The Clean Paper

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

Kriptoqrafik sübut çatışmayan simulator-un yoxluğunu sübut etməyi çətinləşdirərək sirrini gizlədə bilər

Zero-knowledge proofs witness-i açıqlamadan ifadəni sübut etməyə imkan verir. Klassik nəzəriyyə deyir ki, bunu tam mənada bir mesaj, etibarlı setup olmadan və mükəmməl soundness ilə eyni anda əldə etmək mümkün deyil. Rahul Ilango-nun paper-i bu mümkünsüzlüyü yox etmir. Hədəfi dəyişir: simulator-un həqiqətən mövcud olmasını tələb etmək əvəzinə, seçilmiş heç bir proof system-in simulator-un mövcud olmadığını səmərəli şəkildə sübut edə bilməməsini tələb edir. Proof complexity və kriptoqrafiyadan böyük fərziyyələr altında bu, zero-knowledge-un falsifiable, game-based nəticələrini xüsusiyyət-hissə ilə geri almaq üçün kifayətdir. Məqsəd internetə qoşub istifadə ediləcək hazır primitiv deyil. Bu, riyazi unprovability-ni kriptoqrafik örtüyə çevirən proof-theoretic yanaşmadır.

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

Hiylə sirrin gizli olduğunu sübut etmək deyil

Zero-knowledge-un ən sadə versiyasından başlayaq.

Alice Bob-u Sudoku tapmacasının həlli olduğuna inandırmaq istəyir. Həlli göndərsə, Bob inanacaq, amma tapmacanın sirri də bitəcək. Alice-in istədiyi daha qəribədir: həlli açıqlamadan həllin mövcud olduğunu sübut etmək.

Zero-knowledge sübutunun vədi budur. Sübut edən tərəf (Alice) yoxlayıcını (Bob) ifadənin doğru olduğuna inandırır, amma ifadənin doğru olmasından əlavə heç nə açıqlamır.

Problem budur ki, bu vədin bir qiyməti var. Adi riyazi sübutun iki rahat xüsusiyyəti olur. O, **bir mesajdır**: yazırsınız, təqdim edirsiniz və gedirsiniz. Həm də **mükəmməl soundness**-ə malikdir: yanlış ifadənin ümumiyyətlə etibarlı sübutu yoxdur. Klassik mümkünsüzlük nəticələri deyir ki, zero-knowledge hər iki xüsusiyyətdən imtina etməlidir — və təkcə ikisindən eyni anda yox; hər biri ayrıca əlçatmazdır.

Birincisi, zero-knowledge sübutu dialoq tələb edir. Alice əvvəlcədən razılaşdırılmış etibarlı setup olmadan yalnız bir mesaj göndərirsə, zero-knowledge zəmanəti dağılır — və bunun qarşılığında soundness-dən nə qədər güzəşt etməyə hazır olmağınız fərq etmir.

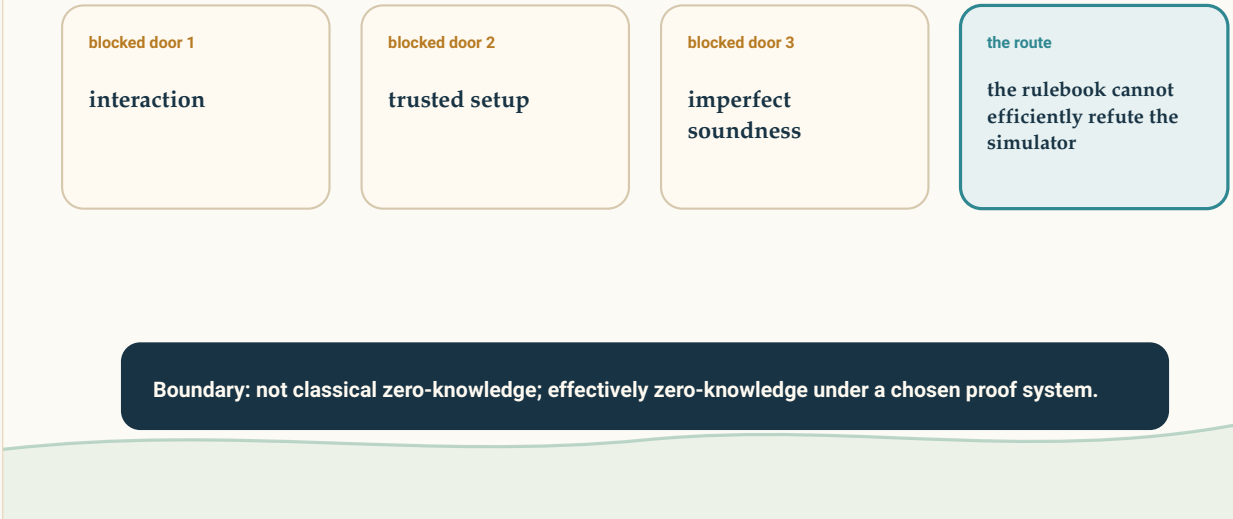
İkincisi, zero-knowledge sübutu kiçik səhv ehtimalına dözməlidir. Mükəmməl soundness tələb etmək qarşılıqlı əlaqəni də səssizcə məhv edir: hansı təsadüfi seçimləri etməsindən asılı olmayaraq heç vaxt aldadıla bilməyən verifier həmin seçimləri əvvəlcədən sabitləyə bilər; verifier proqnozlaşdırıla biləndən sonra isə Alice bütün cavabları bir mesajda verə bilər — bu da artıq pozulduğunu bildiyimiz vəziyyətdir.

Rahul Ilango-nun məqaləsi bu ikiqat divarın ətrafından keçən bir yol haqqındadır. Divarın olmadığını iddia etməklə yox, mümkünsüz şəraitdə klassik zero-knowledge yaratmaqla da yox. Hərəkət daha incədir: “heç nə açıqlamır” ifadəsinin mənasını zəiflətmək, amma bunu kriptoqrafların həqiqətən test edə bildiyi təhlükəsizlik xüsusiyyətlərini qoruyan şəkildə etmək.

Nəticə **effectively zero-knowledge** adlanır.

