



The CLEAN PAPER

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

Cryptographic proof kan lè hide secret rẹ nípa jíjẹ kí missing simulator nira láti prove

Zero-knowledge proofs jẹ kí ẹnikan prove statement kan láì reveal witness. Classical theory sọ pé o kò lè ní full zero-knowledge pẹ̀lú one message, no trusted setup àti perfect soundness. Paper Rahul Ilango kò make impossibility yẹn vanish. Ó change target: dípò requiring pé simulator kan wà gidi, ó ask pé proof system tí a yan kò lè efficiently prove pé simulator kò exist. Under major proof-complexity àti cryptographic assumptions, èyí tó láti recover falsifiable, game-based consequences of zero-knowledge property by property. Point náà kì í ẹ̀se plug-in internet primitive. Ó jẹ proof-theoretic way láti turn mathematical unprovability into cryptographic cover.

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

Ètan náà kì í ẹ́ látí fi ẹ́rí múlẹ̀ pé secret náà farapamó

Jẹ́ ká bèrẹ̀ pẹ̀lú ẹ̀dà zero-knowledge tó rọ̀rùn jù.

Alice ẹ́ convince Bob pé Sudoku puzzle kan ní solution. Bí ó bá send solution náà, Bob máa convinced, ẹ̀gbọ̀n puzzle náà ti bàjẹ́. Ohun tí Alice ẹ́ yàtò díẹ̀: proof pé solution kan wà, láì reveal solution náà.

Ìlẹ́rí zero-knowledge proof nìyẹn. Prover (Alice) convince verifier (Bob) pé statement kan jẹ́ true, nígbà tí kò reveal ohunkóhun ju truth statement náà lọ.

Ìṣòro náà ni pé ilẹ́rí yí ní cost. Ordinary mathematical proof ní àbùdá méjì tó convenient. Ó jẹ́ **ọkan message**: o kọ ọ sílẹ̀, o fún ẹ̀lòmíràn, o sì lọ. Ó tún jẹ́ **perfectly sound**: false statement kò ní valid proof rárá. Classical impossibility èsì sọ pé zero-knowledge gbòdò give up àbùdá méjèèjì — kì í ẹ́ pé méjèèjì pọ̀ nikan; ọkọọkan wọ̀n fúnra rẹ̀ off-limits.

Àkókọ, zero-knowledge proof nílò conversation. Bí Alice bá send message kan ọ̀sọ, láìsì trusted setup tí a arrange tẹ̀lẹ̀, zero-knowledge guarantee collapse — èyí sì hold bó tilẹ̀ jẹ́ pé o willing látí trade soundness púpọ̀ away.

Èkejì, zero-knowledge proof nílò tolerance kékeré fún àṣìṣe. Demanding perfect soundness turns out látí quietly destroy interaction náà: verifier tí a kò lè fool rárá, whatever random choices tó ẹ́, lè kan fix choices yẹn tẹ̀lẹ̀ — nígbà tí verifier bá predictable, Alice lè answer gbogbo nńkan nínú message kan, èyí gan-an ni ọ̀ràn tí a ti mò pé ó break.

ìwé iwádíí Rahul Ilango jẹ́ nípa ọ̀nà kan látí yí double wall yẹn ká. Kì í ẹ́ nípa pretending pé wall kò sí, kì í sì ẹ́ nípa producing classical zero-knowledge nínú setting tí kò ẹ́é ẹ́. Move náà subtle ju: weaken ohun tí “reveals nothing” tùmọ̀ sí, ẹ̀gbọ̀n weaken rẹ̀ ní ọ̀nà tó preserve security properties tí cryptographers lè ìdánwò gidi.

èsì náà ni a pe ní **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.

Zero-knowledge ti blocked ní doors méta — interaction, trusted setup, àti imperfect soundness. Construction llango yọ kọjá ní ẹnu-òná miíràn: rulebook náà kò lè efficiently refute simulator náà.

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.

Classical zero-knowledge béèrè bóyá simulator kan wà; “effectively zero-knowledge” béèrè nikan bóyá rulebook tí o yan lè efficiently fi ẹrí múlẹ pé simulator kò lè wà. Ìbéèrè tó weaker yíí ni ohun tó jẹ kí construction

nàà keep òkan message, no setup àti perfect soundness.

