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

Криптографическое доказательство может скрывать секрет, делая отсутствие симулятора трудным для доказательства

Доказательства с нулевым разглашением позволяют доказать утверждение, не раскрывая witness. Классическая теория говорит, что в полном смысле это невозможно одновременно с одним сообщением, отсутствием доверенного setup и perfect soundness. Статья Рахула Иланго не отменяет эту невозможность. Она меняет цель: вместо требования, чтобы симулятор действительно существовал, достаточно, чтобы никакая выбранная система доказательств не могла эффективно доказать, что симулятора не существует. При сильных предположениях из теории сложности доказательств и криптографии этого хватает, чтобы по одному свойству за раз восстановить фальсифицируемые, игровые последствия zero-knowledge. Это не готовый интернет-примитив, а теоретико-доказательственный способ превратить математическую недоказуемость в криптографическое прикрытие.

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

Фокус не в том, чтобы доказать, что секрет скрыт

Начнем с самой простой версии нулевого разглашения.

Алиса хочет убедить Боба, что судоку имеет решение. Если она отправит само решение, Боб убедится — но головоломка будет испорчена. Ей нужно нечто более странное: доказательство того, что решение существует, без раскрытия самого решения.

Именно это обещает **доказательство с нулевым разглашением (zero-knowledge proof)**. Доказывающий (Алиса) убеждает проверяющего (Боба), что утверждение истинно, не раскрывая ничего, кроме самого факта его истинности.

Проблема в том, что у этого обещания есть цена. Обычное математическое доказательство обладает двумя удобными свойствами. Оно состоит из **одного сообщения**: вы записываете его, передаете и уходите. И оно имеет **совершенную надёжность против ложных утверждений (*perfect soundness*)**: для ложного утверждения вообще не существует корректного доказательства. Классические теоремы невозможности говорят, что доказательство с нулевым разглашением должно отказаться от обеих характеристик — и не только от их сочетания: каждая по отдельности тоже недоступна.

Во-первых, доказательство с нулевым разглашением требует взаимодействия. Если Алиса посылает одно сообщение и нет заранее организованной доверенной настройки, гарантия нулевого разглашения рушится — независимо от того, насколько вы готовы ослабить требование надёжности взамен.

Во-вторых, нулевое разглашение требует небольшой допустимой вероятности ошибки. Требование совершенной надёжности незаметно уничтожает и взаимодействие: если проверяющего невозможно обмануть ни при каком наборе его случайных выборов, он мог бы просто зафиксировать эти выборы заранее. А как только проверяющий становится предсказуемым, Алиса может ответить на все одним сообщением — то есть мы возвращаемся именно к случаю, который уже невозможен.

Статья Рахула Иланго предлагает способ обойти эту двойную стену — не отрицая её существования и не пытаясь построить классическое доказательство с нулевым разглашением там, где оно невозможно. Ход тоньше: ослабить значение фразы «ничего не раскрывает», но так, чтобы сохранить те свойства безопасности, которые криптографы действительно могут проверять.

Результат называется **эффективным нулевым разглашением (effectively zero-knowledge)**.

A proof without leaking the witness

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

blocked door 1

interaction

blocked door 2

trusted setup

blocked door 3

imperfect soundness

the route

the rulebook cannot efficiently refute the simulator

Boundary: not classical zero-knowledge; effectively zero-knowledge under a chosen proof system.

Для нулевого разглашения закрыты тремя дверями — взаимодействием, доверенной настройкой и несовершенной надёжностью. Конструкция Иланго идет другим путем: выбранная формальная система не может эффективно опровергнуть существование симулятора.

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.

classical zero-knowledge

positive claim

A simulator exists and can fake the verifier's view without the witness.

effectively zero-knowledge

weaker claim

Your chosen proof system cannot efficiently prove that no simulator exists.

Boundary: the construction preserves testable consequences, not the full simulator guarantee.

Классическое доказательство с нулевым разглашением спрашивает, существует ли симулятор;

«эффективное нулевое разглашение» спрашивает только, может ли выбранная формальная система эффективно доказать, что симулятора не существует. Именно более слабый вопрос позволяет конструкции сохранить одно сообщение, отсутствие предварительной настройки и совершенную надёжность.

Original diagram — The Clean Paper CC BY 4.0

Старый критерий: симулятор существует

Классическое формальное определение нулевого разглашения использует воображаемого помощника — **симулятор**.

Идея такова. Представим Джейн, которая **не** знает секрета Алисы. Если Джейн может самостоятельно генерировать доказательства, выглядящие так же, как доказательства, которые Боб получил бы от Алисы, то доказательства Алисы не научили Боба ничему новому. Джейн уже могла подделать весь опыт без секрета Алисы.

Поэтому классическое доказательство с нулевым разглашением требует реального симулятора. Должен существовать эффективный алгоритм, способный генерировать правдоподобные «фальшивые» доказательства без знания секрета — **свидетеля** (*witness*) в терминологии области; для судоку такой свидетель — это просто полностью и правильно заполненная сетка.