A proof without leaking the witness

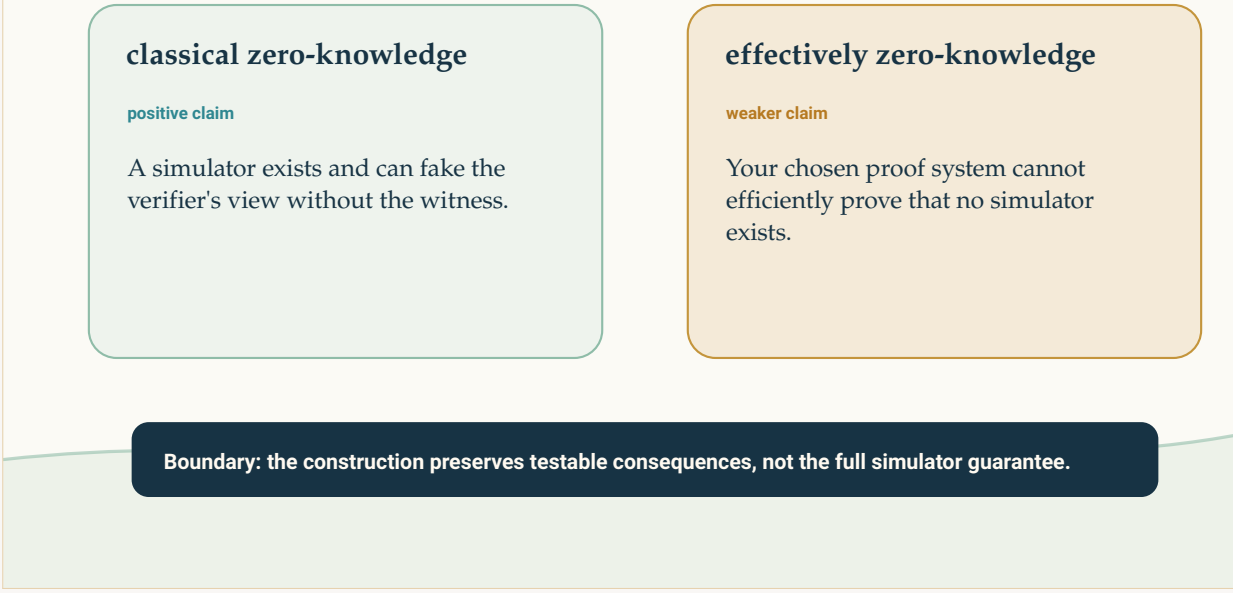
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Zero-knowledge üç qapıda ilişir — qarşılıqlı əlaqə, etibarlı setup və qeyri-mükəmməl soundness. Ilango-nun konstruksiyası başqa qapıdan keçir: qaydalar kitabı simulator-u səmərəli şəkildə təkzib edə bilmir.

Classical privacy vs effective privacy

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



Klassik zero-knowledge simulator-un həqiqətən mövcud olub-olmadığını soruşur; “effectively zero-knowledge” isə yalnız seçdiyiniz qaydalar kitabının onun mövcud ola bilmədiyini səmərəli şəkildə sübut edib-edə bilmədiyini

soruşur. Məhz bu daha zəif sual konstruksiyaya bir mesajı, setup-sızlığı və mükəmməl soundness-i saxlamağa imkan verir.

Köhnə test: simulator mövcuddur

Zero-knowledge-u klassik şəkildə formallaşdırmaq üçün **simulator** adlanan xəyali köməkçidən istifadə edilir.

Fikir belədir: Alice-in sirrini **bilməyən** Jane-i təsəvvür edin. Jane təkbaşına Bob-un Alice-dən alacağı sübutlarla eyni görünən sübutlar yarada bilirsə, deməli Alice-in sübutları Bob-a yeni heç nə öyrətməyib. Jane Alice-in sirrini bilmədən də həmin təcrübəni saxtalaşdıra bilirdi.

Buna görə klassik zero-knowledge həqiqi simulator tələb edir. Sirri — jarqonda *witness* — bilmədən inandırıcı saxta sübutlar yarada bilən səmərəli alqoritm mövcud olmalıdır; Sudoku üçün witness sadəcə doldurulmuş düzgün cədvəldir.

Bu tərif güclüdür, amma köhnə mümkünsüzlüyün dişlədiyi yer də məhz buradır. İntuisiyanı belə düşünün. Həqiqətən non-interactive sübut sadəcə bir sətirdir. Bob həmin sətri aldıqdan sonra onu başqasına göstərə bilər: artıq ifadəni başqalarına sübut etmək qabiliyyəti qazanıb və bu, “heç nə”dən artıq kimi səslənir. Klassik teoremlər bu intuisiyanı yuxarıdakı mümkünsüzlük nəticələrinə çevirir.

