The Clean Paper

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

Bir kriptografik kanıt, eksik simülatörün yokluğunu kanıtlamayı zorlaştırarak sırrını gizleyebilir

Sıfır bilgi kanıtları bir ifadenin tanığı açıklanmadan kanıtlanmasını sağlar. Klasik teori bunun tam anlamıyla tek mesaj, güvenilir kurulum olmadan ve kusursuz sağlamlıkla birlikte elde edilemeyeceğini söyler. Rahul Ilango'nun makalesi bu imkânsızlığı ortadan kaldırmıyor. Hedefi değiştiriyor: bir simülatörün gerçekten var olmasını istemek yerine, seçilmiş hiçbir kanıt sisteminin simülatörün var olmadığını verimli biçimde kanıtlayamamasını istiyor. Kanıt karmaşıklığı ve kriptografideki büyük varsayımlar altında bu, sıfır bilginin yanlışlanabilir, oyun-temelli sonuçlarını özellik özellik geri kazanmak için yeterli oluyor. Nokta internete takılıp kullanılacak hazır bir ilkel değil. Matematiksel kanıtlanamazlığı kriptografik örtüye dönüştürmenin kanıt-kuramsal bir yolu.

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

Hile, sırrın gizli olduğunu kanıtlamak değil

Sıfır bilginin en basit sürümüyle başlayalım.

Alice, Bob'u bir Sudoku bulmacasının çözümü olduğuna ikna etmek istiyor. Çözümü gönderirse Bob ikna olur, ama bulmacanın sırrı ortadan kalkar. Alice'in istediği daha tuhaf bir şey: çözümü açıklamadan, bir çözümün var olduğuna dair kanıt.

Bir sıfır bilgi kanıtının vaadi budur. Kanıtlayıcı (Alice), doğrulayıcıyı (Bob) bir ifadenin doğru olduğuna ikna ederken, ifadenin doğruluğu dışında hiçbir şey açığa çıkarmaz.

Sorun, bu vaadin bir bedeli olması. Sıradan bir matematiksel kanıtın iki rahat özelliği vardır. **Tek mesajdır**: yazarsınız, teslim edersiniz ve gidersiniz. Ve **kusursuz sağlamdır**: yanlış bir ifadenin geçerli hiçbir kanıtı yoktur. Klasik imkânsızlık sonuçları sıfır bilginin bu iki özellikten de vazgeçmesi gerektiğini söyler — yalnızca ikisini aynı anda değil; her biri tek başına da yasaktır.

Birincisi, sıfır bilgi kanıtı konuşma gerektirir. Alice önceden ayarlanmış güvenilir bir kurulum olmadan tek bir mesaj gönderirse, karşılığında sağlamlıktan ne kadar ödün vermeye hazır olursanız olun sıfır bilgi garantisi çöker.

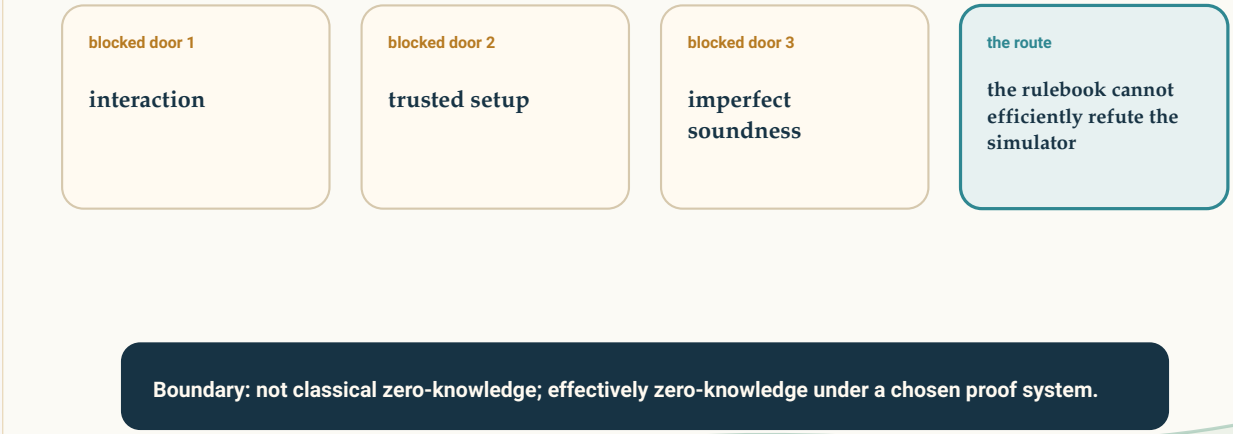
İkincisi, sıfır bilgi kanıtı küçük bir hata toleransı gerektirir. Kusursuz sağlamlık istemek etkileşimi de sessizce yok eder: hangi rastgele seçimleri yaparsa yapsın asla kandırılamayan bir doğrulayıcı, bu seçimleri baştan sabitleyebilir; doğrulayıcı öngörülebilir hâle geldiğinde Alice her şeye tek mesajda yanıt verebilir — bu da zaten bozulduğu bilinen durumdur.

Rahul Ilango'nun makalesi bu çift duvarın etrafından dolaşmanın bir yolunu anlatıyor. Duvar yokmuş gibi davranarak değil, imkânsız ortamda klasik sıfır bilgi ürettiğini iddia ederek de değil. Hamle daha ince: "hiçbir şey açığa çıkarmamak" ifadesinin anlamını zayıflatmak, ama bunu kriptografların gerçekten test edebildiği güvenlik özelliklerini koruyacak biçimde yapmak.

Sonuca **etkin sıfır bilgi** (*effectively zero-knowledge*) deniyor.