Это сильное определение, но именно здесь срабатывает старая невозможность. Интуиция такова. Настоящее невзаимодействующее доказательство — просто строка. Как только Боб получил эту строку, он может показать ее кому-то еще: он приобрел способность убеждать других в утверждении, а это уже звучит как нечто большее, чем «ничего». Классические теоремы превращают эту интуицию в результаты невозможности, описанные выше.

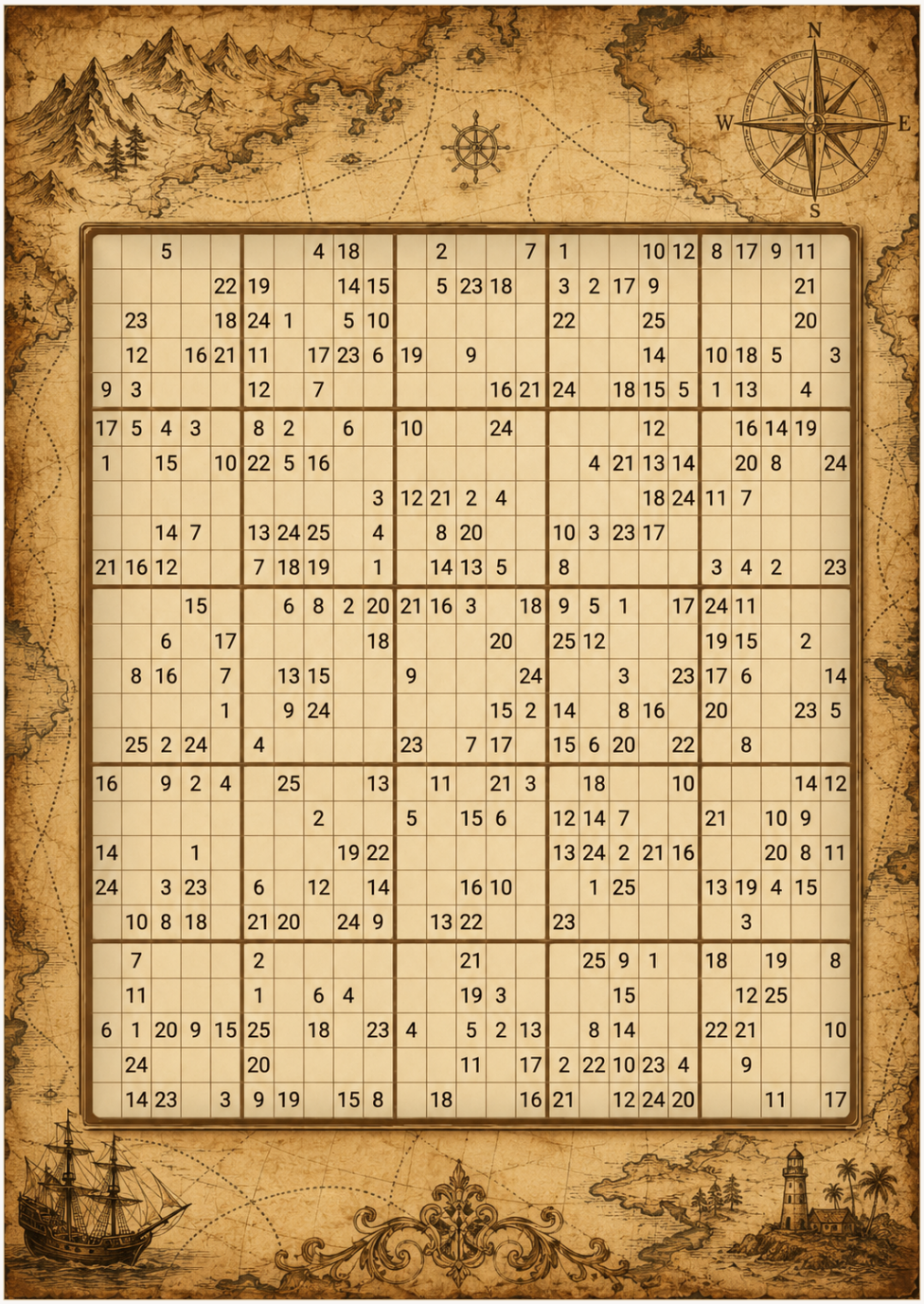
> **Три свойства, от которых эта статья не отказывается**
>
> Название работы прямо указывает на три ограничения:
> **Без взаимодействия:** Алиса посылает одну строку-доказательство. Нет протокола с обменом сообщениями туда и обратно.
> **Без настройки:** Алиса и Боб не полагаются на доверенную общую эталонную строку или другую заранее подготовленную публичную случайность. Многие системы, называемые «невзаимодействующими доказательствами с нулевым разглашением», всё равно требуют доверенной предварительной настройки; здесь её нет вообще.
> **Совершенная надёжность:** ложное утверждение не имеет ни одного корректного доказательства. Не «почти никогда не принимается», а «корректного доказательства не существует».
> Именно этими тремя свойствами обладает обычная письменная математика —

> и, как объяснялось выше, классическое доказательство с нулевым разглашением не может сохранить их вместе.

