تجعل S صحيحة. ولا يقول البرهان D» ليس لها حل، إذن S لها حل». بل يثبت الفصل **S أو D**. وتقول السلامة التامة إن الفصل الكاذب لا يمكن أن يملك برهانًا صالحًا. وبما أن D كاذبة في الواقع — لا حل لها — فلا يمكن أن يكون الفصل صحيحًا إلا إذا كانت S صحيحة. لذلك إذا قُبل البرهان، فلا بد أن يكون لS حل. لا يستطيع الطُّعم جعل S كاذبة تصبح صحيحة.

لكن من أجل الجزء الشبيه بانعدام المعرفة، اسأل ماذا كان سيحدث لو كان لـD حل. كان حل الطُّعم سيعمل كشاهد بديل. وكان سيسمح لشخص بإنتاج البراهين من دون معرفة حل أليس الحقيقي للسودوكو العملاقة — أي إنه كان سيعطي مُحاكيًا. في الواقع لا حل لـD، ولذلك هذا الطريق إلى المُحاكي مغلق. لكن الفكرة أن كتاب القواعد لا يستطيع أن يثبت بكفاءة أن الطريق مغلق.

إذن لـD وظيفتان. من أجل **السلامة**، D كاذبة، ولذلك فإن برهانًا صالحًا على S» أو «D يجبر S على أن تكون صحيحة. ومن أجل **انعدام المعرفة الفعّال**، يصعب دحض ،D ولذلك لا يستطيع كتاب القواعد أن يستبعد بسرعة طريق الطُّعم الذي كان سيجعل المحاكاة ممكنة.

وهكذا لم يعد اختبار الأمان هو:

هل نستطيع إثبات أن مُحاكيًا موجود فعلًا؟

بل يصبح:

هل يستطيع كتاب القواعد لديك أن يثبت بكفاءة أن وجود المُحاكي مستحيل؟

إذا كانت الإجابة لا، ينتج شيء قوي على نحو مفاجئ: كل ضمان أمني (أ) يمكن ملاحظته بإجراء اختبار، و(ب) يثبت داخل كتاب القواعد أنه يتبع من وجود مُحاكٍ، يتحقق بالفعل. فأي هجوم ناجح على أي من هذه الضمانات كان سيشكل بنفسه الدحض القصير المفقود، وهذا الدحض القصير غير موجود. هذا هو الجزء «الفعّال» في انعدام المعرفة الفعّال.

وهكذا يكون الفرق التعليمي:

انعدام المعرفة الكلاسيكي: البراهين آمنة لأن مُحاكيًا موجود.

انعدام المعرفة الفعّال على طريقة غودل: نعامل البراهين على أنها آمنة بالنسبة إلى اختبارات الأمان القابلة للملاحظة لأن كتاب القواعد لا يستطيع أن يثبت بكفاءة أن المُحاكي مستحيل.

الادعاء الثاني أضعف. وهو أيضًا ما يسمح للورقة بالاحتفاظ بالخصائص الثلاث التي حطمت النسخة الكلاسيكية: رسالة واحدة، ومن دون إعداد، وسلامة تامة.

الاختبار الجديد: لا تستطيع إثبات غياب المُحاكي

يغير تخفيف Ilango السؤال.

يسأل انعدام المعرفة الكلاسيكي:

هل يوجد مُحاكٍ؟

أما انعدام المعرفة الفعّال فيسأل سؤالًا أضعف:

هل يستطيع كتاب القواعد الذي اخترته أن يثبت بكفاءة أنه لا يوجد مُحاكٍ؟

قد يبدو هذا مراوغة تقنية، لكنه جوهر الفكرة. يعيش البناء في حالة غريبة: لا يوجد مُحاكٍ في الواقع — والورقة واضحة بشأن ذلك — لكن كتاب القواعد الذي ثبّتّه لا يستطيع أن يثبت بكفاءة عدم وجوده. فإذا كانت كل نتيجة سيئة تهمك ستتطلب مثل هذا الدحض، فإن النظام يظل يتصرف كأنه عديم المعرفة بالنسبة إلى تلك النتائج.

