The Clean Paper

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

Bukti kriptografi boleh menyembunyikan rahsianya dengan menjadikan ketiadaan simulator sukar dibuktikan

Bukti pengetahuan sifar membolehkan seseorang membuktikan satu pernyataan tanpa mendedahkan witness. Teori klasik mengatakan anda tidak boleh mendapatkannya, dalam erti penuh, dengan satu mesej, tiada persediaan dipercayai dan soundness sempurna. Makalah Rahul Ilango tidak membuat kemustahilan itu hilang. Ia mengubah sasaran: daripada menuntut simulator benar-benar wujud, ia meminta agar tiada sistem bukti pilihan boleh membuktikan secara efisien bahawa simulator tidak wujud. Di bawah andaian besar kerumitan bukti dan kriptografi, itu cukup untuk memulihkan akibat pengetahuan sifar berasaskan permainan yang boleh difalsifikasikan, sifat demi sifat. Intinya bukan primitif internet sedia pasang. Ia cara teori-bukti menukar ketidakbolehbuktian matematik menjadi perlindungan kriptografi.

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

Helahnya bukan membuktikan bahawa rahsia itu tersembunyi

Mulakan dengan versi paling mudah bagi pengetahuan sifar (*zero-knowledge*).

Alice mahu meyakinkan Bob bahawa sebuah teka-teki Sudoku mempunyai penyelesaian. Jika dia menghantar penyelesaiannya, Bob akan yakin, tetapi teka-teki itu sudah rosak. Apa yang Alice mahukan lebih pelik: bukti bahawa penyelesaian wujud, tanpa mendedahkan penyelesaian itu.

Itulah janji bukti pengetahuan sifar. Pembukti (*prover*, Alice) meyakinkan pengesah (*verifier*, Bob) bahawa satu pernyataan benar sambil tidak mendedahkan apa-apa selain kebenaran pernyataan tersebut.

Masalahnya ialah janji ini mempunyai harga. Bukti matematik biasa mempunyai dua ciri yang selesa. Ia ialah **satu mesej**: anda menulisnya, menyerahkannya, kemudian pergi. Dan ia mempunyai **soundness sempurna**: pernyataan palsu langsung tidak mempunyai bukti yang sah. Hasil kemustahilan klasik mengatakan pengetahuan sifar perlu melepaskan kedua-dua ciri itu — bukan sekadar gabungan keduanya; setiap satu secara berasingan pun tidak boleh dikekalkan.

Pertama, bukti pengetahuan sifar memerlukan perbualan. Jika Alice hanya menghantar satu mesej, tanpa persediaan dipercayai yang diatur lebih awal, jaminan pengetahuan sifar runtuh — dan ini tetap benar walau sebanyak mana soundness yang sanggup anda korbankan sebagai gantinya.

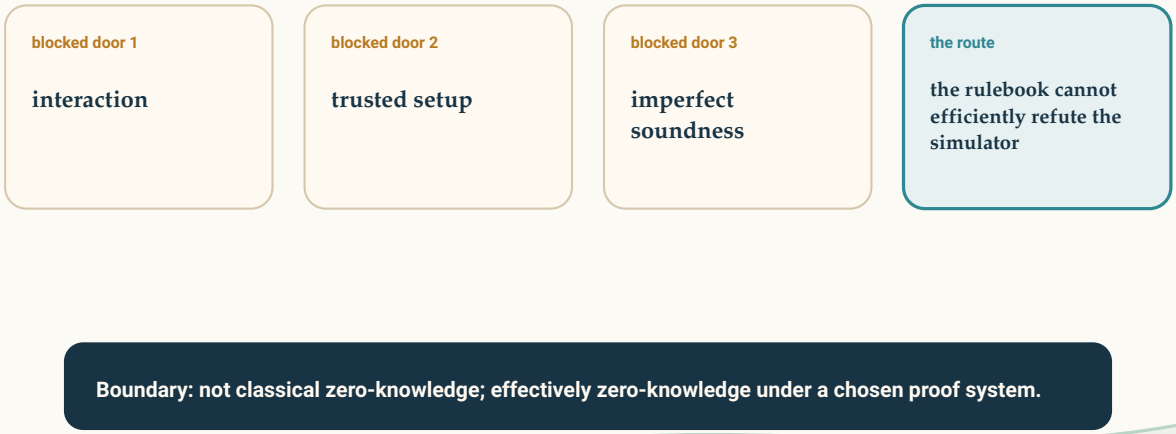
Kedua, bukti pengetahuan sifar memerlukan sedikit toleransi terhadap ralat. Menuntut soundness sempurna ternyata secara senyap memusnahkan interaksi juga: pengesah yang tidak boleh ditipu sama sekali, tidak kira pilihan rawak apa yang dibuatnya, pada asasnya boleh menetapkan semua pilihan itu lebih awal — dan sebaik pengesah menjadi boleh diramal, Alice boleh menjawab segala-galanya dalam satu mesej, iaitu tepat kes yang sudah terbukti gagal.

Makalah Rahul Ilango membincangkan satu jalan mengelilingi dinding berganda itu. Bukan dengan berpura-pura dinding tidak wujud, dan bukan dengan menghasilkan pengetahuan sifar klasik dalam keadaan yang mustahil. Gerakannya lebih halus: melemahkan maksud “tidak mendedahkan apa-apa”, tetapi melemahkannya dengan cara yang mengekalkan sifat keselamatan yang benar-benar boleh diuji oleh ahli kriptografi.

Hasilnya dipanggil **pengetahuan sifar secara efektif** (*effectively zero-knowledge*).

