The Clean Paper

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

หลักฐานทางคริปโทกราฟีซ่อนความลับได้ด้วยการทำให้การพิสูจน์ว่า simulator หายไปเป็นเรื่องยาก

Zero-knowledge proof ทำให้คนหนึ่งพิสูจน์ข้อความได้โดยไม่เปิดเผย witness ทฤษฎีคลาสสิกบอกว่าเราไม่สามารถมีสิ่งนี้ในความหมายเต็ม พร้อมข้อความเดียว ไม่มี trusted setup และ perfect soundness งานของ Rahul Ilango ไม่ได้ทำให้ความเป็นไปไม่ได้นั้นหายไป แต่เปลี่ยนเป้าหมาย: แทนที่จะเรียกร้องว่ามี simulator อยู่จริง มันถามว่า proof system ที่เลือกสามารถพิสูจน์อย่างมีประสิทธิภาพได้หรือไม่ว่า simulator ไม่มีอยู่ ภายใต้สมมติฐานสำคัญจาก proof complexity และคริปโทกราฟี นั่นเพียงพอที่จะกู้ผลของ zero-knowledge แบบ falsifiable และ game-based กลับมาที่ละคุณสมบัติประเด็นไม่ใช่ primitive อินเทอร์เน็ตที่เสียบใช้งานได้ทันที แต่เป็นวิธีเชิง proof theory ที่เปลี่ยน unprovability ทางคณิตศาสตร์ให้เป็นฉากกำบังทางคริปโทกราฟี

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

กลเม็ดไม่ใช่การพิสูจน์ว่าความลับถูกซ่อนอยู่

เริ่มจาก การพิสูจน์แบบไม่เปิดเผยความลับ แบบง่ายที่สุดก่อน

Alice ต้องการทำให้ Bob เชื่อว่าโจทย์ Sudoku มีคำตอบ หากเธอส่งคำตอบให้ Bob เขาก็เชื่อ แต่ปริศนาก็หมดความหมาย สิ่งที่เธอต้องการแปลกกว่านั้น: หลักฐานว่าคำตอบมีอยู่ โดยไม่เปิดเผยคำตอบ

นี่คือคำสัญญาของ หลักฐานแบบไม่เปิดเผยความลับ ผู้พิสูจน์ (Alice) ทำให้ผู้ตรวจสอบ (Bob) เชื่อว่าข้อความหนึ่งเป็นจริง พร้อมกับไม่เปิดเผยอะไรนอกเหนือจากความจริงของข้อความนั้น

ปัญหาคือคำสัญญานี้มีต้นทุน หลักฐานคณิตศาสตร์ธรรมดามีคุณสมบัติที่สบายอยู่สองอย่าง อย่างแรก มันเป็น **ข้อความเดียว**: เขียนลงไป ส่งให้คนอื่น แล้วก็จบ อย่างที่สอง มันมี **ความถูกต้องของระบบพิสูจน์ สมบูรณ์แบบ**: ถ้าข้อความเป็นเท็จ ก็ไม่มีหลักฐานที่ถูกต้องสำหรับมันเลย ผลความเป็นไปไม่ได้แบบคลาสสิกบอกว่า การพิสูจน์แบบไม่เปิดเผยความลับ ต้องยอมเสียทั้งสองอย่าง — และไม่ใช่แค่ห้ามมีพร้อมกัน แต่แต่ละอย่างก็เป็นสิ่งที่รักษาไว้ไม่ได้ด้วยตัวมันเอง

อย่างแรก หลักฐานแบบไม่เปิดเผยความลับ ต้องมีการโต้ตอบ หาก Alice ส่งเพียงข้อความเดียว โดยไม่มีการตั้งค่าล่วงหน้าที่ต้องอาศัยความไว้วางใจ ที่จัดเตรียมไว้ล่วงหน้า การรับประกันของการพิสูจน์แบบไม่เปิดเผยความลับ จะพังลง — และเป็นเช่นนี้ไม่ว่าคุณจะยอมแลก ความถูกต้องของระบบพิสูจน์ไปมากเพียงใด

อย่างที่สอง หลักฐานแบบไม่เปิดเผยความลับ ต้องยอมให้มีโอกาสผิดพลาดเล็กน้อย ปรากฏว่าการเรียกร้อง ความถูกต้องสมบูรณ์ (perfect soundness) ทำลายการโต้ตอบอย่างเงียบ ๆ ด้วย: ผู้ตรวจสอบที่ไม่มีวันถูกหลอกได้ ไม่ว่ามันจะสุ่มเลือกอะไร ก็อาจตรึงการสุ่มเหล่านั้นไว้ล่วงหน้าเสียเลย — และเมื่อ ผู้ตรวจสอบ คาดเดาได้ Alice ก็สามารถตอบทุกอย่างในข้อความเดียว ซึ่งกลับไปเป็นกรณีที่พังอยู่แล้ว

งานของ Rahul Ilango ว่าด้วยทางอ้อมผ่านกำแพงสองชั้นนี้ ไม่ใช่ด้วยการทำเหมือนกำแพงไม่มีอยู่ และไม่ใช่ด้วยการสร้าง การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก ในเงื่อนไขที่เป็นไปไม่ได้ แต่ด้วยการขยับที่ละเอียดกว่า: ทำให้ความหมายของ “ไม่เปิดเผยอะไร” อ่อนลง โดยอ่อนลงในแบบที่ยังรักษาคุณสมบัติด้านความปลอดภัยที่นักเข้ารหัสสามารถทดสอบได้จริง

ผลลัพธ์นี้เรียกว่า **การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล**

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.

Zero-knowledge ถูกปิดทางไว้ที่สามประตู — การโต้ตอบ การตั้งค่าล่วงหน้าที่ต้องอาศัยความไว้วางใจ และ ความถูกต้องของระบบพิสูจน์ที่ไม่สมบูรณ์ — แต่โครงสร้างของ Ilango ลอดออกอีกทางหนึ่ง: ระบบกฎที่เลือกไม่สามารถหักล้างการมีอยู่ของตัวจำลอง ได้อย่างมีประสิทธิภาพ

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.

การพิสูจน์แบบไม่เปิดเผยความลับแบบคลาสสิก ถามว่ามี ตัวจำลองอยู่จริงหรือไม่ ส่วน “การพิสูจน์แบบไม่เปิดเผยความลับเชิงมี

ประสิทธิผล” ถามเพียงว่าระบบกฎที่คุณเลือกสามารถพิสูจน์อย่างมีประสิทธิภาพได้หรือไม่ว่า ตัวจำลองไม่มีอยู่ คำถามที่อ่อนกว่านี้เองทำให้โครงสร้างรักษาข้อความเดียว ไม่มีการตั้งค่าล่วงหน้า และ ความถูกต้องสมบูรณ์ (perfect soundness) ไว้ได้

การทดสอบแบบเดิม: มี ตัวจำลองอยู่จริง

วิธีคลาสสิกในการทำให้ การพิสูจน์แบบไม่เปิดเผยความลับ เป็นนิยามทางคณิตศาสตร์ใช้ผู้ช่วยสมมุติที่เรียกว่า **ตัวจำลอง**

แนวคิดคือ ลองนึกถึง Jane ซึ่ง **ไม่รู้** ความลับของ Alice หาก Jane สามารถสร้างหลักฐานด้วยตัวเองทั้งหมดที่ดูเหมือนหลักฐานซึ่ง Bob จะได้รับจาก Alice ได้ แสดงว่าหลักฐานของ Alice ไม่ได้สอนอะไรใหม่ให้ Bob เพราะ Jane สามารถปลอมประสบการณ์เดียวกันได้อยู่แล้วโดยไม่รู้ความลับของ Alice

ดังนั้น การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก ต้องการ ตัวจำลอง ที่มีอยู่จริง ต้องมีอัลกอริทึมที่มีประสิทธิภาพซึ่งสร้างหลักฐานปลอมที่ดูเหมือนจริงได้โดยไม่รู้ความลับ — หรือ *ข้อมูลพยาน* ในศัพท์เทคนิค; สำหรับ Sudoku ข้อมูลพยานก็คือตารางที่แก้เสร็จแล้ว