MegaSudoku как способ почувствовать разницу

Вот намеренно упрощенная аналогия.

Для серьезной части аналогии не стоит брать обычное судоку 9×9. Оно слишком мало и конечно: компьютер может просто решить его или доказать, что решения нет. Вместо этого представим семейство головоломок **MegaSudoku(n)**. Масштабируем обычное правило: выбираем размер блока n, задаем $N = n^2$ и строим сетку $N \times N$, разделенную на блоки $n \times n$, с N символами. Обычное судоку — лишь крошечный случай $n = 3$, $N = 9$: сетка 9×9, блоки 3×3 и девять символов. История о сложности доказательств начинается только тогда, когда n может расти, а сетка получает дополнительные гаджеты, заставляющие ее вести себя как формула SAT, переодетая в судоку. Формула SAT — это просто набор ограничений «да/нет»: можно ли присвоить переменным значения истина/ложь так, чтобы все ограничения выполнялись?



Судоку 25×25: его правила можно проверять, не раскрывая завершенную сетку — визуальная метафора доказательства, подтверждающего существование скрытого решения, то есть свидетель.

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

Судоку и SAT: одна головоломка в двух костюмах

Утверждение, что судоку может «вести себя как формула SAT», — не метафора. Перевод работает в обе стороны, и более простое направление можно записать полностью.

От судоку к SAT. SAT оперирует только истинностью/ложностью, поэтому введем

одну булеву переменную для каждой тройки (строка, столбец, значение): *x(r,c,v)* означает «клетка в строке *r*, столбце *c* содержит значение *v*». Судоку 4×4 (блоки 2×2, значения 1–4) требует 4·4·4 = 64 переменных; классическое 9×9 — 729. Каждое правило судоку превращается в набор клауз. (Клауза — это OR переменных или их отрицаний; вся формула является AND всех клауз.)
Каждая клетка содержит как минимум одно значение — одна клауза на клетку:

x(1,1,1) ∨ x(1,1,2) ∨ x(1,1,3) ∨ x(1,1,4)

Каждая клетка содержит не более одного значения — клауза «не оба» для каждой пары значений:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … и так далее для всех шести пар.

Каждая строка содержит каждое значение — для строки 1 и значения 3: как минимум один раз,

x(1,1,3) ∨ x(1,2,3) ∨ x(1,3,3) ∨ x(1,4,3)

и не более одного раза: ¬x(1,1,3) ∨ ¬x(1,2,3), и так далее для каждой пары клеток в строке.
Столбцы и блоки — те же наборы; меняется только группа клеток. Для верхнего левого блока и значения 2:

x(1,1,2) ∨ x(1,2,2) ∨ x(2,1,2) ∨ x(2,2,2)

плюс попарные клаузы «не оба».
Напечатанные подсказки — самая простая часть: каждая подсказка является клаузой из одной переменной. Напечатанная 3 в верхнем левом углу становится клаузой

x(1,1,3)

Конъюнкция (AND) всего этого выполнима тогда и только тогда, когда судоку имеет решение, а удовлетворяющее присваивание *и есть* решение: смотрим, какие x(r,c,v) истинны, и заполняем сетку. Для 9×9 это 729 переменных и несколько тысяч клауз — современный SAT-solver разбирается с ними за миллисекунды. Обратите внимание на клаузу подсказки x(1,1,3): она означает «эта клетка равна именно 3», а не «все эти клетки различны». Та же асимметрия ниже заставит нас использовать дополнительный трюк для клеток-подсказок.
От SAT к судоку. Статье нужно противоположное и более сложное направление: по *произвольной* формуле SAT построить mega-Sudoku, которое имеет решение тогда и только тогда, когда формула выполнима. Собственные правила судоку умеют говорить лишь «эти клетки все различны», поэтому произвольные логические ограничения нужно *сконструировать* — именно для этого нужны гаджеты. Гаджет — небольшой заранее спроектированный кластер клеток, по одному на каждую клаузу формулы, в котором выделенные клетки играют

роль переменных (символ в них кодирует истину или ложь), а внутренние ограничения спроектированы так, чтобы единственные допустимые заполнения соответствовали присваиваниям, удовлетворяющим эту клаузу. Это стандартная инженерия из доказательств NP-полноты; для обобщенного судоку ее реализовали Ято и Сэта в 2003 году.
Вместе оба направления говорят, что судоку N×N и SAT — одна и та же задача в двух костюмах. Именно это позволяет этой статье — и самой работе — говорить обо всем NP на языке сеток и символов.