A proof without leaking the witness

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

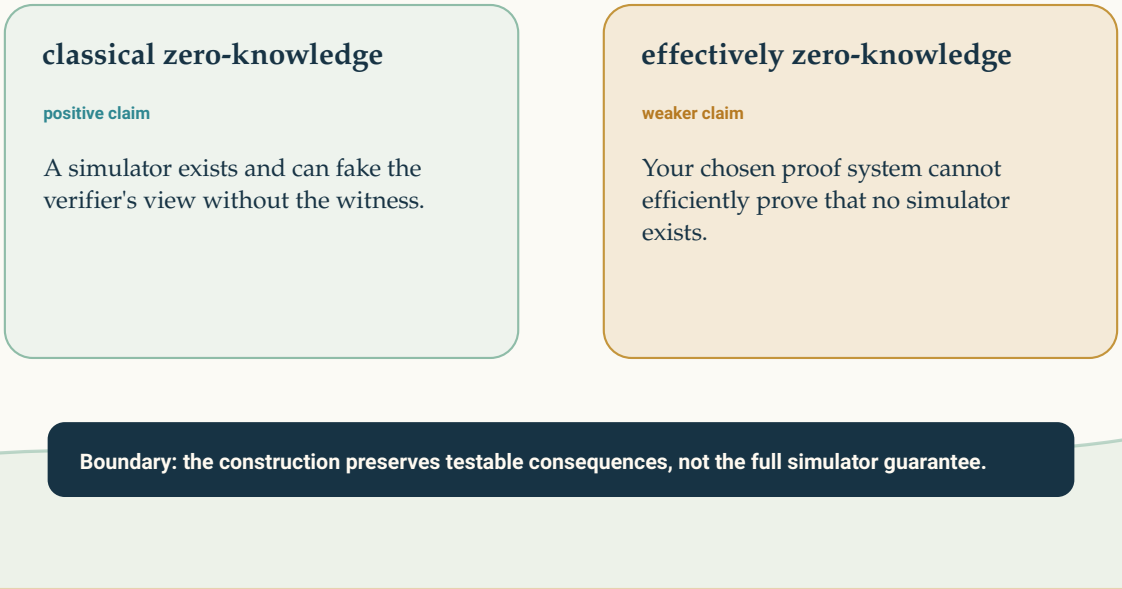


Pengetahuan sifar tersekat di tiga pintu — interaksi, persediaan dipercayai dan soundness tidak sempurna. Pembinaan Ilango melalui pintu lain: buku peraturan tidak dapat menolak simulator secara efisien.

Original diagram — The Clean Paper CC BY 4.0

Classical privacy vs effective privacy

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



Pengetahuan sifar klasik bertanya sama ada simulator wujud; “pengetahuan sifar secara efektif” hanya bertanya sama ada buku peraturan pilihan anda boleh membuktikan secara efisien bahawa simulator tidak

mungkin wujud. Soalan yang lebih lemah inilah yang membolehkan pembinaan mengekalkan satu mesej, tanpa persediaan dan soundness sempurna.

Ujian lama: simulator benar-benar wujud

Cara klasik untuk memformalkan pengetahuan sifar menggunakan pembantu rekaan yang dipanggil **simulator**.

Ideanya begini: bayangkan Jane, yang **tidak** mengetahui rahsia Alice. Jika Jane boleh menghasilkan sendiri bukti yang kelihatan sama seperti bukti yang Bob akan terima daripada Alice, maka bukti Alice tidak mengajar Bob apa-apa yang baharu. Jane sudah boleh memalsukan pengalaman itu tanpa rahsia Alice.

Jadi pengetahuan sifar klasik menuntut simulator sebenar. Mesti ada algoritma efisien yang boleh menghasilkan bukti palsu yang kelihatan sah tanpa mengetahui rahsia — dalam jargon, *witness*; untuk Sudoku, witness hanyalah grid yang telah diselesaikan.

Definisi ini berkuasa, tetapi di sinilah tepatnya kemustahilan lama menggigit. Intuisinya begini. Bukti yang benar-benar tidak interaktif hanyalah satu rentetan. Selepas Bob memiliki rentetan itu, dia boleh menunjukkannya kepada orang lain: dia memperoleh keupayaan untuk membuktikan pernyataan kepada pihak lain, yang sudah terdengar seperti lebih daripada “tiada apa-apa”. Teorem klasik menajamkan intuisi itu menjadi hasil kemustahilan di atas.

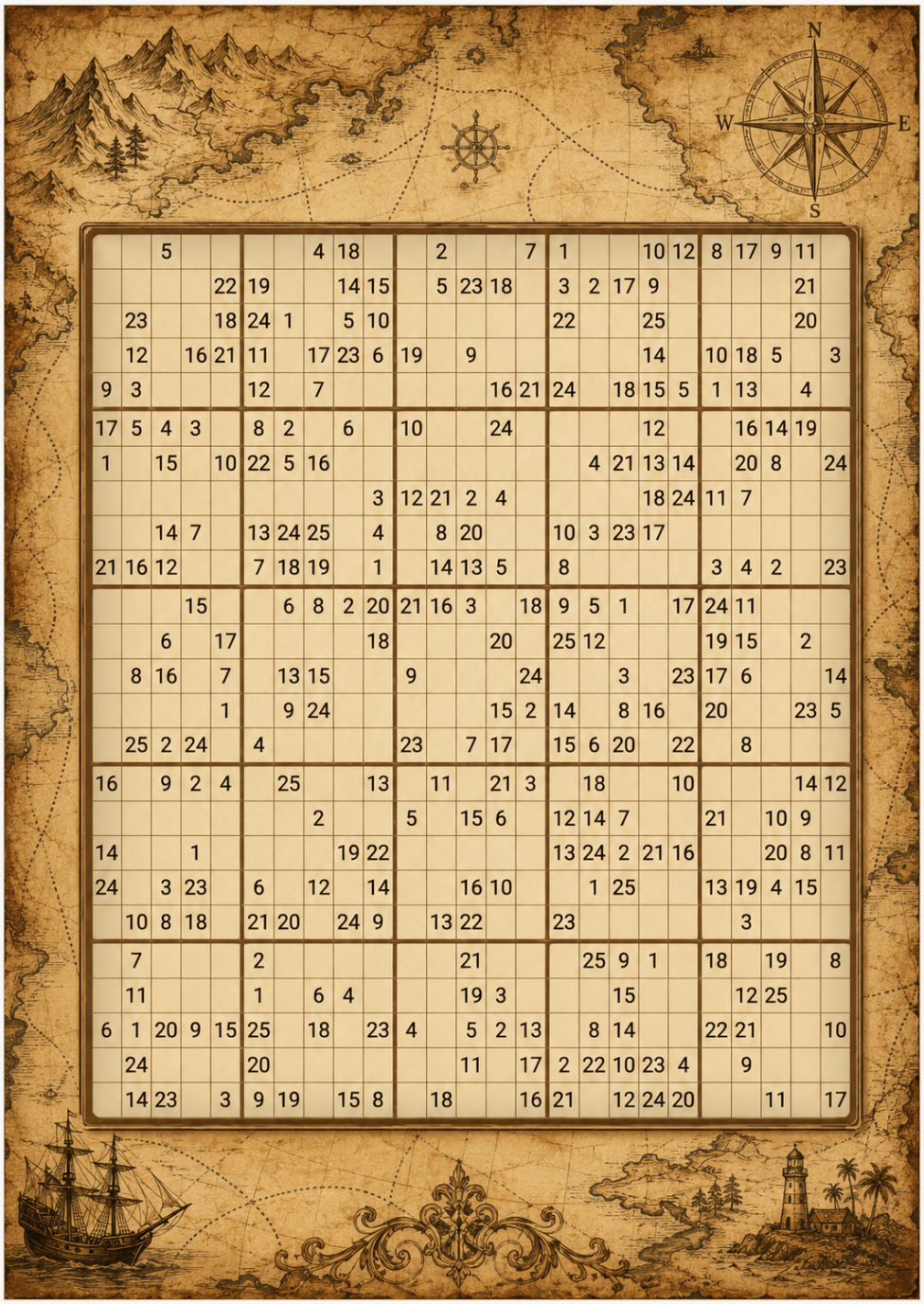
> **Tiga sifat yang makalah ini berkeras mahu kekalkan**
>
> Tajuk makalah menyebut tiga kekangan:
> **Tiada interaksi:** Alice menghantar satu rentetan bukti. Tiada protokol berbalas-balas.
> **Tiada persediaan:** Alice dan Bob tidak bergantung pada rentetan rujukan bersama yang dipercayai atau sumber rawak awam lain yang disediakan terlebih dahulu. Banyak sistem yang dipanggil “pengetahuan sifar tidak interaktif” masih bergantung pada persediaan; makalah ini benar-benar bermaksud tiada persediaan.
> **Soundness sempurna:** pernyataan palsu tidak mempunyai bukti sah. Bukan “hampir tidak pernah diterima”; bukti sah memang tidak wujud.
> Tiga sifat itu tepat seperti yang dimiliki matematik bertulis biasa — dan, seperti dijelaskan di atas, pengetahuan sifar klasik tidak boleh mengekalkannya.