นิยามนี้ทรงพลัง แต่ก็เป็นจุดเดียวกับที่ผลความเป็นไปไม่ได้เดิมเข้ามากัด ลองมองด้วยสัญชาตญาณ: หลักฐานที่ไม่โต้ตอบจริง ๆ ก็คือสตริงหนึ่ง เมื่อ Bob ได้สตริงนั้นแล้ว เขาเอาไปให้คนอื่นดูได้ เขาได้ความสามารถที่จะพิสูจน์ข้อความต่อคนอื่น ซึ่งก็ฟังดูเหมือนได้ “มากกว่าไม่รู้อะไรเลย” อยู่แล้ว ทฤษฎีบทคลาสสิกทำให้สัญชาตญาณนี้คมขึ้นเป็นผลความเป็นไปไม่ได้ข้างต้น

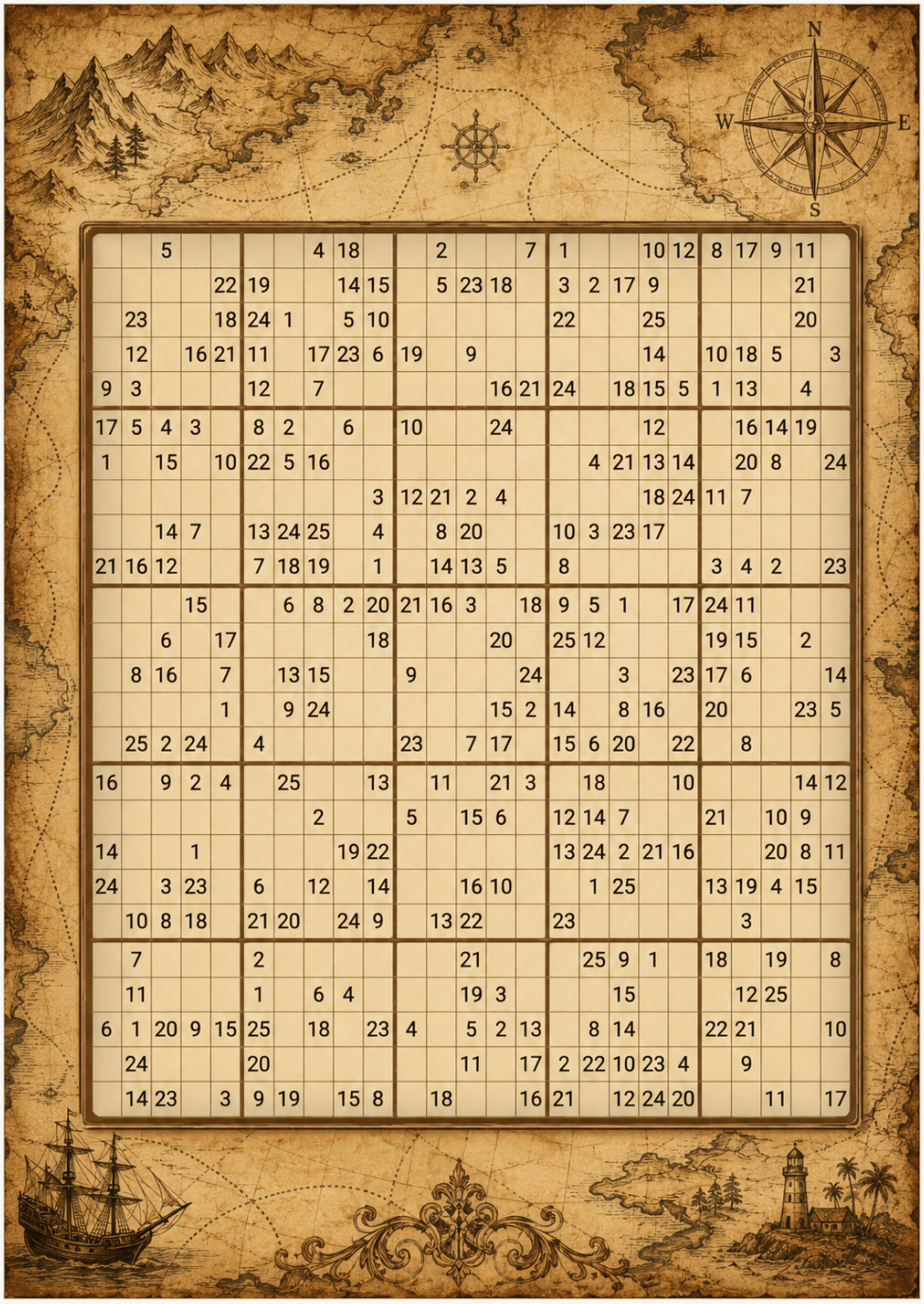
> **คุณสมบัติสามอย่างที่งานนี้ยืนยันว่าจะรักษาไว้**
>
> ชื่อบทความวิจัยระบุข้อจำกัดสามอย่าง:
> **ไม่มีการโต้ตอบ:** Alice ส่งสตริงหลักฐานหนึ่งครั้ง ไม่มีโปรโตคอลถามตอบไปมา
> **ไม่มีการตั้งค่าล่วงหน้า:** Alice และ Bob ไม่พึ่ง สตริงอ้างอิงร่วม ที่เชื่อถือได้หรือ ค่าการสุ่ม สาธารณะที่จัดเตรียมไว้ล่วงหน้า ระบบจำนวนมากที่เรียกว่า “แบบไม่โต้ตอบ การพิสูจน์แบบไม่เปิดเผยความลับ” ยังพึ่งการตั้งค่าล่วงหน้า แต่งานนี้หมายถึงไม่มีการตั้งค่าล่วงหน้า จริง ๆ
> **ความถูกต้องสมบูรณ์ (perfect soundness):** ข้อความเท็จไม่มีหลักฐานที่ถูกต้อง ไม่ใช่ “แทบไม่เคยถูกยอมรับ” แต่ไม่มีหลักฐานที่ถูกต้องอยู่เลย
> สามคุณสมบัตินี้คือสิ่งที่คณิตศาสตร์ที่เขียนบนกระดาษตามปกติมี — และดังที่อธิบายไว้ข้างต้น การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก ไม่สามารถรักษาทั้งหมดไว้ได้

MegaSudoku ช่วยให้เห็นความแตกต่าง

นี่คือเวอร์ชันที่ตั้งใจทำให้ง่ายเพื่อให้สัมผัสความแตกต่างได้

อย่าใช้ Sudoku 9×9 ธรรมดาสำหรับส่วนจริงจังของอุปมา มันเล็กและมีขอบเขตจำกัดเกินไป: คอมพิวเตอร์แค่แก้มัน หรือพิสูจน์ว่าไม่มีคำตอบก็ได้ ลองจินตนาการครอบครัวของปริศนา **MegaSudoku(n)** แทน ขยายกฎเดิม: เลือกขนาดบล็อก n ให้ $N = n^2$ แล้วสร้างตาราง $N \times N$ แบ่งเป็นบล็อก $n \times n$ โดยมีสัญลักษณ์ N แบบ Sudoku ปกติเป็นเพียงกรณีเล็ก $n = 3$, $N = 9$: ตาราง 9×9 บล็อก 3×3 และเก้าสัญลักษณ์ เรื่อง ความซับซ้อนของการพิสูจน์ เริ่มจริง ๆ ก็ต่อเมื่อ n โตได้ และเมื่อในตารางใส่โครงสร้างย่อย เพิ่มเติมให้มันทำตัวเหมือนสูตร SAT ที่แต่งตัวเป็น Sudoku สูตร SAT ก็คือรายการข้อจำกัดแบบใช่/ไม่ใช่: เรา

สามารถกำหนดค่า true/false ให้ตัวแปรเพื่อให้ข้อจำกัดทุกข้อเป็นจริงพร้อมกันได้หรือไม่?