Original diagram — The Clean Paper CC BY 4.0

ìdánwò atijó: simulator kan wà

Ọnà classical láti formalize zero-knowledge lo fictional helper kan tí a ní pè ní **simulator**.

Idea nàà ni èyí: imagine Jane, tí **kò** mọ secret Alice. Bí Jane bá lè generate, fúnra rẹ patapata, proofs tí ó look gégé bí proofs tí Bob bá ti gba láti Alice, nígbà nàà proofs Alice kò kọ Bob ohunkóhun tuntun. Jane ti lè fake experience nàà láìsì secret Alice.

Torí nàà classical zero-knowledge demands actual simulator kan. Efficient algorithm kan gbódò wà tó lè produce fake-looking proofs láì mọ secret — *witness*, ní jargon; fún Sudoku, witness nàà ni solved grid gan-an.

Definition nàà powerful, sùgbón ibẹ gan-an ni old impossibility ti bite. Intuition ni èyí. Truly non-interactive proof jẹ string kan nikan. Nígbà tí Bob bá ní string yẹn, ó lè fi hàn èlòmíràn: ó ti gain ability láti fi ẹrí múlẹ statement nàà fún àwọn mìíràn, èyí sì ti sound bí sí i than “nothing.” Classical theorems sharpen intuition yẹn sí impossibilities tó wà lókè.

Properties mètá tí paper yíi insist lórí

Title ìwé ìwádíí nàà name constraints mètá:

No interaction: Alice send proof string kan. Kò sí back-and-forth protocol.

No setup: Alice àti Bob kò rely lórí trusted common reference string tàbí pre-arranged public randomness mìíràn. Ọpọ̀ ètò tí a pe ní “non-interactive zero-knowledge” sì rely lórí setup; ìwé ìwádíí yíi túmọ̀ sí zero setup.

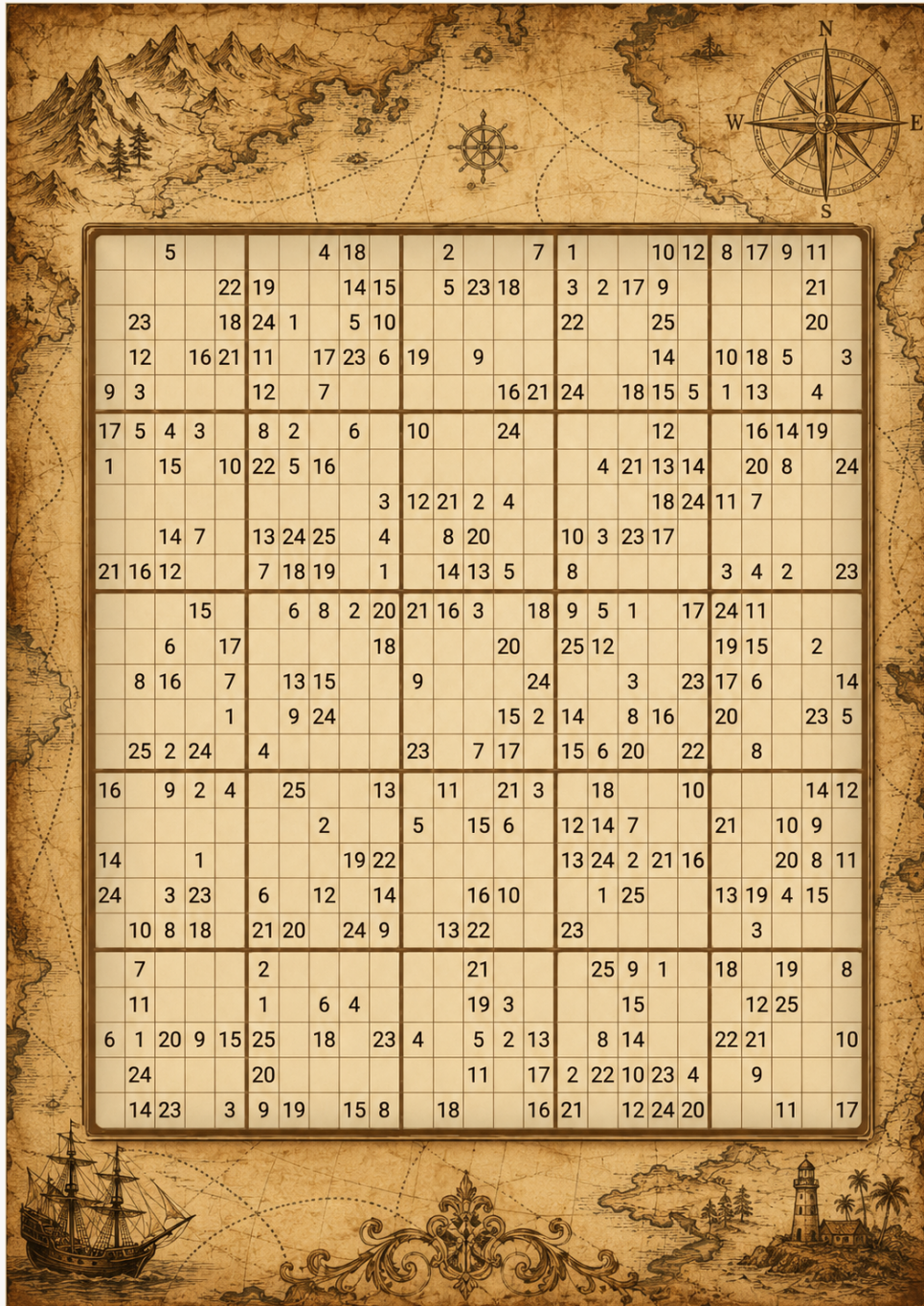
Perfect soundness: false statement kò ní valid proof. Kì í ẹ “almost never accepted”; valid proof kankan kò exist.