هنا يدخل غودل. لا كزينة، ولا بمعنى أن «غودل يجعل التشفير آمنًا». العلاقة من نظرية البراهين. يسمى كتاب القواعد **أمثل** (optimal) إذا كان، بمعنى دقيق، أفضل نظام ممكن: كلما استطاع أي كتاب قواعد دحض صيغة من النوع المعني ببرهان قصير، يستطيع كتاب القواعد الأمثل أن يفعل ذلك أيضًا ببرهان أطول على الأكثر بعامل كثير الحدود. حدس Krajíček وPudlák عام 1989 أن **لا يوجد نظام إثبات أمثل**: أيًا كان كتاب القواعد الذي تثبته، يوجد كتاب آخر يثبت عائلة ما من العبارات الصحيحة بصورة أكثر اختصارًا بكثير. هذه واحدة من الحدوس المفتوحة المركزية في تعقيد البراهين، وهي القريب المحدود، بصيغة نظرية التعقيد، من مبرهنة عدم الاكتمال لغودل: بعض العبارات الصحيحة لا تملك برهانًا قصيرًا في كتاب القواعد الذي ثبّتّه — لا لأنها غير قابلة للإثبات من حيث المبدأ، بل لأن كل كتاب قواعد ثابت يترك بعض الحقائق القصيرة من دون براهين قصيرة.

تفترض الورقة هذا الحدس (بصيغة أقوى قليلًا من نوع «لعدد لانهائي من الأحجام»، وهي صيغة معيارية عندما تُستخدم الحدوس في التشفير). والعائد، بفضل مبرهنة لـKrajíček وPudlák، ملموس: لكل كتاب قواعد توجد سلسلة من الصيغ غير القابلة للإرضاء فعلًا، ولا يستطيع كتاب القواعد دحضها ببراهين قصيرة — والأهم أن خوارزمية كفؤة تستطيع **توليدها**. هذه الخاصية الأخيرة، أي الانتظام (unfiormity)، هي ما يحول الفكرة كلها من ادعاء وجودي إلى خوارزمية فعلية تستطيع أليس تشغيلها: تأتي الطعوم D من خط إنتاج، لا من فراغ.

الحركة التشفيرية هي وضع هذا النقص في قوة الإثبات قيد الاستخدام.

ماذا يفعل البناء؟

إليك بناء الورقة بعد تجريده إلى شكله الأساسي.

ثبّت كتاب قواعد — لنقل ZFC. تحت افتراض تعقيد البراهين، توجد سلسلة قابلة للتوليد بكفاءة من الصيغ غير القابلة للإرضاء في الواقع، لكن كتاب القواعد لا يملك برهانًا قصيرًا على أنها غير قابلة للإرضاء.

والآن ابنِ برهانًا من رسالة واحدة بالشكل التالي:

> إما أن العبارة الحقيقية قابلة للإرضاء، أو أن هذه الصيغة الصعبة الخاصة قابلة للإرضاء.

الصيغة الصعبة الخاصة ليست قابلة للإرضاء. لذلك إذا كانت آلية الإثبات الأساسية تامة السلامة، فإن قبول الرسالة ما زال يعني أن العبارة الحقيقية صحيحة. وهكذا نحصل على السلامة التامة.

لكن بالنسبة إلى الأمان الشبيه بانعدام المعرفة، تخيل أن الصيغة الصعبة الخاصة كانت قابلة للإرضاء. عندها يمكن استخدام شاهدها لمحاكاة البراهين من دون معرفة الشاهد الحقيقي. الصيغة ليست قابلة للإرضاء في الواقع — لكن كتاب القواعد لا يستطيع أن يثبت ذلك بكفاءة. ولذلك لا يستطيع أن يثبت بكفاءة أن المُحاكي مستحيل.

هذه هي نقطة الارتكاز. لا يخفي النظام السر بإنتاج مُحاكٍ كلاسيكي. بل يخفيه، بالنسبة إلى فئة كبيرة من اختبارات الأمان القابلة للملاحظة، خلف عجز كتاب القواعد عن إصدار شهادة بأن المُحاكي غائب.

ماذا تدعي الورقة؟

تأتي المبرهنة الرئيسية على طبقات. والنتيجة الأساسية هي الآتية:

تحت افتراض تشفيري معياري — وجود **إثباتات غير تفاعلية لا يمكن فيها تمييز الشاهد** (non-interactive indistinguishable witness proofs)، وهي كائنات مدروسة جيدًا وتتبع من عدة حزم معروفة من الافتراضات — وتحت حدس تعقيد البراهين القائل إنه **لا يوجد نظام إثبات أمثل (لعدد لانهائي من الأحجام)**، تبني الورقة، لكل اختيار لكتاب القواعد، مُثبِتًا ومتحققًا برسالة واحدة لمسائل NP/SAT، من دون إعداد، مع **سلامة تامة**، ويكونان عديمي المعرفة فعّالًا بالنسبة إلى ذلك الكتاب. (NP/SAT هي «القاسم المشترك الأصعب» القياسي للمسائل الشبيهة بالألغاز؛ والسودوكو العملاقة ليست سوى زي ترتديه.)