Sudoku 25×25: กฎของมันตรวจสอบได้โดยไม่เปิดเผยตารางที่เติมเสร็จ — ใช้เป็นภาพแทนหลักฐานที่ตรวจสอบคำตอบซ่อนอยู่ หรือข้อมูลพยาน

> **Sudoku และ SAT: ปริศนาเดียวกันในสองชุดแต่งกาย**
>
> คำกล่าวที่ว่า Sudoku สามารถ “ทำตัวเหมือนสูตร SAT” ไม่ใช่อุปมา การแปลงไปมาได้ทั้งสองทิศ และทิศที่ง่ายเขียนให้เห็นได้ทั้งหมด

จาก Sudoku ไป SAT SAT พูดได้แค่ true/false ดังนั้นกำหนดตัวแปรบูลีนหนึ่งตัวต่อชุดสามค่า (แถว, คอลัมน์, ค่า): *x(r,c,v)* หมายถึง “ช่องแถว *r* คอลัมน์ *c* มีค่า *v*” Sudoku 4×4 (บล็อก 2×2 ค่า 1–4) ต้องใช้ 4·4·4 = 64 ตัวแปร; แบบคลาสสิก 9×9 ใช้ 729 ตัวแปร จากนั้นกฎ Sudoku ทุกข้อแปลงเป็นชุด ข้อกำหนด ได้ (ข้อกำหนด คือ OR ของตัวแปรหรือค่าปฏิเสธของมัน; สูตรทั้งก้อนคือ AND ของ ข้อกำหนด ทั้งหมด)
ทุกช่องมีอย่างน้อยหนึ่งค่า — หนึ่ง ข้อกำหนด ต่อช่อง:

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

ทุกช่องมีได้ไม่เกินหนึ่งค่า — ข้อกำหนด แบบ “ห้ามทั้งคู่” สำหรับค่าทุกคู่:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \ldots$$ และทำต่อไปสำหรับทั้งหกคู่

ทุกแถวมีทุกค่า — สำหรับแถว 1 และค่า 3: อย่างน้อยหนึ่งครั้ง,

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

และไม่เกินหนึ่งครั้ง: $\neg x(1,1,3) \vee \neg x(1,2,3)$ และทำแบบเดียวกันสำหรับคู่ช่องทุกคู่ในแถว
คอลัมน์และบล็อก — เป็นชุดเดียวกัน เปลี่ยนเพียงกลุ่มของช่อง สำหรับบล็อกซ้ายบนและค่า 2:

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

บวก ข้อกำหนด แบบ “ห้ามทั้งคู่” สำหรับทุกคู่
ตัวเลขโจทย์ที่พิมพ์มา — ส่วนง่ายที่สุด: ตัวเลขแต่ละตัวเป็น ข้อกำหนด ที่มีตัวแปรเดียว ตัวเลข 3 ที่พิมพ์ไว้ในมุมซ้ายบนกลายเป็น ข้อกำหนด

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

AND ของทั้งหมดนี้ satisfiable ก็ต่อเมื่อ Sudoku มีคำตอบ — และ satisfying การกำหนดค่าความจริง *ก็คือ* คำตอบ: ดูว่า x(r,c,v) ใดเป็น true แล้วเติมตาราง สำหรับ 9×9 จะมี 729 ตัวแปรและ ข้อกำหนด ไม่กี่พันข้อ ซึ่ง SAT solver สมัยใหม่จัดการได้ในระดับมิลลิวินาที สังเกต ข้อกำหนด ของโจทย์ x(1,1,3): มันพูดว่า “ช่องนี้เท่ากับ 3 พอดี” ไม่ใช่ “ช่องเหล่านี้ต่างกันทั้งหมด” — ความไม่สมมาตรแบบเดียวกันนี้จะบังคับให้ใช้กลเม็ดเพิ่มสำหรับช่องโจทย์ในหมายเหตุโปรโตคอลด้านล่าง
จาก SAT ไป Sudoku งานวิจัยต้องการทิศตรงข้ามซึ่งยากกว่า: เมื่อมีสูตร SAT *ใด ๆ* ให้สร้าง mega-Sudoku ที่มีคำตอบก็ต่อเมื่อสูตรนั้นมีคำตอบ กฎพื้นฐานของ Sudoku พูดได้เพียงว่า “ช่องเหล่านี้ต่างกันทั้งหมด” ดังนั้นข้อจำกัดตรรกะทั่วไปต้องถูก *สร้างขึ้น* — และนี่คือสิ่งที่ โครงสร้างย่อย ทำ Gadget คือกลุ่มช่องสำเร็จรูปขนาดเล็ก หนึ่งกลุ่มต่อ ข้อกำหนด ของสูตร โดยช่องที่กำหนดทำหน้าที่เป็นตัวแปร (สัญลักษณ์ที่อยู่ในช่องเข้ารหัส true หรือ false) และข้อจำกัดภายในกลุ่มถูกออกแบบให้การเติมที่ถูกกฎมีได้เฉพาะกรณีที่ตรงกับ การกำหนดค่าความจริง ซึ่งทำให้ ข้อกำหนด นั้นจริง นี่เป็นงานช่างมาตรฐานจาก หลักฐานพิสูจน์ ของ NP-completeness; สำหรับ generalized Sudoku Yato และ Seta ทำไว้ในปี 2003
สองทิศทางรวมกันบอกว่า Sudoku N×N และ SAT คือปัญหาเดียวกันในคนละชุด นั่นคือเหตุผลที่ทั้งบทความนี้และงานวิจัยสามารถเล่าเรื่องเกี่ยวกับ NP ทั้งหมดผ่านตารางและสัญลักษณ์ได้

Witness ยังนึกภาพได้ง่าย Alice รู้การเติม mega-Sudoku ที่ถูกต้องครบถ้วน Bob ต้องการมั่นใจว่าการเติมแบบนั้นมีอยู่ แต่ Alice ไม่ต้องการเปิดเผย หากเธอส่งตารางทั้งหมด Bob ก็เชื่อ แต่ความลับก็หายไป

ใน การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก Alice และ Bob โต้ตอบกัน แบบจำลองทางความคิดเก่า ๆ แบบ

หนึ่งใช้แผ่นปิด Alice ซ่อนตารางที่แก้แล้ว เปลี่ยนชื่อสัญลักษณ์อย่างลับ ๆ ก่อนแต่ละรอบ แล้วให้ Bob ตรวจข้อจำกัดเฉพาะจุดหนึ่งแบบสุ่ม: แถว คอลัมน์ กล่อง หรือ โครงสร้างย่อย หากช่องที่เปิดมีสัญลักษณ์ต่างกันทั้งหมด Bob ก็มั่นใจขึ้น จากนั้นปิดทุกอย่างอีกครั้งและสุ่มเปลี่ยนชื่อสัญลักษณ์ใหม่ (มีจุดยุ่งหนึ่ง: ตัวเลขโจทย์ที่กำหนดมาแล้วต้องใช้กลเม็ดเพิ่ม เพราะการเปลี่ยนชื่อสัญลักษณ์ซ่อนตัวเลขเหล่านั้นไปด้วย หมายเหตุด้านล่างอธิบายว่าโปรโตคอลคลาสสิกแก้เรื่องนี้อย่างไร; ภาพแบบง่ายนี้เพียงพอสำหรับสิ่งที่จะตามมา)