A proof without leaking the witness

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

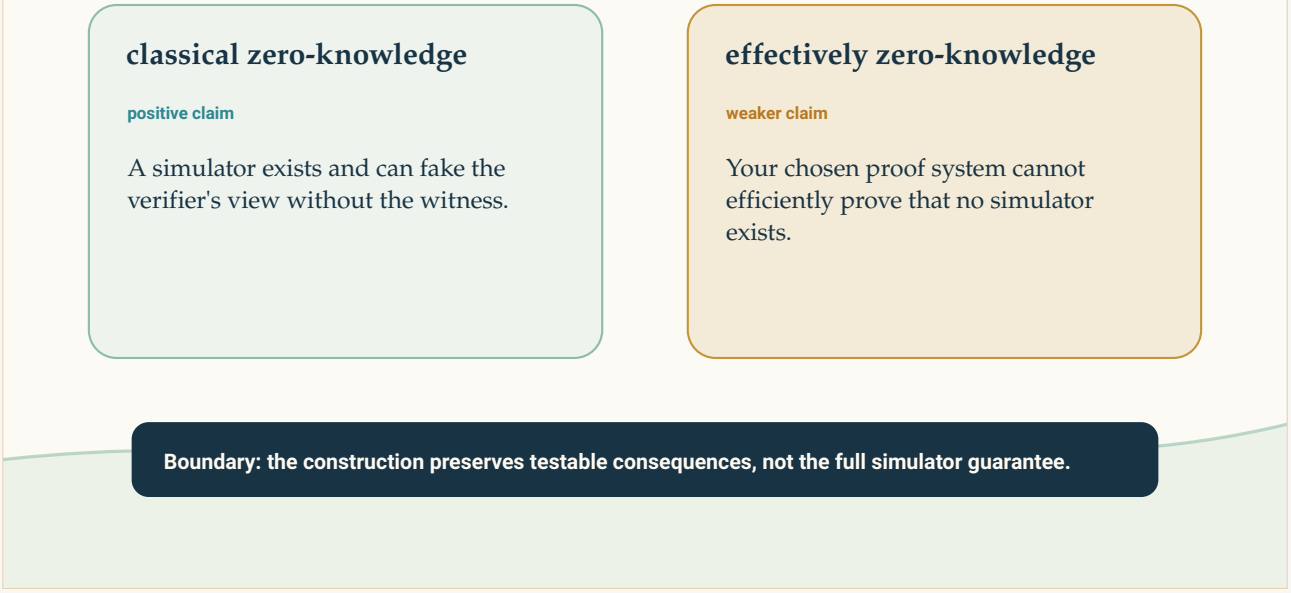


Sıfır bilginin önünde üç kapı kapalı: etkileşim, güvenilir kurulum ve kusurlu sağlamlık. Ilango'nun yapısı farklı bir kapıdan geçiyor: kural kitabı, simülatörün varlığını verimli biçimde çürütemiyor.

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.



Klasik sıfır bilgi bir simülatörün gerçekten var olup olmadığını sorar; "etkin sıfır bilgi" ise yalnızca seçtiğiniz kural kitabının onun var olamayacağını verimli biçimde kanıtlayıp kanıtlayamadığını sorar. Yapının tek mesajı,

kurulumsuzluğu ve kusursuz sağlamlığı korumasını sağlayan daha zayıf soru budur.

Eski test: bir simülatör vardır

Sıfır bilgiyi biçimselleştirmenin klasik yolu, **simülatör** denen kurgusal bir yardımcı kullanır.

Fikir şu: Alice'in sırrını **bilmeyen** Jane'i düşünün. Jane, Alice'in sırrını bilmeden tamamen kendi başına Bob'un Alice'ten alacağı kanıtlara tıpatıp benzeyen kanıtlar üretebiliyorsa, Alice'in kanıtları Bob'a yeni bir şey öğretmemiş demektir. Jane aynı deneyimi Alice'in sırrı olmadan zaten taklit edebiliyordu.

Bu yüzden klasik sıfır bilgi gerçek bir simülatör ister. Sırrı — jargonla *tanığı* — bilmeden sahte görünümlü kanıtlar üretebilen verimli bir algoritma bulunmalıdır; Sudoku'da tanık, basitçe tamamlanmış ızgaradır.

Bu tanım güçlüdür, ama eski imkânsızlığın ısırdığı yer de tam burasıdır. Sezgi şöyle: gerçekten etkileşimsiz bir kanıt yalnızca bir karakter dizisidir. Bob o diziyi eline aldığında başkasına gösterebilir; artık ifadeyi başkalarına kanıtlama yeteneği kazanmıştır ve bu bile "hiçbir şey"den fazlası gibi görünür. Klasik teoremler bu sezgiyi yukarıdaki imkânsızlıklara keskinleştirir.

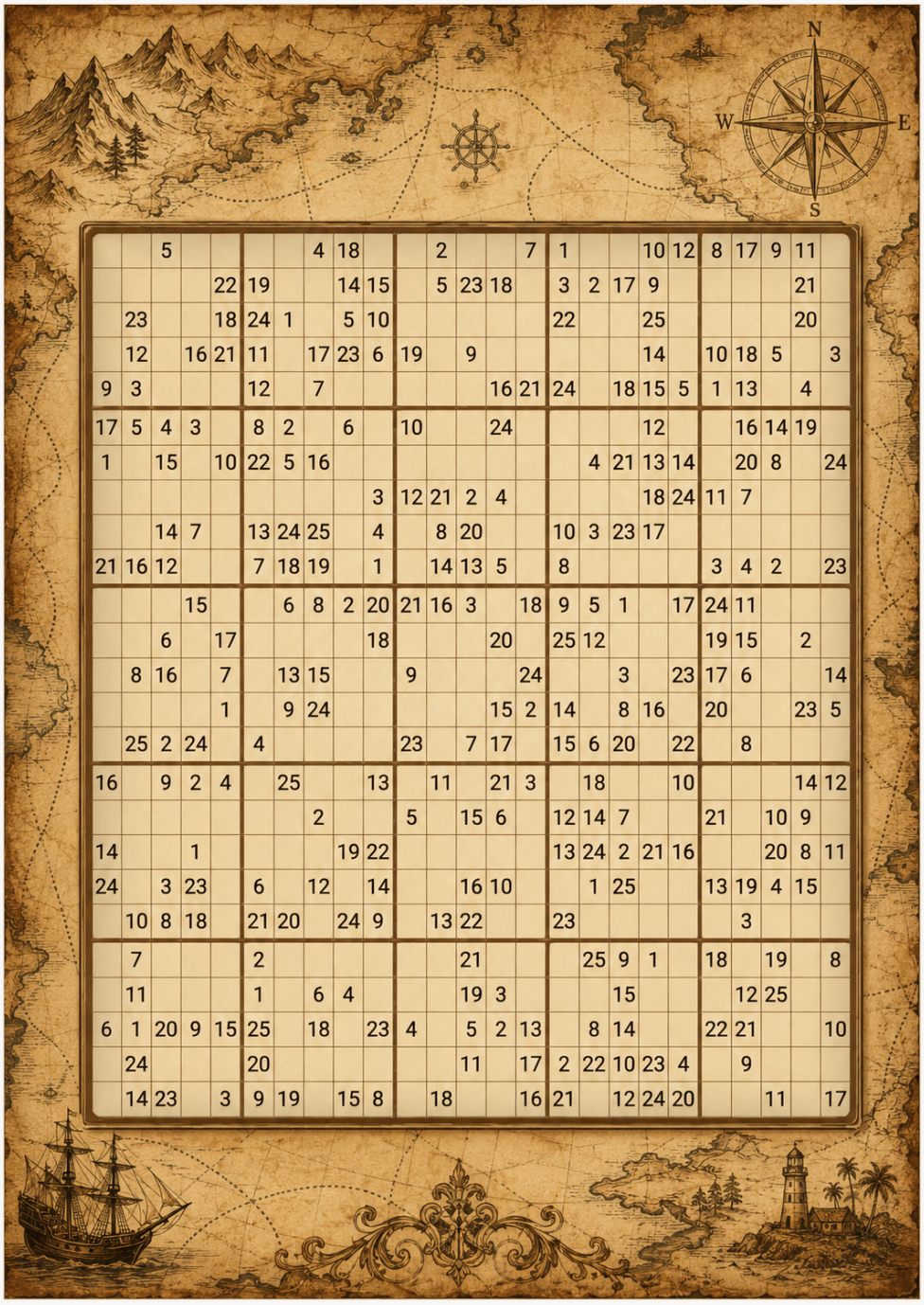
> **Bu makalenin ısrarla koruduğu üç özellik**
>
> Makalenin başlığı üç kısıtı adlandırır:
> **Etkileşim yok:** Alice tek bir kanıt dizisi gönderir. İleri geri giden bir protokol yoktur.
> **Kurulum yok:** Alice ve Bob güvenilir bir ortak referans dizisine ya da önceden hazırlanmış başka bir kamusal rastgeleliğe dayanmaz. "Etkileşimsiz sıfır bilgi" diye adlandırılan birçok sistem yine de kurulum kullanır; bu makale gerçekten sıfır kurulum demektir.
> **Kusursuz sağlamlık:** yanlış bir ifadenin geçerli hiçbir kanıtı yoktur. "Neredeyse hiçbir zaman kabul edilmez" değil; geçerli kanıt hiç yoktur.
> Bu üç özellik sıradan yazılı matematiğin tam olarak sahip olduğu özelliklerdir — ve yukarıda açıklandığı gibi klasik sıfır bilgi üçünü birden koruyamaz.