Versi mega-Sudoku bagi perbezaannya

Berikut cara yang sengaja dipermudah untuk merasakan perbezaannya.

Jangan gunakan Sudoku biasa 9-demi-9 untuk bahagian serius analogi. Ia terlalu kecil dan terlalu

terhingga: komputer boleh sahaja menyelesaikannya, atau membuktikan bahawa tiada penyelesaian. Sebaliknya bayangkan keluarga teka-teki **MegaSudoku(n)**. Skalakan aturan biasa: pilih saiz blok *n*, tetapkan $N = n^2$, lalu bina grid *N* demi *N* yang dibahagikan kepada blok *n* demi *n*, dengan *N* simbol. Sudoku biasa hanyalah kes kecil $n = 3$, $N = 9$: grid 9-demi-9, blok 3-demi-3 dan sembilan simbol. Cerita kerumitan bukti hanya bermula apabila *n* dibenarkan membesar, dan apabila grid boleh membawa gadget tambahan yang membuatnya berkelakuan seperti formula SAT yang menyamar sebagai teka-teki Sudoku. Formula SAT hanyalah senarai kekangan ya/tidak: bolehkah anda menetapkan nilai benar/palsu kepada pemboleh ubah supaya setiap kekangan dipenuhi?



Sudoku 25x25: peraturannya boleh diperiksa tanpa mendedahkan grid lengkap — pengganti visual bagi bukti yang mengesahkan penyelesaian tersembunyi, iaitu witness.

Sudoku dan SAT: teka-teki yang sama dalam dua pakaian

Dakwaan bahawa Sudoku boleh "berkelakuan seperti formula SAT" bukan metafora. Terjemahan berjalan dalam kedua-dua arah, dan arah yang mudah boleh ditulis sepenuhnya.

Daripada Sudoku kepada SAT. SAT hanya bercakap benar/palsu, jadi berikan satu pemboleh ubah boolean bagi setiap tiga serangkai (baris, lajur, nilai): *x(r,c,v)* bermaksud "sel pada baris *r*, lajur *c* mengandungi nilai *v*." Sudoku 4-demi-4 (blok 2-demi-2, nilai 1–4) memerlukan 4·4·4 = 64 pemboleh ubah; Sudoku klasik 9-demi-9 memerlukan 729. Setiap peraturan Sudoku kemudian menjadi satu kelompok klausa. (Klausa ialah OR bagi pemboleh ubah atau negasinya; keseluruhan formula ialah AND bagi semua klausa.)

Setiap sel memegang sekurang-kurangnya satu nilai — satu klausa bagi setiap sel:

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

Setiap sel memegang paling banyak satu nilai — satu klausa "bukan kedua-duanya" bagi setiap pasangan nilai:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3)$$ … dan seterusnya untuk kesemua enam pasangan.

Setiap baris mengandungi setiap nilai — untuk baris 1 dan nilai 3: sekurang-kurangnya sekali,

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

dan paling banyak sekali: $\neg x(1,1,3) \vee \neg x(1,2,3)$, dan seterusnya bagi setiap pasangan sel dalam baris.

Lajur dan blok — kelompok yang sama; hanya kumpulan sel berubah. Untuk blok kiri atas dan nilai 2:

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

ditambah klausa "bukan kedua-duanya" bagi setiap pasangan.

Petunjuk bercetak — bahagian paling mudah: setiap petunjuk ialah klausa dengan satu pemboleh ubah. Angka 3 yang dicetak di sudut kiri atas menjadi klausa

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

AND bagi semua ini boleh dipuaskan tepat apabila Sudoku mempunyai penyelesaian — dan satu penetapan yang memuaskan *ialah* penyelesaian: baca x(r,c,v) mana yang benar dan isi grid. Untuk 9-demi-9, jumlahnya 729 pemboleh ubah dan beberapa ribu klausa, yang diselesaikan SAT solver moden dalam milisaat. Perhatikan klausa petunjuk x(1,1,3): ia berkata "sel ini tepat bernilai 3", bukan "sel-sel ini semuanya berbeza" — asimetri yang sama akan memerlukan helah tambahan bagi sel petunjuk dalam nota protokol di bawah.