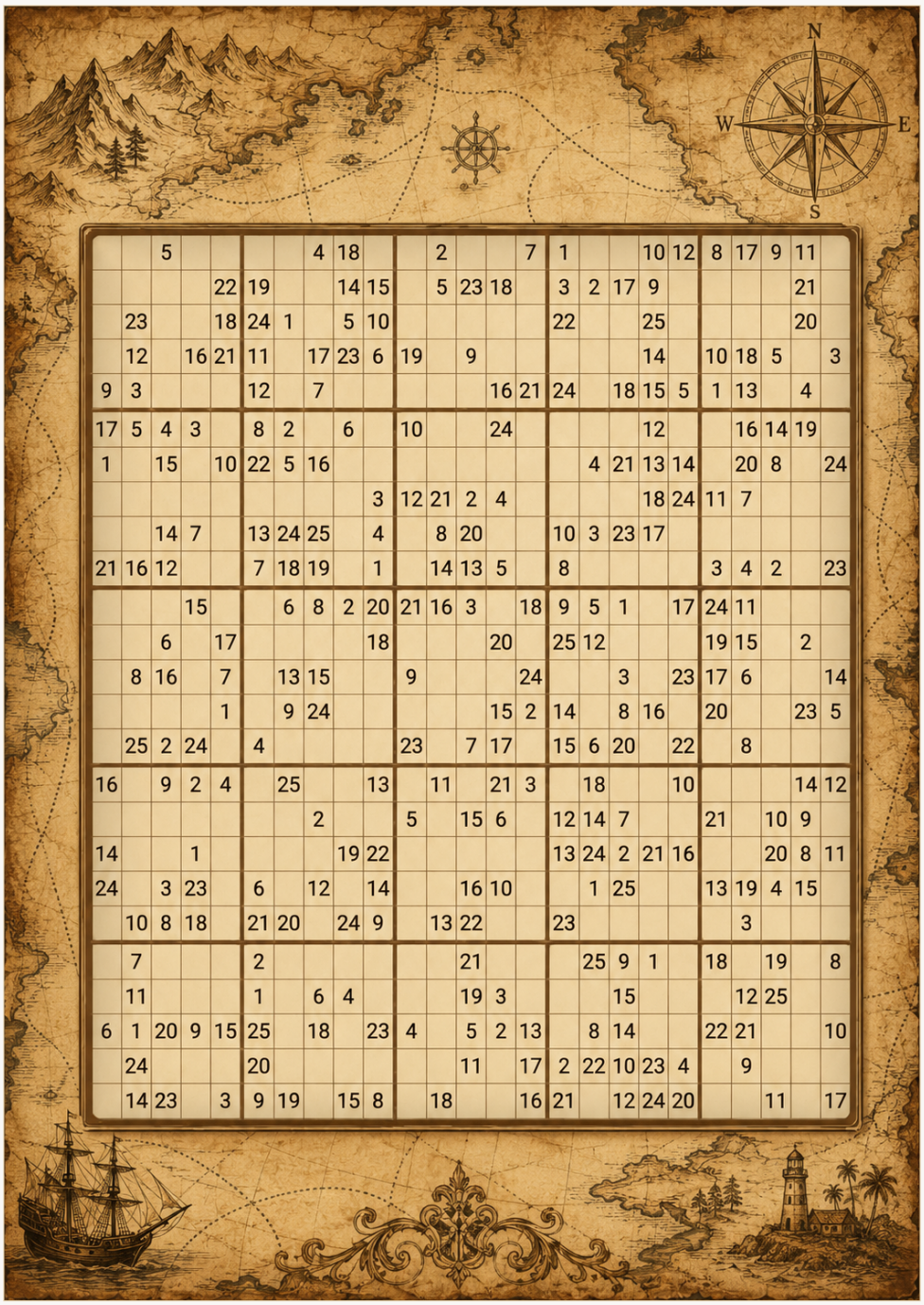
> **Bu məqalənin israr etdiyi üç xüsusiyyət**
>
> Məqalənin başlığı üç məhdudiyyəti adlandırır:
> **Qarşılıqlı əlaqə yoxdur:** Alice bir sübut sətri göndərir. Gediş-gəlişli protokol yoxdur.
> **Setup yoxdur:** Alice və Bob etibarlı ümumi reference string-ə və ya əvvəlcədən razılaşdırılmış başqa ictimai təsadüfiliyə arxalanmırlar. “Non-interactive zero-knowledge” adlanan bir çox sistem yenə setup-a söykənir; bu məqalədə setup sıfırdır.
> **Mükəmməl soundness:** yanlış ifadənin etibarlı sübutu yoxdur. “Demək olar heç vaxt qəbul edilmir” yox; etibarlı sübut ümumiyyətlə mövcud deyil.
> Bu üç xüsusiyyət adi yazılı riyaziyyatda olan xüsusiyyətlərdir — və yuxarıda izah edildiyi kimi, klassik zero-knowledge onların hamısını saxlaya bilməz.

Fərqi MegaSudoku ilə hiss etmək

Fərqi hiss etmək üçün qəsdən sadələşdirilmiş bir yol.

Analogiyanın ciddi hissəsi üçün adi 9-by-9 Sudoku istifadə etməyin. O, çox kiçik və çox sonludur: kompüter sadəcə həll edə və ya həlli olmadığını sübut edə bilər. Əvəzində **MegaSudoku(n)** tapmacaları ailəsini təsəvvür edin. Adi qaydanı böyüdün: blok ölçüsü n

seçin, $N = n^2$ olsun və N simvollu, n by n bloklara bölünmüş N by N cədvəl qurun. Adi Sudoku sadəcə kiçik $n = 3$, $N = 9$ halıdır: 9-by-9 cədvəl, 3-by-3 bloklar və doqquz simvol. Proof-complexity hekayəsi yalnız n böyüyə bildikdə və cədvəl Sudoku kimi geyinmiş SAT formulası kimi işləməsinə imkan verən əlavə gadget-lər daşıya bildikdə başlayır. SAT formulası sadəcə bəli/xeyr məhdudiyyətlərinin siyahısıdır: dəyişənlərə true/false qiymətləri verib bütün məhdudiyyətləri eyni anda ödəmək mümkündürmü?



25x25 Sudoku: tamamlanmış cədvəli açıqlamadan qaydalarının ödəndiyi yoxlanıla bilər — gizli həlli, yəni witness-i təsdiqləyən sübut üçün vizual bənzətmə.

Sudoku və SAT: eyni tapmaca, iki fərqli geyimdə

Sudoku-nun "SAT formulası kimi davrana bilməsi" iddiası metafora deyil. Tərcümə hər iki istiqamətdə işləyir və asan istiqaməti tam yazmaq olar.

Sudoku-dan SAT-a. SAT yalnız true/false ilə danışır, ona görə hər (sətir, sütun, qiymət) üçlüyünə bir Boolean dəyişəni verin: *x(r,c,v)* "*r* sətrinin, *c* sütununun xanasında *v* qiyməti var" deməkdir. 4-by-4 Sudoku (2-by-2 bloklar, 1–4 qiymətləri) üçün 4·4·4 = 64 dəyişən lazımdır; klassik 9-by-9 üçün 729. Sonra hər Sudoku qaydası bir qrup clause-a çevrilir. (Clause dəyişənlərin və ya onların inkarlarının OR-udur; bütün formula isə bütün clause-ların AND-ıdır.)

Hər xanada ən azı bir qiymət var — hər xana üçün bir clause:

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

Hər xanada ən çox bir qiymət var — hər qiymət cütü üçün "ikisi eyni anda yox" clause-u:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3)$$ … və bütün altı cüt üçün belə davam edir.

Hər sətirdə hər qiymət var — 1-ci sətir və 3 qiyməti üçün: ən azı bir dəfə,

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

və ən çox bir dəfə: $\neg x(1,1,3) \vee \neg x(1,2,3)$, sonra sətirdəki hər xana cütü üçün eyni qayda.

Sütunlar və bloklar — eyni clause qruplarıdır, yalnız xanaların qrupu dəyişir. Sol-yuxarı blok və 2 qiyməti üçün:

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

üstəlik cüt-cüt "ikisi eyni anda yox" clause-ları.

Çap olunmuş ipucları — ən sadə hissə: hər ipucu tək dəyişənli clause-dur. Sol-yuxarı küncdə çap olunmuş 3 belə clause-a çevrilir:

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

Bunların hamısının AND-ı məhz Sudoku-nun həlli olduğu halda satisfiable-dır — və satisfying assignment *həllin özüdür*: hansı x(r,c,v)-lərin true olduğuna baxıb cədvəli doldurun. 9-by-9 üçün bu, 729 dəyişən və bir neçə min clause edir; müasir SAT solver bunu millisaniyələrdə həll edir. x(1,1,3) ipucu clause-una diqqət edin: o, "bu xana tam olaraq 3-dür" deyir, "bu xanaların hamısı fərqlidir" yox — aşağıdakı protokol qeydində ipucu xanaları üçün əlavə hiyləni məcburi edən eyni asimmetriya budur.