> **โปรโตคอลคลาสสิกจัดการช่องตัวเลขโจทย์จริง ๆ อย่างไร**
>
> กลเม็ดการเปลี่ยนชื่อมีจุดบอด กฎแถว คอลัมน์ และกล่องล้วนพูดว่า “ช่องเหล่านี้ต่างกันทั้งหมด” และคุณสมบัติ *ต่างกันทั้งหมด* ยังคงอยู่ไม่ว่าจะเปลี่ยนชื่อสัญลักษณ์อย่างไร แต่ตัวเลขโจทย์พูดว่า “ช่องนี้มีค่า 5 พอดี” และหลังเปลี่ยนชื่อ Bob เห็นเพียง $\sigma(5)$ — สัญลักษณ์ที่ถูกพราง — โดยไม่รู้การเปลี่ยนชื่อ σ เขาจึงตรวจอะไรไม่ได้ หากปล่อยไว้ Alice อาจพิสูจน์ว่า *มี* ตารางที่ถูกต้องสักตารางโดยไม่สนใจตัวเลขโจทย์ที่พิมพ์มาเลย ซึ่งไม่ได้พิสูจน์อะไรเกี่ยวกับปริศนา *ข้อนี้* วรรณกรรมคลาสสิกมีวิธีแก้มาตรฐานสองแบบ
>
> **แถวอ้างอิง** เพิ่มแถวพิเศษ N ช่องหนึ่งแถวเข้าไปในตารางที่ซ่อน — แถวอ้างอิง ที่ Alice เติมสัญลักษณ์ 1…N ตามลำดับสาธารณะที่ตายตัว แล้วเปลี่ยนชื่อมันพร้อมกับทุกอย่าง จึงกลายเป็น $\sigma(1)…\sigma(N)$ การท้าทายแบบสุ่มของ Bob มีตัวเลือกเพิ่มหนึ่งอย่าง นอกจากเลือกแถว คอลัมน์ กล่อง หรือ โครงสร้างย่อย มาเปิด เขาอาจเลือก **แถวอ้างอิง บวกช่องตัวเลขโจทย์หนึ่งช่อง** Alice เปิดทั้งสองอย่าง; แถวอ้างอิง เปิดเผยการเปลี่ยนชื่อของรอบนั้น และ Bob ตรวจว่าช่องโจทย์แสดงค่าที่เปลี่ยนชื่อของตัวเลขที่พิมพ์ไว้พอดี วิธีนี้ยังเป็น การพิสูจน์แบบไม่เปิดเผยความลับ เพราะ Bob เรียนรู้เพียง σ — ซึ่งสุ่มใหม่ทุกครั้งและไม่มีประโยชน์ด้วยตัวมันเอง — กับค่าของช่องที่เขารู้อยู่แล้วจากโจทย์ ไม่มีอะไรเกี่ยวกับช่องลับรั่วออกมา และ ตัวจำลอง สามารถปลอมมุมมองนี้ด้วยการสุ่ม σ ได้ ความถูกต้องของระบบพิสูจน์ เกิดจาก Alice ที่โกงมีโอกาสคงที่ที่จะถูกจับในแต่ละรอบ และทำซ้ำหลายรอบจนความสงสัยเล็กมาก
>
> **คอมไพล์ตัวเลขโจทย์ออกไป** แบบที่เป็นโครงสร้างมากกว่าจะเอาการท้าทายพิเศษออกแทนที่จะเพิ่มเข้าไป แทนที่จะ *ตรวจสอบ* ค่าของตัวเลขโจทย์ ให้บังคับมันด้วยข้อจำกัดความแตกต่าง: เชื่อมช่องโจทย์กับทุกช่องใน แถวอ้างอิง ยกเว้นช่องที่ถือค่าของมันเอง — “ต่างจาก $\sigma(1)$, ต่างจาก $\sigma(2)$, …, ต่างจากทุกอย่างยกเว้น $\sigma(5)$” สัญลักษณ์เดียวที่ช่องนี้ถือได้อย่างถูกกฎจึงเป็นค่าของโจทย์ ข้อจำกัดทุกข้อกลับมาเป็นชนิด “สองช่องนี้ต่างกัน” อีกครั้ง — ไม่เปลี่ยนภายใต้การเปลี่ยนชื่อ และตรวจได้เหมือนแถว นี่คือกลเม็ดเดียวกับที่ใช้กับ จุดยอด ที่ลงสีไว้ล่วงหน้าในโปรโตคอล การระบายสีกราฟ แบบคลาสสิก และเป็นจิตวิญญาณของคำว่า *โครงสร้างย่อย* ข้างต้น: ในภาพ MegaSudoku-as-SAT ตัวเลขโจทย์ถูกคอมไพล์เป็น ข้อจำกัดแบบไม่เท่ากัน โครงสร้างย่อย เช่นเดียวกับข้อจำกัดอื่น
>
> **โปรโตคอลทางกายภาพ** โปรโตคอลไพ่ Sudoku ในโลกจริง (Gradwohl, Naor, Pinkas และ Rothblum, 2007) ไม่ใช้การเปลี่ยนชื่อเลย และจัดการตัวเลขโจทย์ก่อนเริ่มซ่อนเสียอีก สำหรับแต่ละช่อง Alice วางไพ่เหมือนกันสามใบที่มีค่าของช่องนั้น — คว่ำหน้าสำหรับช่องลับ แต่ **หงายหน้าสำหรับช่องโจทย์** เพื่อให้ Bob เห็นด้วยตาตัวเองว่าตัวเลขโจทย์ถูกเคารพก่อนคว่ำไพ่ จากนั้นไพ่หนึ่งใบจากแต่ละช่องเข้าแพ็กเก็ตของแถว หนึ่งใบเข้าแพ็กเก็ตของคอลัมน์ และหนึ่งใบเข้าแพ็กเก็ตของกล่อง; แต่ละแพ็กเก็ตถูกสับและเปิด แล้ว Bob ตรวจว่ามีสัญลักษณ์ครบ N แบบการสับทำลายข้อมูลตำแหน่ง (นี่คือ การพิสูจน์แบบไม่เปิดเผยความลับ) แต่ตัวเลขโจทย์ถูกตรึงไว้ตั้งแต่ตอนแจกไพ่แล้ว
>
> ไม่ว่าจะใช้วิธีใด บทเรียนก็เหมือนสิ่งที่บทความนี้ย้ำซ้ำ: โปรโตคอล การพิสูจน์แบบไม่เปิดเผยความลับ คือการทำบัญชีอย่างระมัดระวังว่า *ข้อเท็จจริงใด* ยังอยู่รอดหลังการซ่อน การเปลี่ยนชื่อรักษา “ต่างกันทั้งหมด” แต่ลบ “เท่ากับ 5” ดังนั้น “เท่ากับ 5” ต้องถูกนำกลับเข้ามาด้วยวิธีอื่น

นี่ไม่ใช่โปรโตคอลในงานวิจัย มันเป็นแบบจำลองทางความคิดของ การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก:

- Alice และ Bob โต้ตอบไปมา
- Bob เลือกการตรวจแบบสุ่ม
- Alice เปิดเผยเพียงความสอดคล้องในส่วนเล็ก ๆ ไม่ใช่คำตอบทั้งหมด
- การพิสูจน์ความเป็นส่วนตัวทำโดยแสดงว่ามุมมองของ Bob สามารถถูกสร้างขึ้นได้โดยไม่ต้องรู้คำตอบลับของ Alice

ดังนั้น การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก ตั้งอยู่บนข้อเท็จจริงเชิงบวก:

> มี ตัวจำลองอยู่จริง

ทีนี้เอาส่วนที่สบายออกไป Alice ส่งสตริงหลักฐานหนึ่งครั้งแล้วจบ ไม่มีการตั้งค่าล่วงหน้าที่ต้องอาศัยความไว้วางใจ ไม่มีสตริงสุ่มร่วมที่เตรียมไว้ล่วงหน้า และ Bob ต้องไม่มีวันยอมรับปริศนาที่เป็นเท็จ นี่คือสภาพแวดล้อมที่ การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก อยู่รอดไม่ได้

ก่อนถึงกลเม็ด ต้องมีตัวละครอีกหนึ่งตัว กำหนด **ระบบกฎพิสูจน์**: ระบบพิสูจน์แบบเป็นทางการในความหมายของนักตรรกศาสตร์ — ชุดสัจพจน์ตายตัวบวกกฎเชิงกลสำหรับตรวจหลักฐานคณิตศาสตร์ที่เขียนไว้ ZFC ซึ่งเป็นสัจพจน์มาตรฐานของคณิตศาสตร์คือตัวอย่างหลัก จากนี้ทุกอย่างจะพูดเทียบกับ ระบบกฎพิสูจน์ ที่เลือกไว้ล่วงหน้า และเลือกได้ยืดหยุ่น: โครงสร้างใช้ได้กับ ระบบกฎพิสูจน์ ใด ๆ ที่คุณกำหนด รวมถึง ZFC

(หมายเหตุเรื่องคำศัพท์ตามงานวิจัย: “ระบบพิสูจน์” ในที่นี้หมายถึง ระบบกฎพิสูจน์ นี่เสมอ — ระบบเป็นทางการที่ตรวจหลักฐานคณิตศาสตร์ — ไม่ใช่ข้อความที่ Alice ส่ง เครื่องมือของ Alice และ Bob เรียกว่า “ผู้พิสูจน์ และ ผู้ตรวจสอบ”)

เวอร์ชันสไตล์ Gödel ยังคงเรื่อง mega-Sudoku ไว้ แต่เปลี่ยนหลักฐาน

เลือก constraint system ชุดที่สองที่แสดงผลขนาดเดียวกัน เรียกมันว่า **D** ในเรื่องนี้ S และ D คือปริศนา MegaSudoku(n) สองชุดในรูปแบบเดียวกัน เบื้องหลัง D อาจเริ่มจากสูตรตรรกะยาก ๆ ขนาดต่างกัน; หากจำเป็นสามารถ padding ด้วยข้อจำกัด dummy ที่ไม่เป็นอันตรายให้เข้าขนาดตารางเดียวกัน D สร้างจากสูตรตรรกะที่จริง ๆ แล้ว **unsatisfiable**: ไม่มี การกำหนดค่าความจริง ใดทำให้ข้อจำกัดทั้งหมดเป็นจริง เหมือนปริศนาเสียที่ไม่มีตารางเติมถูกกฎ ตัวอย่างเล่น ๆ คือสูตรที่บังคับทั้ง “X เป็นจริง” และ “X เป็นเท็จ” ดังนั้น D ไม่มีการเติมที่ถูกต้อง