Daripada SAT kepada Sudoku. Makalah memerlukan arah sebaliknya yang lebih sukar: diberi formula SAT *sebarang*, bina mega-Sudoku yang mempunyai penyelesaian tepat apabila

formula itu mempunyai penyelesaian. Aturan asli Sudoku hanya boleh berkata "sel-sel ini semuanya berbeza", jadi kekangan logik sebarang perlu *dibina* — dan itulah fungsi gadget. Gadget ialah kelompok kecil sel pra-bina, satu bagi setiap klausa formula, di mana sel tertentu memainkan peranan pemboleh ubah (simbol yang dipegangnya mengekod benar atau palsu), dan kekangan dalaman kelompok direka supaya hanya pengisian sah yang sepadan dengan penetapan yang memuaskan klausa itu dibenarkan. Ini ialah teknik piawai daripada bukti NP-completeness; untuk Sudoku tergeneralisasi ia dilaksanakan oleh Yato dan Seta pada 2003.
Bersama-sama, dua arah ini mengatakan Sudoku N-demi-N dan SAT ialah masalah yang sama memakai pakaian berbeza. Itulah yang membolehkan artikel ini — dan makalah — menceritakan kisah tentang seluruh NP menggunakan grid dan simbol.

Witness masih mudah dibayangkan. Alice mengetahui pengisian mega-Sudoku yang lengkap dan sah. Bob mahu diyakinkan bahawa pengisian seperti itu wujud, tetapi Alice tidak mahu mendedahkannya. Jika dia menghantar keseluruhan pengisian, Bob yakin, tetapi rahsia hilang.

Dalam versi pengetahuan sifar klasik, Alice dan Bob berinteraksi. Satu model mental gaya lama menggunakan jubin tertutup. Alice menyembunyikan grid selesai, secara rahsia menamakan semula simbol sebelum setiap pusingan, dan membenarkan Bob memeriksa satu kekangan tempatan yang dipilih secara rawak: baris, lajur, kotak atau gadget. Jika sel yang dibuka menunjukkan simbol semuanya berbeza, keyakinan Bob meningkat. Kemudian semuanya ditutup semula dan simbol dinamakan semula dengan pemetaan baharu. (Ada satu kerumitan: petunjuk asal teka-teki memerlukan helah tambahan, kerana penamaan semula simbol menyembunyikannya juga. Nota di bawah menerangkan bagaimana protokol klasik menyelesaikan hal ini; gambaran mainan ini mencukupi untuk apa yang menyusul.)

Bagaimana protokol klasik benar-benar mengendalikan sel petunjuk

Helah penamaan semula mempunyai titik buta. Peraturan baris, lajur dan kotak semuanya berkata "sel-sel ini semuanya berbeza", dan sifat *semuanya berbeza* kekal benar di bawah sebarang penamaan semula simbol. Tetapi petunjuk berkata "sel ini tepat mengandungi 5", dan selepas penamaan semula Bob hanya melihat $\sigma(5)$ — satu simbol terselindung — tanpa mengetahui pemetaan σ. Dia tidak boleh memeriksa apa-apa. Jika tidak diperbaiki, Alice boleh membuktikan bahawa *sesuatu* grid sah wujud sambil mengabaikan semua petunjuk bercetak, yang langsung tidak membuktikan apa-apa tentang *teka-teki ini*. Literatur klasik mempunyai dua pembaikan piawai.
Palet. Tambahkan satu baris tambahan N sel kepada grid tersembunyi — palet yang Alice isi dengan simbol 1…N dalam susunan awam tetap, kemudian namakan semula bersama segala-galanya, sehingga ia mengandungi $\sigma(1)$…$\sigma(N)$. Cabaran rawak Bob kini mempunyai satu pilihan tambahan. Selain memilih baris, lajur, kotak atau gadget untuk dibuka, dia boleh memilih **palet bersama satu sel petunjuk**. Alice membuka kedua-duanya; palet mendedahkan penamaan semula bagi pusingan itu, dan Bob memeriksa bahawa sel petunjuk menunjukkan tepat versi yang dinamakan semula bagi petunjuk bercetak. Ini kekal pengetahuan sifar kerana Bob hanya belajar σ — yang dipilih semula secara segar setiap pusingan dan tidak berguna

sendiri — serta nilai sel yang sudah diketahuinya daripada teka-teki. Tiada apa tentang sel rahsia bocor, dan simulator boleh memalsukan pandangan dengan memilih σ rawak. Ia sound kerana Alice yang menipu akan ditangkap dengan kebarangkalian tetap pada setiap pusingan, dan pusingan diulang sehingga keraguan menjadi boleh diabaikan.

Menyusun petunjuk ke dalam kekangan. Varian lebih berstruktur membuang cabaran khas itu, bukannya menambahkannya. Daripada *mengesahkan* nilai petunjuk, paksa nilai itu menggunakan kekangan perbezaan: hubungkan sel petunjuk dengan setiap sel palet kecuali yang membawa nilainya sendiri — "berbeza daripada $\sigma(1)$, berbeza daripada $\sigma(2)$, …, berbeza daripada semuanya kecuali $\sigma(5)$." Satu-satunya simbol yang boleh dipegang secara sah ialah simbol petunjuk. Kini setiap kekangan sekali lagi berbentuk "dua ini berbeza" — invariant di bawah penamaan semula, dan boleh diperiksa sama seperti baris. Ini ialah gerakan yang sama digunakan untuk bucu yang telah diwarnakan awal dalam protokol pewarnaan graf klasik, dan inilah semangat perkataan *gadget* di atas: dalam gambaran MegaSudoku-sebagai-SAT, petunjuk disusun menjadi gadget ketaksamaan seperti kekangan lain.

Protokol fizikal. Protokol kad dunia sebenar untuk Sudoku (Gradwohl, Naor, Pinkas dan Rothblum, 2007) tidak menggunakan penamaan semula langsung dan menyelesaikan petunjuk sebelum proses penyembunyian bermula. Untuk setiap sel, Alice meletakkan tiga kad sama dengan nilai sel — menghadap ke bawah untuk sel rahsia, tetapi **menghadap ke atas untuk sel petunjuk**, supaya Bob melihat sendiri bahawa petunjuk dipatuhi sebelum kad diterbalikkan. Kemudian satu kad daripada setiap sel dimasukkan ke paket baris, satu ke paket lajur, satu ke paket kotak; setiap paket dikocok dan didedahkan, dan Bob memeriksa bahawa ia mengandungi semua N simbol. Pengocokan memusnahkan maklumat kedudukan (itulah pengetahuan sifar), tetapi petunjuk sudah dipastikan ketika kad mula dibahagikan.