SAT-dan Sudoku-ya. Məqaləyə əks, daha çətin istiqamət lazımdır: *istənilən* SAT formulasını götürüb yalnız formula satisfiable olduqda həlli olan mega-Sudoku qurmaq. Sudoku-nun təbii qaydaları yalnız "bu xanaların hamısı fərqlidir" deyə bilir, buna görə ixtiyari məntiqi məhdudiyyətlər *qurulmalıdır* — gadget-lər də məhz bunun üçündür. Gadget formulasının hər clause-u üçün əvvəlcədən hazırlanmış kiçik xana qrupudur; müəyyən xanalar dəyişən rolunu oynayır (daşıdığı simvol true və ya false-u kodlayır),

qrupun daxili məhdudiyyətləri isə elə qurulur ki, onun yeganə qanuni doldurulmaları həmin clause-u ödəyən qiymətləndirmələrə uyğun olsun. Bu, NP-completeness sübutlarının standart mühəndisliyidir; generalized Sudoku üçün Yato və Seta bunu 2003-cü ildə qurmuşdular.
İki istiqamət birlikdə N-by-N Sudoku ilə SAT-ın fərqli geyimdə eyni problem olduğunu deyir. Bu, həm bu məqaləyə, həm də orijinal paper-ə cədvəllər və simvollar vasitəsilə bütün NP haqqında danışmağa əsas verir.

Witness-i təsəvvür etmək yenə asandır. Alice mega-Sudoku-nun tam və düzgün doldurulmasını bilir. Bob belə bir doldurmanın mövcud olduğuna inanmaq istəyir, amma Alice onu açıqlamaq istəmir. Tam cədvəli göndərsə, Bob inanacaq, amma sirr yox olacaq.

Klassik zero-knowledge versiyasında Alice və Bob qarşılıqlı əlaqədədir. Köhnə tipli mental model örtülü plitələrdən istifadə edir. Alice həll olunmuş cədvəli gizlədir, hər raunddan əvvəl simvolların adını gizlicə dəyişir və Bob-a təsadüfi seçilmiş bir lokal məhdudiyyəti yoxlamağa icazə verir: sətir, sütun, blok və ya gadget. Açılan xanalar bütün-fərqli simvollar göstərirsə, Bob-un əminliyi artır. Sonra hər şey yenidən örtülür və simvollar təzədən adlandırılır. (Bir incəlik var: tapmacanın verilmiş ipucları əlavə hiylə tələb edir, çünki simvolların adını dəyişmək onları da gizlədir. Aşağıdakı qeyd klassik protokolların bunu necə həll etdiyini izah edir; sonrakı hissə üçün bu sadə şəkil kifayətdir.)

Klassik protokollar ipucu xanalarını həqiqətən necə idarə edir

Ad dəyişdirmə hiyləsinin kor nöqtəsi var. Sətir, sütun və blok qaydalarının hamısı "bu xanalar bir-birindən fərqlidir" deyir və *hamısı fərqlidir* xüsusiyyəti simvolların istənilən ad dəyişməsindən sonra qalır. Amma ipucu "bu xanada tam olaraq 5 var" deyir və ad dəyişdirildikdən sonra Bob yalnız $\sigma(5)$ — maskalanmış hansısa simvol — görür, σ ad dəyişməsini isə bilmir. Heç nəyi yoxlaya bilməz. Bu düzəldilməsə, Alice çap olunmuş ipuclarını tamamilə görməzliyə vurub *hansısa* düzgün cədvəlin mövcud olduğunu sübut edə bilərdi; bu isə *bu* tapmaca haqqında heç nə sübut etmir. Klassik ədəbiyyatda iki standart düzəliş var.
Palitra. Gizli cədvələ N xanadan ibarət bir əlavə sətir — palitra — əlavə edin. Alice onu 1…N simvolları ilə sabit və hamıya məlum ardıcıllıqda doldurur, sonra hər şeylə birlikdə adlarını dəyişir; beləliklə o, $\sigma(1)$…$\sigma(N)$ saxlayır. Bob-un təsadüfi çağırışında indi əlavə seçim var. Sətir, sütun, blok və ya gadget açmaqla yanaşı, **palitranı və bir ipucu xanasını** da seçə bilər. Alice hər ikisini açır; palitra həmin raundun ad dəyişməsini üzə çıxarır və Bob ipucu xanasında çap olunmuş ipucunun məhz ad dəyişdirilmiş versiyasının olduğunu yoxlayır. Bu, zero-knowledge olaraq qalır, çünki Bob yalnız hər raund təzədən təsadüfi seçilən və təkbaşına heç bir dəyəri olmayan σ-nı, üstəlik tapmacadan onsuz da bildiyi bir xananın qiymətini öyrənir. Gizli xanalar haqqında heç nə sızmır və simulator təsadüfi σ seçərək görünüşü saxtalaşdıra bilər. Soundness də qalır: hiyləgər Alice hər raundda sabit ehtimalla tutulur və şübhə cüzi olana qədər raundlar təkrarlanır.

> **İpuclarını kompilyasiya edib aradan qaldırmaq.** Daha struktur bir variant xüsusi çağırış əlavə etmək əvəzinə onu ləğv edir. İpucu qiymətini *yoxlamaq* yerinə fərqlilik məhdudiyyətləri ilə məcbur edin: ipucu xanasını öz qiymətini daşıyan palitra xanasından başqa bütün palitra xanaları ilə bağlayın — "$\sigma(1)$-dən fərqli, $\sigma(2)$-dən fərqli, …, $\sigma(5)$-dən başqa hər şeydən fərqli." Xananın qanuni olaraq saxlaya bildiyi yeganə simvol ipucunun özüdür. İndi bütün məhdudiyyətlər yenidən "bu ikisi fərqlidir" tipindədir — ad dəyişməsinə invariantdır və sətir kimi dəqiq yoxlanıla bilir. Bu, klassik graph-coloring protokolunda əvvəlcədən rənglənmiş vertices üçün istifadə olunan eyni manevrdir və yuxarıdakı *gadget* sözünün ruhunu göstərir: MegaSudoku-as-SAT şəklində ipucları bütün digər məhdudiyyətlər kimi inequality gadget-lərinə kompilyasiya olunur.
> **Fiziki protokol.** Sudoku üçün real kart protokolu (Gradwohl, Naor, Pinkas və Rothblum, 2007) ümumiyyətlə ad dəyişdirmədən istifadə etmir və ipuclarını gizlətmə başlamazdan əvvəl həll edir. Hər xana üçün Alice eyni qiymətli üç eyni kart qoyur — gizli xanalar üçün üzüaşağı, amma **ipucu xanaları üçün üzüaçıq** — beləliklə Bob kartlar çevrilməzdən əvvəl ipuclarına əməl olunduğunu öz gözləri ilə görür. Sonra hər xananın bir kartı öz sətrinin paketinə, biri sütununun, biri blokunun paketinə gedir; hər paket qarışdırılıb açılır və Bob onun bütün N simvolu saxladığını yoxlayır. Qarışdırma mövqe məlumatını məhv edir (zero-knowledge hissəsi budur), amma ipucları artıq kartlar paylananda sabitlənmişdi.
> Hansı üsul seçilirsə seçilsin, dərs bu məqalənin dəfələrlə qayıtdığı eynidir: zero-knowledge protokolu gizlətmədən sonra *hansı* faktların sağ qaldığının diqqətli hesabıdır. Ad dəyişdirmə "hamısı fərqlidir" faktını qoruyur, "5-ə bərabərdir" faktını silir — buna görə "5-ə bərabərdir" başqa vasitə ilə geri gətirilməlidir.