แต่ D ต้องไม่ใช่ปริศนาเสียที *เปิดโปงได้ง่าย* ตัวอย่างเล่น ๆ ข้างต้นใช้ไม่ได้ เพราะ ระบบกฎพิสูจน์ ใดก็ หักล้าง “X และ not-X” ได้ในบรรทัดเดียว D ต้องเป็นเท็จในแบบที่ ระบบกฎพิสูจน์ ที่เลือกไม่สามารถรับรองด้วยข้อโต้แย้งสั้น ๆ หาก ระบบกฎพิสูจน์ สามารถ หักล้าง D ด้วยหลักฐานสั้น เรื่องด้านล่างจะพัง: ทางเลือกที่อาจใช้สร้างหลักฐานโดยไม่รู้ความลับของ Alice จะถูกตัดทิ้งอย่างเป็นทางการ และความรับประกันด้านความเป็นส่วนตัวก็หายไปด้วย ดังนั้น D ถูกเลือกจากครอบครัวที่ ระบบกฎพิสูจน์ คงที่ไม่สามารถ หักล้าง ได้อย่างมีประสิทธิภาพ: ไม่มีหลักฐานสั้น ๆ ภายใน ระบบกฎพิสูจน์นั้นว่า D ไม่มีคำตอบ

หลักฐานข้อความเดียวของ Alice จึงว่าด้วยข้อความแบบ either/or:

> mega-Sudoku จริง S มีคำตอบ หรือ decoy D มีคำตอบ

นี่คือจุดเชื่อมทางตรรกะ D **ไม่ได้** ถูกสร้างอย่างวิเศษให้ S กลายเป็นจริง หลักฐานไม่ได้โต้แย้งว่า “D ไม่มีคำตอบ ดังนั้น S มีคำตอบ” แต่มันพิสูจน์ disjunction **S หรือ D** ความถูกต้องสมบูรณ์ (perfect soundness) บอกว่า disjunction ที่เป็นเท็จไม่มีหลักฐานที่ถูกต้อง เพราะ D เป็นเท็จในความเป็นจริง — มันไม่มีคำตอบ — วิธีเดียวที่ disjunction จะเป็นจริงคือ S ต้องจริง ดังนั้นหากหลักฐานได้รับการยอมรับ S ต้องมีคำตอบ Decoy ไม่สามารถทำให้ S ที่เป็นเท็จกลายเป็นจริงได้

แต่สำหรับส่วนที่คล้าย การพิสูจน์แบบไม่เปิดเผยความลับ ลองถามว่าจะเกิดอะไรขึ้นหาก D *มี* คำตอบ คำตอบของ decoy นั้นจะทำหน้าที่เป็น ข้อมูลพยาน ทางเลือก มันจะทำให้ใครสักคนสร้างหลักฐานได้โดยไม่รู้คำตอบ mega-Sudoku จริงของ Alice — กล่าวอีกอย่างคือเป็น ตัวจำลอง ในความเป็นจริง D ไม่มีคำตอบ ดังนั้นทาง ตัวจำลอง นี้ปิดอยู่ ประเด็นคือ ระบบกฎพิสูจน์ ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพว่ามันปิดอยู่

ดังนั้น D มีสองหน้าที่ สำหรับ **ความถูกต้องของระบบพิสูจน์** D เป็นเท็จ หลักฐานที่ถูกต้องของ “S หรือ D” จึงบังคับให้ S เป็นจริง สำหรับ **การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล** D หักล้างได้ยาก ดังนั้น ระบบกฎพิสูจน์ ไม่สามารถตัดทาง decoy ที่ถ้าเปิดอยู่จะทำให้ การจำลองเป็นไปได้อย่างรวดเร็ว

ดังนั้นการทดสอบความปลอดภัยไม่ใช่อีกต่อไปว่า:

> เราพิสูจน์ได้ไหมว่ามี ตัวจำลองอยู่จริง?

แต่กลายเป็น:

> ระบบกฎพิสูจน์ ของคุณพิสูจน์อย่างมีประสิทธิภาพได้ไหมว่า ตัวจำลอง เป็นไปไม่ได้?

หากคำตอบคือไม่ สิ่งที่แข็งแรงอย่างน่าประหลาดตามมา: การรับประกันด้านความปลอดภัยทุกข้อที่ (a) สังเกตได้ด้วยการรันทดสอบ และ (b) พิสูจน์ภายใน ระบบกฎพิสูจน์นั้นได้ว่าตามมาจากการมี ตัวจำลอง จะเป็นจริง การโจมตีที่สำเร็จต่อคุณสมบัติใดในกลุ่มนี้จะเทียบเท่ากับการมี หลักฐานหักล้าง สั้นที่หายไป และ หลักฐานหักล้าง สั้นนั้นไม่มีอยู่ นี่คือส่วน “effective” ใน การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล

ดังนั้นความแตกต่างในชั้นเรียนคือ:

การพิสูจน์แบบไม่เปิดเผยความลับแบบคลาสสิก: หลักฐานปลอดภัยเพราะมี ตัวจำลองอยู่จริง

Effective การพิสูจน์แบบไม่เปิดเผยความลับ แบบ Gödel: หลักฐานถูกถือว่าปลอดภัยสำหรับการทดสอบความปลอดภัยที่สังเกตได้ เพราะ ระบบกฎพิสูจน์ ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพว่า ตัวจำลอง เป็นไปไม่ได้

ข้ออ้างที่สองอ่อนกว่า และนี่คือเหตุผลที่งานสามารถรักษาคุณสมบัติสามอย่างซึ่งทำให้เวอร์ชันคลาสสิกพังได้: ข้อความเดียว ไม่มีการตั้งค่าล่วงหน้า และ ความถูกต้องสมบูรณ์ (perfect soundness)

การทดสอบใหม่: คุณพิสูจน์ไม่ได้ว่า ตัวจำลองไม่มีอยู่

การผ่อนนิยามของ Ilango เปลี่ยนคำถาม

การพิสูจน์แบบไม่เปิดเผยความลับแบบคลาสสิก ถามว่า:

> มี ตัวจำลองอยู่หรือไม่?

Effectively การพิสูจน์แบบไม่เปิดเผยความลับ ถามสิ่งที่อ่อนกว่า:

> ระบบกฎพิสูจน์ ที่คุณเลือกพิสูจน์อย่างมีประสิทธิภาพได้ไหมว่าไม่มี ตัวจำลอง?

มันอาจฟังเหมือนหลบด้วยเทคนิค แต่นี่คือแก่นของแนวคิด โครงสร้างอยู่ในสถานะประหลาด: ตัวจำลองจริง ๆ **ไม่มีอยู่** — งานวิจัยระบุเรื่องนี้ชัด — แต่ ระบบกฎพิสูจน์ ที่คุณตรึงไว้ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพว่ามันไม่มี หากผลเสียทุกอย่างที่คุณสนใจต้องอาศัย หลักฐานหักล้าง แบบนั้น ระบบก็ยังทำตัวเหมือน การพิสูจน์แบบไม่เปิดเผยความลับ สำหรับผลเหล่านั้น

ตรงนี้เองที่ Gödel เข้ามา ไม่ใช่เป็นของตกแต่ง และไม่ใช่ “Gödel ทำให้คริปโทปลอดภัย” ความเชื่อมโยงเป็นเรื่อง ทฤษฎีการพิสูจน์ Rulebook ถูกเรียกว่า **เหมาะที่สุด** หากในความหมายที่แม่นยำ มันดีที่สุดเท่าที่เป็นไปได้: เมื่อใดก็ตามที่ ระบบกฎพิสูจน์ใดสามารถ หักล้าง สูตรชนิดที่เกี่ยวข้องด้วยหลักฐานสั้น ระบบกฎพิสูจน์ เหมาะที่สุด ก็ทำได้เช่นกัน โดยหลักฐานยาวกว่าไม่เกินปัจจัยพหุนาม Krajíček และ Pudlák เสนอข้อคาดการณ์ในปี 1989 ว่า **ไม่มี ระบบพิสูจน์ที่เหมาะที่สุด อยู่จริง**: ไม่ว่าคุณ

