The Clean Paper

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

Cryptographic proof secret লুকাতে পারে—কারণ missing simulator-এর অনুপস্থিতি প্রমাণ করাই কঠিন

Classical zero-knowledge actual simulator দাবি করে, কিন্তু one message, no setup ও perfect soundness-এর setting-এ তা impossible। Rahul Ilango-র effectively zero-knowledge notion target বদলায়: chosen formal proof system যেন efficiently প্রমাণ করতে না পারে যে simulator নেই। Major proof-complexity ও cryptographic assumptions-এর অধীনে এই দুর্বল, proof-theoretic guarantee falsifiable game-based ZK consequence property-by-property recover করতে পারে। এটা classical ZK বা deploy-ready primitive নয়।

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

কৌশলটি গোপন সত্যটি লুকানো—এ কথা প্রমাণ করা নয়

শূন্য-জ্ঞানের সবচেয়ে সহজ ছবি দিয়ে শুরু করা যাক।

Alice Bob-কে বোঝাতে চায় যে একটি Sudoku ধাঁধার দ্রবণ আছে। দ্রবণ-টি পাঠিয়ে দিলে Bob বিশ্বাস করবে, কিন্তু ধাঁধার গোপন শেষ। Alice যা চায় তা আরও অদ্ভুত: **দ্রবণ আছে—এটি প্রমাণ করা, দ্রবণ না দেখিয়ে।**

শূন্য-জ্ঞান প্রমাণের প্রতিশ্রুতি এটিই। প্রমাণদাতা (Alice) যাচাইকারীকে (Bob) বিবৃতি সত্য বলে convince করে, কিন্তু বিবৃতি সত্য—এই তথ্যের বাইরে সাক্ষ্য সম্পর্কে কিছু প্রকাশ করে না।

সমস্যা হলো, ধ্রুপদি তত্ত্বে এই প্রতিশ্রুতির দাম আছে। সাধারণ গাণিতিক প্রমাণের দুইটি আরামদায়ক বৈশিষ্ট্য থাকে। এক, এটি **একটি বার্তা**—লিখে দিলেই শেষ। দুই, এটি **সম্পূর্ণভাবে শব্দ**—ভুল বিবৃতির কোনো বোঝা প্রমাণ নেই। ধ্রুপদি অসম্ভবতা ফল বলে সম্পূর্ণ শূন্য-জ্ঞান এই বিন্যাসে দুটোই রাখতে পারে না।

প্রথমত, বিশ্বস্ত বিন্যাস ছাড়া ধ্রুপদি শূন্য-জ্ঞান সাধারণত মিথস্ক্রিয়া চায়। Alice যদি একবারে একটি প্রমাণ স্ট্রিং পাঠিয়ে চলে যায়, ধ্রুপদি সিমুলেশন নিশ্চিয়তা ভেঙে পড়ে।

দ্বিতীয়ত, **নখিুঁত যথার্থতা**-ও টান তৈরি করে। যাচাইকারী যদি কোনো এলোমেলো পছন্দে কখনো ভুল বিবৃতি গ্রহণ করা না করে, সেই এলোমেলোতা আগে থেকেই সংশোধন করা যায়; তখন মিথস্ক্রিয়া পতন করে একটি-বার্তা ক্ষেত্রে চলে আসে—যে ক্ষেত্রের আগেই অসম্ভব।

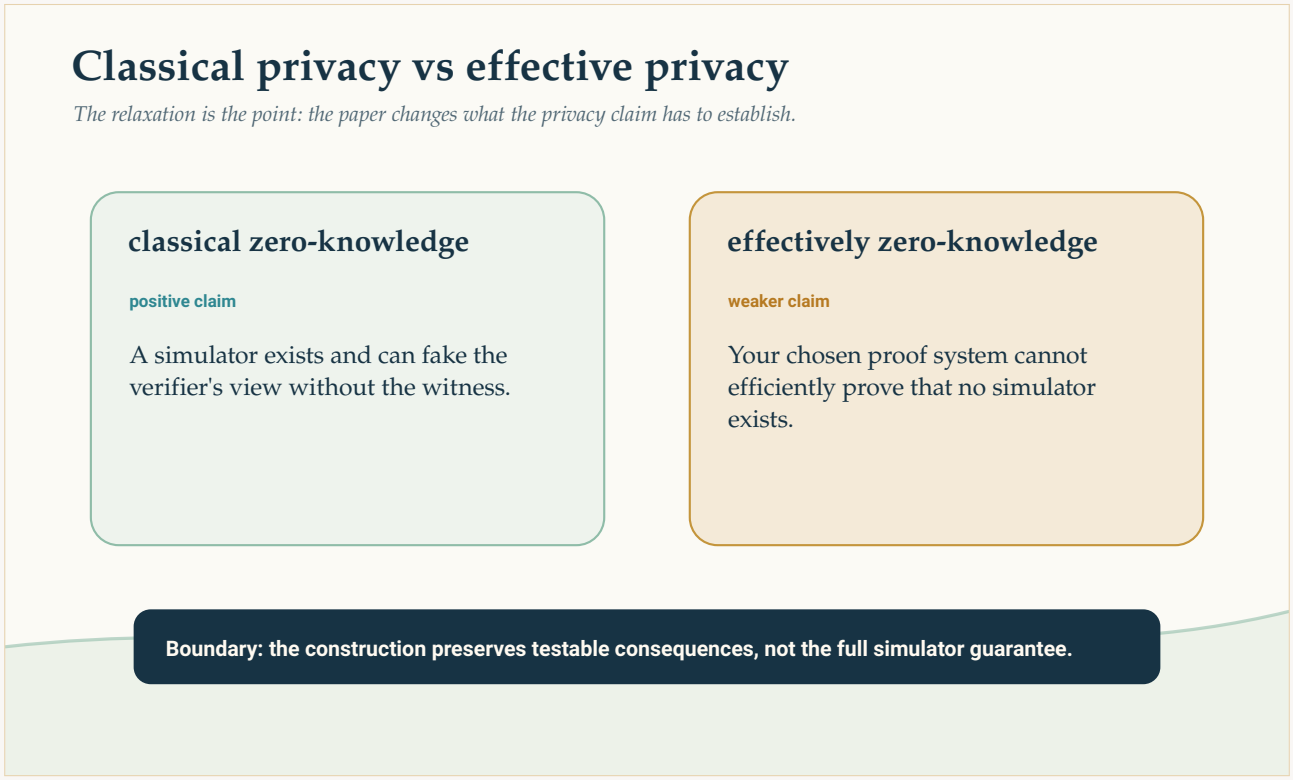
Rahul Ilango-র গবেষণাপত্র এই দুই দেয়াল "ভুল" প্রমাণ করে না। পদক্ষেপে-টি সূক্ষ্ম: **"reveals nothing" মানে কী—সেটি দুর্বল করা**, তবে এমনভাবে যাতে cryptographer-রা যে পর্যবেক্ষণযোগ্য, গেম-ভিত্তিক নিরাপত্তা পরিণতি পরীক্ষা করে সেগুলো অনেকটাই ফিরে আসে।