Farkı hissettiren bir MegaSudoku sürümü

Farkı sezmek için kasıtlı olarak basitleştirilmiş bir yol kullanalım.

Analojinin ciddi kısmında sıradan 9'a 9 Sudoku kullanmayın. Fazla küçük ve fazla sonludur: bilgisayar onu doğrudan çözebilir ya da çözümü olmadığını kanıtlayabilir. Bunun yerine **MegaSudoku(n)** bulmacalarından oluşan bir aile düşünün. Alışılmış kuralı ölçekleyin: blok boyutu n olsun, $N = n^2$ alın ve n'ye n bloklara ayrılmış, N sembollü N'ye N bir ızgara kurun. Sıradan Sudoku yalnızca küçücük $n = 3$, $N = 9$ durumudur: 9'a 9 ızgara, 3'e 3 bloklar ve dokuz sembol. Kanıt karmaşıklığı hikâyesi ancak

n büyüyebildiğinde ve ızgara, Sudoku kılığına girmiş bir SAT formülü gibi davranmasını sağlayan ek araçlar taşıyabildiğinde başlar. SAT formülü yalnızca evet/hayır kısıtlarının listesidir: değişkenlere doğru/yanlış değerleri atayıp bütün kısıtları aynı anda karşılayabilir misiniz?



25x25 bir Sudoku: kuralları tamamlanmış ızgarayı göstermeden kontrol edilebilir — gizli çözümü, yani tanığı doğrulayan bir kanıt için görsel bir benzetme.

Sudoku ve SAT: aynı bulmacanın iki kostümü

Bir Sudoku'nun "SAT formülü gibi davranabileceği" sözü metafor değildir. Çeviri iki yönde de yapılabilir ve kolay yönü bütünüyle yazılabilir.

Sudoku'dan SAT'a. SAT yalnızca doğru/yanlış konuşur; dolayısıyla her (satır, sütun, değer) üçlüsü için bir Boole değişkeni verin: *x(r,c,v)*, "*r* satırı, *c* sütunundaki hücre *v* değerini içeriyor" demektir. 4'e 4 bir Sudoku (2'ye 2 bloklar, 1–4 değerleri) 4·4·4 = 64 değişken ister; klasik 9'a 9 için 729. Her Sudoku kuralı daha sonra bir dizi tümceciğe dönüşür. (Tümcecik, değişkenlerin ya da olumsuzlarının OR'udur; tüm formül bütün tümceciklerin AND'idir.)

Her hücre en az bir değer içerir — hücre başına bir tümcecik:

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

Her hücre en fazla bir değer içerir — her değer çifti için "ikisi birden değil" tümceciği:

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

… ve altı çiftin tümü için böyle devam eder.

Her satır her değeri içerir — 1. satır ve 3 değeri için en az bir kez:

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

ve en fazla bir kez: $\neg x(1,1,3) \vee \neg x(1,2,3)$, satırdaki her hücre çifti için böyle devam eder.

Sütunlar ve bloklar — aynı tümcecik grupları; yalnızca hücre grubu değişir. Sol üst blok ve 2 değeri için:

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

artı çiftler için "ikisi birden değil" tümcecikleri.

Basılı ipuçları — en basit kısım: her ipucu tek değişkenli bir tümceciktir. Sol üst köşede basılı 3 şu tümceciğe dönüşür:

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

Bunların tümünün AND'i tam olarak Sudoku'nun bir çözümü olduğunda doyurulabilirdir — ve doyuran atamanın kendisi çözümdür: hangi x(r,c,v)'lerin doğru olduğunu okuyup ızgarayı doldurun. 9'a 9 için bu, 729 değişken ve birkaç bin tümcecik eder; modern bir SAT çözücü bunu milisaniyelerde halleder. x(1,1,3) ipucu tümceciğine dikkat edin: "bu hücre tam olarak 3'tür" der, "bu hücrelerin hepsi farklıdır" demez — aşağıdaki protokol notunda ipucu hücreleri için ek hileyi zorunlu kılan asimetri de budur.