ตรึง ระบบกฎพิสูจน์ ใด จะมี ระบบกฎพิสูจน์ อื่นที่พิสูจน์ครอบครัวของข้อความจริงบางชุดได้สั้นกว่ามาก นี่เป็นหนึ่งในข้อคาดการณ์เปิดสำคัญของ ความซับซ้อนของการพิสูจน์ และเป็นญาติแบบจำกัดขนาดในโลก ทฤษฎีความซับซ้อน ของทฤษฎีบทความไม่สมบูรณ์ของ Gödel: ข้อความจริงบางอย่างไม่มีหลักฐานสั้นใน ระบบกฎพิสูจน์ ที่คุณตรึงไว้ — ไม่ใช่เพราะมันพิสูจน์ไม่ได้โดยหลักการ แต่เพราะ ระบบกฎพิสูจน์ คงที่ทุกชุดจะทึ่งความจริงบางอย่างที่มีคำอธิบายสั้นไว้โดยไม่มีหลักฐานสั้น

งานวิจัยสมมติข้อคาดการณ์นี้ (ในรูปที่แข็งกว่าเล็กน้อยแบบ “เกิดซ้ำอย่างไม่สิ้นสุด” ซึ่งเป็นมาตรฐานเมื่อใช้ข้อคาดการณ์ในคริปโทกราฟี) ผลตอบแทนจากทฤษฎีบทของ Krajíček และ Pudlák เป็นรูปธรรม: สำหรับ ระบบกฎพิสูจน์ ทุกชุด มีลำดับของสูตรที่ unsatisfiable จริง ซึ่ง ระบบกฎพิสูจน์นั้นไม่สามารถ หักล้าง ด้วยหลักฐานสั้น — และที่สำคัญ อัลกอริทึมที่มีประสิทธิภาพสามารถ *สร้าง* สูตรเหล่านั้นได้ คุณสมบัติหลังนี้คือ uniformity และเปลี่ยนแนวคิดทั้งหมดจากข้ออ้างการมีอยู่ให้เป็นอัลกอริทึมจริงที่ Alice รันได้: decoy D ของเธอออกจากสายการผลิต ไม่ได้โผล่มาจากอากาศ

กลเม็ดทางคริปโทกราฟีคือเอาการขาดพลังในการพิสูจน์นี้มาใช้งาน

โครงสร้างนี้กำลังทำอะไร

นี่คือโครงสร้างของงานวิจัย เมื่อตัดรายละเอียดออกเหลือแต่รูปทรง

ตรึง ระบบกฎพิสูจน์ หนึ่งชุด — เช่น ZFC ภายใต้สมมติฐาน ความซับซ้อนของการพิสูจน์ จะมีลำดับสูตรที่สร้างได้อย่างมีประสิทธิภาพ ซึ่งจริง ๆ แล้ว unsatisfiable แต่ ระบบกฎพิสูจน์ ไม่มีหลักฐานสั้นว่ามัน unsatisfiable

จากนั้นสร้างหลักฐานข้อความเดียวในรูป:

> ข้อความจริง satisfiable หรือสูตรยากพิเศษนี้ satisfiable

สูตรยากพิเศษไม่ได้ satisfiable ดังนั้นหากกลไกหลักฐานพื้นฐานมี ความถูกต้องสมบูรณ์ (perfect soundness) การยอมรับข้อความยังหมายความว่าข้อความจริงต้องเป็นจริง นั่นให้ ความถูกต้องสมบูรณ์ (perfect soundness)

แต่สำหรับความปลอดภัยแบบคล้าย การพิสูจน์แบบไม่เปิดเผยความลับ ลองจินตนาการว่าสูตรยากพิเศษ *satisfiable* หากเป็นเช่นนั้น ข้อมูลพยาน ของมันจะใช้จำลองหลักฐานโดยไม่รู้ ข้อมูลพยาน จริงได้ สูตรนั้นไม่ satisfiable ในความเป็นจริง — แต่ ระบบกฎพิสูจน์ ไม่สามารถพิสูจน์เรื่องนี้ได้อย่างมีประสิทธิภาพ ดังนั้นมันก็ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพว่า ตัวจำลอง เป็นไปไม่ได้

นี่คือจุดหมุน ระบบไม่ได้ซ่อนความลับด้วยการสร้าง ตัวจำลอง แบบคลาสสิก มันซ่อนความลับ สำหรับการทดสอบความปลอดภัยที่สังเกตได้กลุ่มใหญ่ ไว้หลังความไม่สามารถของ ระบบกฎพิสูจน์ ที่จะรับรองว่า ตัวจำลองไม่มีอยู่

งานวิจัยอ้างอะไร

ทฤษฎีบทหลักมีหลายชั้น ผลแกนกลางคือ:

ภายใต้สมมติฐานมาตรฐานทางคริปโทกราฟี — การมีอยู่ของ **หลักฐานแบบไม่โต้ตอบที่ซ่อนข้อมูลพยานจนแยกไม่ออก (non-interactive witness indistinguishable proofs)** ซึ่งเป็นวัตถุที่ศึกษากันมากและตามมาจากชุดสมมติฐานที่เป็นที่ยอมรับหลายแบบ — และภายใต้ข้อคาดการณ์ ความซับซ้อนของการพิสูจน์ ว่า **ไม่มี (เกิดซ้ำอย่างไม่สิ้นสุด) ระบบพิสูจน์ที่เหมาะที่สุด** งานสร้าง ผู้พิสูจน์ และ ผู้ตรวจสอบ แบบข้อความเดียวสำหรับ NP/SAT สำหรับ ระบบกฎพิสูจน์ ทุกตัวเลือก โดยมี

ความถูกต้องสมบูรณ์ (perfect soundness) ไม่มีการตั้งค่าล่วงหน้า และ การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล เทียบกับ ระบบกฎพิสูจน์นั้น (NP/SAT คือ “ตัวหารร่วมที่ยากที่สุด” มาตรฐานของปัญหาแบบปริศนา; mega-Sudoku เป็นหนึ่งในชุดที่มันสวม)

สำหรับข้ออ้างที่กว้างกว่าว่ารักษาคุณสมบัติด้านความปลอดภัยที่ ตรวจสอบการล้มเหลวได้ ได้ งานเพิ่มสมมติฐานมาตรฐานอีกหนึ่งอย่าง คือความเชื่อเรื่อง derandomization **P = BPP** (โดยคร่าว: ค่าการสุ่ม ไม่ได้เพิ่มพลังสำคัญให้กับอัลกอริทึม)

แปลจากภาษาทฤษฎีบท:

- หลักฐานเป็นข้อความเดียว
- ไม่มีการตั้งค่าล่วงหน้าที่ต้องอาศัยความไว้วางใจ
- ข้อความเท็จพิสูจน์ไม่ได้
- ผู้พิสูจน์ ไม่ใช่ การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก — ไม่มี ตัวจำลอง
- แต่ผลด้านความปลอดภัยแบบ ตรวจสอบการล้มเหลวได้ และ ที่นิยามและทดสอบด้วยเกม ทุกอย่างของ การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก สามารถทำให้เกิดได้ในสภาพแวดล้อมนี้

คำว่า “ตรวจสอบการล้มเหลวได้” สำคัญ หมายถึงความล้มเหลวด้านความปลอดภัยสามารถทดสอบได้ด้วยการให้อ ผู้โจมตี เล่นเกม นิยามความปลอดภัยทางคริปโทจำนวนมากมีรูปนี้: ผู้โจมตี แยก ข้อความเข้ารหัส สองอันได้ไหม, invert ฟังก์ชันได้ไหม, กู้ข้อมูลพยาน ได้ไหม, หรือชนะการทดลองที่กำหนดได้ไหม ทฤษฎีบทให้ ผู้พิสูจน์ สำหรับแต่ละคุณสมบัติ ตรวจสอบการล้มเหลวได้ ทีละอย่าง ผู้พิสูจน์ ตัวเดียวที่มี *ทุก* คุณสมบัติ ตรวจสอบการล้มเหลวได้ พร้อมกันน่าจะเป็นไปไม่ได้ — การโจมตีเรื่อง นำกลับมาใช้ซ้ำ แบบเดิม (“Bob เอาหลักฐานไปให้คนอื่นดูได้”) เองก็เป็นคุณสมบัติ ตรวจสอบการล้มเหลวได้ และมันล้มเหลวจริงที่นี่ ข้อเสนอของงานคือ ผู้พิสูจน์ ตัวเดียวอาจครอบคลุมคุณสมบัติ ตรวจสอบการล้มเหลวได้ ที่ *เป็นธรรมชาติ* ทั้งหมด — สิ่งที่เกิดจริงในงานคริปโท — แต่ส่วนนั้นเป็นทฤษฎีบทแบบมีเงื่อนไขที่พึ่งแนวคิด “natural” ซึ่งยังไม่เป็นทางการ พร้อมข้อคาดการณ์ชัดเจนอีกหนึ่งข้อ การรับประกันมุ่งไปที่ความล้มเหลวที่สังเกตได้ ไม่ใช่ทุกความหมายเชิงปรัชญาหรือ การจำลอง-based ของความลับ