এই notion-এর নাম **কার্যকর অর্থে শূন্য-জ্ঞান**।

ধ্রুপদি শূন্য-জ্ঞানের তিনটি বন্ধ দরজা—মিথস্ক্রিয়া ছাড়া, বিশ্বস্ত বিন্যাস ছাড়া, এবং নখিুঁত যথার্থতা সহ। Ilango-র নির্মাণ অন্য পথ নেয়: নির্বাচিতি

আনুষ্ঠানিক নিয়মপুস্তক দক্ষভাবে প্রমাণ করতে পারে না যে সিমুলেটর অসম্ভব।

Original diagram — The Clean Paper CC BY 4.0



ধ্রুপদি শূন্য-জ্ঞান ধনাত্মক দাবি করে: সিমুলেটর আছে। কার্যকর অর্থে শূন্য-জ্ঞান দুর্বলতর দাবি করে: নির্বাচিত নিয়মপুস্তক দক্ষভাবে প্রমাণ করতে পারে না যে সিমুলেটর নেই। এই দুর্বলতাই একটি বার্তা, না বিন্যাস এবং নখুঁত যথার্থতা একসঙ্গে রাখার সুযোগ দেয়।

Original diagram — The Clean Paper CC BY 4.0

পুরোনো পরীক্ষা: একটি সিমুলেটর সত্যিই আছে

ধ্রুপদি শূন্য-জ্ঞান আনুষ্ঠানিকভাবে সংজ্ঞায়িত করতে **সিমুলেটর** নামে একটি fictional অ্যালগরিদম ব্যবহার করা হয়।

ভাবুন Jane Alice-এর গোপন জানে না। Jane যদি নিজেরাই এমন transcript/প্রমাণ তৈরি করতে পারে যা Bob Alice-এর কাছ থেকে পেলে যেমন দেখত ঠিক তেমনই বণ্টন তৈরি করে, তাহলে Bob গোপন থেকে আলাদা কোনো উপযোগী তথ্য পায়নি। Bob-এর "দৃষ্টভিঙ্গি" গোপন ছাড়াই সিমুলেট করা গেছে।

Sudoku-তে গোপন দ্রবণটাই **সাক্ষ্য**। ধ্রুপদি সংজ্ঞা তাই বাস্তব দক্ষ সিমুলেটর দাবি করে—একটি অ্যালগরিদম যা সাক্ষ্য না জেনেও যাচাইকারীর দৃষ্টভিঙ্গি পুনরুৎপাদন করতে পারে।

এই সংজ্ঞা শক্তিশালী, কিন্তু অসম্ভবতা-ও এখানেই কামড়ায়। Truly অ-পারস্পরিক প্রমাণ একটি স্ট্রিং। Bob স্ট্রিং পেলে অন্য কাউকে দেখাতে পারে; অর্থাৎ সে বিতরি প্রমাণ reuse করার ক্ষমতা পায়। ধ্রুপদি উপপাদ্য এই অন্তর্দৃষ্টিকে আনুষ্ঠানিক অসম্ভবতা-তে পরিণত করে।

