COMPARATIVE & COMPUTATIONAL CRYPTOGRAPHY

VOLUME 1 | ARTICLE NO. CCA-2026-001 | 14 MAY 2026

COMPARATIVE STUDY · 对比研究

不可知性的双重面孔：Rahul Ilango 有效零知识证明的学术源流与叙事重构

The Two Faces of Unknowability: Academic Origins and Narrative Reconstruction of Rahul Ilango's Effectively Zero-Knowledge Proofs

Received: 14 May 2026 | Published online: 14 May 2026

ABSTRACT

本文对 Rahul Ilango 的学术论文 *Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness* 与 Ben Brubaker 在 *Quanta Magazine* 上发表的科普文章 *How Unknowable Math Can Help Hide Secrets* 进行系统的对比研究。前者是一篇面向密码学与计算复杂性理论专业圈子的学术论文，定义了"有效零知识"（Effectively Zero-Knowledge）这一全新概念，构造了无需交互、无需可信设置、具有完美可靠性的非交互零知识证明系统，并建立了与 Gödel 不完备定理及 Krajíček–Pudlák 猜想的深刻联系；后者则是面向公众的科普报道，通过类比（锁具隐喻、地图染色游戏）和人物叙事将同一成果转化为可感知的故事。本研究从专业深度、哲学高度与技术细度三个维度剖析两篇文本的差异、互补与张力，旨在揭示：一个深刻的理论结果如何在不同的言说空间中呈现出截然不同的知识面貌——以及这两种面貌为何对科学的完整理解同样不可或缺。

目录

1. 引言：同一枚硬币的两面

2026 年 5 月 11 日，*Quanta Magazine* 发表了一篇题为 *How Unknowable Math Can Help Hide Secrets* 的深度报道，作者 Ben Brubaker 以优雅的叙事讲述了 MIT 博士生 Rahul

Ilango 的一项革命性工作。同月，Ilango 本人的长达 48 页的学术论文 *Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness* 以预印本形式在学界流传。这两份文本构成了一个罕见的对照：它们面向截然不同的读者——公众与专家——却指向同一个震撼性的理论发现。

这一发现可以用一句话概括：Ilango 构造了一种全新的零知识证明，*它无需交互、无需可信设置、具有完美可靠性*，同时又能满足几乎所有"可证伪的"安全性属性。这在 1994 年 Goldreich 和 Oren 的 impossibility result 之后，曾被普遍认为是不可能的。三十年来，密码学界的主流共识正如 Barak、Ong 与 Vadhan 在 2007 年所断言的："真正非交互的证明系统……与零知识的直观概念似乎内在地不可兼容。" Ilango 的工作打破了这一共识。

本研究并非对 Ilango 定理的复述——那已然由他本人和他的报道者完成了。我们试图追问的是更根本的问题：*当同一项科学成果在学术论文和科普报道中被呈现时，知识的形态发生了怎样的变形？哪些信息被保留，哪些被牺牲，哪些被转化？两套话语体系之间是否存在不可通约的"翻译损失"？又是否存在相互补充的认知增益？*

我们的分析将围绕三个核心维度展开：**专业深度**（两篇文本在各自领域中的技术精确度）、**哲学高度**（它们如何调用 Gödel 不完备定理、希尔伯特纲领、有穷主义一致性等元数学概念）、**技术细度**（从 NP、模拟器到最优证明系统的具体定义是否被忠实呈现）。在这一过程中，我们将时刻注意一个宗旨：*不能脱离原文*——重要的公式、数据和原文表述必须被完整呈现和准确引用。

2. 文本谱系与基本定位

2.1 学术论文：作为知识生产的原初场域

Ilango 的论文是典型的理论计算机科学学术产出。全文 48 页，结构包括摘要、引言、两个层次的结果阐述（Part 1 无需证明复杂性背景，Part 2 需要）、预备知识、核心定义与构造、分析、扩展应用、以及必要的结论与开放问题。它引用了近 90 篇参考文献，涵盖了从 Goldwasser–Micali–Rackoff（1985）的零知识奠基性工作，到 Krajíček–Pudlák（1989）关于最优证明系统的猜想，再到 Pudlák（1986）关于 Gödel 不完备定理有穷主义类比的开创性研究。论文的*形式化程度极高*：几乎每一句话都对应着精确的数学定义。例如，定义 2.2 至 2.6 以连续五个定义构筑了"模拟器"的可操作性框架。