ผลตามหนึ่งข้อควรเอ่ยชื่อ: โครงสร้างนี้ให้ แบบไม่โต้ตอบ *ข้อมูลพยาน hiding* หลักฐานพิสูจน์ แบบแรกที่มี uniform ผู้พิสูจน์ — “หลักฐานว่าปริศนามีคำตอบไม่ได้ช่วยให้คุณหาคำตอบนั้น” โดยไม่มี การโต้ตอบ และไม่มีการตั้งค่าล่วงหน้า — วัตถุที่ฟังดูเรียบง่ายแต่ต้านการสร้างมาหลายทศวรรษ

สิ่งที่งานนี้ไม่ได้พูด

ส่วนนี้คือสิ่งที่ช่วยให้บทความตรงไปตรงมา

มัน **ไม่ได้** บอกว่าทฤษฎีบทความเป็นไปไม่ได้เดิมผิด โครงสร้างเลี่ยงมันด้วยการเปลี่ยนนิยาม

มัน **ไม่ได้** ให้ แบบคลาสสิกทั่วไป การพิสูจน์แบบไม่เปิดเผยความลับ ที่ไม่มี การโต้ตอบ ไม่มีการตั้งค่าล่วงหน้า และมี ความถูกต้องสมบูรณ์ (perfect soundness) งานระบุชัดว่า ผู้พิสูจน์ ที่สร้างไม่มี ตัวจำลอง

มัน **ไม่ได้** หมายความว่าหลักฐาน นำกลับมาใช้ซ้ำ ไม่ได้ หลักฐานข้อความเดียวยังเอาไปให้คนอื่นดูได้ งานไม่ได้รักษาคุณสมบัติแบบ การปฏิเสธความเกี่ยวข้องภายหลัง (แบบไม่โต้ตอบ การพิสูจน์แบบไม่เปิดเผยความลับ ที่มี การตั้งค่าล่วงหน้าที่ต้องอาศัยความไว้วางใจ ก็มีข้อจำกัดเดียวกัน)

มัน **ไม่ได้** หมายความว่านี่คือโปรโตคอลใช้จริงที่พร้อม deploy นี่คือ ทฤษฎีความซับซ้อน และรากฐานของคริปโทกราฟี ผลพึงสมมติฐานขนาดใหญ่จาก ความซับซ้อนของการพิสูจน์ และคริปโทกราฟี และโครงสร้างว่าด้วยสิ่งที่เป็นไปได้ในหลักการ

มัน **ไม่ได้** เปลี่ยน “Gödel” ให้เป็น องค์ประกอบพื้นฐาน ความปลอดภัยวิเศษ ความเชื่อมโยงกับ Gödel ผ่าน ระบบพิสูจน์, ระบบพิสูจน์ที่เหมาะที่สุด และ รูปแบบเทียบเคียง แบบจำกัดของ incompleteness สัญชาตญาณที่ใช้ได้ไม่ใช่ “ความไม่สมบูรณ์ปกป้องรหัสผ่านของคุณ” แต่คือ: หาก ระบบกฎพิสูจน์ ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพว่า ตัวจำลอง เป็นไปไม่ได้ การโจมตีที่ต้องอาศัยการพิสูจน์นั้นก็ถูกสกัดในระดับนิยามความปลอดภัยได้

ถึงอย่างนั้นทำไมจึงน่าสนใจ

คริปโทกราฟีมักเปลี่ยนความยากให้เป็นความปลอดภัย การแยกตัวประกอบยาก สมมติฐานแบบ RSA จึงมีประโยชน์ ปัญหา lattice ยาก lattice คริปโทกราฟี จึงมีประโยชน์ แต่ที่นี่ความยากแปลกกว่า: ไม่ใช่ “คำนวณความลับยาก” แต่ “พิสูจน์ว่าวัตถุหลักฐานบางอย่างไม่มีทางมีอยู่ยาก”

นั่นคือเหตุผลที่งานนี้ให้ความรู้สึกผิดแผก มันปฏิบัติกับสัจพจน์และ ระบบกฎพิสูจน์ แทบเหมือนทรัพยากรทางคริปโท ความเป็นไปไม่ได้ตามปกติบอกว่ามีแรงดึงระหว่าง ความถูกต้องของระบบพิสูจน์ กับ การจำลอง การขยับของ Ilango คือเอาแรงดึงนั้นไปไว้หลังม่าน ทฤษฎีการพิสูจน์: ตัวจำลองไม่มีอยู่ แต่ระบบเป็นทางการไม่สามารถเปิดโปงการไม่มีอยู่นั้นได้อย่างมีประสิทธิภาพ

สำหรับผู้อ่าน สิ่งน่าประหลาดใจไม่ใช่ว่านี่จะมาแทน การพิสูจน์แบบไม่เปิดเผยความลับ system ในปัจจุบัน มันน่าจะไม่ทำอย่างนั้น อย่างน้อยก็ไม่โดยตรง สิ่งน่าประหลาดใจคือข้อจำกัดจากตรรกศาสตร์คณิตศาสตร์สามารถใช้ในทางสร้างสรรค์ได้: ไม่ใช่แค่เป็นกำแพง แต่เป็นเหมือนฉากบัง

หลักฐานแข็งแรงแค่ไหน?

นี่เป็นงานทฤษฎีบท ดังนั้น “หลักฐาน” หมายถึงคนละอย่างกับงานชีววิทยาหรือดาราศาสตร์ คำถามไม่ใช่ว่าการทดลองทำซ้ำได้หรือไม่ แต่คือนิยาม สมมติฐาน และห่วงโซ่การพิสูจน์รองรับข้ออ้างหรือไม่

การพิสูจน์เป็นทางการ และงานระบุสมมติฐานอย่างชัดเจน สมมติฐานเหล่านั้นไม่ใช่เรื่องเล็ก Non-interactive ข้อมูลพยาน indistinguishable หลักฐานพิสูจน์ เป็นวัตถุมาตรฐานในคริปโทกราฟีและตามมาจากชุดสมมติฐานที่เป็นที่ยอมรับหลายชุด ข้อคาดการณ์ no-เหมาะที่สุด-หลักฐานพิสูจน์-system เป็นข้อคาดการณ์สำคัญใน ความซับซ้อนของการพิสูจน์ ส่วน P = BPP เป็นความเชื่อมาตรฐานเรื่อง derandomization ซึ่งใช้เฉพาะสำหรับทฤษฎีบทที่กว้างขึ้นเกี่ยวกับคุณสมบัติ ตรวจสอบการล้มเหลวได้

งานยังโต้แย้งว่าสมมติฐานเหล่านี้เป็นราคาที่เหมาะสม ไม่ใช่โครงค้ำแบบตามใจ: มันพิสูจน์ข้อความย้อนกลับ ว่าโดยแก่นแล้วสมมติฐานเหล่านี้จำเป็น — หากโครงสร้างแบบนี้มีอยู่เลย หลักฐานแบบไม่โต้ตอบที่ซ่อนข้อมูลพยานจนแยกไม่ออก (non-interactive witness indistinguishable proofs) ก็ต้องมีอยู่ และ (เมื่อยอมรับ ฟังก์ชันทางเดียว มาตรฐาน) ระบบพิสูจน์ที่เหมาะที่สุด ต้องไม่มีอยู่ นอกจากนี้สมมติฐานยังเป็นแบบ “ได้ประโยชน์ทั้งสองทาง”: การหักล้างข้อใดข้อหนึ่งเองก็จะเป็นการค้นพบระดับหลักชัยใน ความซับซ้อนของการพิสูจน์, คริปโทกราฟี หรือ ทฤษฎีความซับซ้อน

แต่เพราะผลเป็นแบบมีเงื่อนไข ความมั่นใจก็มีเงื่อนไขด้วย หากสมมติฐานเหล่านี้ล้มเหลว การตีความทฤษฎีบทก็เปลี่ยน และแม้สมมติฐานจะจริง การรับประกันก็ไม่ใช่ full การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก แต่เป็นเวอร์ชันผ่อนคลายเชิงทฤษฎีการพิสูจน์ ของงาน