أما الادعاء الأوسع بشأن الحفاظ على خصائص الأمان القابلة للتكذيب تجريبيًا، فتضيف الورقة افتراضًا معياريًا آخر: الاعتقاد في إزالة العشوائية **BPP = P** (بصورة تقريبية: أن العشوائية لا تمنح الخوارزميات قوة أساسية إضافية).

وباللغة الخارجة من صياغة المبرهنة:

- البرهان رسالة واحدة.
- لا يوجد إعداد موثوق.
- لا يمكن إثبات العبارات الكاذبة.
- المُثبِت ليس عديم المعرفة بالمعنى الكلاسيكي — فلا يوجد له مُحاكٍ.
- لكن يمكن تحقيق كل نتيجة أمنية قابلة للتكذيب ومبنية على لعبة من نتائج انعدام المعرفة الكلاسيكي في هذه البيئة.

وكلمة «قابل للتكذيب» مهمة. فهي تعني أن فشل الأمان يمكن اختباره بتشغيل خصم داخل لعبة. كثير من تعريفات الأمان التشفيري تأتي بهذا الشكل: هل يستطيع الخصم التمييز بين تشفيرين، أو عكس دالة، أو استعادة شاهد، أو الفوز في تجربة محددة؟ تعطي المبرهنة مُثبِتًا لكل خاصية قابلة للتكذيب، **واحدة في كل مرة**. أما وجود مُثبِت واحد يملك كل الخصائص القابلة للتكذيب دفعة واحدة فمرجح أن يكون مستحيلًا — لأن هجوم إعادة الاستخدام القديم («يستطيع بوب عرض البرهان على الآخرين») هو نفسه خاصية قابلة للتكذيب، وهو يفشل فعلًا هنا. وتقترح الورقة أن مُثبِتًا واحدًا قد يستطيع بصورة معقولة تغطية كل الخصائص القابلة للتكذيب الطبيعية — أي الخصائص التي تظهر فعلًا في الممارسة التشفيرية — لكن هذا الجزء مبرهنة مشروطة تعتمد على مفهوم غير رسمي لـ«طبيعي»، إلى جانب حدس صريح. الضمان موجه إلى الإخفاقات القابلة للملاحظة، لا إلى كل معنى فلسفي أو قائم على المحاكاة للسرية.

هناك نتيجة فرعية ملموسة تستحق الاسم: يعطي البناء أول براهين غير تفاعلية من نوع **إخفاء الشاهد** (witness hiding) مع مُثبِت منتظم — أي «إثبات وجود حل للغز لا يساعدك على العثور على الحل»، من دون تفاعل ولا إعداد — وهو كائن يبدو متواضعًا لكنه قاوم البناء لعقود.

ما الذي لا تقوله الورقة؟

هذا هو القسم الذي يبقي القطعة أمينة.

هي لا تقول إن مبرهنات الاستحالة القديمة كانت خاطئة. البناء يتجنبها بتغيير التعريف.

وهي لا تعطي انعدام معرفة عاديًا وكلاسيكيًا من دون تفاعل ولا إعداد ومع سلامة تامة. فالورقة تقول صراحة إن المُثبِت الذي بنته لا يملك مُحاكيًا.

وهي لا تعني أن البرهان لا يمكن إعادة استخدامه. فما زال من الممكن عرض برهان من رسالة واحدة على شخص آخر؛ والورقة لا تحافظ على خصائص من نوع قابلية الإنكار. (وانعدام المعرفة غير التفاعلي مع إعداد موثوق يملك القيد نفسه.)

كما أنها لا تقدم بروتوكولًا عمليًا جاهزًا للنشر. هذا عمل في نظرية التعقيد وأسس التشفير. تعتمد النتيجة على افتراضات كبيرة من تعقيد البراهين والتشفير، ويتعلق البناء بما هو ممكن من حيث المبدأ.

ولا تجعل كلمة «غودل» بدائية أمنية سحرية. علاقة غودل تمر عبر أنظمة الإثبات، وأنظمة الإثبات المثلى، والنظائر المحدودة لعدم الاكتمال. والحدس المفيد ليس «عدم الاكتمال يحمي كلمة مرورك». بل: إذا كان كتّاب القواعد لا يستطيع أن يثبت بكفاءة أن المُحاكي مستحيل، فيمكن صد الهجمات التي كانت ستتطلب هذا الإثبات على مستوى تعريفات الأمان.