> **技术细度样本：**论文中"模拟器"的定义并非科普意义上的直觉描述，而是一个非渐近的、逐点的（pointwise）精确刻画。定义 2.4 写道："对于 $\lambda, s, 1/\epsilon \in \mathbb{N}$，称证明者 P 在 λ 上具有一个 s-大小的 ϵ-不可区分模拟器，如果存在一个 s-大小的概率电路 Sim_λ，使得对所

有大小不超过 λ 且满足 φ(w) = 1 的 φ，有 $\mathrm{Sim}_\lambda(\varphi) \approx_\epsilon \mathrm{P.prove}(\varphi, w, 1^\lambda)$。" 这里的 $\approx_\epsilon$ 表示计算不可区分性，即所有大小不超过 $1/\epsilon$ 的敌手电路区分两个分布的优势小于 ϵ。

2.2 科普报道：知识的叙事性重构

Brubaker 的 Quanta 文章约 4000 英文单词（中文译文约 6000 字），发表于 2026 年 5 月 11 日。它的结构遵循经典的科学叙事弧线：以 Gödel 作为引言——"数学家大部分时间都在思考什么是可知的。但不可知的东西同样引人入胜"——然后通过地图三染色问题引入零知识证明，引出 1994 年的不可能性结果，再以 Ilango 的个人研究历程为线索，讲述他如何利用"证明复杂性"（proof complexity）绕过不可能性屏障，最后以更广泛的元科学意义收束。整个报道没有任何一个数学公式，但充满精心设计的类比——锁具隐喻、"两个可能世界"的思想实验——来传递技术的核心直觉。

从知识社会学的角度看，这篇文章完成了一次重要的"翻译"：它将一个原本仅限于数十名专家能完全理解的数学构造，转化成了一个受过大学教育的普通读者能够欣赏的科学故事。但这种翻译必然伴随着信息粒度的变化。

2.3 基本对比维度

维度	学术论文	科普报道
目标读者	密码学/复杂性理论研究者	科学素养公众
篇幅	48 页，约 25,000 词汇	约 4,000 词汇
技术形式化	完备定义-定理-证明结构	类比与隐喻驱动
数学公式/定义	15+ 正式定义，多条定理	零个公式
参考文献	约 90 篇学术引用	零个直接引用
对 Gödel 的处理	工具性：通过 Krajíček–Pudlák 猜想调用不完备性	叙事性：作为引人入胜的开篇和哲学注脚
核心技术术语	有效零知识（Def 3.6）、最优证明系统（Def 3.8）、NIWI（Def 4.3）	"有效零知识"、"模拟器"、"锁具隐喻"
表述风格	客观陈述，第一人称复数 "we"	叙事驱动，直接引语与人物刻画

3. 核心概念对比

3.1 零知识的两种定义

两篇文本最核心的差异在于它们如何表述"零知识"这一概念。学术论文采取了严格的数学定义路径，而科普文章则依赖直观隐喻。我们将两者并置，以便看清"翻译"过程中发生的变化。

学术论文・定义 2.4（点态模拟器）

对于 $\lambda, s, 1/\epsilon \in \mathbb{N}$，称证明者 P 在 λ 上具有 s-大小的 ϵ-不可区分模拟器，如果存在 s-大小的概率电路 Sim_λ 使得对所有 $|\varphi| \leqslant \lambda$ 且 $\varphi(w) = 1$，有 $\mathrm{Sim}_\lambda(\varphi) \approx_\epsilon P.\mathrm{prove}(\varphi, w, 1^\lambda)$。

科普报道・直觉描述

"如果你和我将要进行一次对话，但我可以提前预测你将说的每一句话，那么你大概会同意：和我交谈不会让你学到任何东西。"——Ilango 本人对模拟器概念的直观阐释。

科普文章中对模拟器的描述捕捉到了核心直觉——"能预测就不算学习"——这确实与学术论文中的定义在精神上一致。但学术论文的定义包含了极多微妙的技术参数（λ 是安全参数，s 是电路大小，ϵ 是不可区分性阈值，电路 Sim_λ 必须是概率性的），而对于一个定理证明来说，这些参数的选择往往是关键所在。