Properties mètá yíi gan-an ni ordinary written mathematics ní — àti, gégé bí a ẹ explain lókè, classical zero-knowledge kò lè keep wọn.

Mega-Sudoku èdà kan ti iyàtò nàà

Ẹ jẹ ká lo deliberately simplified way láti feel difference nàà.

Má ẹ lo ordinary 9-by-9 Sudoku fún serious part of analogy. Ó kere ju, ó sì finite ju: computer lè kan solve rẹ, tàbí fi ẹrí múlẹ pé kò ní solution. Dípò bẹẹ imagine family of **MegaSudoku(n)** puzzles. Scale usual òfin up: yan block ìwọ̀n n , jẹ kí $N = n^2$, kí o sì build N by N grid tí a divide sí n by n blocks, pẹ́lú N symbols. Ordinary Sudoku jẹ tiny $n = 3$, $N = 9$ ọ̀ràn nìkan: 9-by-9 grid, 3-by-3 blocks àti symbols mèsàn-án. Proof-complexity itàn bèrẹ̀ gidi nígbà tí n lè grow, àti nígbà tí grid lè carry extra gadgets tí yóò jẹ kó behave bí SAT formula tí a wọ̀ ní aṣọ Sudoku. SAT formula jẹ list of yes/no constraints nìkan: ẹ̀ o lè assign true/false values sí variables kí gbogbo constraints satisfy?



25x25 Sudoku kan: a lè check òfin rẹ lài reveal finished grid — visual stand-in fún proof kan tó verify hidden solution, witness náà.

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

Sudoku àti SAT: puzzle kan náà nínú aṣọ méjì

Claim pé Sudoku kan lè “behave like a SAT formula” kì í ṣe metaphor. Translation náà ní lọ ní ìtọṣọ̀nà méjèèjì, easy ìtọṣọ̀nà sì lè kọ sílẹ̀ patapata.

Láti Sudoku sí SAT. SAT sọ true/false nìkan, torí náà fún un ní boolean variable kan fún every (row, column, value) triple: $x(r,c,v)$ túmọ̀ sí “ṣẹ̀lì ní row r , column c contains value v .” 4-by-4 Sudoku (2-by-2

blocks, values 1–4) nílò $4 \cdot 4 \cdot 4 = 64$ variables; classical 9-by-9 nílò 729. Every Sudoku òfin nàà di batch of clauses. (Clause jẹ OR of variables tàbí negations wọn; whole formula ni AND of gbogbo clauses.)

Every seçli holds at least òkan value — òkan clause per seçli:

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

Every seçli holds at most òkan value — “not both” clause kan fún each pair of values:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3) \quad \dots \text{ àti bẹ̀ẹ̀ lọ fún gbogbo six pairs.}$$

Every row contains every value — fún row 1 àti value 3: at least once,

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

àti at most once: $\neg x(1,1,3) \vee \neg x(1,2,3)$, àti bẹ̀ẹ̀ lọ fún each pair of seçli nínú row.