لماذا تظل النتيجة مثيرة للاهتمام؟

غالبًا ما يحول التشفير الصعوبة إلى أمان. تحليل الأعداد إلى عوامل صعب، فتغدو الافتراضات من نمط RSA مفيدة. ومسائل الشبكات صعبة، فتغدو تشفيرات الشبكات مفيدة. هنا الصعوبة أغرب: ليست «من الصعب حساب السر»، بل «من الصعب إثبات أن كائن إثبات معين لا يمكن أن يوجد».

ولهذا تبدو الورقة غير مألوفة. فهي تعامل البديهيات وكتب القواعد تقريبًا كموارد تشفيرية. تقول الاستحالة المعتادة إن هناك توترًا بين السلامة والمحاكاة. أما حركة Ilango فتضع هذا التوتر خلف ستار من نظرية البراهين: المُحاكي غائب، لكن النظام الرسمي لا يستطيع بكفاءة كشف غيابه.

بالنسبة إلى القارئ، الجزء المدهش ليس أن هذا سيحل محل أنظمة انعدام المعرفة الحالية. على الأرجح لن يفعل، أو على الأقل ليس مباشرة. المفاجأة هي أن قيدًا من المنطق الرياضي يمكن استخدامه بصورة بناءة: لا كجدار فحسب، بل كنوع من الغطاء.

ما مدى قوة الأدلة؟

هذه ورقة مبرهنات، ولذلك تعني كلمة «الأدلة» شيئًا مختلفًا عنها في ورقة أحياء أو فلك. السؤال ليس هل تكررت تجربة. السؤال هو هل تدعم التعريفات والافتراضات وسلسلة البرهان الادعاء.

البرهان صوري، والورقة صريحة بشأن افتراضاتها. وهذه الافتراضات ليست عابرة. فالإثباتات غير التفاعلية غير القابلة لتمييز الشاهد كائنات معيارية في التشفير وتتبع من عدة حزم معروفة من الافتراضات. وحدس عدم وجود نظام إثبات أمثل حدس مركزي في تعقيد البراهين. أما BPP = P فهو اعتقاد معياري في إزالة العشوائية، ولا يُستخدم إلا في المبرهنة الأوسع الخاصة بالخصائص القابلة للتكذيب.

وتجادل الورقة أيضًا بأن هذه الافتراضات هي الثمن المناسب لا هيكل اعتباطي: فهي تثبت اتجاهًا عكسيًا يبين أنها ضرورية في الجوهر — إذا وجدت أبنية من هذا النوع أصلًا، فلا بد من وجود إثباتات غير تفاعلية غير قابلة لتمييز الشاهد، ومع افتراض الدوال أحادية الاتجاه المعيارية لا يمكن أن يوجد نظام إثبات أمثل. والافتراضات من نوع «فوز في كلتا الحالتين»: دحض أي منها سيكون بحد ذاته اكتشافًا بارزًا في تعقيد البراهين أو التشفير أو نظرية التعقيد.

لكن لأن النتيجة مشروطة، فالثقة فيها مشروطة أيضًا. إذا فشلت تلك الافتراضات، يتغير تفسير المبرهنة. وحتى إذا كانت صحيحة، فالضمان ليس انعدام المعرفة الكلاسيكي الكامل؛ بل النسخة المخففة القائمة على نظرية البراهين التي تعرفها الورقة.

لذلك فالثقة المناسبة: عالية بأن الورقة تثبت نتيجة إمكانية مشروطة ومتسقة؛ ومتوسطة بأن افتراضاتها تصف العالم التشفيري الذي نعيش فيه فعلًا؛ ومنخفضة لأي أثر عملي فوري.

لماذا يهم الأمر؟

تفتح الورقة مسارًا كان يُفترض أنه مغلق.

تقول النظرية الكلاسيكية: لا يمكن ضغط انعدام المعرفة الكامل في رسالة واحدة بلا إعداد، ولا يمكن أن يكون تام السلامة. وتقول ورقة Ilango: إذا طلبنا نتائج انعدام المعرفة التي يمكن اختبارها في ألعاب أمنية، وسمحنا لتعريف الأمان بأن يعتمد على ما يستطيع كتاب قواعد ما دحضه أو لا يستطيع دحضه بكفاءة، فيمكن استعادة قدر كبير من السلوك المفيد — برسالة واحدة، ومن دون إعداد، ومع سلامة تامة.

هذه ليست مجرد رتوش صغيرة على تعريف. إنها طريقة مختلفة للتفكير في الضمانات التشفيرية. بدل أن تسأل فقط ما الذي يوجد، اسأل ما الذي يستطيع كتاب القواعد استبعاده. وبدل أن تعامل عدم القابلية للإثبات بوصفها إزعاجًا فلسفيًا، استخدمها كبنية.