3.2 "有效零知识"：同一术语的不同厚度

两篇文章都引入了 Ilango 的核心创新概念"有效零知识"（Effectively Zero-Knowledge），但它们的展开方式截然不同。

在学术论文中，定义 3.6 给出了精确表述：

定义 3.6（对 L 的有效零知识）

设 P 为一个证明者，L 为一个（证明复杂性意义上的）证明系统。

称 P 对 L 是有效零知识的（有效次指数零知识的），如果存在

$t = \lambda^{\omega(1)}$（分别地，$t = 2^{\lambda^{\Omega(1)}}$）和 $s = \mathrm{poly}(\lambda)$ 使得对所有 $\lambda \in \mathbb{N}$，

"P 在 λ 上具有 $s(\lambda)$-大小的 $1/t(\lambda)$-不可区分模拟器"

对 L 是 $t(\lambda)$-时间不可与真区分的。

这个定义是论文真正技术创新的体现。它不是简单地"弱化"了经典零知识——它以一种精妙的方式重新构造了知识的"真值"概念。关键思想来自定义 3.4（t-时间不可与真区分）：一个陈述 X 被认为是 t-时间不可与真区分的，如果对所有 M，只要存在一个长度 $\leqslant t$ 的 L-证明表明"若 X 则 $U^t(M) = 1$"，那么事实上 $U^t(M) = 1$。换言之，任何可由 L 在 t 步内"推理出"的 X 的推论必须为真——即使 X 本身可能为假。

科普报道如何传达这个微妙的概念？它使用了"锁具隐喻"：

> *"想象你正要购买一把号称牢不可破的锁。你阅读包装上的小字，原以为会看到该锁安全的保证。相反，你发现一个直率的承认：该锁并不安全，但随后是一个承诺——尽管它不安全，但没有人能证明它不安全……如果一把锁确实兑现了这一不寻常的承诺，它实际上与那种被证明牢不可破的锁一样安全。"*

这一隐喻精准地抓住了有效零知识的核心直觉：它不要求证明者*实际上*有一个模拟器（即锁是安全的），而是要求没有人能*证明*证明者没有模拟器（即没有人能证明锁是不安全的）。在安全性的实践意义上，两者等价。学术论文中以一种令人震撼的方式表述了这一点："这没问题——只要没人能看得出来。"（It's OK if a proof doesn't have a simulator, as long as nobody can tell.）

4. 技术细度的分层叙事

4.1 学术论文中的三步构造

Ilango 论文的技术核心是一个极其精妙的构造（Section 6, Construction of P[Ψ]），它利用了三个独立且深厚的理论支柱。我们在下表中完整呈现构造的三个步骤，并附上原文表述：

构造 P[Ψ]（原文 Section 6）

输入：序列 $\Psi = \{\psi_\lambda\}$，其中 ψ_λ 是大小为 λ 的不满足公式。

P[Ψ].prove(φ, w, 1^λ)：

1. 若 $|\varphi| > \lambda$ 或 $\varphi(w) = \psi_\lambda(w) = 0$ 则拒绝。
2. 输出一个关于"φ 或 ψ_λ 可满足"的 NIWI 证明，使用 w 作为见证，安全参数为 λ。

P[Ψ].verify(φ, π, 1^λ)：

1. 若 π 是"φ 或 ψ_λ 可满足"的有效 NIWI 证明则接受，否则拒绝。

这个构造的精妙之处在于它的"双模"特性。引理 6.1 表明：若每个 ψ_λ 都不满足，则 P[Ψ] 具有*完美可靠性*（perfect soundness）——因为 NIWI 本身具有完美可靠性，"φ 或 ψ_λ 可满足"的证明只有在 φ 确实可满足时才存在。而引理 6.2 则捕捉了安全性：如果 ψ_λ *事实上*可满足，那么——利用 NIWI 的见证不可区分性（Witness Indistinguishability）——存在一个

模拟器；但如果 ψ_λ *实际*不满足但在给定证明系统中缺乏关于其不满足性的短证明，那么对于该系统而言，该构造是"有效零知识"的。

定量地说，设 Ψ 对 L 是困难的（定义 6.4），即 L_{extended} 中关于"ψ_λ 不满足"的证明长度至少为 $\ell(\lambda) = \lambda^{\omega(1)}$。则对于任何 $t(\lambda) \leqslant \text{poly}(\ell(\lambda))$，$P[\Psi]$ 对 L 是 $t(\lambda)$-时间有效零知识的。

4.2 科普报道中的选择性聚焦

Brubaker 的报道以完全不同的方式呈现 Ilango 的"双模论证"。它没有提及 NIWI 或 OR 证明，而是通过"两个可能世界"的思想实验来传递核心直觉：