Columns àti blocks — identical batches; ẹgbẹ of seçli nìkan ló yàtò. Fún top-left block àti value 2:

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

plus pairwise “not both” clauses.

Printed clues — easiest part: clue kọọkan jẹ clause pèlú single variable. Printed 3 ní top-left corner di clause

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

AND of gbogbo èyí satisfiable exactly when Sudoku ní solution — satisfying assignment nàà sì jẹ solution: ka $x(r,c,v)$ wo ni true, kí o fill grid. Fún 9-by-9, èyí jẹ variables 729 àti a few thousand clauses, tí modern SAT solver lè dispatch ní milliseconds. Ẹ akiyesi clue clause $x(1,1,3)$: ó sọ “seçli yí equals exactly 3,” kì í ẹ “seçli wònyí are gbogbo yàtò” — asymmetry kan nàà tó máa force extra trick fún clue seçli nínú protocol note tó wà ní isalẹ.

Láti SAT sí Sudoku. ìwé ìwádíí nílò opposite, harder ìtọ́sọ̀nà: fún *arbitrary* SAT formula, build mega-Sudoku tó ní solution exactly when formula nàà does. Native òfin Sudoku lè sọ “seçli wònyí gbogbo yàtò” nìkan, torí nàà arbitrary logical constraints gbódò *built* — èyí gan-an ni gadgets. Gadget jẹ small pre-fabricated cluster of seçli, òkan per clause of formula, níbi tí designated seçli ẹ role of variables (symbol tí wọn hold encode true tàbí false), internal constraints cluster nàà sì engineered kí nìkan legal fillings correspond sí assignments tí satisfy clause. Èyí jẹ standard craftsmanship láti NP-completeness proofs; fún generalized Sudoku, Yato àti Seta ẹ é ní 2003.

Together, ìtọ́sọ̀nà méjèjè sọ pé N-by-N Sudoku àti SAT jẹ ìṣòro kan nàà tí wọn wọ aṣo yàtò. Èyí ni ohun tó license article yí — àti ìwé ìwádíí nàà — láti tell itàn nípa gbogbo NP pèlú grids àti symbols.

Witness nàà sì rọrùn láti picture. Alice mọ complete valid filling ti mega-Sudoku. Bob fẹ convinced pé filling bẹ̀ẹ̀ wà, ṣùgbọ́n Alice kò fẹ reveal rẹ. Bí ó bá send whole filling, Bob convinced, ṣùgbọ́n secret ti gone.

Nínú classical zero-knowledge èdà, Alice àti Bob interact. Old-style mental àwòṣe kan lo covered tiles. Alice hide solved grid, secretly rename symbols sáájú round kọọkan, ó sì jẹ kí Bob inspect òkan randomly chosen agbègbè constraint: row, column, box, tàbí gadget. Bí opened seçli bá fi hàn all-different symbols, Bob gain ìgbẹ̀kẹ̀lẹ̀. Lẹ́yìn nàà gbogbo nìkan ni a cover lẹ́ẹ̀kan síí, symbols sì freshly renamed. (Wrinkle kan: given clues puzzle nàà nílò extra trick, torí renaming symbols hide wọn nàà. Note tó wà ní isalẹ explain bí classical protocols ẹ solve èyí; toy

picture náà tó fún ohun tó tẹ̀lé.)

Bí classical protocols ẹ̀se handle clue cells gidi

Renaming trick ní blind spot. Row, column àti box òfin gbogbo sọ “these ẹ̀ṣẹ̀li are gbogbo yàtò,” *gbogbo yàtò* sì survive renaming of symbols *èyíkéyí*. Şùgbón clue kan sọ “ẹ̀ṣẹ̀li yí contains exactly 5,” lẹ́yìn renaming Bob rí $\sigma(5)$ nìkan — masked symbol kan — láì mọ́ renaming σ . Kò lè check ohunkóhun. Bí a kò bá fix *èyí*, Alice lè fi *èrí* múlẹ́ pé *some* valid grid exists nígbà tó ignore printed clues patapata, *èyí* kò fi *èrí* múlẹ́ ohunkóhun nípa *this* puzzle. Classical literature ní standard repairs méjì.