Свидетель по-прежнему легко представить. Алиса знает полное корректное заполнение mega-Sudoku. Боб хочет убедиться, что такое заполнение существует, но Алиса не хочет его раскрывать. Если она отправит всю сетку, Боб убедится, но секрет исчезнет.

В классической версии протокола с нулевым разглашением Алиса и Боб взаимодействуют. Старый наглядный образ использует закрытые плитки. Алиса прячет решенную сетку, перед каждым раундом тайно переименовывает символы и позволяет Бобу проверить одно случайно выбранное локальное ограничение: строку, столбец, блок или гаджет. Если открытые клетки содержат все разные символы, доверие Боба растет. Затем все снова закрывают, а символы заново переименовывают. (Есть одна тонкость: заданные подсказки головоломки требуют отдельного трюка, потому что переименование скрывает и их. Примечание ниже объясняет, как классические протоколы это решают.)

Как классические протоколы на самом деле работают с клетками-подсказками

У трюка с переименованием есть слепая зона. Правила строки, столбца и блока все говорят «эти клетки попарно различны», а свойство *все различны* сохраняется при любом переименовании символов. Но подсказка говорит: «эта клетка содержит именно 5». После переименования Боб видит только $\sigma(5)$ — какой-то замаскированный символ — и не знает перестановку σ. Проверить ничего нельзя. Если это не исправить, Алиса могла бы доказать существование *какой-то* правильной сетки, полностью игнорируя напечатанные подсказки, а это ничего не доказывает о *данной* головоломке. В классической литературе есть два стандартных способа исправления.
Палитра. К скрытой сетке добавляют одну дополнительную строку из N клеток — палитру, которую Алиса заполняет символами 1…N в фиксированном публичном порядке, а затем переименовывает вместе со всем остальным, так что там оказываются $\sigma(1)$…$\sigma(N)$. Теперь у случайного вызова Боба появляется еще один вариант. Помимо строки, столбца, блока или гаджета он может выбрать **палитру плюс одну клетку-подсказку**. Алиса открывает обе; палитра показывает переименование этого раунда, а Боб проверяет, что клетка-подсказка содержит именно переименованную версию напечатанной подсказки. Нулевое разглашение сохраняется, потому что Боб узнает только σ — новую случайную перестановку для этого раунда, которая сама по себе ничего не дает, — и значение клетки, которое он уже знал из головоломки. Ничего о секретных клетках не

утекает, а симулятор может подделать такую картину, просто выбрав случайную σ. Надёжность сохраняется, потому что жульничающую Алису в каждом раунде ловят с фиксированной вероятностью, а раунды повторяют, пока вероятность ошибки не станет ничтожной.

Компиляция подсказок в ограничения. Более структурный вариант не добавляет специальную проверку, а устраняет необходимость в ней. Вместо того чтобы *проверять* значение подсказки, его заставляют выполняться через ограничения неравенства: клетку-подсказку соединяют со всеми клетками палитры, кроме той, которая несет ее собственное значение — «не равна $\sigma(1)$, не равна $\sigma(2)$, …, не равна всему, кроме $\sigma(5)$». Единственным символом, который эта клетка может законно содержать, остается нужный. Все ограничения снова имеют форму «эти две клетки различны» — они инвариантны к переименованию и проверяются так же, как строка. Именно такой прием используют для заранее окрашенных вершин в классическом протоколе раскраски графа; он передает и смысл слова *гаджеты* выше: в картине MegaSudoku-как-SAT подсказки компилируются в гаджеты неравенства так же, как все остальные ограничения.

Физический протокол. Реальный карточный протокол для судоку (Gradwohl, Naor, Pinkas и Rothblum, 2007) вообще не использует переименование и фиксирует подсказки еще до начала сокрытия. Для каждой клетки Алиса выкладывает три одинаковые карты со значением клетки — рубашкой вверх для секретных клеток, но **лицом вверх для клеток-подсказок**, чтобы Боб собственными глазами видел соблюдение подсказок до того, как карты перевернут. Затем одна карта из каждой клетки идет в пакет ее строки, одна — в пакет столбца, одна — в пакет блока; каждый пакет перемешивают и открывают, а Боб проверяет, что он содержит все N символов. Перемешивание разрушает информацию о позициях — это и обеспечивает нулевое разглашение, — но подсказки уже были зафиксированы при раскладке.

В любом варианте урок тот же, к которому эта статья постоянно возвращается: протокол с нулевым разглашением — это тщательный учет того, *какие именно* факты переживают сокрытие. Переименование сохраняет «все различны» и стирает «равно 5», поэтому «равно 5» нужно вернуть другим способом.

Это не протокол из самой статьи. Это лишь мысленная модель классического доказательства с нулевым разглашением:

- Алиса и Боб обмениваются сообщениями.
- Боб выбирает случайные проверки.
- Алиса раскрывает только локальную согласованность, а не все решение.
- Доказательство приватности состоит в том, что картину, которую видит Боб, можно было бы сгенерировать без знания секретного решения Алисы.