Apa pun kaedahnya, pelajarannya sama seperti yang terus diulang artikel ini: protokol pengetahuan sifar ialah perakaunan berhati-hati tentang fakta *mana* yang kekal selepas penyembunyian. Penamaan semula mengekalkan "semuanya berbeza" tetapi memadam "sama dengan 5" — jadi "sama dengan 5" perlu dimasukkan semula melalui cara lain.

Itu bukan protokol dalam makalah. Ia ialah model mental bagi pengetahuan sifar klasik:

- Alice dan Bob berbalas-balas.
- Bob memilih pemeriksaan rawak.
- Alice mendedahkan hanya konsistensi tempatan, bukan keseluruhan penyelesaian.
- Bukti privasi berfungsi dengan menunjukkan bahawa pandangan Bob boleh dihasilkan tanpa penyelesaian rahsia Alice.

Jadi pengetahuan sifar klasik dibina di sekitar satu fakta positif:

> Simulator benar-benar wujud.

Sekarang buang bahagian yang selesa. Alice menghantar satu rentetan bukti dan pergi. Tiada persediaan dipercayai, tiada rentetan rawak bersama yang disediakan terlebih dahulu, dan Bob tidak boleh sekali-kali menerima teka-teki palsu. Inilah keadaan di mana pengetahuan sifar klasik tidak boleh bertahan.

Satu watak lagi diperlukan sebelum helah bermula. Tetapkan satu **buku peraturan**: sistem bukti formal, dalam erti ahli logik — set aksiom tetap bersama peraturan mekanikal untuk memeriksa bukti matematik bertulis. ZFC, aksiom piawai matematik, ialah contoh kanonik. Segala yang menyusul dinyatakan relatif kepada buku peraturan yang dipilih lebih awal, dan pilihannya fleksibel: pembinaan berfungsi untuk mana-mana buku peraturan yang anda tetapkan, termasuk ZFC.

(Satu nota tentang istilah, mengikut makalah itu sendiri: "proof system" di sini sentiasa bermaksud buku peraturan ini — sistem formal yang memeriksa bukti matematik — bukan mesej yang dihantar Alice. Mesin Alice dan Bob dipanggil "pembukti dan pengesah".)

Versi gaya Gödel mengekalkan cerita mega-Sudoku tetapi mengubah buktinya.

Pilih sistem kekangan kedua dengan saiz paparan yang sama, panggilnya **D**. Dalam cerita ini, S dan D ialah dua teka-teki MegaSudoku(n) dalam format sama. Di belakang tabir, D mungkin bermula sebagai formula logik sukar dengan saiz berbeza; jika perlu, ia boleh dipanjangkan dengan kekangan dummy yang tidak berbahaya supaya muat pada grid sama. D dibina daripada formula logik yang sebenarnya **tidak boleh dipuaskan** (*unsatisfiable*): tiada penetapan nilai yang boleh membuat semua kekangannya benar, sama seperti teka-teki rosak yang tiada grid lengkap sah. Contoh mainan ialah formula yang menuntut serentak "X benar" dan "X palsu". Jadi D tidak mempunyai pengisian sah.

Tetapi D tidak boleh menjadi teka-teki rosak yang *mudah dibongkar*. Contoh mainan tadi gagal syarat ini: mana-mana buku peraturan boleh menolak "X dan bukan-X" dalam satu baris. D perlu palsu dengan cara yang tidak boleh disahkan oleh buku peraturan pilihan menggunakan hujah pendek. Jika buku peraturan boleh menolak D dengan bukti pendek, cerita di bawah runtuh: laluan alternatif yang mungkin menghasilkan bukti tanpa rahsia Alice boleh ditolak secara formal, dan bersama-sama dengannya hilang jaminan privasi. Jadi D dipilih daripada keluarga yang tidak dapat ditolak secara efisien oleh buku peraturan tetap: tiada bukti pendek, di dalam buku peraturan itu, bahawa D tiada penyelesaian.

Bukti satu mesej Alice kemudian mengenai pernyataan sama ada/atau:

> sama ada mega-Sudoku sebenar S mempunyai penyelesaian, atau decoy D mempunyai penyelesaian.

Inilah pautan logiknya. D **bukan** dihasilkan secara ajaib supaya S menjadi benar. Bukti tidak berhujah "D tiada penyelesaian, maka S mempunyai penyelesaian." Ia membuktikan disjungsi **S atau D**. Soundness sempurna mengatakan disjungsi palsu tidak boleh mempunyai bukti sah. Oleh sebab D sebenarnya palsu — ia tiada penyelesaian — satu-satunya cara disjungsi boleh benar ialah S benar. Jadi jika bukti diterima, S mesti mempunyai penyelesaian. Decoy tidak boleh membuat S yang palsu menjadi benar.

Tetapi untuk bahagian gaya pengetahuan sifar, tanyakan apa akan berlaku jika D *memang* mempunyai penyelesaian. Penyelesaian decoy itu akan bertindak sebagai witness alternatif. Ia membolehkan seseorang menghasilkan bukti tanpa mengetahui penyelesaian mega-Sudoku sebenar Alice — dengan kata lain, sebuah simulator. Dalam realiti D tiada penyelesaian, jadi laluan simulator itu tertutup. Intinya ialah buku peraturan tidak boleh membuktikan secara efisien bahawa laluan itu tertutup.

Jadi D mempunyai dua tugas. Untuk **soundness**, D palsu, jadi bukti sah bagi "S atau D" memaksa

S benar. Untuk **pengetahuan sifar secara efektif**, D sukar ditolak, jadi buku peraturan tidak boleh cepat menolak laluan decoy yang sekiranya terbuka akan membolehkan simulasi.

Maka ujian keselamatan bukan lagi:

> Bolehkah kita membuktikan bahawa simulator benar-benar wujud?

Ia menjadi:

> Bolehkah buku peraturan anda membuktikan secara efisien bahawa simulator itu mustahil?