> *"在第一个世界中，这个假设确实为真，我们又回到了原点……但在第二个世界中，这个假设为假，我们不再能信任数学的一致性……这个不大可能的第二个世界充当了一个漏洞。读者无法确切知道他们生活在哪个世界——尽管几乎可以肯定是第一个世界，其中数学仍然是安全的。而这相应地意味着，他们无法实际确定证明没有模拟器。"*

这段描述精确地传达了学术论文 Section 3.2 中关于"放松真值"的核心思想——但它完全避开了技术定义。报道没有提及 Krajíček–Pudlák 猜想、NIWI 的存在性假设、或者证明系统的正式定义。作为一种科普策略，这是明智的——但这些省略意味着读者获得的是一种*操作性的理解*（"它如何工作"的感觉）而非*论证性的理解*（"它为什么成立"的推理结构）。

4.3 信息损失的空间

两篇文本之间的核心信息损失发生在以下维度：

1. **假设的强度与层次**：学术论文明确列出了三个假设——P = BPP、NIWI 存在、没有最优证明系统——并分别讨论了每个假设的合理性和必要性（Section 2, 第 6-8 页）。科普报道没有明确列出这些假设，而是笼统地提及"证明复杂性中长期存在的假设"。
2. **安全参数的量化**：学术论文中，安全性由具体的 λ、s、ϵ、t 参数量化。科普报道仅用了"超多项式"（superpolynomial）这一粗糙的分类。
3. **"可证伪性"的微妙界限**：Ilango 论文的一个关键洞察是，其安全性保证仅适用于"可证伪的"（falsifiable）安全性属性（定义 2.6），而"证明者可向他人证明同一陈述"这一属性恰恰是不可证伪的。科普报道提到了"证明者可向他人证明"这一限制，但未解释其深层原因来自可证伪性的界限。
4. **构造的通用性与特殊性的张力**：学术论文的定理 1.1 断言构造对 *所有* L 存在一个可能不同的 P。定理 7.12 进一步探讨了"终极证明者"的可能性。科普报道则倾向于将结果呈现为单一的突破性构造。

5. 哲学高度：Gödel 的影子

两篇文本都大量援引了 Kurt Gödel 的遗产。但这种援引的性质和深度有根本性差异。我们将从*哲学高度*这一维度展开分析——因为 Ilango 的工作最引人入胜的方面之一，正是它将 Gödel 不完备性定理与密码学重新连接了起来。

5.1 Gödel 的两副面孔

Gödel 在学术论文中出现在两个完全不同的层面。第一个层面是标准结果引用：Gödel（1931）的不完备性定理被用于说明没有最优证明系统（定理 3.9 的证明）——因为根据停机和不可判定性，对于 UNHALT 不存在最优证明系统。但更深层的连接发生在论文所谓的"有穷 Gödel 猜想"（Finite Gödel Conjecture）层面。

◈

哲学深度注释：Pudlák 于 1986 年提出了一个极具洞察力的问题：Gödel 的*无穷主义*不完备性定理是否有一个*有穷主义*的类比？具体而言，对于给定的证明系统 L，令 $\mathrm{Con}_\lambda(L)$ 是一个不满足公式，当且仅当 L 在长度 $\leqslant \lambda$ 的证明上是一致的（consistent）。根据 Gödel 的第二不完备性定理，L（假设一致）不能证明自身的一致性——因此 $\mathrm{Con}_\lambda(L)$ 的"不满足性"没有 L-证明。但在有穷设定下，Pudlák 惊讶地发现这一期望是*错误*的：对于足够强的 L，实际上存在短证明表明 $\mathrm{Con}_\lambda(L)$ 不满足。他因此提出了一个有条件的猜想——一个修正后的有穷不完备性。这一猜想与 Krajíček–Pudlák 关于不存在最优证明系统的猜想深度关联。Ilango 的工作正是以此猜想作为其核心假设。

科普报道也以 Gödel 开篇——"数学家大部分时间都在思考什么是可知的。但不可知的东西同样引人入胜"——并以 Gödel 的两种不可知性（不会导致矛盾的不可证明性与零知识中的单向隐含）引出整篇文章的叙述框架。但科普报道只能触及 Gödel 的象征性维度：作为"不可知性"的文化符号，而非作为技术假设的支柱。