Palette náà. Fi extra row kan ti N ẹ̀ṣẹ̀li kun hidden grid — palette tí Alice fill pẹ̀lú symbols $1 \dots N$ ní fixed public order, lẹ́yìn náà ó rename rẹ́ pẹ̀lú everything else, torí náà ó contains $\sigma(1) \dots \sigma(N)$. Random challenge Bob ní extra option kan bá yí. Yàtò sí picking row, column, box tàbí gadget láti open, ó lè pick **palette plus òkan clue ẹ̀ṣẹ̀li**. Alice uncover méjèjì; palette reveal renaming round yẹn, Bob sì check pé clue ẹ̀ṣẹ̀li fi hàn exactly renamed *èdà* of printed clue. *Èyí* stay zero-knowledge torí Bob learn σ nìkan — freshly drawn every round, useless on its own — àti value of ẹ̀ṣẹ̀li tí ó ti mọ́ láti puzzle. Kò sí secret ẹ̀ṣẹ̀li information tó leak, simulator sì lè fake view nípa drawing random σ . Ó sound torí cheating Alice máa caught pẹ̀lú fixed probability per round, rounds sì repeated tí tí doubt fi negligible.

Compiling clues away. Structural variant mún remove special challenge dípò kó add rẹ́. Dípò *verifying* clue value, force rẹ́ pẹ̀lú difference constraints: link clue ẹ̀ṣẹ̀li sí every palette ẹ̀ṣẹ̀li except òkan carrying own value — “yàtò láti $\sigma(1)$, yàtò láti $\sigma(2)$, ..., yàtò láti everything şùgbón $\sigma(5)$.” Only symbol ẹ̀ṣẹ̀li náà lè legally hold ni clue náà. Every constraint bá yí jẹ́ “these méjì differ” lẹ́ẹ̀kan sí — invariant lábẹ́ renaming, checkable exactly like row. Maneuver kan náà ni a lo fún pre-colored vertices nínú classical graph-coloring protocol, ó sì jẹ́ spirit of word *gadgets* lókè: nínú MegaSudoku-as-SAT picture, clues are compiled sínú inequality gadgets bí every other constraint.

Physical protocol náà. ayé gidi card protocol fún Sudoku (Gradwohl, Naor, Pinkas àti Rothblum, 2007) kò lo renaming rárá, ó sì settle clues *şáájú* kí hiding tó bèrẹ́. Fún every ẹ̀ṣẹ̀li, Alice lay down identical cards méta pẹ̀lú value ẹ̀ṣẹ̀li náà — face-down fún secret ẹ̀ṣẹ̀li, şùgbón **face-up fún clue ẹ̀ṣẹ̀li**, kí Bob fi ojú ara rẹ́ rí pé clues respected *şáájú* kí cards flipped. Lẹ́yìn náà card kan láti each ẹ̀ṣẹ̀li wọ́ packet row rẹ́, òkan sínú column, òkan sínú box; packet kọ́kan shuffled àti revealed, Bob sì check pé ó contains gbogbo N symbols. Shuffling destroy position information (iyẹn ni zero-knowledge), şùgbón clues ti nailed down ní dealing *àkókò*.

Either way, lesson náà jẹ́ ohun kan náà tí article yí ní padà sí: zero-knowledge protocol jẹ́ careful bookkeeping ti *which* facts survive hiding. Renaming preserve “gbogbo yàtò” ó sì erase “equals 5” — torí náà “equals 5” gbọ́dọ́ smuggled back in ní other means.

Èyí kì í ẹ̀se protocol inú iwé iwádíí. Ó jẹ́ mental àwòşẹ́ fún classical zero-knowledge:

- Alice àti Bob go back àti forth.
- Bob choose random checks.
- Alice reveal agbègbè consistency nìkan, kì í ẹ̀se whole solution.
- Privacy proof *şişẹ́* nípa showing pé Bob’s view lè have been generated láìsí secret solution Alice.

Torí náà classical zero-knowledge built around positive fact kan:

Simulator kan wà gidi.

Báyí remove comfortable parts. Alice send proof string kan, ó sì walk away. Kò sí trusted setup, kò sí shared random string prepared in advance, Bob sì gbòdò never accept false puzzle. Èyí ni setting tí classical zero-knowledge kò lè survive.