Bu, paper-dəki protokol deyil. Bu, klassik zero-knowledge üçün mental modeldir:

- Alice və Bob qarşılıqlı mesajlaşırlar.
- Bob təsadüfi yoxlamalar seçir.
- Alice bütün həlli yox, yalnız lokal uyğunluğu açıqlayır.
- Məxfiliyin sübutu Bob-un gördüyü şeyin Alice-in gizli həllini bilmədən də yaradıla biləcəyini göstərməklə işləyir.

Deməli, klassik zero-knowledge müsbət fakta söykənir:

> Simulator həqiqətən mövcuddur.

İndi rahat hissələri götürün. Alice bir sübut sətri göndərib gedir. Etibarlı setup yoxdur, əvvəlcədən hazırlanmış ortaq random string yoxdur və Bob yanlış tapmacanı heç vaxt qəbul etməməlidir. Klassik zero-knowledge-un sağ qala bilmədiyi şərait budur.

Hiylədən əvvəl bir personaj da lazımdır. Bir **qaydalar kitabı** seçin: məntiqçilərin mənasında formal proof system — sabit aksiomlar dəsti və yazılı riyazi sübutları mexaniki yoxlama qaydaları. Riyaziyyatın standart aksiomları olan ZFC kanonik nümunədir. Bundan sonra hər şey əvvəlcədən seçilmiş bir qaydalar kitabına nisbətən ifadə edilir və seçim çevikdir: konstruksiya

sabitlədiyiniz istənilən qaydalar kitabı, o cümlədən ZFC üçün işləyir.

(Paper-in öz terminologiyasından bir qeyd: burada “proof system” həmişə bu qaydalar kitabını — riyazi sübutları yoxlayan formal sistemi — bildirir, heç vaxt Alice-in göndərdiyi mesajları yox. Alice və Bob-un mexanizmləri “prover və verifier” adlanır.)

Gödel-üslublu versiya mega-Sudoku hekayəsini saxlayır, amma sübutu dəyişir.

Ekranda göstərilən eyni ölçüdə ikinci məhdudiyyət sistemi seçin və ona **D** deyin. Hekayədə S və D eyni formatda iki MegaSudoku(n) tapmacasıdır. Arxa planda D başqa ölçülü çətin məntiqi formuladan başlaya bilər; lazım gələrsə, eyni cədvələ sığması üçün zərərsiz dummy məhdudiyyətlərlə doldurula bilər. D əslində **unsatisfiable** olan məntiqi formuladan qurulur: bütün məhdudiyyətləri eyni anda doğru edən heç bir qiymət təyinatı yoxdur, necə ki, pozulmuş tapmacanın qanuni tamamlanmış cədvəli yoxdur. Oyuncaq nümunə eyni anda həm “X true-dur”, həm də “X false-dur” tələb edən formula ola bilər. Deməli D-nin düzgün doldurulması yoxdur.

Amma D *asanlıqla ifşa edilən* pozulmuş tapmaca olmamalıdır. Yuxarıdakı oyuncaq nümunə buna yaramır: istənilən qaydalar kitabı “X və not-X” ifadəsini bir sətirdə təkzib edir. D elə yanlış olmalıdır ki, seçilmiş qaydalar kitabı bunu qısa arqumentlə təsdiqləyə bilməsin. Qaydalar kitabı D-ni qısa sübutla təkzib edə bilsəydi, aşağıdakı hekayə dağılardı: Alice-in sirri olmadan sübut yarada bilən alternativ yol formal şəkildə istisna edilə bilərdi və bununla məxfilik zəmanəti də itərdi. Buna görə D sabit qaydalar kitabının səmərəli şəkildə təkzib edə bilmədiyi ailədən seçilir: həmin qaydalar kitabının daxilində D-nin həlli olmadığını göstərən qısa sübut yoxdur.

Alice-in bir-mesajlı sübutu sonra “ya bu, ya o” ifadəsi haqqındadır:

> ya həqiqi mega-Sudoku S-in həlli var, ya da saxta D-nin həlli var.

Məntiqi əlaqə budur. D S-i hansısa sehrli yolla doğru etmək üçün yaradılmır. Sübut “D-nin həlli yoxdur, deməli S-in həlli var” arqumenti deyil. O, **S və ya D** disjunksiyasını sübut edir. Mükəmməl soundness deyir ki, yanlış disjunksiyanın etibarlı sübutu ola bilməz. D reallıqda yanlış olduğuna — həlli olmadığına — görə disjunksiyanın doğru olmasının yeganə yolu S-in doğru olmasıdır. Deməli sübut qəbul edilirsə, S-in həlli olmalıdır. Saxta D yanlış S-i doğru edə bilməz.

Amma zero-knowledge-üslublu hissə üçün D-nin *həlli olsaydı* nə baş verəcəyini soruşun. Həmin saxta həll alternativ witness rolunu oynayardı. Alice-in həqiqi mega-Sudoku həllini bilmədən sübut yaratmağa imkan verərdi — başqa sözlə simulator olardı. Reallıqda D-nin həlli yoxdur, deməli bu simulator yolu bağlıdır. Əsas məqam budur ki, qaydalar kitabı yolun bağlı olduğunu səmərəli şəkildə sübut edə bilmir.

Beləliklə D-nin iki işi var. **Soundness** üçün D yanlışdır; deməli “S və ya D” ifadəsinin etibarlı sübutu S-i məcbur edir. **Effective zero-knowledge** üçün D-ni təkzib etmək çətindir; deməli qaydalar kitabı simulyasiyanı mümkün edəcək saxta yolun olmadığını tez şəkildə istisna edə bilmir.