SAT'tan Sudoku'ya. Makalenin ihtiyaç duyduğu ters ve daha zor yön şudur: *keyfî* bir SAT formülü verildiğinde, tam olarak formül doyurulabilir olduğunda çözümü olan bir mega-Sudoku inşa etmek. Sudoku'nun doğal kuralları yalnızca "bu hücrelerin hepsi farklıdır" diyebilir; dolayısıyla keyfî mantıksal kısıtlar *inşa edilmelidir* — araçların (*gadgets*) yaptığı tam olarak budur. Bir araç, formülün her tümceciği için önceden tasarlanmış küçük bir hücre kümesidir; belirlenmiş hücreler değişken rolü oynar (taşıdıkları sembol doğru ya da yanlışı kodlar) ve kümenin iç kısıtları, yalnızca o tümceciği doyuran atamalara karşılık gelen

doldurmaların yasal olacağı biçimde tasarlanır. Bu, NP-tamlık kanıtlarının standart zanaatıdır; genelleştirilmiş Sudoku için Yato ve Seta bunu 2003'te gerçekleştirdi.
İki yön birlikte, N'ye N Sudoku ile SAT'ın farklı kostümler giymiş aynı problem olduğunu söyler. Bu da bu makalenin — ve özgün makalenin — ızgaralar ve semboller kullanarak tüm NP hakkında hikâye anlatmasına izin verir.

Tanığı gözünüzde canlandırmak hâlâ kolay. Alice mega-Sudoku'nun eksiksiz ve geçerli bir dolduruluşunu biliyor. Bob böyle bir dolduruluşun var olduğuna ikna olmak istiyor, ama Alice onu açıklamak istemiyor. Tam dolduruluşu gönderirse Bob ikna olur, fakat sır ortadan kalkar.

Klasik sıfır bilgi sürümünde Alice ve Bob etkileşir. Eski tarz bir zihinsel model kapalı taşlar kullanır. Alice çözülmüş ızgarayı gizler, her turdan önce sembolleri gizlice yeniden adlandırır ve Bob'un rastgele seçilmiş tek bir yerel kısıtı incelemesine izin verir: bir satır, sütun, kutu ya da araç. Açılan hücrelerde birbirinden farklı semboller görülürse Bob'un güveni artar. Sonra her şey yeniden kapatılır ve semboller taze biçimde yeniden adlandırılır. (Bir ayrıntı var: bulmacanın verilmiş ipuçları ek bir hile gerektirir, çünkü sembolleri yeniden adlandırmak onları da gizler. Aşağıdaki not klasik protokollerin bunu nasıl çözdüğünü anlatıyor; devamı için bu oyuncak resim yeterli.)

Klasik protokoller ipucu hücrelerini gerçekte nasıl ele alıyor?

Yeniden adlandırma hilesinin kör bir noktası vardır. Satır, sütun ve kutu kurallarının tümü "bu hücrelerin hepsi farklı" der ve *hepsi farklı* özelliği sembollerin her türlü yeniden adlandırılmasında korunur. Fakat bir ipucu "bu hücre tam olarak 5 içerir" der ve yeniden adlandırmadan sonra Bob yalnızca $\sigma(5)$'i — maskelenmiş bir sembolü — görür; σ yeniden adlandırmasını bilmediği için kontrol yapamaz. Bu düzeltilmezse Alice basılı ipuçlarını tamamen görmezden gelerek *bir* geçerli ızgaranın var olduğunu kanıtlayabilir; bu da *bu* bulmaca hakkında hiçbir şey kanıtlamaz. Klasik literatürde iki standart çözüm vardır.
Palet. Gizli ızgaraya N hücrelik fazladan bir satır ekleyin — Alice'in 1…N sembolleriyle sabit ve herkese açık sırada doldurduğu, sonra her şeyle birlikte yeniden adlandırdığı bir palet; böylece $\sigma(1)…\sigma(N)$ içerir. Bob'un rastgele sınamasına artık bir seçenek daha eklenir. Satır, sütun, kutu ya da araç açmak yerine **palet artı bir ipucu hücresini** seçebilir. Alice ikisini de açar; palet o turun yeniden adlandırmasını gösterir ve Bob ipucu hücresinin basılı ipucunun yeniden adlandırılmış biçimini tam olarak gösterdiğini kontrol eder. Bu sıfır bilgi olarak kalır; çünkü Bob yalnızca her tur yeniden rastgele seçilen ve tek başına işe yaramayan σ'yı ve bulmacadan zaten bildiği bir hücre değerini öğrenir. Gizli hücreler hakkında hiçbir şey sızmaz ve bir simülatör rastgele σ seçerek görünümü taklit edebilir. Sağlamdır; çünkü hile yapan Alice her tur sabit bir olasılıkla yakalanır ve şüphe ihmal edilebilir hâle gelene kadar turlar tekrarlanır.
İpuçlarını yapının içine derlemek. Daha yapısal bir sürüm özel sınama eklemek yerine onu ortadan kaldırır. İpucu değerini *doğrulamak* yerine fark kısıtlarıyla zorlayın: ipucu hücresini kendi değerini taşıyan hariç her palet hücresine bağlayın — "$\sigma(1)$'den farklı, $\sigma(2)$'den farklı, …, $\sigma(5)$ dışındaki her şeyden farklı." Hücrenin yasal olarak taşıyabileceği tek sembol ipucunun sembolüdür. Artık her kısıt yine "bu ikisi farklıdır" biçimindedir — yeniden adlandırma altında değişmez ve bir satır gibi kontrol edilebilir. Klasik grafik boyama protokolündeki önceden

renklendirilmiş köşeler için kullanılan hamle de budur; yukarıdaki *araçlar* sözcüğünün ruhu da bu: MegaSudoku-as-SAT resminde ipuçları, diğer bütün kısıtlar gibi eşitsizlik araçlarına derlenir.
Fiziksel protokol. Sudoku için gerçek dünyadaki kart protokolü (Gradwohl, Naor, Pinkas ve Rothblum, 2007) yeniden adlandırma hiç kullanmaz ve ipuçlarını gizleme başlamadan önce sabitler. Alice her hücre için hücrenin değerini taşıyan üç özdeş kart koyar — gizli hücreler için yüzleri kapalı, ama **ipucu hücreleri için yüzleri açık**; böylece Bob kartlar çevrilmeden önce ipuçlarına uyulduğunu kendi gözleriyle görür. Daha sonra her hücreden bir kart satır paketine, biri sütun paketine, biri kutu paketine gider; her paket karıştırılır ve açılır, Bob da N sembolün tümünü içerdiğini kontrol eder. Karıştırma konum bilgisini yok eder (sıfır bilgi kısmı budur), ama ipuçları dağıtım anında zaten sabitlenmiştir.
Her iki durumda da ders, bu yazının tekrar tekrar döndüğü dersle aynıdır: sıfır bilgi protokolü, gizleme sonrasında *hangi* gerçeklerin ayakta kaldığının dikkatli muhasebesidir. Yeniden adlandırma "hepsi farklı"yı korur ve "5'e eşittir"i siler — dolayısıyla "5'e eşittir" başka yollardan geri sokulmalıdır.