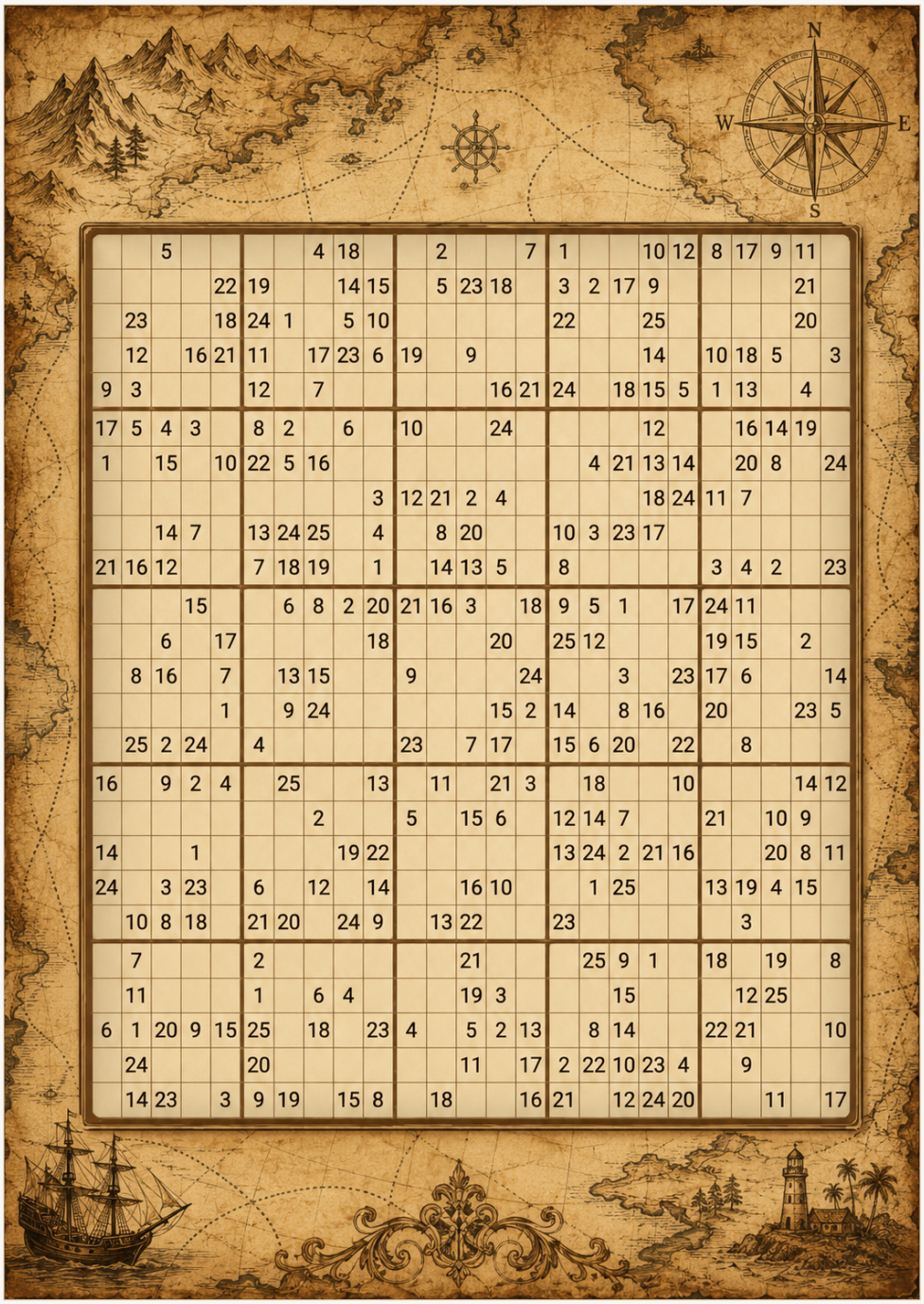
এই গবেষণাপত্র যে তিনটি বৈশিষ্ট্য ছাড়তে চায় না

না মথিস্ক্রিয়া: Alice একটি প্রমাণ স্ট্রিং পাঠায়; পেছনেবেং-forth নেই।
না বিন্যাস: কোনো বিস্তৃত সাধারণ রেফারেন্স স্ট্রিং, pre-arranged জনসাধারণের এলোমেলো তা বা ceremony নেই। "অ-পারস্পরিক শূন্য-জ্ঞান" নামে পরিচিত বহু ব্যবহারিক ব্যবস্থা বিন্যাস ব্যবহার করে; এখানে সেটিও নেই।
নখুঁত যথার্থতা: ভুল বিতরি বেধে প্রমাণ একটিও নেই। "খুব কম সম্ভাবনা-তে গ্রহণ করা" নয়—একেবারেই নেই।
এই তিনটি সাধারণ written গাণিতিক প্রমাণের স্বাভাবিক বৈশিষ্ট্য। ধ্রুপদি শূন্য-জ্ঞান এগুলো একসঙ্গে রাখতে পারে না।

MegaSudoku দিয়ে পার্থক্যটি অনুভব করা

সাধারণ 9×9 Sudoku গুরুতর জটিলতা উপমার জন্য খুব ছোট: কম্পিউটার সহজেই সমাধান করা বা অসন্তোষজনক নিশ্চিত করতে পারে। তাই **MegaSudoku(n)** পরিবার ভাবুন। বাধা আকার n, মোট প্রতীক $N = n^2$, grid $N \times N$, বাধা $n \times n$। সাধারণ Sudoku হলো ছোট $n=3$, $N=9$ ক্ষেত্রে।

প্রমাণ-জটিলতা গল্প শুরু হয় n বড় হলে, এবং grid-এ যন্ত্র যোগ করা গেলে যাতে এটি ইচ্ছামতো **SAT সূত্র**-র মতো behave করে। SAT হলো হ্যাঁ/না সীমাবদ্ধতার সমস্যা: চলকে সত্য/ভুল নির্ধারণ করে কি সব উপবাক্য পূরণ করা যায়?



একটি 25×25 Sudoku—গোপন দ্রবণ বা সাক্ষ্যরে দৃশ্যমান stand-in। নিয়ম যাচাই করা যায়, কিন্তু সম্পন্ন grid দেখানো গোপন প্রকাশ করবে।

AI-generated editorial thumbnail — The Clean Paper CC BY 4.0

Sudoku আর SAT: একই ধাঁধা দুই পোশাকে

"Sudoku SAT-এর মতো behave করতে পারে" শুধু রূপক নয়। অনুবাদ দুই দিকেই করা যায়।

Sudoku → SAT. প্রতিটি (সারি, স্তম্ভ, মান) ত্রিগুণের জন্য boolean চলক নিন: $x(r,c,v)$ মানে সারি r, স্তম্ভ c-এর কোষে মান v আছে। 4×4 Sudoku-তে 4·4·4 = 64 চলক; 9×9-তে 729।

"প্রতিটি কোষে অন্তত একটি মান" উপবাক্য:

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

"এক কোষে দুই মান একসঙ্গে নয়"—প্রতিজোড়ার জন্য:

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

সারি 1-এ মান 3 অন্তত একবার:

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

এবং pairwise উপবাক্য দিয়ে "at অধিকাংশ একবার"। স্তম্ভ ও বাধায় একই কাঠামো। Printed সূত্র "top-বাম কোষ = 3" স্রফে:

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

সব উপবাক্যরে এবং সন্তোষজনক ঠিক তখনই যখন Sudoku solvable; সন্তোষজনক বরাদ্দ থকেে সত্য $x(r,c,v)$ পড়ে grid পাওয়া যায়।