Jika jawapannya tidak, sesuatu yang mengejutkan kuat menyusul: setiap jaminan keselamatan yang (a) boleh diperhatikan dengan menjalankan ujian, dan (b) boleh dibuktikan — di dalam buku peraturan itu — sebagai akibat daripada kewujudan simulator, benar-benar berlaku. Serangan berjaya terhadap mana-mana sifat itu sendiri akan menjadi penolakan pendek yang hilang, dan penolakan pendek itu memang tidak wujud. Itulah bahagian “efektif” dalam pengetahuan sifar secara efektif.

Jadi perbandingan dalam kelas ialah:

Pengetahuan sifar klasik: bukti selamat kerana simulator wujud.

Pengetahuan sifar secara efektif gaya Gödel: bukti dianggap selamat bagi ujian keselamatan yang boleh diperhatikan kerana buku peraturan tidak boleh membuktikan secara efisien bahawa simulator mustahil.

Dakwaan kedua lebih lemah. Tetapi itulah juga sebab makalah boleh mengekalkan tiga ciri yang memecahkan versi klasik: satu mesej, tiada persediaan dan soundness sempurna.

Ujian baharu: anda tidak boleh membuktikan simulator itu tiada

Relaksasi Ilango mengubah soalan.

Pengetahuan sifar klasik bertanya:

> Adakah simulator wujud?

Pengetahuan sifar secara efektif bertanya sesuatu yang lebih lemah:

> Bolehkah buku peraturan pilihan anda membuktikan secara efisien bahawa tiada simulator wujud?

Ini kedengaran seperti helah teknikal, tetapi itulah idea teras. Pembinaan berada dalam keadaan yang pelik: simulator sebenarnya tidak wujud — makalah menyatakannya dengan jelas — tetapi buku peraturan yang telah ditetapkan tidak dapat membuktikan secara efisien bahawa ia tidak wujud. Jika setiap akibat buruk yang anda pedulikan memerlukan penolakan seperti itu, sistem masih berkelakuan seperti pengetahuan sifar untuk akibat tersebut.

Di sinilah Gödel masuk. Bukan sebagai hiasan, dan bukan sebagai "Gödel menjadikan kripto selamat." Hubungannya bersifat teori bukti. Satu buku peraturan dipanggil **optimal** jika, dalam erti tepat, ia ialah yang terbaik: apabila mana-mana buku peraturan boleh menolak formula jenis berkaitan dengan bukti pendek, buku peraturan optimal juga boleh melakukannya, dengan bukti paling banyak lebih panjang secara polinomial. Krajíček dan Pudlák pada 1989 mengemukakan konjektur bahawa **tiada sistem bukti optimal wujud**: apa pun buku peraturan yang anda tetapkan, ada buku peraturan lain yang membuktikan sesuatu keluarga pernyataan benar dengan jauh lebih ringkas. Ini salah satu konjektur terbuka pusat dalam kerumitan bukti, dan merupakan sepupu terhingga dalam teori kerumitan kepada teorem ketaklengkapan Gödel: sesetengah pernyataan benar tidak mempunyai bukti pendek dalam buku peraturan yang anda pilih — bukan kerana ia tidak boleh dibuktikan sama sekali, tetapi kerana setiap buku peraturan tetap meninggalkan beberapa kebenaran ringkas tanpa bukti ringkas.

Makalah menganggap konjektur ini benar (dalam bentuk "infinitely often" yang sedikit lebih kuat, seperti biasa apabila konjektur digunakan dalam kriptografi). Hasilnya, melalui teorem Krajíček dan Pudlák, sangat konkrit: untuk setiap buku peraturan ada urutan formula yang benar-benar tidak boleh dipuaskan, yang tidak dapat ditolak oleh buku peraturan dengan bukti pendek — dan, yang paling penting, boleh *dihasilkan* oleh algoritma efisien. Sifat terakhir itu, uniformity, menukar seluruh idea daripada dakwaan kewujudan menjadi algoritma sebenar yang boleh dijalankan Alice: decoy D keluar dari barisan pemasangan, bukan muncul dari udara kosong.

Gerakan kriptografi ialah menggunakan kekurangan kuasa pembuktian itu.

Apa yang dilakukan oleh pembinaan ini

Berikut bentuk pembinaan makalah, dikupas kepada rangkanya.

Tetapkan buku peraturan — misalnya ZFC. Di bawah andaian kerumitan bukti, terdapat urutan formula yang boleh dihasilkan secara efisien dan sebenarnya tidak boleh dipuaskan, tetapi buku peraturan tidak mempunyai bukti pendek bahawa formula itu tidak boleh dipuaskan.

Kemudian bina bukti satu mesej dalam bentuk ini:

> sama ada pernyataan sebenar boleh dipuaskan, atau formula sukar khas ini boleh dipuaskan.

Formula sukar khas itu sebenarnya tidak boleh dipuaskan. Jadi jika mesin bukti asas mempunyai soundness sempurna, penerimaan mesej tetap bermaksud pernyataan sebenar benar. Itulah yang memberikan soundness sempurna.

Tetapi bagi keselamatan menyerupai pengetahuan sifar, bayangkan formula sukar khas itu *boleh* dipuaskan. Witness-nya kemudian boleh digunakan untuk mensimulasikan bukti tanpa mengetahui witness sebenar. Formula itu sebenarnya tidak boleh dipuaskan — tetapi buku peraturan tidak boleh membuktikannya secara efisien. Jadi ia tidak boleh membuktikan secara efisien bahawa simulator mustahil.

Itulah engselnya. Sistem tidak menyembunyikan rahsia dengan menghasilkan simulator klasik. Ia menyembunyikan rahsia, bagi kelas besar ujian keselamatan yang boleh diperhatikan, di sebalik ketidakupayaan buku peraturan untuk mengesahkan bahawa simulator tidak wujud.

Apa yang didakwa oleh makalah

Teorem utama datang dalam beberapa lapisan. Hasil teras ialah ini:

Di bawah satu andaian kriptografi piawai — kewujudan **non-interactive witness indistinguishable proofs**, objek yang dikaji dengan baik dan terhasil daripada beberapa pakej andaian yang mapan — serta konjektur kerumitan bukti bahawa **tiada sistem bukti optimal (infinitely often) wujud**, makalah membina, untuk setiap pilihan buku peraturan, pembukti dan pengesah satu mesej bagi NP/SAT dengan **soundness sempurna** dan tanpa persediaan, yang merupakan pengetahuan sifar secara efektif relatif kepada buku peraturan itu. (NP/SAT ialah "penyebut sepunya paling sukar" piawai bagi masalah menyerupai teka-teki; mega-Sudoku ialah salah satu pakaiannya.)