Character kan sí nílò sháájú trick náà. Fix **rulebook** kan: formal proof ètò, ní sense ti logician — fixed set of axioms plus mechanical òfin fún checking written mathematical proofs. ZFC, standard axioms of mathematics, ni canonical example. Gbogbo nìkan láti ibi lọ ni stated relative sí rulebook tí a choose in advance, choice sì flexible: construction sìṣẹ́ fún rulebook èyíkẹyí tí o fix, ZFC included.

(Note kan lóri words, borrowed láti iwé iwádíí fúnra rẹ: “proof ètò” níbí nigbagbogbo tùmò sí rulebook yí — formal ètò tó check mathematical proofs — kò tùmò sí messages Alice send. Machinery Alice àti Bob ni a pé ní “prover àti verifier.”)

Gödel-style èdà keep mega-Sudoku itàn, ṣùgbón ó change proof náà.

Yan second constraint ètò kan ti displayed iwọn kan náà, pè é ní **D**. Fún itàn náà, S àti D jẹ MegaSudoku(n) puzzles méjì ní format kan náà. Behind scenes, D lè have started as hard logical formula of yàtò iwọn; bí needed, a lè pad rẹ pẹ̀lú harmless dummy constraints kí ó fit grid kan náà. D built láti logical formula tó jẹ **unsatisfiable** gidi: kò sí ṣeé ṣe assignment of values tó make gbogbo constraints true, bí broken puzzle tí kò ní legal completed grid. Toy example ni formula tó demand “X is true” àti “X is false” méjèjì. Torí náà D kò ní valid filling.

Ṣùgbón D kò gbòdò jẹ broken puzzle tí ó *easy to expose*. Toy example lókè fail: rulebook èyíkẹyí refute “X àti not-X” ní line kan. D gbòdò false ní way tí chosen rulebook kò lè certify pẹ̀lú short argument. Bí rulebook bá lè refute D pẹ̀lú short proof, itàn tó wà ní isalẹ collapse: alternative route tó lè have produced proofs láìsí secret Alice lè formally ruled out, àṣírí guarantee náà sì parí. Torí náà a yan D láti family tí fixed rulebook kò lè efficiently refute: kò sí short proof, nínú rulebook yẹn, pé D has no solution.

One-message proof Alice jẹ nípa either/tàbí statement:

either gidi mega-Sudoku S has a solution, tàbí decoy D has a solution.

Èyí ni logical link. D **kò** generated ní magical way kan tó make S true. Proof náà kò argue “D has no solution, therefore S has a solution.” Ó ní fi ẹrí múlẹ́ disjunction **S tàbí D**. Perfect soundness sọ pé false disjunction kò lè ní valid proof. Níwọn bí D ti false gidi — kò ní solution — nìkan way disjunction lè true ni pé S true. Torí náà bí proof accepted, S gbòdò ní solution. Decoy kò lè make false S true.

Ṣùgbón fún zero-knowledge-style part, béèrè ohun tó máa ṣẹ̀lẹ́ bí D *bá ní* solution. Decoy solution yẹn máa act as alternative witness. Ó máa jẹ kí ẹnìkan produce proofs láì mọ gidi mega-Sudoku solution Alice — simulator, ní other words. Ní reality D kò ní solution, torí náà simulator route yí closed. Point náà ni pé rulebook kò lè efficiently fi ẹrí múlẹ́ pé route náà closed.

Torí náà D ní jobs méjì. Fún **soundness**, D false, torí valid proof of “S tàbí D” force S. Fún **effective zero-knowledge**, D hard to refute, torí rulebook kò lè quickly òfin out decoy route tó bá ti make simulation ṣeé ṣe.

Torí náà security idánwò kò longer jẹ:

Ṣé a lè fi ẹrí múlẹ́ pé simulator kan wà gidi?

Ó di:

Şé rulebook rẹ lè efficiently fi ẹrí múlẹ pé simulator impossible?

Bí answer bá jẹ no, nńkan surprisingly lágbára follow: every security guarantee tí (a) a lè observe nípa running ìdánwò, àti (b) provably follows — inside rulebook yẹn — láti existence of simulator, actually holds. Successful ìkọlù lóri eyikeyi wọn yòò fúnra rẹ amount sí missing short refutation, missing short refutation yẹn kò sì exist. Ìyẹn ni “effective” part of effectively zero-knowledge.