SAT → Sudoku. কঠনি দকি হলো ইচ্ছামতো SAT সূত্র থকেে সাধারণীকৃত Sudoku বানানো, যাতে Sudoku-টি সমাধানযোগ্য হয় ঠকি তখনই, যখন সূত্রটি সন্তোষজনক। Sudoku-র নজিস্ব নয়িম মূলত "সব ভন্নি", তাই ইচ্ছামতো যৌক্তকি সম্পর্ক **যন্ত্র** দিয়ে সংকতোয়তি করতে হয়। উপবাক্য যন্ত্রে নর্িধারতি কোষ চলকরে ভূমকিা নয়ে; অভ্যন্তরীণ সীমাবদ্ধতা এমনভাবে বানানো হয় যাতে বধৈ পূরণ ঠকি সন্তোষজনক বরাদ্দগুলো র সঙ্গে মলে। সাধারণীকৃত Sudoku-র NP-পূর্ণতা নর্িমাণ এই ধরনরে যন্ত্র ব্যবহার করে।

তাই সাধারণীকৃত Sudoku ও SAT জটলিতার অর্থে একই সমস্যার দুই costume। এই কারণইে grid-এর গল্প দিয়ে NP-এর বর্িতি বোঝানো বধৈ।

Alice MegaSudoku-এর সম্পূর্ণ বধৈ পূরণ জানে। Bob দ্রবণ আছে জানতে চায়, কন্তিু কন্তিু গ্রডিরে সমাধানটি জানতে চায় না। ধ্রুপদি পারস্পরকি মানসকি মডলেে Alice ঘরগুলো ঢকেে রাখে, প্রতি দফায় প্রতীক গোপনে নাম বদলানো করে, আর Bob এলোমলেো স্থানীয় সীমাবদ্ধতা—সারি, স্তম্ভ, বাক্স বা যন্ত্র—খুলে যাচাই করে। সব-ভন্নি ঠকি থাকলে আস্থা বাড়ে; তারপর আবার আবৃত করা, নতুন নামবদল।

ধ্রুপদি প্রোটোকল সূত্র কোষ কীভাবে সামলায়

নামবদলরে একটি ব্লাইন্ড spot আছে। সারি/স্তম্ভ/বাক্স নয়িম "সব প্রতীক আলাদা"—permutation-এর পরওে সত্য। কন্তিু সূত্র বলে "এই কোষ ঠকি 5"। নামবদল σ করলে Bob শুধু $\sigma(5)$ দখেে; σ না জানলে printed 5 যাচাই করতে পারে না।

দুইটি মানক সংশোধন আছে।

প্যালটে কৌশল. গোপন grid-এর পাশে জনসাধারণরে নর্িদশে দওেয়ায় 1…N প্রতীক-সহ অতরিক্তি প্যালটে সারি রাখা হয়, সটেওি একই σ দিয়ে নাম বদলানো করা হয়। Bob-এর চ্যালঞ্জে প্যালটে + একটি সূত্র কোষ খুলতে পারে। প্যালটে থকেে সে সইে দফার σ বুঝে সূত্র-তে $\sigma(5)$ আছে কনি া যাচাই করে। σ প্রতি দফা নতুন; গোপন কোষ সম্পর্কে নতুন তথ্য দয়ে না।

সূত্র compile করে অসমতা বানানো। সূত্র কোষকে সব প্যালটে প্রতীকরে সঙ্গে "ভন্নি" সীমাবদ্ধতায় সংযোগ করুন, শুধু তার উদ্দশ্যেকৃত মান বাদে। তখন একমাত্র আইনগত প্রতীক সূত্ররর মান। সব সীমাবদ্ধতা আবার নামবদল-invariant "ভন্নি" রূপে ফরিে আসে।

ভোত কার্ড প্রোটোকলরে আরকে রূপভদেে সূত্র কার্ড শুরুতইে মুখ-up দখোনো হয়; সারি/স্তম্ভ/বাধা packet shuffle করে অবস্থান তথ্য লুকয়িে সব-প্রতীক যাচাই করা হয়।

শক্ষিা একই: শূন্য-জ্ঞান হলো কোন তথ্য hiding-এর পরে টকিে থাকা করে তার সতর্ক হসিাবরক্ষণ। নামবদল "সব ভন্নি" বাঁচায়, "equals 5" মুছে দয়ে; তাই দ্বতিীয় তথ্য অন্য প্রক্রয়িায় ফরিয়িে আনতে হয়।

এই পারস্পরকি চত্রি গবষেণাপত্ররে বাস্তব প্রোটোকল নয়; ধ্রুপদি শূন্য-জ্ঞান অন্তর্দৃষ্টি:

- Alice–Bob প্রোটোকল-forth করে।
- Bob এলোমেলো যাচাই বেছে নেয়।
- Alice স্থানীয় সামঞ্জস্য দেখায়, সাক্ষ্য নয়।
- গোপনীয়তা প্রমাণ বলে Bob-এর দৃষ্টিভঙ্গি গোপন ছাড়াই সিমুলেটর তৈরি করতে পারত।

ধ্রুপদি দাবি তাই ধনাত্মক:

> **সিমুলেটর সত্যই আছে।**

এখন comfortable বৈশিষ্ট্য সরিয়ে দিন: Alice একটি-বার্তা প্রমাণ পাঠায়; বিনিময় নেই; ভুল ধাঁধা কখনো গ্রহণ করা যাবে না। ধ্রুপদি শূন্য-জ্ঞান এখানে টিকে থাকা করে না।

এবার **নিয়মপুস্তক** সংশোধন করুন: logician-এর আনুষ্ঠানিক প্রমাণ ব্যবস্থা—স্বতঃসিদ্ধ + যান্ত্রিক প্রমাণ-checking নিয়ম। ZFC প্রচলিত উদাহরণ। এখানে "প্রমাণ ব্যবস্থা" মানে Alice-এর বার্তা প্রোটোকল নয়; আনুষ্ঠানিক গাণিতিক নিয়মপুস্তক।

ছদ্মলক্ষ্য D: ভুল, কিন্তু সংক্ষিপ্ত প্রমাণে খণ্ডন করা কঠিন

বাস্তব MegaSudoku-কে **S** বলি। একই displayed format-এর আরেকটি সীমাবদ্ধতা ব্যবস্থা বানাই, **D**। D বাস্তবে **অসন্তোষজনক**—তার বেধে পূরণ নেই। Toy উদাহরণ "X সত্য এবং X ভুল" হতে পারে, কিন্তু সেটি খুব সহজে খণ্ডন করা যায়; তাই উপযোগী D আরও subtle।