Bagi dakwaan lebih luas tentang mengekalkan sifat keselamatan yang boleh difalsifikasikan, makalah menambah satu lagi andaian piawai, kepercayaan derandomisasi **P = BPP** (secara kasar: randomness tidak memberi algoritma kuasa tambahan yang penting).

Diterjemahkan keluar daripada bahasa teorem:

- Bukti ialah satu mesej.
- Tiada persediaan dipercayai.
- Pernyataan palsu tidak boleh dibuktikan.
- Pembukti bukan pengetahuan sifar klasik — ia tiada simulator.
- Tetapi setiap akibat keselamatan berasaskan permainan dan boleh difalsifikasikan daripada pengetahuan sifar klasik boleh dicapai dalam keadaan ini.

"Boleh difalsifikasikan" penting. Ia bermaksud kegagalan keselamatan boleh diuji dengan menjalankan adversari dalam satu permainan. Banyak definisi keselamatan kriptografi berbentuk begini: bolehkah adversari membezakan dua enkripsi, menyongsangkan fungsi, mendapatkan witness, atau memenangi eksperimen tertentu? Teorem memberi satu pembukti bagi setiap sifat yang boleh difalsifikasikan, satu demi satu. Satu pembukti yang menikmati *semua* sifat boleh difalsifikasikan serentak berkemungkinan mustahil — serangan kebolehgunaan semula lama ("Bob boleh menunjukkan bukti kepada orang lain") sendiri ialah sifat yang boleh difalsifikasikan, dan ia benar-benar gagal di sini. Cadangan makalah ialah satu pembukti secara munasabah boleh merangkumi semua sifat boleh difalsifikasikan yang *semula jadi* — yang benar-benar muncul

dalam amalan kriptografi — tetapi bahagian itu ialah teorem bersyarat yang bergantung pada tanggapan informal "semula jadi", ditambah satu konjektur eksplisit. Jaminan disasarkan kepada kegagalan yang boleh diperhatikan, bukan setiap maksud falsafah atau berasaskan simulasi tentang kerahsiaan.

Satu korolari konkrit wajar disebut: pembinaan menghasilkan bukti *witness hiding* tidak interaktif pertama dengan pembukti uniform — "bukti bahawa teka-teki mempunyai penyelesaian tidak membantu anda mencari penyelesaiannya", tanpa interaksi dan tanpa persediaan — objek yang kedengaran sederhana tetapi telah menolak pembinaan selama beberapa dekad.

Apa yang tidak dikatakan oleh hasil ini

Bahagian inilah yang memastikan cerita kekal jujur.

Ia **tidak** mengatakan teorem kemustahilan lama salah. Pembinaan mengelakkannya dengan mengubah definisi.

Ia **tidak** memberikan pengetahuan sifar biasa, klasik, dengan tiada interaksi, tiada persediaan dan soundness sempurna. Makalah dengan jelas menyatakan pembukti yang dibina tidak mempunyai simulator.

Ia **tidak** bermaksud bukti tidak boleh digunakan semula. Bukti satu mesej masih boleh ditunjukkan kepada orang lain; makalah tidak mengekalkan sifat gaya deniability. (Pengetahuan sifar tidak interaktif dengan persediaan dipercayai mempunyai had sama.)

Ia **tidak** bermaksud ini protokol praktikal yang sedia digunakan. Ini ialah teori kerumitan dan asas kriptografi. Hasil bergantung pada andaian besar daripada kerumitan bukti dan kriptografi, dan pembinaan membincangkan apa yang mungkin secara prinsip.

Ia **tidak** menjadikan "Gödel" satu primitif keselamatan ajaib. Hubungan Gödel melalui sistem bukti, sistem bukti optimal dan analog terhingga ketaklengkapan. Intuisi berguna bukan "ketaklengkapan melindungi kata laluan anda." Sebaliknya: jika sebuah buku peraturan tidak boleh membuktikan secara efisien bahawa simulator mustahil, maka serangan yang memerlukan bukti itu boleh disekat pada aras definisi keselamatan.

Mengapa ia tetap menarik

Kriptografi sering menukar kesukaran menjadi keselamatan. Pemfaktoran sukar, jadi andaian gaya RSA menjadi berguna. Masalah lattice sukar, jadi kriptografi lattice menjadi berguna. Di sini kesukarannya lebih aneh: bukan "sukar mengira rahsia", tetapi "sukar membuktikan bahawa objek bukti tertentu tidak mungkin wujud."

Itulah sebabnya makalah ini terasa luar biasa. Ia menganggap aksiom dan buku peraturan hampir

seperti sumber kriptografi. Kemustahilan biasa mengatakan ada ketegangan antara soundness dan simulasi. Gerakan Ilango ialah meletakkan ketegangan itu di belakang tirai teori bukti: simulator tiada, tetapi sistem formal tidak boleh mendedahkan ketiadaan itu secara efisien.

Bagi pembaca, bahagian mengejutkan bukan bahawa ini akan menggantikan sistem pengetahuan sifar hari ini. Mungkin tidak, sekurang-kurangnya bukan secara langsung. Yang mengejutkan ialah had daripada logik matematik boleh digunakan secara konstruktif: bukan hanya sebagai dinding, tetapi sebagai sejenis perlindungan.

Sejauh mana kukuh buktinya?

Ini makalah teorem, jadi "bukti" bermaksud sesuatu yang berbeza daripada makalah biologi atau astronomi. Soalannya bukan sama ada eksperimen telah direplikasi. Soalannya ialah sama ada definisi, andaian dan rantaian pembuktian menyokong dakwaan.

Buktinya formal, dan makalah jelas tentang andaian. Andaian itu bukan sembarangan. Non-interactive witness indistinguishable proofs ialah objek piawai dalam kriptografi dan terhasil daripada beberapa pakej andaian yang mapan. Konjektur tiada-sistem-bukti-optimal ialah konjektur pusat dalam kerumitan bukti. P = BPP ialah kepercayaan derandomisasi piawai yang digunakan hanya untuk teorem lebih luas tentang sifat boleh difalsifikasikan.