Bu, makaledeki protokol değildir. Klasik sıfır bilgi için zihinsel modeldir:

- Alice ile Bob ileri geri iletişim kurar.
- Bob rastgele kontroller seçer.
- Alice tüm çözümü değil, yalnızca yerel tutarlılığı açığa çıkarır.
- Gizlilik kanıtı, Bob'un gördüklerinin Alice'in gizli çözümü olmadan da üretilebileceğini göstererek çalışır.

Dolayısıyla klasik sıfır bilgi olumlu bir gerçek üzerine kuruludur:

> Bir simülatör gerçekten vardır.

Şimdi rahat parçaları kaldırın. Alice tek bir kanıt dizisi gönderip gider. Güvenilir kurulum yok, önceden hazırlanmış ortak rastgele dizi yok ve Bob yanlış bir bulmacayı hiçbir zaman kabul etmemeli. Klasik sıfır bilginin yaşayamadığı ortam budur.

Hileden önce bir karakter daha gerekiyor. Bir **kural kitabı** sabitleyin: mantıkçıların anlamında biçimsel bir kanıt sistemi — sabit bir aksiyom kümesi artı yazılı matematiksel kanıtları mekanik olarak denetleyen kurallar. Matematiğin standart aksiyomları ZFC, kanonik örnektir. Bundan sonraki her ifade önceden seçilmiş bir kural kitabına göredir ve seçim esnektir: yapı ZFC dahil sabitlediğiniz herhangi bir kural kitabı için çalışır.

(Makalenin kendisinden ödünç alınmış bir terminoloji notu: burada "kanıt sistemi" her zaman bu kural kitabı — matematiksel kanıtları kontrol eden biçimsel sistem — anlamına gelir; Alice'in gönderdiği mesajlar anlamına asla gelmez. Alice ve Bob'un mekanizmaları "kanıtlayıcı ve doğrulayıcı" diye adlandırılır.)

Gödel tarzı sürüm mega-Sudoku hikâyesini korur ama kanıtı değiştirir.

Aynı görünen boyutta ikinci bir kısıt sistemi seçin ve ona **D** deyin. Hikâyede S ve D aynı formatta iki MegaSudoku(n) bulmacasıdır. Perde arkasında D farklı boyutta zor bir mantıksal formül olarak başlamış olabilir; gerekirse aynı ızgaraya sığması için zararsız kukla kısıtlarla doldurulabilir. D gerçekte **doyurulamaz** bir mantıksal formülden yapılmıştır: bozuk bir bulmacanın yasal tamamlanmış ızgarası olmadığı gibi, bütün kısıtlarını doğru yapan hiçbir değer ataması yoktur. Oyuncak örnek, aynı anda hem "X doğrudur" hem "X yanlıştır" isteyen bir formül olurdu. Dolayısıyla D'nin geçerli dolduruluşu yoktur.

Ama D, bozukluğu *kolayca gösterilebilen* bir bulmaca olmamalıdır. Yukarıdaki oyuncak örnek bu yüzden işe yaramaz: herhangi bir kural kitabı "X ve değil-X" ifadesini tek satırda çürütür. D, seçilmiş kural kitabının kısa bir argümanla doğrulayamadığı bir biçimde yanlış olmalıdır. Kural kitabı D'yi kısa kanıtla çürütebilse aşağıdaki hikâye çökerdi: Alice'in sırrı olmadan kanıt üretmiş olabilecek alternatif yol biçimsel olarak dışlanabilir ve gizlilik garantisi de onunla birlikte giderdi. Bu yüzden D, sabit kural kitabının verimli biçimde çürütemediği bir aileden seçilir: o kural kitabının içinde D'nin çözümü olmadığına dair kısa kanıt yoktur.

Alice'in tek mesajlık kanıtı daha sonra bir ya/ya da ifadesi hakkındadır:

> ya gerçek mega-Sudoku S'nin bir çözümü vardır, ya da yem D'nin bir çözümü vardır.

Mantıksal bağlantı budur. D, S'yi sihirli biçimde doğru yapan bir yöntemle **üretilmiyor**. Kanıt "D'nin çözümü yok, öyleyse S'nin çözümü var" demiyor. **S veya D** ayrışımını kanıtlıyor. Kusursuz sağlamlık, yanlış bir ayrışımın geçerli kanıtı olamayacağını söyler. D gerçekte yanlış olduğuna — çözümü olmadığına — göre ayrışımın doğru olmasının tek yolu S'nin doğru olmasıdır. Kanıt kabul edilirse S'nin çözümü olmalıdır. Yem, yanlış bir S'yi doğru yapamaz.

Ama sıfır bilgi tarzı kısım için D'nin *çözümü olsaydı* ne olacağını sorun. O yem çözümü alternatif tanık görevi görürdü. Alice'in gerçek mega-Sudoku çözümünü bilmeden kanıt üretmeye izin verirdi — yani bir simülatör olurdu. Gerçekte D'nin çözümü yok, dolayısıyla bu simülatör yolu kapalı. Nokta şu ki kural kitabı bu yolun kapalı olduğunu verimli biçimde kanıtlayamıyor.

Dolayısıyla D'nin iki görevi var. **Sağlamlık** için D yanlış, dolayısıyla "S veya D"nin geçerli kanıtı S'yi zorunlu kılıyor. **Etkin sıfır bilgi** için D'yi çürütmek zor, dolayısıyla kural kitabı simülasyonu mümkün kılacak yem yolunu hızla dışlayamıyor.

Böylece güvenlik testi artık şu değil:

> Bir simülatörün gerçekten var olduğunu kanıtlayabilir miyiz?

Şuna dönüşüyor:

> Kural kitabınız simülatörün imkânsız olduğunu verimli biçimde kanıtlayabilir mi?