Итак, классическое доказательство с нулевым разглашением построено вокруг положительного факта:

> Симулятор действительно существует.

Теперь уберем удобные части. Алиса посылает одну строку-доказательство и уходит. Нет доверенной предварительной настройки, нет общей случайной строки, подготовленной заранее, а Боб никогда не должен принимать ложную головоломку. Именно в такой среде классическое доказательство с нулевым разглашением не выживает.

Перед самим трюком нужен еще один персонаж. Зафиксируем **книгу правил**: формальную систему доказательств в логическом смысле — фиксированный набор аксиом плюс механические правила проверки письменных математических доказательств. Канонический пример — ZFC, стандартная система аксиом математики. Все дальнейшее формулируется относительно заранее выбранной книги правил, но выбор гибок: конструкция работает для любой фиксированной формальной системы, включая ZFC.

(Терминологическое примечание, взятое из самой статьи: «система доказательств» (*proof system*) здесь всегда означает именно такую книгу правил — формальную систему, проверяющую математические доказательства, — а не сообщения, которые посылает Алиса. Механизмы Алисы и Боба называются «доказывающим» и «проверяющим».)

Версия в стиле Гёделя сохраняет историю про mega-Sudoku, но меняет само доказательство.

Выберем вторую систему ограничений такого же отображаемого размера и назовем ее **D**. В нашей истории S и D — две головоломки MegaSudoku(n) одного формата. За кулисами D могла начинаться как сложная логическая формула другого размера; при необходимости ее можно дополнить безвредными фиктивными ограничениями, чтобы она помещалась в такую же сетку. D строится из логической формулы, которая на самом деле **невыполнима**: не существует присваивания значений, удовлетворяющего всем ее ограничениям, так же как сломанная головоломка не имеет законно заполненной сетки. Игрушечный пример — формула, одновременно требующая «X истинно» и «X ложно». Значит, D не имеет правильного заполнения.

Но D не должна быть сломанной головоломкой, которую *легко разоблачить*. Игрушечный пример не подходит: любая формальная система опровергнет «X и не-X» одной строкой. D должна быть ложной так, чтобы выбранная книга правил не могла сертифицировать это коротким аргументом. Если бы она могла коротко опровергнуть D, вся конструкция ниже развалилась бы: альтернативный путь, который мог бы позволить генерировать доказательства без секрета Алисы, формально исключался бы, а вместе с ним исчезла бы гарантия приватности. Поэтому D берут из семейства, которое фиксированная книга правил не может эффективно опровергнуть: внутри этой системы нет короткого доказательства того, что D не имеет решения.

Односообщенческое доказательство Алисы теперь касается дизъюнкции:

> либо настоящее mega-Sudoku S имеет решение, либо приманка D имеет решение.

Вот логическая связь. D **не** генерируется каким-то магическим способом, который

делает S истинной. Доказательство не утверждает «D не имеет решения, значит S имеет решение». Оно доказывает дизъюнкцию **S или D**. Совершенная надёжность означает, что ложная дизъюнкция не может иметь корректного доказательства. Поскольку в реальности D ложна — решения нет, — единственный способ, чтобы дизъюнкция была истинной, состоит в истинности S. Значит, если доказательство принято, S должна иметь решение. Приманка не может превратить ложную S в истинную.

Но для части, отвечающей за нулевое разглашение спросим, что произошло бы, если бы D *имела* решение. Такое решение-приманка было бы альтернативным свидетелем. Оно позволило бы генерировать доказательства, не зная настоящего решения mega-Sudoku Алисы — то есть дало бы симулятор. В реальности D решения не имеет, поэтому этот путь симуляции закрыт. Суть в том, что книга правил не может эффективно доказать, что он закрыт.

Итак, D выполняет две работы. Для **надёжности** D ложна, поэтому корректное доказательство «S или D» заставляет S быть истинной. Для **эффективного нулевого разглашения** D трудно опровергнуть, поэтому книга правил не может быстро исключить путь через приманку, который сделал бы симуляцию возможной.

Поэтому тест безопасности теперь не такой:

> Можем ли мы доказать, что симулятор действительно существует?

Вместо этого он становится таким:

> Может ли ваша книга правил эффективно доказать, что симулятор невозможен?

Если ответ «нет», следует нечто неожиданно сильное: каждая гарантия безопасности, которая (а) наблюдается путем выполнения теста и (б) внутри этой книги правил доказанно следует из существования симулятора, на самом деле выполняется. Успешная атака на любую из них сама стала бы тем недостающим коротким опровержением — а такого короткого опровержения нет. Именно это означает «effective» в эффективном нулевом разглашении.

Итак, учебное противопоставление выглядит так:

Классическое доказательство с нулевым разглашением: доказательства безопасны, потому что симулятор существует.

Эффективное нулевое разглашение в стиле Гёделя: для наблюдаемых тестов безопасности доказательства ведут себя как безопасные, потому что книга правил не может эффективно доказать, что симулятор невозможен.