Makalah juga berhujah bahawa andaian itu ialah harga yang betul, bukan perancah sewenang-wenangnya: ia membuktikan konvers yang menunjukkan andaian tersebut pada asasnya perlu — jika pembinaan seperti ini wujud sama sekali, maka non-interactive witness indistinguishable proofs mesti wujud dan (dengan andaian fungsi sehala piawai) sistem bukti optimal tidak boleh wujud. Andaian itu juga bersifat "win-win": menyangkal mana-mana satunya sendiri akan menjadi penemuan besar dalam kerumitan bukti, kriptografi atau teori kerumitan.

Tetapi kerana hasilnya bersyarat, keyakinannya juga bersyarat. Jika andaian itu gagal, tafsiran teorem berubah. Dan walaupun andaian benar, jaminannya bukan pengetahuan sifar klasik penuh; ia ialah versi relaksasi dan teori-bukti milik makalah.

Jadi keyakinan yang tepat ialah tinggi bahawa makalah menetapkan hasil kemungkinan bersyarat yang koheren; sederhana bahawa andaian menggambarkan dunia kriptografi sebenar yang kita diami; dan rendah bagi sebarang akibat praktikal segera.

Mengapa ia penting

Makalah membuka laluan yang sepatutnya tertutup.

Teori klasik berkata: pengetahuan sifar penuh tidak boleh menjadi satu mesej tanpa persediaan, dan tidak boleh mempunyai soundness sempurna. Makalah Ilango berkata: jika kita meminta akibat pengetahuan sifar yang boleh diuji dalam permainan keselamatan, dan jika kita membenarkan

definisi keselamatan bergantung pada apa yang buku peraturan boleh atau tidak boleh tolak secara efisien, maka banyak tingkah laku berguna boleh dipulihkan — dengan satu mesej, tiada persediaan dan soundness sempurna.

Itu bukan sekadar pelarasan kecil definisi. Ia cara berbeza untuk berfikir tentang jaminan kriptografi. Daripada hanya bertanya apa yang wujud, tanyakan apa yang boleh disingkirkan oleh buku peraturan anda. Daripada menganggap ketidakbolehbuktian sebagai gangguan falsafah, gunakan ia sebagai struktur.

Dunia praktikal mungkin tidak berubah esok. Tetapi peta konseptual berubah. Kini ada pengertian formal di mana "tiada siapa boleh membuktikan secara efisien bahawa rahsia bocor" boleh cukup kuat untuk memulihkan banyak perlindungan berasaskan permainan yang kita mahukan daripada "rahsia tidak bocor."

Itulah sebabnya Gödel berada dalam tajuk.

Ringkasan utama

Bukti pengetahuan sifar membolehkan pembukti meyakinkan pengesah bahawa satu pernyataan benar tanpa mendedahkan witness. Hasil kemustahilan klasik mengatakan pengetahuan sifar tidak boleh dipadatkan menjadi satu mesej tanpa persediaan, dan tidak boleh mempunyai soundness sempurna. Makalah Rahul Ilango tidak menyangkal kemustahilan tersebut. Ia mentakrifkan tanggapan lebih lemah, pengetahuan sifar secara efektif: daripada menuntut simulator benar-benar wujud, ia menuntut sistem bukti pilihan — buku peraturan formal seperti ZFC — tidak dapat membuktikan secara efisien bahawa simulator tidak wujud. Di bawah andaian besar daripada kriptografi (non-interactive witness indistinguishable proofs) dan kerumitan bukti (tiada sistem bukti optimal wujud), makalah membina pembukti satu mesej bagi NP/SAT tanpa persediaan dan dengan soundness sempurna yang mencapai akibat pengetahuan sifar berasaskan permainan dan boleh difalsifikasikan, sifat demi sifat. Satu pembukti tunggal yang merangkumi semua sifat "semula jadi" seperti itu ialah peluasan lanjut yang sebahagiannya masih bersifat konjektur — dan merangkumi secara literal setiap sifat boleh difalsifikasikan mungkin mustahil, kerana bukti masih boleh digunakan semula. Hasilnya teoritis dan bersyarat, bukan primitif yang sudah digunakan, tetapi ia menunjukkan cara baharu menggunakan ketidakbolehbuktian teori-bukti sebagai sumber kriptografi.

Semakan tanpa gembar-gembur

Apa yang ditunjukkan oleh makalah: Di bawah andaian yang dinyatakan, pembukti satu mesej tanpa persediaan dan dengan soundness sempurna boleh dibina untuk NP/SAT yang merupakan pengetahuan sifar secara efektif relatif kepada mana-mana sistem bukti pilihan, serta mencapai setiap akibat pengetahuan sifar klasik berasaskan permainan yang boleh difalsifikasikan.

Apa yang munasabah tetapi belum dibuktikan tanpa syarat: Bahawa andaian kerumitan bukti dan

kriptografi yang diperlukan benar. Ia andaian serius dan telah banyak dikaji — dan makalah menunjukkan ia pada asasnya perlu serta mencukupi — tetapi masih andaian.

Apa yang tidak ditunjukkan: Pengetahuan sifar klasik dengan tiada interaksi, tiada persediaan dan soundness sempurna; sistem praktikal yang sedia digunakan; deniability atau ketidakbolehgunaan semula bukti; atau bahawa teorem ketaklengkapan Gödel dengan sendirinya menjamin keselamatan kriptografi.

Had utama: Jaminan ialah relaksasi pengetahuan sifar; versi terluas bergantung pada beberapa andaian; dakwaan satu pembukti universal masih sebahagiannya bersifat konjektur; dan hasil ini terutama bersifat asas teori.

Berapa banyak keyakinan patut diberikan pembaca umum? Tinggi bahawa ini hasil teori bersyarat yang penting jika definisinya diterima. Sederhana bahawa andaian menggambarkan realiti. Rendah untuk penggunaan praktikal segera. Kesimpulan selamat ialah: makalah tidak memecahkan kemustahilan pengetahuan sifar; ia menemui jalan teori-bukti baharu mengelilingi bahagian kemustahilan itu yang penting untuk banyak permainan keselamatan.

Sumber

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`