قد لا يتغير العالم العملي غدًا، لكن الخريطة المفاهيمية تغيرت. أصبح هناك الآن معنى صوري يمكن فيه لعبارة «لا أحد يستطيع بكفاءة إثبات أن السر قد تسرّب» أن تكون قوية بما يكفي لاستعادة كثير من الحمايات القائمة على الألعاب التي أردناها من عبارة «السر لم يتسرّب».

ولهذا تنتمي كلمة غودل إلى العنوان.

الخلاصة

تسمح إثباتات انعدام المعرفة لمُثبِت بإقناع متحقق بأن عبارة ما صحيحة من دون كشف الشاهد. وتقول نتائج الاستحالة الكلاسيكية إن انعدام المعرفة لا يمكن ضغطه في رسالة واحدة بلا إعداد، ولا يمكن أن يملك سلامة تامة. لا تدحض ورقة Ilango Rahul هذه الاستحالات. بل تعرّف مفهومًا أضعف، هو **انعدام المعرفة الفعّال**: بدل اشتراط وجود مُحاكٍ حقيقي، تشترط أن نظام إثبات مختارًا — كتاب قواعد رسمي مثل ZFC — لا يستطيع بكفاءة إثبات أنه لا يوجد مُحاكٍ. تحت افتراضات كبيرة من التشفير (إثباتات غير تفاعلية غير قابلة لتمييز الشاهد) وتعقيد البراهين (عدم وجود نظام إثبات أمثل)، تبني الورقة مُثبِتين برسالة واحدة لمسائل NP/SAT، من دون إعداد ومع سلامة تامة، يحققون النتائج القابلة للتكذيب والمبنية على ألعاب من انعدام المعرفة خاصيةً بعد خاصية. أما مُثبِت واحد يغطي جميع هذه الخصائص «الطبيعية» فهو امتداد إضافي مشروط وجزئيًا حدسي — وتغطية كل خاصية قابلة للتكذيب حرفيًا مرجح أن تكون مستحيلة لأن البراهين تظل قابلة لإعادة الاستخدام. النتيجة نظرية ومشروطة، لا بدائية منشورة، لكنها تعرض طريقة جديدة لاستخدام عدم القابلية للإثبات في نظرية البراهين بوصفه موردًا تشفيريًا.

مراجعة بلا تهويل

ما الذي تُظهره الورقة: تحت الافتراضات المعلنة، يمكن بناء مُثبِتين لمسائل NP/SAT برسالة واحدة، ومن دون إعداد، ومع سلامة تامة، يكونون عديمي المعرفة فعّالًا بالنسبة إلى أي نظام إثبات مختار، ويحققون كل نتيجة قابلة للتكذيب ومبنية على لعبة من نتائج انعدام المعرفة

الكلاسيكي كلًّا على حدة.

ما هو معقول لكنه غير مثبت بلا شروط: أن افتراضات تعقيد البراهين والتشفير المطلوبة صحيحة. إنها افتراضات جادة ومدروسة جيدًا — وتبين الورقة أنها ضرورية في الجوهر كما أنها كافية — لكنها تظل افتراضات.

ما الذي لا تُظهره: انعدام معرفة كلاسيكيًا بلا تفاعل ولا إعداد ومع سلامة تامة؛ أو نظامًا عمليًا جاهزًا للنشر؛ أو قابلية إنكار البراهين أو عدم إعادة استخدامها؛ أو أن مبرهنة عدم الاكتمال لغودل تؤمّن التشفير بمفردها.

القيود الرئيسية: الضمان تخفيف لمفهوم انعدام المعرفة؛ وأوسع نسخة تعتمد على عدة افتراضات؛ وادعاءات المُثبِت العالمي الواحد تظل جزئيًا حدسية؛ والنتيجة في المقام الأول تأسيسية.

ما مقدار الثقة المناسبة للقارئ العام؟ ثقة عالية بأن هذه نتيجة نظرية مشروطة مهمة إذا قُبلت التعريفات. وثقة متوسطة بأن الافتراضات تصف الواقع. وثقة منخفضة في نشر عملي قريب. والخلاصة الآمنة هي: الورقة لا تكسر استحالات انعدام المعرفة؛ بل تجد طريقًا جديدًا من نظرية البراهين للالتفاف حول الأجزاء منها التي تهم كثيرًا من ألعاب الأمان.

المصادر

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

00058.2025.FOCS63196/1109.10 DOI ,2025 FOCS
https://doi.org/10.1109/FOCS63196.2025.00058