Beləliklə təhlükəsizlik testi artıq bu deyil:

> Simulator-un həqiqətən mövcud olduğunu sübut edə bilərikmi?

Bu olur:

> Qaydalar kitabınız simulator-un mümkünsüz olduğunu səmərəli şəkildə sübut edə bilirmi?

Cavab xeyrdirsə, təəccüblü dərəcədə güclü nəticə gəlir: (a) test işlətməklə müşahidə edilə bilən və (b) simulator-un mövcudluğundan həmin qaydalar kitabı daxilində sübut edilə bilən hər təhlükəsizlik zəmanəti faktiki olaraq təmin olunur. Onlardan hər hansı birinə uğurlu hücumun özü çatışmayan qısa təkzibə bərabər olardı — amma həmin qısa təkzib mövcud deyil. Effectively zero-knowledge-dakı “effective” məhz budur.

Sinif otağı üçün kontrast belədir:

Klassik zero-knowledge: sübutlar təhlükəsizdir, çünki simulator mövcuddur.

Gödel-üslublu effective zero-knowledge: müşahidə edilə bilən təhlükəsizlik testləri üçün sübutlar təhlükəsiz kimi davranır, çünki qaydalar kitabı simulator-un mümkünsüz olduğunu səmərəli şəkildə sübut edə bilmir.

İkinci iddia daha zəifdir. Məhz buna görə paper klassik versiyanı pozan üç xüsusiyyəti saxlaya bilir: bir mesaj, setup yoxdur və mükəmməl soundness.

Yeni test: simulator-un olmadığını sübut edə bilmirsiniz

Ilango-nun yumşaldılması sualı dəyişir.

Klassik zero-knowledge soruşur:

> Simulator mövcuddurmu?

Effectively zero-knowledge daha zəif bir sual verir:

> Seçdiyiniz qaydalar kitabı simulator-un mövcud olmadığını səmərəli şəkildə sübut edə bilirmi?

Bu texniki yayınma kimi səslənə bilər, amma əsas fikir budur. Konstruksiya qəribə vəziyyətdə yaşayır: simulator əslində mövcud deyil — paper bunu açıq deyir — amma sabitlədiyiniz qaydalar kitabı onun mövcud olmadığını səmərəli şəkildə sübut edə bilmir. Əgər sizi narahat

edən hər pis nəticə belə bir təkzib tələb edərsə, sistem həmin nəticələr baxımından yenə zero-knowledge kimi davranır.

Gödel burada daxil olur. Dekorasiya kimi yox və "Gödel kriptoqrafiyanı təhlükəsiz edir" mənasında da yox. Əlaqə proof-theoretic-dir. Qaydalar kitabı dəqiq mənada mümkün olan ən yaxşısıdırsa **optimal** adlanır: uyğun tipli formulanı hər hansı qaydalar kitabı qısa sübutla təkzib edə bilirsə, optimal qaydalar kitabı da bunu ən çox polynomial qədər uzun sübutla edə bilir. Krajíček və Pudlák 1989-cu ildə **optimal proof system mövcud deyil** fərziyyəsini irəli sürdülər: hansı qaydalar kitabını sabitləsəniz, başqa bir qaydalar kitabı bəzi doğru ifadələr ailəsini xeyli daha qısa şəkildə sübut edir. Bu, proof complexity-nin əsas açıq fərziyyələrindən biridir və Gödel-in incompleteness teoreminin sonlu, complexity-theoretic qohumudur: bəzi doğru ifadələrin sabitlədiyiniz qaydalar kitabında qısa sübutu yoxdur — prinsipcə sübut edilə bilmədiklərinə görə yox, hər sabit qaydalar kitabının bəzi qısa doğruları qısa sübutsuz buraxdığına görə.

Paper bu fərziyyəni qəbul edir (kriptoqrafiyada fərziyyələrdən istifadə ediləndə standart olan bir qədər güclü "infinitely often" formasında). Krajíček və Pudlák teoreminə görə nəticə konkretdir: hər qaydalar kitabı üçün həqiqətən unsatisfiable olan, amma həmin qaydalar kitabının qısa sübutlarla təkzib edə bilmədiyi formulalar ardıcıllığı var — və kritik olaraq, səmərəli alqoritm onları *yarada bilir*. Sonuncu xüsusiyyət, uniformity, bütün fikri sırf mövcudluq iddiasından Alice-in işlədə biləcəyi real alqoritmə çevirir: onun D saxtaları havadan yox, istehsal xəttindən gəlir.

Kriptoqrafik hərəkət həmin sübut gücü çatışmazlığını işə salmaqdır.

Konstruksiya nə edir

Paper-in konstruksiyasını skeletinə qədər sadələşdirsək belədir.

Bir qaydalar kitabı seçin — məsələn ZFC. Proof-complexity fərziyyəsi altında səmərəli şəkildə yaradıla bilən, reallıqda unsatisfiable olan, amma qaydalar kitabının unsatisfiable olduqlarına dair qısa sübut verə bilmədiyi formulalar ardıcıllığı mövcuddur.

İndi bu formada bir-mesajlı sübut qurun:

> ya həqiqi ifadə satisfiable-dır, ya da bu xüsusi çətin formula satisfiable-dır.

Xüsusi çətin formula satisfiable deyil. Buna görə əsas sübut mexanizmi mükəmməl soundness-ə malikdirsə, mesajın qəbul edilməsi yenə həqiqi ifadənin doğru olması deməkdir. Mükəmməl soundness buradan gəlir.

Amma zero-knowledge-a bənzər təhlükəsizlik üçün xüsusi çətin formulanın *satisfiable olduğunu* təsəvvür edin. Onda onun witness-i həqiqi witness-i bilmədən sübutları simulyasiya etmək üçün istifadə oluna bilərdi. Formula reallıqda satisfiable deyil — amma qaydalar kitabı bunu səmərəli şəkildə sübut edə bilmir. Buna görə simulator-un mümkünsüz olduğunu da

səmərəli şəkildə sübut edə bilmir.

Menteşə budur. Sistem klassik simulator yaradaraq sirri gizlətmir. Müşahidə edilə bilən təhlükəsizlik testlərinin böyük sinfi üçün sirri qaydalar kitabının simulator-un yoxluğunu təsdiqləyə bilməməsinin arxasında gizlədir.