Второе утверждение слабее. Но именно поэтому статья может сохранить три свойства, разрушавшие классическую версию: одно сообщение, отсутствие предварительной настройки и совершенную надёжность.

Новый критерий: вы не можете доказать отсутствие симулятора

Ослабление Иланго меняет сам вопрос.

Классическое доказательство с нулевым разглашением спрашивает:

> Существует ли симулятор?

Эффективное нулевое разглашение задаёт нечто более слабое:

> Может ли выбранная вами книга правил эффективно доказать, что симулятора не существует?

Это может звучать как техническая лазейка, но именно здесь центральная идея. Конструкция находится в странном состоянии: симулятора на самом деле **не существует** — статья говорит об этом прямо, — но зафиксированная вами книга правил не может эффективно доказать его отсутствие. Если каждый нежелательный результат, который вас интересует, требовал бы такого опровержения, система все равно ведет себя как система с нулевым разглашением относительно этих результатов.

Именно здесь появляется Гёдель. Не как украшение и не в смысле «Гёдель делает криптографию безопасной». Связь теоретико-доказательственная. Книгу правил называют **оптимальной**, если она в точном смысле является наилучшей возможной: когда любая формальная система может опровергнуть формулу нужного типа коротким доказательством, оптимальная тоже может это сделать, причем ее доказательство будет не более чем полиномиально длиннее. Крайичек и Пудлак в 1989 году выдвинули гипотезу, что **оптимальной системы доказательств не существует**: какую книгу правил ни зафиксируй, найдется другая, которая доказывает некоторое семейство истинных утверждений намного короче. Это одна из центральных открытых гипотез теории сложности доказательств и конечный, теоретико-сложностный родственник теоремы Гёделя о неполноте: некоторые истинные утверждения не имеют короткого доказательства в фиксированной вами системе — не потому, что их в принципе невозможно доказать, а потому, что каждая фиксированная книга правил оставляет некоторые коротко сформулированные истины без коротких доказательств.

Статья предполагает эту гипотезу — в немного более сильной форме «бесконечно часто», стандартной для криптографического использования гипотез. По теореме Крайичека и Пудлака выигрыш конкретен: для каждой книги правил существует последовательность формул, которые действительно невыполнимы, но которые эта система не может опровергнуть короткими доказательствами — и, что критически важно, эффективный алгоритм может их *генерировать*. Именно это последнее свойство, однородность (uniformity), превращает всю идею из утверждения о существовании в настоящий алгоритм, который может выполнять Алиса: ее приманки D сходят с конвейера, а не возникают из воздуха.

Криптографический ход состоит в том, чтобы использовать эту нехватку доказательной силы.

Что делает конструкция

Вот конструкция статьи в оголенном виде.

Зафиксируйте книгу правил — скажем, ZFC. При предположении из теории сложности доказательств существует эффективно генерируемая последовательность формул, которые на самом деле невыполнимы, но книга правил не имеет короткого доказательства их невыполнимости.

Теперь постройте односообщенческое доказательство такого типа:

> либо настоящее утверждение выполнимо, либо эта специальная сложная формула выполнима.

Специальная сложная формула невыполнима. Следовательно, если базовый механизм доказательства обладает совершенной надёжностью, принятие сообщения всё равно означает, что исходное утверждение истинно. Тем самым совершенная надёжность сохраняется.

Но для безопасности в духе нулевого разглашения представим, что специальная сложная формула *была бы* выполнимой. Тогда ее свидетель можно было бы использовать для симуляции доказательств без знания настоящего свидетеля. В действительности формула невыполнима — но книга правил не может эффективно это доказать. Значит, она не может эффективно доказать, что симулятор невозможен.

Именно это — шарнир всей конструкции. Система не скрывает секрет путем создания классического симулятора. Для большого класса наблюдаемых тестов безопасности она прячет секрет за неспособностью книги правил сертифицировать отсутствие симулятора.

Что утверждает статья

Главная теорема имеет несколько слоев. Ядро результата таково.

При стандартном криптографическом предположении — существовании **невзаимодействующих доказательств с неразличимыми свидетелями (non-interactive witness indistinguishable proofs)**, хорошо изученных объектов, следующих из нескольких устоявшихся наборов предположений, — и при гипотезе теории сложности доказательств, что **не существует (бесконечно часто) оптимальной системы доказательств**, статья для каждой выбранной книги правил строит односообщенческие доказывающий

и проверяющий для NP/SAT с **совершенной надёжностью**, без предварительной настройки и с эффективным нулевым разглашением относительно этой книги правил. (NP/SAT — стандартный «самый трудный общий знаменатель» задач-головоломок; mega-Sudoku — лишь один из его костюмов.)

Для более широкого утверждения о сохранении фальсифицируемых свойств безопасности статья добавляет еще одно стандартное предположение — гипотезу дерандомизации **P = BPP** (грубо говоря: случайность не дает алгоритмам принципиальной дополнительной силы).