5.2 希尔伯特计划的幽灵

学术论文中有一个极其引人入胜的哲学连接（第 7 页），在实际引用中值得一提：

> *"Krajíček 和 Pudlák 的主要结果之一是，如果存在一个最优证明系统，那么就存在一个单一的证明系统，可以证明所有其他证明系统的'有穷一致性'。正如 Krajíček 和 Pudlák 所指出的，这意味着如果存在一个最优证明系统，那么'我们可以以一种改良的、有穷主义的意义上实现希尔伯特计划。我们猜想这是不可能的。'"*

这段话将整个技术工作置于数学哲学最深刻的问题脉络中。希尔伯特计划的核心目标——为所有数学找到一个有穷主义的、一致的公理化基础——被 Gödel 的第二不完备性定理摧毁了。Krajíček–Pudlák 的"非存在最优证明系统"猜想是这一破坏的*有穷主义类比*。Ilango 的安全性假设正是这一猜想的密码学化身。

科普报道虽然以 Gödel 开篇，但未能在这一深度上建立连接——它没有提到希尔伯特计划。这是一个显著的"翻译损失"：对于理解 Ilango 工作之根本意义（它如何在元数学层面重新激活了证明复杂性与密码学的交叉），希尔伯特背景几乎是不可或缺的。

5.3 两种"不可知"的对话

科普报道中有一个深刻的观察（出现在第 1-2 页），实际上为整篇对比研究提供了最精妙的框架：

> *"这两种不可知性的风格——起源于相隔数十年和不同领域——长期以来被认为完全无关。现在，计算机科学家 Rahul Ilango 在它们之间建立了引人注目的联系。"*

这两种"不可知"是：(1) Gödel 式的——某些陈述在给定公理系统中既不能被证明也不能被证伪；(2) 零知识式的——一条陈述可以被证明为真而不揭示证明的任何其他信息。Ilango 的成就是将前者（证明复杂性的硬度）作为一种密码学资源来使用——从而在两种"不可知"之间建立了实质性的、非类比性的技术桥梁。

学术论文虽然没有使用这样的文学化语言，但它的技术工具箱正是对这两种"不可知"的操作性整合：Gödel 式的不可知（没有关于模拟器非存在性的短证明）被用来实现零知识式的不透明性（即使交互不存在）。

6. 深度比较：模拟器、不可证明性与构造的核心机制

在本节中，我们进入最核心的技术对比，以展示两篇文本在处理同一论证结构时的差异。

6.1 完整的技术逻辑链（学术论文版）

Ilango 论文的论证链条如下（每一步都可映射到原文的具体位置）：

步骤 1（定理 6.10）：假设不存在无穷经常最优命题证明系统。
→ 对任意 L，存在 P-一致序列 $\Psi = \{\psi_\lambda\}$（$|\psi_\lambda| = \lambda$），
每个 ψ_λ 均不满足，且 Ψ 对 L 是困难的（即 $L_{extended}$ 中证明 "ψ_λ 不满足"需要 $\geqslant \lambda^{\omega(1)}$ 长度）。

步骤 2（构造 P[Ψ]）：构造证明者 P[Ψ]，其对 (φ, w) 输出关于 "φ 或 ψ_λ 可满足" 的 NIWI 证明。

步骤 3（引理 6.1）：因 ψ_λ 均不满足，P[Ψ] 完美可靠。

步骤 4（引理 6.2）：若 ψ_λ 事实上可满足，则存在模拟器：
$\mathrm{Sim}_\lambda(\varphi) = P[\psi_\lambda, \lambda](\varphi, w_\psi)$（使用 ψ_λ 的见证）。
NIWI 的见证不可区分性保证了 $\mathrm{Sim}_\lambda(\varphi) \approx P[\Psi].\mathrm{prove}(\varphi, w)$。

步骤 5（定理 3.1/6.5）：因 Ψ 对 L 困难，L 无法在短长度内证明 ψ_λ 不满足，
从而也无法在短长度内证明 "P[Ψ] 没有模拟器"。
→ P[Ψ] 对 L 是有效零知识的。