Yanıt hayırsa şaşırtıcı derecede güçlü bir sonuç çıkıyor: (a) bir test çalıştırarak gözlenebilen ve (b) simülatörün varlığından o kural kitabının içinde kanıtlanabilir biçimde çıkan her güvenlik garantisi

gerçekten sağlanır. Bunlardan herhangi birine yapılan başarılı saldırı, eksik olan kısa çürütmeyi kendisi oluştururdu; o kısa çürütme ise yoktur. “Etkin sıfır bilgi”deki *etkin* kısmı budur.

Dolayısıyla sınıf içi karşılaştırma şöyle:

Klasik sıfır bilgi: kanıtlar güvenlidir, çünkü bir simülatör vardır.

Gödel tarzı etkin sıfır bilgi: gözlenebilir güvenlik testleri bakımından kanıtlar güvenli kabul edilir, çünkü kural kitabı simülatörün imkânsız olduğunu verimli biçimde kanıtlayamaz.

İkinci iddia daha zayıf. Makalenin klasik sürümü bozan üç özelliği — tek mesaj, kurulum yok ve kusursuz sağlamlık — koruyabilmesinin nedeni de bu.

Yeni test: simülatörün yok olduğunu kanıtlayamıyorsunuz

Ilango’nun gevşetmesi soruyu değiştiriyor.

Klasik sıfır bilgi şunu sorar:

> Bir simülatör var mı?

Etkin sıfır bilgi daha zayıf bir şey sorar:

> Seçtiğiniz kural kitabı hiçbir simülatörün var olmadığını verimli biçimde kanıtlayabilir mi?

Bu teknik bir kaçamak gibi gelebilir, ama ana fikir budur. Yapı tuhaf bir durumda yaşar: bir simülatör gerçekte **yoktur** — makale bu konuda açıktır — ama sabitlediğiniz kural kitabı onun olmadığını verimli biçimde kanıtlayamaz. Önemsediğiniz her kötü sonuç böyle bir çürütme gerektiriyorsa sistem, bu sonuçlar bakımından yine de sıfır bilgi gibi davranır.

Gödel burada devreye giriyor. Süs olarak değil, “Gödel kriptografiyi güvenli yapar” diye de değil. Bağlantı kanıt kuramsaldır. Bir kural kitabına, kesin bir anlamda mümkün olan en iyi sistemse **optimal** denir: ilgili türdeki bir formülü herhangi bir kural kitabı kısa bir kanıtla çürütebiliyorsa, optimal kural kitabı da en fazla polinom ölçüde daha uzun bir kanıtla bunu yapabilir. Krajíček ve Pudlák 1989’da **optimal kanıt sisteminin var olmadığını** öne sürdü: hangi kural kitabını sabitlerseniz sabitleyin, başka bir kural kitabı bazı doğru ifade ailelerini çok daha kısa kanıtlarla ispatlar. Bu, kanıt karmaşıklığının merkezi açık varsayımlarından biridir ve Gödel’in eksiklik teoreminin sonlu, karmaşıklık-kuramsal kuzenidir: bazı doğru ifadelerin sabitlediğiniz kural kitabında kısa kanıtı yoktur — ilke olarak kanıtlanamaz oldukları için değil, her sabit kural kitabı bazı kısa gerçekleri kısa kanıtsız bıraktığı için.

Makale bu varsayımı kabul eder (kriptografide varsayımlar kullanılırken standart olan, biraz daha güçlü “sonsuz sıklıkta” biçimiyle). Krajíček ve Pudlák’ın bir teoremi sayesinde getirisi somuttur: her kural kitabı için gerçekten doyurulamaz, ancak o kural kitabının kısa kanıtlarla çürütemediği bir

formül dizisi vardır — ve kritik olarak, verimli bir algoritma bunları *üretebilir*. Son özellik, yani uniformluk, fikri yalnızca varlık iddiası olmaktan çıkarıp Alice'in gerçekten çalıştırabileceği algoritmaya dönüştürür: yem D'ler havadan değil, bir üretim hattından çıkar.

Kriptografik hamle, kanıt gücündeki bu eksikliği işe koşmaktır.

Yapı ne yapıyor?

Makalenin yapısını iskeletine indirgersek şöyle.

Bir kural kitabı sabitleyin — örneğin ZFC. Kanıt karmaşıklığı varsayımı altında, gerçekte doyurulamaz olan ama kural kitabının doyurulamaz olduklarına dair kısa kanıtı bulunmayan, verimli biçimde üretilebilir bir formül dizisi vardır.

Şimdi şu biçimde tek mesajlık bir kanıt kurun:

> ya gerçek ifade doyurulabilirdir, ya da bu özel zor formül doyurulabilirdir.

Özel zor formül doyurulabilir değildir. Dolayısıyla alttaki kanıt mekanizması kusursuz sağlamsa mesajın kabul edilmesi yine gerçek ifadenin doğru olduğu anlamına gelir. Kusursuz sağlamlık buradan gelir.

Ama sıfır bilgi benzeri güvenlik için, özel zor formülün *doyurulabilir olduğunu* hayal edin. O zaman tanığı, gerçek tanığı bilmeden kanıtları simüle etmek için kullanılabilirdi. Formül gerçekte doyurulabilir değil — ancak kural kitabı bunu verimli biçimde kanıtlayamıyor. Dolayısıyla simülatörün imkânsız olduğunu da verimli biçimde kanıtlayamıyor.

Menteşe budur. Sistem sırrı klasik bir simülatör üreterek gizlemiyor. Sırrı, geniş bir gözlenebilir güvenlik testi sınıfı için, kural kitabının simülatörün yokluğunu sertifikalandıramamasının arkasında gizliyor.

Makale ne iddia ediyor?

Ana teorem katmanlar hâlinde geliyor. Çekirdek sonuç şu:

Standart bir kriptografik varsayım — birkaç yerleşik varsayım paketinden çıkan ve iyi çalışılmış nesneler olan **etkileşimsiz tanık ayırt edilemez kanıtların** varlığı — ve **(sonsuz sıklıkta) optimal kanıt sisteminin bulunmadığı** yönündeki kanıt karmaşıklığı varsayımı altında makale, her kural kitabı seçimi için NP/SAT üzerinde tek mesajlı, kurulumsuz, **kusursuz sağlam** bir kanıtlayıcı ve doğrulayıcı kurar; yapı o kural kitabına göre etkin sıfır bilgidir. (NP/SAT bulmaca benzeri problemlerin standart "en zor ortak paydasıdır"; mega-Sudoku onun giydiği kostümlerden biridir.)