D এমন পরিবার থেকে আসবে যার অসন্তোষজনকতা নির্বাচিত নিয়মপুস্তক **সংক্ষিপ্ত প্রমাণে নিশ্চিত করতে পারে না**। যদি নিয়মপুস্তক দ্রুত D খণ্ডন করতে পারে, সিমুলেটর পথ formally বন্ধ প্রমাণ হয়ে যাবে এবং কার্যকর গোপনীয়তা পতন করবে।

Alice-এর একটি-বার্তা প্রমাণ বিবৃতি:

> **S সন্তোষজনক অথবা D সন্তোষজনক।**

D বাস্তবে ভুল। নিখুঁত যথার্থতা বলে ভুল disjunction বেধে প্রমাণ পেতে পারে না। তাই প্রমাণ গ্রহণ করা হলে S সত্য হওয়া বাধ্যতামূলক। ছদ্মলক্ষ্য ভুল S-কে সত্য বানাতে পারে না।

কিন্তু গোপনীয়তা-শৈলী বিবেচনামূলক চিন্তায় প্রতিকল্পিত ভাবুন: D-র যদি সাক্ষ্য থাকত, সেই সাক্ষ্য দিয়ে বাস্তব S-এর গোপন না জেনেই প্রমাণ তৈরি করা যেত—অর্থাৎ সিমুলেটর পথ থাকত। বাস্তবে D অসন্তোষজনক, তাই পথ নেই। **কিন্তু নিয়মপুস্তক দক্ষ প্রমাণে পথ-টি নেই—এ কথা দেখোতে পারে না।**

D-র দুই কাজ:

- **যথার্থতা:** D ভুল, তাই গৃহীত "S or D" প্রমাণ S-কে বল করে।
- **কার্যকর শূন্য-জ্ঞান:** D খণ্ডন করা প্রমাণ-তাত্ত্বিকভাবে কঠিন, তাই নিয়মপুস্তক সিমুলেটরের অসম্ভবতা দ্রুত নিশ্চিত করতে পারে না।

ধ্রুপদি প্রশ্ন:

> সিমুলেটর কি সত্যই আছে?

নতুন প্রশ্ন:

> নির্বাচিত নিয়মপুস্তক কি দক্ষভাবে প্রমাণ করতে পারে যে সিমুলেটের অসম্ভব?

দ্বিতীয়টি দুর্বলতর। এই দুর্বলতাই একটি বার্তা + না বিন্যাস + নিখুঁত যথার্থতা রাখতে সাহায্য করে।

নতুন পরীক্ষা: সিমুলেটের নেই—এ কথা আপনি কি প্রমাণ করতে পারেন?

কার্যকর অর্থে শূন্য-জ্ঞানে সিমুলেটের **বাস্তবে নেই**—গবেষণাপত্র এটি লুকায় না। কিন্তু স্থির নিয়মপুস্তক দক্ষভাবে তার nonexistence প্রমাণ করতে পারে না। যদি কোনো খারাপ পর্যবেক্ষণযোগ্য পরিণতি ঘটলে সেই পরিণতি থেকেই সংক্ষিপ্ত খণ্ডন তৈরি করা যেত, তাহলে সংক্ষিপ্ত খণ্ডন না থাকার কারণে খারাপ পরিণতি-টিও ঘটতে পারে না—অন্তত উপপাদ্য যে পরীক্ষা শ্রেণি আবৃত করে সেখানে।

এইখানে Gödel ফেলো connection আসে। “Gödel ফেলো crypto নির্ভরযোগ্য করে” এমন জাদু স্লোগান নয়; connection **প্রমাণ জটিলতা**।

একটি প্রমাণ ব্যবস্থা **সর্বোত্তম** হলে, প্রাসঙ্গিক সূত্র পরিবার-তে অন্য কোনো প্রমাণ ব্যবস্থা সংক্ষিপ্ত খণ্ডন দিলে সর্বোত্তম ব্যবস্থা-ও polynomially দীর্ঘতর প্রমাণে তা দিতে পারে। Krajíček ও Pudlák 1989 সালে অনুমানপ্রস্তাব করেন যে **কোনো সর্বোত্তম প্রমাণ ব্যবস্থা নেই**। অর্থাৎ যেকোনো স্থির নিয়মপুস্তকের তুলনায় কোনো অন্য নিয়মপুস্তক কিছু সত্য/অসন্তোষজনক পরিবারকে অনেক succinctly প্রমাণ করা/খণ্ডন করতে পারে। এটি Gödel ফেলো অসম্পূর্ণতার সীমা, জটিলতা-তাত্ত্বিক cousin: স্থির নিয়মপুস্তক কিছু truth-এর জন্য সংক্ষিপ্ত প্রমাণ হারায়।

গবেষণাপত্র এই অনুমানপ্রস্তাবের একটি মানক “infinitely প্রায়ই” ধরনের শক্তিশালী রূপ ধরে নেয়ে করে। Krajíček–Pudlák উপপাদ্য থেকে তখন নির্দিষ্ট প্রাপ্তি আসে: প্রতিটি নিয়মপুস্তকের জন্য দক্ষভাবে উৎপাদনযোগ্য এমন অসন্তোষজনক সূত্র ক্রম আছে যেগুলোর সংক্ষিপ্ত খণ্ডন নিয়মপুস্তকে নেই। **দক্ষভাবে উৎপাদনযোগ্য** হওয়া অত্যন্ত গুরুত্বপূর্ণ—Alice ছদ্মলক্ষ্য D অ্যালগরিদমিকিভাবে বানাতে পারে, অস্তিত্ব উপপাদ্য থেকে জাদুকরী বস্তু চাইতে হয় না।

নির্মাণ কী করছে

আকৃতি-টি আবার সংক্ষিপ্তভাবে:

1. একটি নিয়মপুস্তক সংশোধন করুন—ধরা যাক ZFC।
2. প্রমাণ-জটিলতা অনুমান থেকে দক্ষভাবে উৎপন্ন কঠিন-অসন্তোষজনক D নিন।
3. বাস্তব NP/SAT বিবৃতি S-এর জন্য একটি-বার্তা প্রমাণ বানান: **S or D** সন্তোষজনক।
4. D বাস্তবে অসন্তোষজনক; নিখুঁত যথার্থতা তাই গৃহীত প্রমাণে S সত্য বলে করে।
5. প্রতিকল্পিত D সাক্ষ্য থাকলে প্রমাণ সিমুলেট করা যেত। D-র সাক্ষ্য বাস্তবে নেই, কিন্তু নিয়মপুস্তক তার অনুপস্থিতি সংক্ষিপ্ত প্রমাণে দেখাতে পারে না।
6. ফলে সিমুলেটের অস্তিত্ব থেকে যে **খণ্ডনযোগ্য গেম-ভিত্তিক নিরাপত্তা বৈশিষ্ট্য** আনুষ্ঠানিকভাবে অনুসরণ করে, সেই বৈশিষ্ট্য ভাঙার দক্ষ আক্রমণ থাকলে সেটি নিয়মপুস্তকে অনুপস্থিতি সংক্ষিপ্ত খণ্ডন তৈরি করত। বিরোধ।

ব্যবস্থা গোপন “ধ্রুপদি সিমুলেটের” দিয়ে লুকায় না; পর্যবেক্ষণযোগ্য নিরাপত্তা পরীক্ষাগুলোর জন্য সিমুলেটের অনুপস্থিতি—এই তথ্য দক্ষভাবে উন্মুক্ত করতে নিয়মপুস্তকের অক্ষমতাকে আবৃত করা হিসেবে ব্যবহার করে।

গবেষণাপত্র কী দাবি করে

প্রধান উপপাদ্য অনুমান-নির্ভর।

ক্রিপ্টোগ্রাফিক দিকে দরকার **অ-পারস্পরিক সাক্ষ্য পার্থক্যহীন (NIWI) proofs**—ভালো ভাবে-studied মৌলিক ক্রিপ্টোগ্রাফিক উপাদান, বিভিন্ন প্রতিষ্ঠিত অনুমান প্যাকেটে থেকে পাওয়া যায়। প্রমাণ-জটিলতা দিকে দরকার **না (infinitely প্রায়ই) সর্বোত্তম প্রমাণ ব্যবস্থা** অনুমানপ্রস্তাব।

এই অনুমানগুলোর অধীনে, **প্রতিটি নির্বাচিত নিয়মপুস্তকের জন্য** NP/SAT-এ একটি-বার্তা, না-বিশ্বাস, **সম্পূর্ণভাবে শব্দ** প্রমাণদাতা/যাচাইকারী তৈরি করা যায় যা ওই নিয়মপুস্তকের আত্মীয় **কার্যকর অর্থে শূন্য-জ্ঞান**।

বিস্তৃততর বিবৃতি—ধ্রুপদি শূন্য-জ্ঞানের খণ্ডনযোগ্য, গেম-ভিত্তিক পরিণতি বৈশিষ্ট্য-by-বৈশিষ্ট্য পুনরুদ্ধার করা—পেতে গবেষণাপত্র আরও একটি মানক derandomisation বিশ্বাস ব্যবহার করে: **P = BPP** (প্রায়, দক্ষ এলোমেলো তা কম্পিউটেশনাল ক্ষমতা fundamentally বাড়ায় না)।

উপপাদ্য ভাষার বাইরে:

- প্রমাণ একটি বার্তা;
- বিশ্বস্ত বিন্যাস নেই;
- ভুল বিবৃতির বিধে প্রমাণ নেই;
- ধ্রুপদি শূন্য-জ্ঞান সিমুলেটর নেই;
- কিন্তু ধ্রুপদি ZK থেকে যে খণ্ডনযোগ্য নিরাপত্তা বৈশিষ্ট্য উৎপন্ন করা যায়, সেই বৈশিষ্ট্য **একটি করে** এই বিন্যাসে achieve করা যায়।

"খণ্ডনযোগ্য" শব্দটি গুরুত্বপূর্ণ: ব্যর্থতা adversary গেম চালিয়ে শনাক্ত করা যায়—distinguish, invert, সাক্ষ্য পুনরুদ্ধার করা, নির্দিষ্ট গেমে সাফল্য ইত্যাদি।

একটি **একক প্রমাণদাতা** আক্ষরিক অর্থে সব খণ্ডনযোগ্য বৈশিষ্ট্য একসঙ্গে পাবে—গবেষণাপত্র তা দাবি করে না; সম্ভবত সেটি অসম্ভব। কারণ এক-বার্তার প্রমাণ পুনর্ব্যবহারযোগ্য, আর "প্রমাণটি অন্য কাউকে দেখানো যাবে না" নিজেই এমন একটি খণ্ডনযোগ্য বৈশিষ্ট্য যা এখানে ব্যর্থ হয়। লেখকদের আরও অনুমাননির্ভর বক্তব্য হলো, ব্যবহারিক ক্রিপ্টোগ্রাফিতে ব্যবহৃত **স্বাভাবিক** খণ্ডনযোগ্য বৈশিষ্ট্যগুলো একটি একক প্রমাণদাতার মধ্যে ধরা যেতে পারে—এই অংশটি শর্তসাপেক্ষ ও অনুমানমূলক, এবং "স্বাভাবিক" শব্দটিও এখানে অনানুষ্ঠানিক।

একটি নির্দিষ্ট corollary: একরূপ প্রমাণদাতা-সহ অ-পারস্পরিক **সাক্ষ্য-hiding** প্রমাণ—"ধাঁধা solvable প্রমাণ পেলেও দ্রবণ খুঁজতে সাহায্য হয় না"—মথিস্ক্রিয়া বা বিন্যাস ছাড়া, এমন বস্তু বহুদিন নির্মাণ resist করেছিল।