ดังนั้นระดับความมั่นใจที่เหมาะสมคือสูงว่างานพิสูจน์ผลความเป็นไปได้แบบมีเงื่อนไขที่สอดคล้องกันได้; ปานกลางว่าสมมติฐานอธิบายโลกคริปโทที่เราอาศัยอยู่จริง; และต่ำสำหรับผลใช้จริงทันที

ทำไมจึงสำคัญ

งานเปิดเส้นทางที่เคยคิดว่าปิดอยู่

ทฤษฎีคลาสสิกบอกว่า: full การพิสูจน์แบบไม่เปิดเผยความลับ ไม่สามารถเป็นข้อความเดียวโดยไม่มีการตั้งค่าล่วงหน้า และไม่สามารถมี ความถูกต้องสมบูรณ์ (perfect soundness) งานของ Ilango บอกว่า: หากเราเรียกร้องผลของ การพิสูจน์แบบไม่เปิดเผยความลับ ที่ทดสอบได้ใน security game และยอมให้นิยามความปลอดภัยขึ้นกับสิ่งที่ ระบบกฎพิสูจน์ สามารถหรือไม่สามารถหักล้าง ได้อย่างมีประสิทธิภาพ เราสามารถกู้พฤติกรรมที่เป็นประโยชน์กลับมาได้มาก — ด้วยข้อความเดียว ไม่มีการตั้งค่าล่วงหน้า และ ความถูกต้องสมบูรณ์ (perfect soundness)

นี่ไม่ใช่การปรับนิยามเล็กน้อย แต่เป็นวิธีคิดเรื่องการรับประกันทางคริปโทอีกแบบ แทนที่จะถามเพียงว่าอะไรมีอยู่ ให้ถามด้วยว่าระบบกฎพิสูจน์ ของคุณตัดอะไรทิ้งได้ แทนที่จะมอง unprovability เป็นปัญหาเชิงปรัชญา ให้ใช้มันเป็นโครงสร้าง

โลกใช้จริงอาจไม่เปลี่ยนในวันพรุ่งนี้ แต่แผนที่แนวคิดเปลี่ยนไปแล้ว ตอนนี้มีความหมายแบบเป็นทางการที่ว่า “ไม่มีใครสามารถพิสูจน์อย่างมีประสิทธิภาพได้ว่าความลับรั่ว” อาจแข็งแรงพอที่จะกู้การปกป้องแบบ ที่นิยามและทดสอบด้วยเกม หลายอย่างที่เราต้องการจาก “ความลับไม่ได้รั่ว”

นี่คือเหตุผลที่ Gödel อยู่ในชื่อเรื่อง

สรุป

หลักฐานแบบไม่เปิดเผยความลับ (หลักฐานแบบไม่เปิดเผยความลับ) ทำให้ ผู้พิสูจน์ โน้มน้าว ผู้ตรวจสอบ ว่าข้อความหนึ่งเป็นจริงได้โดยไม่เปิดเผย ข้อมูลพยาน ผลความเป็นไปไม่ได้คลาสสิกบอกว่า การพิสูจน์แบบไม่เปิดเผยความลับ ไม่สามารถบีบให้เป็นข้อความเดียวโดยไม่มีการตั้งค่าล่วงหน้า และไม่สามารถมี ความถูกต้องสมบูรณ์ (perfect soundness) งานของ Rahul Ilango ไม่ได้หักล้างความเป็นไปไม่ได้เหล่านั้น แต่กำหนดแนวคิดที่อ่อนกว่า คือ การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล: แทนที่จะเรียกร้องว่ามี ตัวจำลองอยู่จริง มันเรียกร้องให้ระบบพิสูจน์ที่เลือก — ระบบกฎพิสูจน์ แบบเป็นทางการอย่าง ZFC — ไม่สามารถพิสูจน์อย่างมีประสิทธิภาพได้ว่าไม่มี ตัวจำลอง ภายใต้สมมติฐานสำคัญจากคริปโทกราฟี (หลักฐานแบบไม่โต้ตอบที่ซ่อนข้อมูลพยานจนแยกไม่ออก (non-interactive witness indistinguishable proofs)) และ ความซับซ้อนของการพิสูจน์ (ไม่มี ระบบพิสูจน์ที่เหมาะที่สุด) งานสร้าง ผู้พิสูจน์ ข้อความเดียวสำหรับ NP/SAT ที่ไม่มีการตั้งค่าล่วงหน้า มีความถูกต้องสมบูรณ์ (perfect soundness) และบรรลุผลแบบ ตรวจสอบการล้มเหลวได้ และ ที่นิยามและทดสอบด้วยเกม ของการพิสูจน์แบบไม่เปิดเผยความลับ ทีละคุณสมบัติ ผู้พิสูจน์ ตัวเดียวที่ครอบคลุมคุณสมบัติ “natural” ทั้งหมดเป็นส่วนขยายที่ยังพึงข้อคาดการณ์บางส่วน — และการครอบคลุมทุกคุณสมบัติ ตรวจสอบการล้มเหลวได้ อย่างแท้จริงน่าจะเป็นไปไม่ได้ เพราะหลักฐานยัง นำกลับมาใช้ซ้ำ ได้ ผลนี้เป็นทฤษฎีและมีเงื่อนไข ไม่ใช่ องค์ประกอบพื้นฐาน ที่ deploy แล้ว แต่แสดงวิธีใหม่ในการใช้ unprovability เชิง ทฤษฎีการพิสูจน์ เป็นทรัพยากรทางคริปโทกราฟี

ประเมินแบบไม่เกินจริง

งานวิจัยแสดงอะไร: ภายใต้สมมติฐานที่ระบุ สามารถสร้าง ผู้พิสูจน์ สำหรับ NP/SAT ที่เป็นข้อความเดียว ไม่มีการตั้งค่าล่วงหน้า มี ความถูกต้องสมบูรณ์ (perfect soundness) และ การพิสูจน์แบบไม่เปิดเผยความลับเชิงมีประสิทธิผล เทียบกับระบบพิสูจน์ใด ๆ ที่เลือก พร้อมบรรลุผลแต่ละอย่างของ การพิสูจน์แบบไม่เปิดเผยความลับในความหมายคลาสสิก ที่ ตรวจสอบการล้มเหลวได้ และ ที่นิยามและทดสอบด้วยเกม

อะไรที่เป็นไปได้แต่ยังไม่ได้พิสูจน์แบบไม่มีเงื่อนไข: สมมติฐานด้าน ความซับซ้อนของการพิสูจน์ และคริปโทกราฟีที่ต้องใช้เป็นจริง สมมติฐานเหล่านี้จริงจังและศึกษากันมาก — และงานแสดงว่ามันโดยแก่นแล้วทั้งจำเป็นและเพียงพอ — แต่ก็ยังเป็นสมมติฐาน

มันไม่ได้แสดงอะไร: การพิสูจน์แบบไม่เปิดเผยความลับแบบคลาสสิก ที่ไม่มี การโต้ตอบ ไม่มีการตั้งค่าล่วงหน้า และมี ความถูกต้องสมบูรณ์ (perfect soundness); ระบบใช้จริงที่พร้อม deploy; การปฏิเสธความเกี่ยวข้องภายหลัง หรือ non-reusability ของหลักฐาน; หรือว่าทฤษฎีบทความไม่สมบูรณ์ของ Gödel ด้วยตัวมันเองทำให้คริปโทกราฟีปลอดภัย

ข้อจำกัดหลัก: การรับประกันเป็นการผ่อนนิยาม การพิสูจน์แบบไม่เปิดเผยความลับ; เวอร์ชันที่กว้างที่สุดพึ่งสมมติฐานหลายข้อ; ข้ออ้างเรื่อง ผู้พิสูจน์ สากลตัวเดียวยังมีส่วนที่เป็น conjectural; และผลนี้เป็นงานรากฐานเป็นหลัก

ผู้อ่านทั่วไปควรมั่นใจแค่ไหน? สูงว่านี่เป็นผลทฤษฎีแบบมีเงื่อนไขที่สำคัญ หากยอมรับนิยาม ปานกลางว่าสมมติฐานสะท้อนความเป็นจริง ต่ำสำหรับการนำไป deploy ทันที ข้อสรุปที่ปลอดภัยคือ งานไม่ได้ทำลายผลความเป็นไปไม่ได้ของ การพิสูจน์แบบไม่เปิดเผยความลับ; มันหาเส้นทางเชิง ทฤษฎีการพิสูจน์ แบบใหม่เพื่ออ้อมส่วนของความเป็นไปไม่ได้นั้นที่สำคัญต่อ security game จำนวนมาก

แหล่งข้อมูล

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`