Если перевести с языка теорем:

- Доказательство — одно сообщение.
- Доверенной предварительной настройки нет.
- Ложные утверждения невозможно доказать.
- Доказывающий не является классическим доказательством с нулевым разглашением — симулятора у него нет.
- Но в этой среде можно получить каждое фальсифицируемое, игровое последствие безопасности классического доказательства с нулевым разглашением.

Слово «фальсифицируемое» важно. Оно означает, что провал безопасности можно проверить, запустив противника в определенной игре. Многие криптографические определения безопасности имеют именно такую форму: может ли противник различить два шифротекста, обратить функцию, восстановить свидетель или выиграть конкретный эксперимент? Теорема дает доказывающего для каждого такого свойства отдельно, по одному за раз. Один доказывающий, который одновременно обладает *всеми* фальсифицируемыми свойствами, скорее всего невозможен: старая атака через повторное использование («Боб может показать доказательство другим») сама является фальсифицируемым свойством, и здесь она действительно не выполняется. Предложение статьи состоит в том, что один доказывающий может правдоподобно покрыть все *естественные* фальсифицируемые свойства — те, которые реально встречаются в криптографической практике, — но эта часть является условной теоремой, опирающейся на неформальное понятие «естественности» плюс явную гипотезу. Гарантия нацелена на наблюдаемые провалы, а не на каждое философское или симуляционное значение секретности.

Одно конкретное следствие стоит назвать отдельно: конструкция дает первые невзаимодействую доказательства с **сокрытием свидетеля** (*witness hiding*) и однородным доказывающим — «доказательство существования решения головоломки не помогает вам найти само решение», без взаимодействия и без предварительной настройки. Звучит скромно, но такой объект не удавалось построить десятилетиями.

Чего это не означает

Именно этот раздел не дает материалу превратиться в гиперболу.

Это **не** означает, что старые теоремы невозможности были неверны. Конструкция обходит их, изменив определение.

Это **не** дает обычного классического доказательства с нулевым разглашением без взаимодействия, без предварительной настройки и с совершенной надёжностью. Статья прямо говорит, что построенный доказывающий не имеет симулятора.

Это **не** означает, что доказательство невозможно повторно использовать. Односообщенческое доказательство все еще можно показать кому-то еще; статья не сохраняет свойства вроде отрицаемости (deniability). (Невзаимодействующее доказательство с нулевым разглашением и доверенной предварительной настройкой имеет ту же границу.)

Это **не** практический протокол, готовый к развертыванию. Это теория сложности и фундаментальная криптография. Результат зависит от сильных предположений из теории сложности доказательств и криптографии, а конструкция отвечает на вопрос о том, что принципиально возможно.

И это **не** превращает «Гёделя» в магический примитив безопасности. Связь с Гёделем проходит через системы доказательств, оптимальные системы доказательств и конечные аналоги неполноты. Полезная интуиция здесь не «неполнота защищает ваш пароль», а такая: если книга правил не может эффективно доказать, что симулятор невозможен, то атаки, которые требовали бы такого доказательства, можно блокировать на уровне определений безопасности.

Почему это все равно интересно

Криптография часто превращает сложность в безопасность. Факторизация трудна — значит, предположения в стиле RSA становятся полезными. Решеточные задачи трудны — значит, полезной становится решеточная криптография. Здесь сложность страннее: не «трудно вычислить секрет», а «трудно доказать, что определенный объект доказательства не может существовать».

Именно поэтому работа ощущается необычно. Она обращается с аксиомами и книгами правил почти как с криптографическими ресурсами. Обычная невозможность говорит о напряжении между надёжностью и симуляцией. Ход Иланго помещает это напряжение за теоретико-доказательную завесу: симулятора нет, но формальная система не может эффективно разоблачить это отсутствие.

Для читателя неожиданно не то, что это заменит современные системы с нулевым разглашением. Скорее всего, по крайней мере напрямую, не заменит. Неожиданно то, что ограничение из математической логики можно использовать конструктивно: не

только как стену, но как своего рода укрытие.

Насколько убедительны основания?

Это статья с теоремой, поэтому «доказательства» здесь означают другое, чем в биологии или астрономии. Вопрос не в том, повторился ли эксперимент. Вопрос в том, поддерживают ли определения, предположения и цепочка математического доказательства заявленный результат.

Доказательство формально, а статья четко перечисляет предположения. И они не случайны. Невзаимодействующие доказательства с неразличимыми свидетелями — стандартные объекты криптографии, следующие из нескольких устоявшихся наборов предположений. Гипотеза об отсутствии оптимальной системы доказательств является центральной гипотезой теории сложности доказательств. **P** = **BPP** — стандартное предположение о дерандомизации, нужное только для более широкой теоремы о фальсифицируемых свойствах.