Paper nə iddia edir

Əsas teorem bir neçə qatdadır. Nüvə nəticə belədir:

Standart kriptoqrafik fərziyyə — bir neçə möhkəm fərziyyə paketindən alınan, yaxşı öyrənilmiş obyektlər olan **non-interactive witness indistinguishable proofs**-un mövcudluğu — və **heç bir (infinitely often) optimal proof system mövcud deyil** proof-complexity fərziyyəsi altında paper hər seçilmiş qaydalar kitabı üçün NP/SAT üzərində **mükəmməl soundness**-ə malik, setup tələb etməyən və həmin qaydalar kitabına nisbətən effectively zero-knowledge olan bir-mesajlı prover və verifier qurur. (NP/SAT tapmaca tipli problemlərin standart "ən çətin ortaq məxrəci"dir; mega-Sudoku onun geyimlərindən biridir.)

Falsifiable təhlükəsizlik xüsusiyyətlərini qorumaq barədə daha geniş iddia üçün paper əlavə standart fərziyyə, derandomization inancı **P** = **BPP** qəbul edir (təxminən: təsadüfilik alqoritmlərə mahiyyətcə əlavə güc vermir).

Teorem dilindən çıxarıb desək:

- Sübut bir mesajdır.
- Etibarlı setup yoxdur.
- Yanlış ifadələr sübut edilə bilməz.
- Prover klassik zero-knowledge deyil — onun simulator-u yoxdur.
- Amma klassik zero-knowledge-un hər falsifiable, game-based təhlükəsizlik nəticəsi bu şəraitdə əldə edilə bilər.

"Falsifiable" vacib sözdür. Təhlükəsizlik uğursuzluğunun adversary-ni bir oyun içində işlədərək test edilə bilməsi deməkdir. Bir çox kriptoqrafik təhlükəsizlik tərifi bu formadadır: adversary iki şifrələməni ayırd edə, funksiyanı invert edə, witness-i bərpa edə və ya müəyyən edilmiş eksperimenti uda bilirmi? Teorem hər falsifiable xüsusiyyət üçün ayrıca, bir-bir prover verir. *Bütün* falsifiable xüsusiyyətlərə eyni anda malik tək prover yəqin ki, mümkün deyil — köhnə reusability hücumu ("Bob sübutu başqalarına göstərə bilər") özü falsifiable xüsusiyyətdir və burada həqiqətən uğursuz olur. Paper-in təklifi odur ki, tək prover bütün *təbii* falsifiable xüsusiyyətləri — kriptoqrafik praktikada həqiqətən görünənləri — əhatə edə bilər; amma bu hissə "təbii" anlayışının qeyri-formal mənasına və açıq bir conjecture-a söykənən şərti teoremdir. Zəmanət hər fəlsəfi və ya simulation-based məxfilik mənasına yox, müşahidə edilə bilən uğursuzluqlara yönəlib.

Bir konkret corollary-ni adlandırmağa dəyər: konstruksiya uniform prover-li ilk non-interactive *witness hiding* proofs verir — "tapmacanın sübutu onun həllini tapmağa kömək

etmir,” qarşılıqlı əlaqəsiz və setup-sız — sadə səslənən, amma onilliklər boyu qurulmağa müqavimət göstərmiş obyekt.

Bu nə demir

Məqaləni dürüst saxlayan hissə budur.

Köhnə mümkünsüzlük teoremlərinin yanlış olduğunu **demir**. Konstruksiya tərifi dəyişdirərək onlardan yayınır.

Qarşılıqlı əlaqəsiz, setup-sız və mükəmməl soundness-li adi klassik zero-knowledge **vermir**. Paper açıq şəkildə deyir ki, qurulan prover-in simulator-u yoxdur.

Sübutun yenidən istifadə edilə bilmədiyini **demir**. Bir-mesajlı sübut hələ də başqasına göstərilə bilər; paper deniability tipli xüsusiyyətləri qorumur. (Etibarlı setup-lı non-interactive zero-knowledge-da eyni məhdudiyyət var.)

Bunun istifadəyə hazır praktik protokol olduğunu **demir**. Bu complexity theory və kriptoqrafik fundamentlərdir. Nəticə proof complexity və kriptoqrafiyadan böyük fərziyyələrə söykənir və konstruksiya prinsipcə nəyin mümkün olduğu haqqındadır.

“Gödel”i sehrli təhlükəsizlik primitivinə **çevirmir**. Gödel əlaqəsi proof systems, optimal proof systems və incompleteness-in sonlu analoqları üzərindən gəlir. Faydalı intuisiya “incompleteness parolunuzu qoruyur” deyil. Budur: qaydalar kitabı simulator-un mümkünsüz olduğunu səmərəli şəkildə sübut edə bilmirsə, həmin sübutu tələb edən hücumlar təhlükəsizlik tərifləri səviyyəsində bloklana bilər.

Buna baxmayaraq niyə maraqlıdır

Kriptoqrafiya tez-tez çətinliyi təhlükəsizliyə çevirir. Faktorlaşdırma çətindir, buna görə RSA tipli fərziyyələr faydalı olur. Lattice problemləri çətindir, buna görə lattice cryptography faydalı olur. Buradakı çətinlik daha qəribədir: “sirri hesablamaq çətindir” yox, “müəyyən sübut obyektinin mövcud ola bilməyəcəyini sübut etmək çətindir.”

Paper-in qeyri-adi hiss etdirən tərəfi budur. Aksiomlara və qaydalar kitabına demək olar kriptoqrafik resurs kimi yanaşır. Adi mümkünsüzlük soundness ilə simulation arasında gərginlik olduğunu deyir. Ilango-nun hərəkəti bu gərginliyi proof-theoretic pərdənin arxasına qoymaqdır: simulator yoxdur, amma formal sistem onun yoxluğunu səmərəli şəkildə üzə çıxara bilmir.

Oxucu üçün sürpriz bu sistemin bugünkü zero-knowledge sistemlərini əvəz etməsi deyil. Yəqin ki, heç olmasa birbaşa əvəz etməyəcək. Sürpriz budur ki, riyazi məntiqdən gələn məhdudiyyət konstruktiv şəkildə işlədilə bilir: sadəcə divar kimi yox, örtük kimi.

Dəlil nə qədər güclüdür?

Bu teorem paper-idir, ona görə “dəlil” biologiya və ya astronomiya məqaləsindən fərqli məna daşıyır. Sual eksperimentin təkrarlanıb-təkrarlanmaması deyil. Sual tərifl ərin, fərziyyələrin və sübut zəncirinin iddianı dəstəkləyib-dəstəkləməməsidir.

Sübut formaldır və paper fərziyyələrini açıq göstərir. Fərziyyələr təsadüfi deyil. Non-interactive witness indistinguishable proofs kriptoqrafiyada standart obyektlərdir və bir neçə formalaşmış fərziyyə paketindən alınır. No-optimal-proof-system conjecture proof complexity-də mərkəzi fərziyyədir. P = BPP isə yalnız daha geniş falsifiable-property teoremi üçün işlədilən standart derandomization inancıdır.