এটি কী বলে না

- ধ্রুপদি অসম্ভবতা উপপাদ্য ভুল—**না**। সংজ্ঞা বদলে পথ বের করা হয়েছে।
- না মথিস্ক্রিয়া + না বিন্যাস + নিখুঁত যথার্থতা সহ সাধারণ ধ্রুপদি শূন্য-জ্ঞান—**না**। গবেষণাপত্র স্পষ্ট বলে constructed প্রমাণদাতার সিমুলেটর নেই।
- প্রমাণ reusable নয়—না; একটি-বার্তা প্রমাণ অন্যকে দেখানো যায়। Deniability-শৈলী বৈশিষ্ট্য সংরক্ষিত নয়।
- ব্যবহারের জন্য প্রস্তুত internet প্রোটোকল—না। এটি জটিলতা তত্ত্ব ও ক্রিপ্টোগ্রাফিক ভিত্তিগতের শর্তসাপেক্ষ নির্মাণ।
- "Gömußo ফলো উপপাদ্য password নির্ভরযোগ্য করে"—না। Connection সর্বোত্তম প্রমাণ ব্যবস্থা, সংক্ষিপ্ত খণ্ডন এবং প্রমাণ-তাত্ত্বিক অপ্রমাণযোগ্যতার মাধ্যমে।

তবু কেন এটি আকর্ষণীয়

ক্রিপ্টোগ্রাফি কঠিন সমস্যাকেই সম্পদে পরিণত করে। গুণনীয়কে বিশ্লেষণ কঠিন → RSA-ধরনের অনুমান। lattice সমস্যা কঠিন → lattice-ভিত্তিক ক্রিপ্টোগ্রাফি। এখানে কঠিনতার ধরন আলাদা: **গোপন মান গণনা করা কঠিন নয়; বরং কোনো সিমুলেটর নেই—এই অস্তিত্বকে সংক্ষিপ্ত প্রমাণে প্রতিষ্ঠা করাই কঠিন।**

স্বতঃসিদ্ধ/নিয়মপুস্তককে ক্রিপ্টোগ্রাফি সম্পদের মতো ধরে নেওয়া অস্বাভাবিক। ধ্রুপদি টান ছিল যথার্থতা বনাম সিমুলেশন। Ilango সেই টানকে প্রমাণ-তাত্ত্বিক curtain-এর পিছনে রাখে: সিমুলেটর নেই, কিন্তু আনুষ্ঠানিক ব্যবস্থা তার অনুপস্থিতি দৃক্‌ষভাবে উন্মুক্ত করতে পারে না।

ব্যবহারিক শূন্য-জ্ঞান ব্যবস্থা কাল বদলে যাবে না। ধারণাগত মানচিত্র বদলায়: গাণিতিক অপ্রমাণযোগ্যতা শুধু সীমাবদ্ধতা নয়; সতর্কভাবে নির্ধারিত নিরাপত্তা বৈশিষ্ট্যের জন্য আবৃত করা হতে পারে।

প্রমাণ কতটা শক্তিশালী?

এটি উপপাদ্য গবেষণাপত্র; “প্রমাণ” মানে প্রতিলিপি নয়, definitions + অনুমানগুলো + প্রমাণ শৃঙ্খল। আনুষ্ঠানিক ফল শর্তসাপেক্ষ এবং অনুমানগুলো স্পষ্ট।

- NIWI মানক ক্রিপ্টোগ্রাফি বস্তু এবং একাধিক প্রতিষ্ঠিত অনুমান প্যাকেটে থেকে পাওয়া যায়।
- না-সর্বোত্তম-প্রমাণ-ব্যবস্থা অনুমানপ্রস্তাব প্রমাণ জটিলতার কেন্দ্রীয় উন্মুক্ত অনুমানপ্রস্তাব।
- P = BPP বিস্তৃততর খণ্ডনযোগ্য-বৈশিষ্ট্য উপপাদ্যের জন্য মানক derandomisation বিশ্বাস।

গবেষণাপত্র আরও converse দেয়: এই ধরনের নির্মাণ অস্তিত্ব থাকা করলে NIWI-এর মতো মৌলিক ক্রিপ্টোগ্রাফি উপাদান দরকার, এবং মানক একটি-way-কার্য অনুমানের সঙ্গে না-সর্বোত্তম-প্রমাণ-ব্যবস্থা শর্ত essentially ফিরে আসে। অর্থাৎ অনুমানগুলো ইচ্ছামতো অলংকরণ নয়; ফলের সঙ্গে গভীরভাবে tied।

তবুও শর্তসাপেক্ষ মানে শর্তসাপেক্ষ। অনুমানপ্রস্তাব ভুল হলে ব্যাখ্যা বদলাবে। আর অনুমানগুলো সত্য হলেও নিশ্চিয়তা **ধ্রুপদি ZK নয়**—relaxed প্রমাণ-তাত্ত্বিক notion।

সঠিক আস্থা বিভক্ত করা:

- সুসংগত শর্তসাপেক্ষ উপপাদ্য হিসেবে **উচ্চ**;
- অনুমানগুলো আমাদের কম্পিউটেশনাল জগতে সত্য—**মাঝারি**;
- তাৎক্ষণিক ব্যবহারিক ব্যবহারিক মোতায়নে—**কম**।

কেন এটি গুরুত্বপূর্ণ

ধ্রুপদি মানচিত্র বলত: বিশ্বাস ছাড়া অ-পারস্পরিক সম্পূর্ণ ZK এবং নিখুঁত যথার্থতা—বন্ধ রাস্তা। এই গবেষণাপত্রে বলা হয়েছে, যদি objective বদলে পর্যবেক্ষণযোগ্য/গেম-ভিত্তিক পরিণতি ধরে এবং নিরাপত্তাকে নিয়মপুস্তকের দক্ষ খণ্ডন ক্ষমতার আত্মীয় করা হয়, তাহলে উপযোগী আচরণের বড় অংশ ফিরে পাওয়া যায়।

এটি শুধু wording tweak নয়। “কী বস্তু সত্যিই আছে?” প্রশ্নের পাশে “স্থির আনুষ্ঠানিক ব্যবস্থা কী দক্ষভাবে নিয়ম বাইরে করতে পারে?”