Yanlışlanabilir güvenlik özelliklerini korumaya ilişkin daha geniş iddia için makale bir standart

varsayım daha ekler: derandomizasyon inancı **P = BPP** (kabaca: rastgelelik algoritmalara özsel bir ek güç sağlamaz).

Teorem dilinden çıkarırsak:

- Kanıt tek mesajdır.
- Güvenilir kurulum yoktur.
- Yanlış ifadeler kanıtlanamaz.
- Kanıtlayıcı klasik sıfır bilgi değildir — simülatörü yoktur.
- Ama klasik sıfır bilginin yanlışlanabilir, oyun-temelli her güvenlik sonucu bu ortamda elde edilebilir.

"Yanlışlanabilir" sözcüğü önemli. Güvenlik hatasının bir saldırganı bir oyunda çalıştırarak test edilebilmesi demektir. Birçok kriptografik güvenlik tanımı bu biçimdedir: saldırgan iki şifrelemeyi ayırt edebilir mi, bir fonksiyonun tersini bulabilir mi, tanığı ele geçirebilir mi, belirlenmiş bir deneyi kazanabilir mi? Teorem her yanlışlanabilir özellik için tek tek bir kanıtlayıcı verir. *Bütün* yanlışlanabilir özelliklere aynı anda sahip tek bir kanıtlayıcı muhtemelen imkânsızdır — eski yeniden kullanılabilirlik saldırısı ("Bob kanıtı başkalarına gösterebilir") kendisi de yanlışlanabilir bir özelliktir ve burada gerçekten başarısız olur. Makalenin önerisi, tek bir kanıtlayıcının tüm *doğal* yanlışlanabilir özellikleri — kriptografik pratikte gerçekten karşılaşılanları — makul biçimde kapsayabileceğidir; ancak bu bölüm "doğal" sözcüğünün gayriresmî anlamına ve açık bir varsayıma dayanan koşullu bir teoremdir. Garanti, her felsefi ya da simülasyon-temelli gizlilik anlamına değil, gözlenebilir arızalara yöneliktir.

Somut bir yan sonuç adlandırmaya değer: yapı, uniform bir kanıtlayıcıyla ilk etkileşimsiz *tanık gizleyen* kanıtları verir — "bir bulmacanın kanıtı çözümünü bulmanıza yardım etmez", etkileşim ve kurulum olmadan — kulağa mütevazı gelen ama onlarca yıldır kurulamamış bir nesne.

Bu ne demiyor?

Parçayı dürüst tutan bölüm bu.

Eski imkânsızlık teoremlerinin yanlış olduğunu **söylemiyor**. Yapı tanımı değiştirerek onlardan kaçınıyor.

Etkileşimsiz, kurulumsuz ve kusursuz sağlam sıradan klasik sıfır bilgi **vermiyor**. Makale, oluşturulan kanıtlayıcının simülatörü olmadığını açıkça söylüyor.

Kanıtın yeniden kullanılamayacağı anlamına **gelmiyor**. Tek mesajlık bir kanıt hâlâ başkasına gösterilebilir; makale inkâr edilebilirlik türü özellikleri korumuyor. (Güvenilir kurulumlu etkileşimsiz sıfır bilgi de aynı sınırlamaya sahiptir.)

Bunun kullanıma hazır pratik bir protokol olduğu anlamına **gelmiyor**. Bu karmaşıklık teorisi ve kriptografik temellerdir. Sonuç kanıt karmaşıklığı ve kriptografide büyük varsayımlara dayanır; yapı ilke olarak neyin mümkün olduğu hakkındadır.

"Gödel"i sihirli bir güvenlik ilkeline **dönüştürmüyor**. Gödel bağlantısı kanıt sistemleri, optimal kanıt sistemleri ve eksikliğin sonlu benzerleri üzerinden gelir. Yararlı sezgi "eksiklik şifrenizi korur" değildir. Şudur: bir kural kitabı simülatörün imkânsız olduğunu verimli biçimde kanıtlayamıyorsa, o kanıtı gerektirecek saldırılar güvenlik tanımları düzeyinde engellenebilir.

Yine de neden ilginç?

Kriptografi sık sık zorluğu güvenliğe dönüştürür. Çarpanlara ayırma zordur, dolayısıyla RSA türü varsayımlar işe yarar. Kafes problemleri zordur, dolayısıyla kafes kriptografisi işe yarar. Buradaki zorluk daha tuhaf: "bir sırrı hesaplamak zor" değil, "belirli bir kanıt nesnesinin var olamayacağını kanıtlamak zor."

Makalenin alışılmadık hissettirmesinin nedeni bu. Aksiyomları ve kural kitaplarını neredeyse kriptografik kaynaklar gibi ele alıyor. Alışılmış imkânsızlık, sağlamlık ile simülasyon arasında gerilim olduğunu söyler. Ilango'nun hamlesi bu gerilimi kanıt-kuramsal bir perdenin arkasına yerleştirmek: simülatör yoktur, ama biçimsel sistem onun yokluğunu verimli biçimde ortaya çıkaramaz.

Okuyucu için şaşırtıcı olan, bunun günümüz sıfır bilgi sistemlerinin yerini alacak olması değil. En azından doğrudan, muhtemelen almayacak. Şaşırtıcı olan, matematiksel mantıktan gelen bir sınırlamanın yapıcı biçimde kullanılabilmesi: yalnızca bir duvar değil, bir çeşit örtü olarak.

Kanıt ne kadar güçlü?

Bu bir teorem makalesi, dolayısıyla "kanıt" biyoloji ya da astronomi makalesindekinden farklı bir şey demek. Soru bir deneyin tekrarlanıp tekrarlanmadığı değil. Tanımların, varsayımların ve kanıt zincirinin iddiayı destekleyip desteklemediği.

Kanıt biçimseldir ve makale varsayımları konusunda açıktır. Varsayımlar gelişigüzel değil. Etkileşimsiz tanık ayırt edilemez kanıtlar kriptografide standart nesnelerdir ve birkaç yerleşik varsayım paketinden çıkar. Optimal kanıt sistemi olmadığı varsayımı kanıt karmaşıklığının merkezi varsayımlarındandır. P = BPP, yalnızca daha geniş yanlışlanabilir-özellik teoreminde kullanılan standart bir derandomizasyon inancıdır.