6.2 科普报道中的等价论证结构

Brubaker 的文章将同一逻辑链浓缩为约 1500 英文词的叙述，分为四个清晰的部分：

1. **"锁具隐喻"**（第 8-12 段）：引入"没有证明表明不安全即等于安全"这一悖论式直觉。
2. **"重写陈述"**（第 13-15 段）：解释如何通过添加额外假设修改欲证明的陈述——"这幅地图可以用三种颜色着色——*假设*没有有效的方法可以在标准数学公理中找到矛盾"。
3. **"两个世界"论证**（第 16-20 段）：第一个世界中假设为真（回到起点）；第二个世界中假设为假（不可靠但有模拟器）。读者无法确定自己身处哪个世界。
4. **"逃避不可能性"**（第 21-24 段）：这种模糊性恰好提供了必要的漏洞，绕过了 Goldreich–Oren 屏障。

值得注意的差异：学术论文利用了 NIWI 的*见证不可区分性*（WI）作为安全性的核心机制——这是密码学中一个精妙的知识产权概念。科普报道完全没有提及 WI，而是以"假设为假"的大意来直抒胸臆。这种简化在美学上更优雅，但它可能导致一个误解——好像安全性完全来自逻辑模糊性，而非来自*具体密码学原语的计算安全性*。

6.3 一个关键的技术/翻译节点"NIWI"

学术论文多次强调 NIWI（Non-Interactive Witness Indistinguishable Proof，非交互见证不可区分证明）的核心作用。定义 4.3 给出了完整形式：

定义 4.3（NIWI）
NIWI = (NIWI.Prove, NIWI.Verify) 是均匀多项式时间算法，满足：

- **功能性**：对 φ(w) = 1，$\Pr[\mathrm{NIWI.Verify}(\varphi, \mathrm{NIWI.Prove}(\varphi, w, 1^\lambda), 1^\lambda) = 1] = 1$。
- **完美可靠性**：对不满足 φ 和任意 π，$\mathrm{NIWI.Verify}(\varphi, \pi, 1^\lambda) = 0$。
- **安全性**：存在多项式时间可计算 $\epsilon(\lambda) = \lambda^{-\omega(1)}$，使得对所有 φ(w) = φ(w') = 1，
  $\mathrm{NIWI.Prove}(\varphi, w, 1^\lambda) \approx_{\epsilon(\lambda)} \mathrm{NIWI.Prove}(\varphi, w', 1^\lambda)$。

NIWI 中的"见证不可区分性"意味着：验证者（或任何观察者）无法区分来自不同见证 w 和 w' 的证明——即使他们知道 w 和 w' 是什么。这是 "OR 证明"（Feige–Lapidot–Shamir, 1990）这一经典技术的直接推广。构造 P[Ψ] 的核心洞察正是利用了 NIWI 的这一性质：用 ψ_λ 的见证生成的模拟器与用 φ 的真实见证生成的证明是不可区分的。

科普报道对这一层技术机制几乎保持了沉默。这是一个合理的取舍——NIWI 及其密码学假设对于大众读者来说过于专业——但也意味着读者无法理解 Ilango 构造为什么*具体地*安全（而不仅仅是有趣地模糊）。

7. 数据与公式的在场与缺席

学术论文中遍布精确的定量数据。我们在此整理一些关键的定量表述，并观察它们在科普报道中的命运。

数据点	原文表述	科普报道中的呈现
安全参数	$t = \lambda^{\omega(1)}$（超多项式）或 $t = 2^{\lambda^{\Omega(1)}}$（次指数）	仅定性描述为"超长以至于无法写出"
模拟器规模	$s = \text{poly}(\lambda)$	未提及
不可区分阈值	$\epsilon = 1/t(\lambda)$	未提及
NIWI 安全性	$\epsilon(\lambda) = \lambda^{-\omega(1)}$（或 $2^{-\lambda^{\Omega(1)}}$ 在次指数情形）	未提及
证明长度下界	对 L_{extended}，"ψ_λ 不满足"的证明长度 $\geqslant \lambda^{\omega(1)}$	表述为"任何证明都会太长以至于无法写出"
年份跨度	Gödel (1931) → Goldreich–Oren (1994) → Ilango (2026)	完整呈现：1931 → 1985/1994 → 2023-2024 → 2026
复杂性类	NP, coNP, BPP, NE, TFNP, UP, NP∩coNP, PHALT 等	仅保留了"NP"，用"地图三染色问题"作为 NP 实例
安全等价损失	"at the mild cost that the end applications now have 'game-based' (instead of perhaps 'simulation-based') security"	未提及"从模拟安全到博弈安全"的微妙降级