Paper həmçinin fərziyyələrin təsadüfi dayaq yox, düzgün qiymət olduğunu əsaslandırır: əks istiqaməti sübut edərək onların mahiyyətcə zəruri olduğunu göstərir — belə konstruksiyalar ümumiyyətlə mövcuddursa, non-interactive witness indistinguishable proofs mövcud olmalıdır və (standart one-way functions qəbul edilərsə) optimal proof system mövcud ola bilməz. Fərziyyələr həm də “win-win” xarakterlidir: onlardan hər hansının təkzibi proof complexity, kriptoqrafiya və ya complexity theory-də özü böyük kəşf olardı.

Amma nəticə şərti olduğu üçün ona inam da şərtidir. Fərziyyələr yanlış çıxsa, teoremin interpretasiyası dəyişir. Fərziyyələr doğru olsa belə, zəmanət tam klassik zero-knowledge deyil; paper-in yumşaldılmış, proof-theoretic versiyasıdır.

Ona görə uyğun inam belədir: paper-in məntiqli şərti mümkünlük nəticəsi yaratdığına yüksək; fərziyyələrin yaşadığımız real kriptoqrafik dünyanı təsvir etdiyinə orta; dərhal praktik nəticəyə isə aşağı.

Niyə vacibdir

Paper bağlı olduğu düşünülən bir yol açır.

Klassik nəzəriyyə deyir: tam zero-knowledge setup-sız bir mesaj ola bilməz və mükəmməl soundness-ə malik ola bilməz. Ilango-nun paper-i deyir: əgər zero-knowledge-un təhlükəsizlik oyunlarında test edilə bilən nəticələrini tələb ediriksə və təhlükəsizlik tərifinin qaydalar kitabının nəyi səmərəli şəkildə təkzib edə və ya edə bilməməsindən asılı olmasına icazə veririksə, faydalı davranışın böyük hissəsini geri qaytarmaq mümkündür — bir mesaj, setup yoxdur və mükəmməl soundness ilə.

Bu, kiçik tərif dəyişikliyi deyil. Kriptoqrafik zəmanətlər barədə fərqli düşünmə üsuludur. Yalnız nəyin mövcud olduğunu soruşmaq əvəzinə qaydalar kitabınızın nəyi istisna edə bildiyini soruşun. Sübut edilə bilməməyi fəlsəfi narahatlıq kimi görmək əvəzinə struktur kimi istifadə edin.

Praktik dünya sabah dəyişməyə bilər. Amma konseptual xəritə dəyişir. İndi formal mənada “heç kim sirrin sızdığını səmərəli şəkildə sübut edə bilmir” ifadəsi, “sirr sızmadı” ifadəsindən

istədiyimiz game-based müdafiələrin çoxunu geri qaytaracaq qədər güclü ola bilər.

Başlıqda Gödel-in olmasının səbəbi budur.

Qısa xülasə

Zero-knowledge proofs prover-ə witness-i açıqlamadan verifier-i ifadənin doğru olduğuna inandırmağa imkan verir. Klassik mümkünsüzlük nəticələri deyir ki, zero-knowledge setup olmadan bir mesaja sıxışdırıla bilməz və mükəmməl soundness-ə malik ola bilməz. Rahul Ilango-nun paper-i bu mümkünsüzlükləri təkzib etmir. Daha zəif anlayış — effectively zero-knowledge — müəyyən edir: simulator-un həqiqətən mövcud olmasını tələb etmək əvəzinə seçilmiş proof system-in — ZFC kimi formal qaydalar kitabının — simulator-un mövcud olmadığını səmərəli şəkildə sübut edə bilməməsini tələb edir. Kriptoqrafiyadan (non-interactive witness indistinguishable proofs) və proof complexity-dən (optimal proof system mövcud deyil) böyük fərziyyələr altında paper NP/SAT üçün setup-sız, mükəmməl soundness-li bir-mesajlı prover-lər qurur və zero-knowledge-un falsifiable, game-based nəticələrini xüsusiyyət-hissə ilə əldə edir. Bütün "təbii" belə xüsusiyyətləri əhatə edən tək prover əlavə, qismən conjectural genişlənmədir — literally hər falsifiable xüsusiyyəti əhatə etmək isə çox güman mümkün deyil, çünki sübutlar yenidən istifadə edilə bilir. Nəticə nəzəri və şərtidir, istifadədə olan primitiv deyil, amma proof-theoretic unprovability-ni kriptoqrafik resurs kimi işlətməyin yeni yolunu göstərir.

No-BS yoxlaması

Paper-in göstərdiyi: Açıqlanmış fərziyyələr altında NP/SAT üçün bir-mesajlı, setup-sız, mükəmməl soundness-li prover-lər qurmaq olar; onlar seçilmiş istənilən proof system-ə nisbətən effectively zero-knowledge-dur və klassik zero-knowledge-un hər falsifiable game-based nəticəsini ayrıca əldə edə bilir.

Mümkün, amma şərtsiz sübut olunmayan: Lazım olan proof-complexity və kriptoqrafik fərziyyələrin doğru olması. Bunlar ciddi və yaxşı öyrənilmiş fərziyyələrdir — paper onların mahiyyətcə həm zəruri, həm də kifayət olduğunu göstərir — amma yenə fərziyyədir.

Göstərmədiyi: Qarşılıqlı əlaqəsiz, setup-sız və mükəmməl soundness-li klassik zero-knowledge; istifadəyə hazır praktik sistem; sübutların deniability-si və ya non-reusability-si; yaxud Gödel-in incompleteness teoreminin öz-özlüyündə kriptoqrafiyanı təhlükəsiz etməsi.

Əsas məhdudiyyətlər: Zəmanət zero-knowledge-un yumşaldılmış formasıdır; ən geniş versiya bir neçə fərziyyədən asılıdır; tək universal prover barədə iddialar qismən conjectural olaraq qalır; nəticə əsasən fundamentaldır.

Ümumi oxucu nə qədər əmin ola bilər? Tərifər qəbul edilirsə, bunun mühüm şərti nəzəri nəticə olduğuna yüksək. Fərziyyələrin reallığı tutduğuna orta. Dərhal praktik tətbiqə aşağı.

Təhlükəsiz nəticə budur: paper zero-knowledge mümkünsüzlüklərini pozmur; onların çoxlu təhlükəsizlik oyunları üçün vacib olan hissələrinin ətrafından keçmək üçün yeni proof-theoretic yol tapır.

Mənbələr

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