Makale ayrıca varsayımların keyfî bir iskele değil, doğru bedel olduğunu savunuyor: ters yönde bir sonuçla bunların özünde gerekli olduğunu gösteriyor — bu tür yapılar varsa etkileşimsiz tanık ayırt edilemez kanıtlar da var olmalı ve (standart tek-yönlü fonksiyonlar kabul edilirse) optimal kanıt sistemi bulunmamalı. Varsayımlar ayrıca bir "kazan-kazan" durumudur: herhangi birini çürütmek, kanıt karmaşıklığı, kriptografi ya da karmaşıklık teorisinde başlı başına dönüm noktası olurdu.

Ancak sonuç koşullu olduğundan ona duyulan güven de koşulludur. Bu varsayımlar başarısız olursa teoremin yorumu değişir. Ve varsayımlar doğru olsa bile garanti tam klasik sıfır bilgi değildir; makalenin gevşetilmiş, kanıt-kuramsal sürümüdür.

Dolayısıyla doğru güven düzeyi şudur: makalenin tutarlı bir koşullu olabilirlik sonucu ortaya koyduğuna yüksek güven; varsayımların gerçekten içinde yaşadığımız kriptografik dünyayı tanımladığına orta güven; hemen pratik sonuç beklemeye düşük güven.

Neden önemli?

Makale kapalı olduğu düşünülen bir yol açıyor.

Klasik teori şunu söyler: tam sıfır bilgi kurulumsuz tek mesaja sıkıştırılamaz ve kusursuz sağlam olamaz. Ilango'nun makalesi şunu söylüyor: güvenlik oyunlarında test edilebilen sıfır bilgi sonuçlarını istersek ve güvenlik tanımının bir kural kitabının neleri verimli biçimde çürütebildiğine ya da çürütemediğine bağlı olmasına izin verirsek, yararlı davranışın büyük bölümünü tek mesaj, kurulum yok ve kusursuz sağlamlıkla geri kazanabiliriz.

Bu küçük bir tanım düzeltmesi değil. Kriptografik garantileri düşünmenin farklı bir yolu. Yalnızca neyin var olduğunu sormak yerine, kural kitabınızın neyi dışlayabildiğini sorun. Kanıtlanamazlığı felsefi bir rahatsızlık olarak görmek yerine yapısal bir kaynak olarak kullanın.

Pratik dünya yarın değişmeyebilir. Ama kavramsal harita değişiyor. Artık "kimse sırrın sızdığını verimli biçimde kanıtlayamaz" ifadesinin, "sır sızmadı"dan istediğimiz oyun-temelli korumaların çoğunu geri kazanmaya yetecek kadar güçlü olabildiği biçimsel bir anlam var.

Gödel'in başlıkta bulunmasının nedeni bu.

Kısa özet

Sıfır bilgi kanıtları, kanıtlayıcının tanığı açıklamadan doğrulayıcıyı bir ifadenin doğru olduğuna ikna etmesini sağlar. Klasik imkânsızlık sonuçları sıfır bilginin kurulumsuz tek mesaja sıkıştırılamayacağını ve kusursuz sağlam olamayacağını söyler. Rahul Ilango'nun makalesi bu imkânsızlıkları çürütmüyor. Daha zayıf bir kavram, etkin sıfır bilgi tanımlıyor: gerçek bir simülatörün var olmasını istemek yerine, seçilmiş bir kanıt sisteminin — ZFC gibi biçimsel bir kural kitabının — hiçbir simülatörün var olmadığını verimli biçimde kanıtlayamamasını istiyor. Kriptografiden (etkileşimsiz tanık ayırt edilemez kanıtlar) ve kanıt karmaşıklığından (optimal kanıt sisteminin bulunmaması) büyük varsayımlar altında makale, NP/SAT için kurulumsuz ve kusursuz sağlam, tek mesajlı kanıtlayıcılar kuruyor ve sıfır bilginin yanlışlanabilir, oyun-temelli sonuçlarını özellik özellik elde ediyor. Bütün "doğal" özellikleri kapsayan tek bir kanıtlayıcı daha ileri ve kısmen varsayımsal bir uzantı; kelimenin tam anlamıyla her yanlışlanabilir özelliği kapsamak ise muhtemelen imkânsız, çünkü kanıtlar yeniden kullanılabilir. Sonuç teorik ve koşullu; kullanımda olan bir kriptografik ilkel değil. Ama kanıt-kuramsal kanıtlanamazlığı kriptografik kaynak olarak kullanmanın yeni bir yolunu gösteriyor.

Abartısız değerlendirme

Makale neyi gösteriyor: Belirtilen varsayımlar altında NP/SAT için tek mesajlı, kurulumsuz, kusursuz sağlam ve seçilen herhangi bir kanıt sistemine göre etkin sıfır bilgi olan kanıtlayıcılar kurulabileceğini; ayrıca klasik sıfır bilginin her yanlışlanabilir oyun-temelli sonucunun elde edilebileceğini.

Makul ama koşulsuz kanıtlanmamış olan: Gerekli kanıt-karmaşıklığı ve kriptografik varsayımların doğru olması. Bunlar ciddi ve iyi çalışılmış varsayımlar — makale özünde yalnızca yeterli değil, gerekli olduklarını da gösteriyor — ama yine de varsayım.

Neyi göstermiyor: Etkileşimsiz, kurulumsuz ve kusursuz sağlam klasik sıfır bilgi; kullanıma hazır pratik sistem; kanıtların inkâr edilebilirliği ya da yeniden kullanılamazlığı; veya Gödel'in eksiklik teoreminin tek başına kriptografiyi güvenli kıldığı.

Başlıca sınırlamalar: Garanti sıfır bilginin gevşetilmiş bir sürümüdür; en geniş sürüm birden fazla varsayıma dayanır; tek evrensel kanıtlayıcı iddiaları kısmen varsayımsal kalır; sonuç öncelikle temellerle ilgilidir.

Genel okuyucu ne kadar güvenmeli? Tanımlar kabul edilirse bunun önemli bir koşullu teori sonucu olduğuna yüksek güven. Varsayımların gerçekliği yakaladığına orta güven. Hemen pratik kullanım için düşük güven. Güvenli sonuç şu: makale sıfır bilgi imkânsızlıklarını kırmıyor; birçok güvenlik oyunu için önemli olan kısımlarının etrafından dolaşmak üzere yeni, kanıt-kuramsal bir yol buluyor.

Kaynaklar

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`