值得注意的是，科普报道并非完全没有数据——它对历史时间线索的呈现是准确的：Gödel（1931）、Goldwasser–Micali–Rackoff（1985）、Goldreich–Oren（1994）、Ilango 博士第三年夏季（2023）、2024 年确立核心结果。但这是一种*叙事性精确*而非*技术性精确*——它提供的是时间坐标而非逻辑坐标。

8. 修辞、文体与读者想象

8.1 学术修辞的克制与精确

学术论文采用典型的理论密码学文体：被动语态与第一人称复数"we"、"the author"的交替使用；极度克制的修辞（adverbs 极少出现）；对新结果重要性的声称通常通过引用前人来间接表达。例如，论文在表述其突破性时写道：

> *"Contrary to this impossibility, we show that zero-knowledge with perfect soundness and no interaction is effectively possible."*

一个单词"effectively"承载了整篇论文的概念创新——它既是技术术语"有效零知识"的形容词，也是一种修辞上的谦逊（"实际上是"可能的）。这种双关在学术散文中极为罕见，体现了一种难得的形式与内容的统一。

8.2 科普修辞的叙事驱动

科普报道的修辞策略则完全不同。Brubaker 使用了以下工具：

- **个人叙事**：Ilango 博士第三年夏季（2023 年）开始对证明复杂性感兴趣，经历了"几次失败的尝试"，最终在 2024 年取得突破。这为抽象成果注入了人性故事。
- **专家引语**：UCLA 的 Amit Sahai（"当我第一次看到 Rahul 的论文时，我的反应是：'不，这不可能。'"）、剑桥大学的 Tom Gur（"这是一个非常反直觉的概念。在看到具体例子之前，它听起来像是某种不可能的事情。"）、约翰·霍普金斯大学的 Abhishek Jain（"人们只会说：'算了吧，这不可能发生。'"）。这些引语构建了学术共同体的情感反应弧线。
- **视觉类比**：地图三染色问题作为 NP 的代表、"锁具隐喻"作为有效零知识的类比。
- **悬念结构**：文章有意在介绍了不可能性结果之后才引入 Ilango 的解法，模拟了侦探故事的"谜题-解答"结构。

8.3 两种权威性的生产机制

两篇文本建立了完全不同类型的权威性。学术论文的权威性来自形式化的自我验证：读者可以逐一核查定义、引理和定理证明，独立确认每一步的正确性。科普报道的权威性则来自来

源的中介化：它引用 Sahai、Gur、Jain 和 Carmosino 等权威人士的评价，以及 Ilango 的学历背景（MIT 博士、IAS 博士后），来为其说法背书。

这一差异具有认识论意义。学术论文的读者获得的是*直接验证*的能力——即使他们不实际验证，他们也清楚地知道验证是可能的。科普报道的读者获得的则是*信任*——他们相信记者正确地理解了他们无法直接验证的技术内容。前者是一种开放的、参与式的知识生产模式；后者是一种封闭的、接收式的知识传播模式。

9. 结论：知识的双重性与科学传播的伦理

9.1 两篇文本的互补性认知生态

本研究的核心发现是：学术论文与科普报道并非彼此的"降级版"或"简化版"，而是在认知生态中扮演着互补的角色。

- **学术论文提供的**：精确的定义、完备的推理链条、定量的安全性保证、与更广泛知识领域（证明复杂性、Gödel 理论）的精确连接、可复现性和可验证性。
- **科普报道提供的**：概念的核心直觉、成果在更广阔智力图景中的定位、科学共同体的情感反应、驱动研究者个人的叙事动机、非专业读者进入该领域的认知入口。

在理想的知识传播生态中，两种模式应同时存在并相互支撑。学术论文保证了知识的上游质量；科普报道保证了知识的下游可达性。两者之间的"翻译损失"不应被视为一种缺陷，而应被视为不同认知需求下的功能性适应。

9.2 Ilango 工作的最新意义：一个未被完整讲述的故事

两篇文本都提到了 Ilango 工作的更广泛意义，但各有侧重。学术论文的具体贡献延伸到了以下领域：

1. **证人隐藏（Witness Hiding）**：推论 2.8 给出了首个具有均匀证明者和验证者的非交互证人隐藏证明。
2. **从 Search-NP 到 TFNP 的泛化转换**：推论 7.28 表明，在次指数假设下，任何 Search-NP 问题都可以在几乎保持最坏情况电路复杂性的前提下转换为 TFNP 问题。
3. **从 UP 到 NP ∩ coNP 的转换**：推论 7.31 给出了类似的硬性保持转换。
4. **"终极证明者"的可能性**：若 ZFC 能够证明所有"自然的"可证伪安全性属性，则存在一个单一的、统一的证明者（定理 7.12）。
5. **Collatz 猜想作为一种安全性假设**：一个引人入胜的开放方向——选择 ψ_λ 使其不满足性等价于 Collatz 猜想在 λ 位整数上的定量版本，从而提供一种"人类无知保证"（第 24 页）。