প্রশ্নকে ক্রিপ্টোগ্রাফিক নিশ্চয়তার অংশ বানায়।

এক অর্থে গবেষণাপত্রের শিক্ষা:

> "গোপন ফাঁস করেনি" এই সবচেয়ে শক্তিশালী সিমুলেশন বিবৃতি পাওয়া যায় না; কিন্তু "এই নিয়মপুস্তক দক্ষভাবে এমন আক্রমণ নিশ্চিত করতে পারবে না" শর্ত অনেক পরীক্ষায়োগ্য সুরক্ষা পুনরুদ্ধার করার জন্য যথেষ্ট হতে পারে।

এই কারণেই title-এ Gömülü ফোলোর নাম শুধু ornament নয়।

সংক্ষিপ্ত সারাংশ

ধ্রুপদি শূন্য-জ্ঞান প্রমাণদাতা গোপন সাক্ষ্য না দেখিয়ে বিবৃতি সত্য প্রমাণ করে, এবং গোপনীয়তা একটি বাস্তব সিমুলেটরের অস্তিত্ব দিয়ে আনুষ্ঠানিকভাবে সংজ্ঞায়িত হয়। ধ্রুপদি অসম্ভবতা ফল বলে না বিশ্বাস, একটি বার্তা ও নখিঁুত যথার্থতার বিশ্বাসে সম্পূর্ণ ZK রাখা যায় না। Rahul Ilango সংজ্ঞা দুর্বল করে **কার্যকর অর্থে শূন্য-জ্ঞান** প্রস্তাব করেন: সিমুলেটর সত্যই আছে দাবি না করে, নির্বাচিত আনুষ্ঠানিক প্রমাণ ব্যবস্থা দক্ষভাবে প্রমাণ করতে পারে না যে সিমুলেটর নেই—এটাই চাওয়া হয়। খণ্ডন করা কঠিন অসন্তোষজনক ছদ্মলক্ষ্য সূত্র D ব্যবহার করে প্রমাণ "S or D" বানানো হয়; D ভুল হওয়ায় নখিঁুত যথার্থতা S-কে বল করে, কিন্তু D-র অসন্তোষজনকতা সংক্ষিপ্ত প্রমাণে ধরা-ছোঁয়ার বাইরে হওয়ায় সিমুলেটর-পথরে অসম্ভবতাও নিয়মপুস্তক সহজে নিশ্চিত করতে পারে না। NIWI ও না-সর্বোত্তম-প্রমাণ-ব্যবস্থা অনুমানপ্রস্তাবের মতো প্রধান অনুমানের অধীনে ফল NP/SAT-এর জন্য একটি-বার্তা, না-বিশ্বাস, সম্পূর্ণভাবে শব্দ কার্যকর অর্থে-ZK প্রমাণ দেয় এবং খণ্ডনযোগ্য গেম-ভিত্তিক ZK পরিভাষা বিশেষিত্য-by-বিশেষিত্য পুনরুদ্ধার করে। এটি ধ্রুপদি ZK নয়, ব্যবহারের জন্য প্রস্তুত মৌলিক ক্রিপ্টোগ্রাফিক উপাদান নয়, এবং Gömülü ফোলো অসম্পূর্ণতা নিজে নিরাপত্তা প্রক্রিয়া নয়; এটি প্রমাণ-তাত্ত্বিক অপ্রমাণযোগ্যতাকে ক্রিপ্টোগ্রাফিক আবৃত করা হিসেবে ব্যবহার করা একটি শর্তসাপেক্ষ ভিত্তিগত ফল।

বাড়াবাড়ি ছাড়া যাচাই

গবেষণা যা দেখায়: বলা অনুমানগুলোর অধীনে যেকোনো স্থির নিয়মপুস্তকের আত্মীয় একটি-বার্তা, না-বিশ্বাস, সম্পূর্ণভাবে শব্দ কার্যকর অর্থে-শূন্য-জ্ঞান প্রমাণদাতা বানানো যায়; ধ্রুপদি ZK-এর খণ্ডনযোগ্য গেম-ভিত্তিক পরিভাষা বিশেষিত্য-by-বিশেষিত্য পুনরুদ্ধার করা যায়।

যা সম্ভাব্য কিন্তু unconditional নয়: প্রমাণ-জটিলতা ও ক্রিপ্টোগ্রাফিক অনুমানগুলো সত্য। এগুলো গুরুতর, কেন্দ্রীয় অনুমান; উপপাদ্য converse দেখায় এগুলো ফলের সঙ্গে tightly সংযুক্ত।

যা দেখায় না: প্রচলিত শূন্য-জ্ঞান প্রমাণ, ব্যবহারকিভাবে মোতায়েনযোগ্য প্রোটোকল, প্রমাণের পুনর্ব্যবহার-অযোগ্যতা বা অস্বীকারযোগ্যতা, কিংবা "Gödel-এর উপপাদ্য নিজে থেকেই গোপন তথ্য সুরক্ষিত করে"—এসবের কোনোটিই গবেষণাপত্রটি দেখায় না।

মূল সীমাবদ্ধতা: Relaxed সংজ্ঞা; একাধিক প্রধান অনুমানগুলো; সর্বজনীন একক-প্রমাণদাতা দাবি partly conjectural; ভিত্তিগত rather than ব্যবহারিক।

সাধারণ পাঠকের আস্থা: শর্তসাপেক্ষ তত্ত্ব ফল হিসেবে উচ্চ। অনুমান-জগৎ বাস্তব কিনা—মাঝারি। তাৎক্ষণিক প্রয়োগ—কম। নিরাপদ মূল কথা: গবেষণাপত্র অসম্ভবতা ভাঙে না; নিরাপত্তা-প্রাসঙ্গিক অংশের চারপাশে প্রমাণ-তাত্ত্বিক নতুন পথ বানায়।

উৎস

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