Статья также аргументирует, что эти предположения — не произвольные строительные леса, а фактически необходимая цена. Она доказывает обратный результат: если такие конструкции вообще существуют, должны существовать невзаимодействующие доказательства с неразличимыми свидетелями, а при стандартном предположении о существовании односторонних функций оптимальной системы доказательств существовать не может. И предположения имеют характер «win-win»: опровержение любого из них само стало бы знаковым открытием в теории сложности доказательств, криптографии или теории сложности.

Но поскольку результат условен, уверенность в его интерпретации тоже условна. Если предположения ложны, содержание теоремы меняется. И даже если они верны, гарантия не является полным классическим нулевым разглашением; это ослабленная, теоретико-доказательственная версия статьи.

Поэтому правильная оценка такова: высокая уверенность, что статья устанавливает цельный условный результат о возможности; умеренная — что предположения описывают криптографический мир, в котором мы действительно живем; и низкая — относительно любого немедленного практического последствия.

Почему это важно

Статья открывает маршрут, который считался закрытым.

Классическая теория говорит: полное нулевое разглашение не может состоять из одного сообщения без предварительной настройки и не может иметь совершенную надёжность. Статья Иланго говорит: если спрашивать о тех последствиях нулевого

разглашения, которые можно проверять в играх безопасности, и позволить определению безопасности зависеть от того, что книга правил может или не может эффективно опровергнуть, то значительную часть полезного поведения можно вернуть — с одним сообщением, без предварительной настройки и с совершенной надёжностью.

Это не небольшая подкрутка определения. Это другой способ думать о криптографических гарантиях. Вместо того чтобы спрашивать только, что существует, спросите, что ваша книга правил способна исключить. Вместо того чтобы считать недоказуемость философским неудобством, используйте ее как структуру.

Практический мир, возможно, не изменится завтра. Но концептуальная карта уже изменилась. Теперь существует формальный смысл, в котором «никто не может эффективно доказать, что секрет утек» может быть достаточно сильным, чтобы восстановить многие игровые защиты, которых мы хотели от утверждения «секрет не утек».

Именно поэтому Гёдель — в названии.

Краткий итог

Доказательства с нулевым разглашением позволяют доказывающему убедить проверяющего в истинности утверждения, не раскрывая свидетель. Классические результаты невозможности говорят, что доказательство с нулевым разглашением нельзя втиснуть в одно сообщение без предварительной настройки и что оно не может иметь совершенную надёжность. Статья Рахула Иланго не опровергает эти теоремы. Она определяет более слабое понятие — эффективное нулевое разглашение: вместо требования реального существования симулятора нужно, чтобы выбранная система доказательств — формальная книга правил вроде ZFC — не могла эффективно доказать, что симулятора не существует. При сильных предположениях из криптографии (невзаимодействующие доказательства с неразличимыми свидетелями) и теории сложности доказательств (отсутствие оптимальной системы доказательств) статья строит односообщенческие доказывающие для NP/SAT без предварительной настройки и с совершенной надёжностью, которые по одному свойству за раз воспроизводят фальсифицируемые, игровые последствия нулевого разглашения. Один доказывающий для всех «естественных» таких свойств — дальнейшее, частично гипотетическое расширение, а буквально все фальсифицируемые свойства одновременно, вероятно, невозможны, потому что доказательства остаются повторно используемыми. Результат теоретический и условный, а не готовый криптографический примитив, но он показывает новый способ превратить теоретико-доказательную недоказуемость в криптографический ресурс.

Проверка без прикрас

Что показывает статья: При явно сформулированных предположениях можно построить односообщенческие, без предварительной настройки и с совершенной надёжностью доказывающие для NP/SAT, которые являются системой эффективного нулевого разглашения относительно любой выбранной системы доказательств и реализуют каждое фальсифицируемое, игровое последствие классического доказательства с нулевым разглашением.

Что правдоподобно, но не доказано безусловно: Что необходимые предположения из теории сложности доказательств и криптографии верны. Это серьезные, хорошо изученные предположения — и статья показывает, что они по сути не только достаточны, но и необходимы, — однако они все равно остаются предположениями.

Чего она не показывает: Классического доказательства с нулевым разглашением без взаимодействия, без предварительной настройки и с совершенной надёжностью; практической системы, готовой к развертыванию; отрицаемости или невозможности повторного использования доказательств; либо того, что сама по себе теорема Гёделя о неполноте обеспечивает криптографическую безопасность.

Главные ограничения: Гарантия является ослаблением классического нулевого разглашения; самая широкая версия зависит от нескольких предположений; утверждения об одном универсальном доказывающем частично остаются гипотетическими; а результат прежде всего фундаментальный.

Какой уверенности заслуживает вывод для обычного читателя? Высокой, что это важный условный теоретический результат, если принять его определение. Умеренной, что предположения соответствуют реальности. Низкой относительно немедленного практического применения. Безопасный вывод: статья не ломает теоремы невозможности для доказательств с нулевым разглашением; она находит новый теоретико-доказательственный способ обойти те их части, которые важны для многих игр безопасности.

Источники

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