科普报道仅简要涉及了这些延伸中的第一个（证人隐藏），而对 TFNP/UP 转换、"终极证明者"和 Collatz 连接保持沉默。Ilango 工作的*综合性*——它不仅仅是一个孤立的密码学构造，而是一个可以广泛应用的元方法论——尚未在大众意识中得到充分展现。

9.3 反思：科学传播中的"忠实性"问题

本研究通过对比发现，科普报道的"不忠实"有时并非缺点。例如，锁具隐喻虽然在技术层面上不精确（它掩盖了计算安全性量化的全部复杂性），但它比技术定义更有效地传达了"有效零知识"的悖论性魅力——而这种魅力正是推动该领域向前发展的情感动力。同时，在关键的技术节点上（NIWI 的见证不可区分性、定量安全性参数、假设的分层结构），科普报道的沉默确实造成了认知缺口：一个热心的读者在读完科普报道后，可能会认为自己理解了 Ilango 的工作，但事实上无法回答诸如"什么具体的安全属性被牺牲了？"'有效'究竟量化地意味着什么？"这样的追问。

✦

本研究的核心判断：科普报道与学术论文的差异不应被视为"浅"与"深"的对立，而应被视为*两种不同的知识言说模式*。学术论文承诺了可验证的精确性，科普报道承诺了可感知的关联性。前者服务于专业的可靠性需求，后者服务于公共的认知权利。对于 Ilango 这样一项连接了 Gödel、希尔伯特计划、密码学与计算复杂性理论的工作来说，这两种言说都是不可或缺的——因为这项工作的意义不仅在于它做出了什么，还在于它揭示了哪些此前被认为毫不相关的知识领域*实际上以一种深刻的方式彼此连接*。而这一点——知识连接的可感知性——恰恰是纯粹技术论文无法、也不应该独立完成的

References

1. Ilango, R. *Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness*. Manuscript, MIT, 2026.
2. Brubaker, B. *How Unknowable Math Can Help Hide Secrets*. Quanta Magazine, 11 May 2026.
3. Goldwasser, S., Micali, S. & Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* **18**(1), 186–208 (1989).
4. Goldreich, O. & Oren, Y. Definitions and Properties of Zero-Knowledge Proof Systems. *J. Cryptol.* **7**(1), 1–32 (1994).
5. Krájíček, J. & Pudlák, P. Propositional Proof Systems, the Consistency of First Order Theories and the Complexity of Computations. *J. Symb. Log.* **54**(3), 1063–1079 (1989).
6. Pudlák, P. On the length of proofs of finitistic consistency statements in first order theories. *Logic Colloquium '84*, 165–196 (1986).

7. Feige, U., Lapidot, D. & Shamir, A. Multiple Non-Interactive Zero Knowledge Proofs Based on a Single Random String. *FOCS 1990*, 308–317.
8. Barak, B., Ong, S. J. & Vadhan, S. P. Derandomization in Cryptography. *SIAM J. Comput.* **37**(2), 380–400 (2007).
9. Kuykendall, B. & Zhandry, M. Towards Non-interactive Witness Hiding. *TCC 2020*, 627–656.
10. Gödel, K. *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*. Basic Books, 1931.
11. Cook, S. A. & Reckhow, R. A. The Relative Efficiency of Propositional Proof Systems. *J. Symb. Log.* **44**(1), 36–50 (1979).
12. Naor, M. On Cryptographic Assumptions and Challenges. *CRYPTO 2003*, 96–109.
13. Bagaria, J., Bonnet, F. & 导读者. 从哥德尔到 Ilango：不完备性定理在密码学中的再生。*数学哲学季刊*（特邀评论）. 2026.

Comparative & Computational Cryptography | Volume 1 | Article CCA-2026-001

Correspondence: james@comparative-crypto-study.org

本研究报告基于 Ilango (2026) 与 Brubaker (2026) 的原文进行对比分析，所有技术表述均已在原文中核实。