Torí náà classroom contrast ni:

Classical zero-knowledge: proofs láilẹwu torí simulator exists.

Gödel-style effective zero-knowledge: proofs treated as láilẹwu fún observable security ìdánwò torí rulebook kò lè efficiently fi ẹrí múlẹ pé simulator impossible.

Claim kejì weaker. Ó tún jẹ reason tí ìwé ìwádíí lè keep àbùdá mẹta tí broke classical ẹdà: ọkan message, no setup àti perfect soundness.

ìdánwò tuntun: o kò lè fi ẹrí múlẹ pé simulator absent

Relaxation Ilango change ìbéèrè náà.

Classical zero-knowledge asks:

Does a simulator exist?

Effectively zero-knowledge asks something weaker:

Can your chosen rulebook efficiently fi ẹrí múlẹ that no simulator exists?

Èyí sound bí technical dodge, şùgbọn core idea ni. Construction náà wà nínú strange ipò: simulator gidi kò exist — ìwé ìwádíí explicit nípa èyí — şùgbọn rulebook tí o fix kò lè efficiently fi ẹrí múlẹ pé kò exist. Bí every bad consequence tí o care nípa bá require such refutation, ètò náà şì behave like zero-knowledge fún consequences wònyẹn.

Ibí ni Gödel enter. Kì í şe decoration, kì í şe “Gödel makes crypto secure.” Connection náà proof-theoretic. Rulebook kan ni a pe ní **optimal** bí, ní precise sense, ó jẹ best şeé şe ọkan: whenever any rulebook lè refute formula of relevant kind pẹlú short proof, optimal rulebook náà lè şe bẹẹ náà, pẹlú proof at most polynomially longer. Krajíček àti Pudlák conjectured ní 1989 pé **no optimal proof ètò exists**: whichever rulebook o fix, some other rulebook proves some family of true statements far sí i succinctly. Èyí jẹ ọkan of central open conjectures of proof complexity, ó sì jẹ finite, complexity-theoretic cousin of Gödel’s incompleteness theorem: some true statements have no short proof nínú rulebook tí o fix — kì í şe torí wọn unprovable in principle, şùgbọn torí every fixed rulebook leave some short truths láísí short proofs.

ìwé ìwádìí assume conjecture yíí (ní mildly stronger “infinitely often” form, standard when conjectures lè cryptographically). Payoff, nípa theorem of Krajíček àti Pudlák, concrete ni: fún every rulebook sequence of formulas kan wà tí genuinely unsatisfiable, tí rulebook kò lè refute pèlú short proofs — àti, crucially, efficient algorithm lè generate wọn. Last property yẹn, uniformity, ni ohun tó turn whole idea láti existence claim sí actual algorithm tí Alice lè run: decoys D rẹ wá láti assembly line, kì í ẹ out of thin air.

Cryptographic move náà ni láti put shortage of proof power yẹn to ẹ.

Ohun tí construction náà ní ẹ

Ẹ jẹ ká strip construction ìwé ìwádìí sí shape rẹ.

Fix rulebook kan — ZFC, say. Under proof-complexity assumption, sequence of formulas kan wà tí a lè efficiently generate, tí actually unsatisfiable, ẹgbọn rulebook kò ní short proof pé wọn unsatisfiable.

Báyí build one-message proof in form yíí:

either gidi statement is satisfiable, tàbí this special hard formula is satisfiable.

Special hard formula náà kò satisfiable. Torí náà bí underlying proof machinery perfectly sound, accepting message náà ẹí mean gidi statement true. Ẹyí give perfect soundness.

Ẹgbọn fún zero-knowledge-like security, imagine special hard formula *were* satisfiable. Witness rẹ lè then be lè to simulate proofs láì mọ gidi witness. Formula náà kò satisfiable in reality — ẹgbọn rulebook kò lè efficiently fi ẹrí múlẹ bẹ. Torí náà kò lè efficiently fi ẹrí múlẹ pé simulator impossible.

Ìyẹn ni hinge. System kò hide secret nípa producing classical simulator. Ó hide secret, fún large class of observable security idánwò, behind rulebook’s inability to certify pé simulator absent.

Ohun tí ìwé ìwádìí claim

Main theorem wá ní layers. Core ẹsì ni ẹyí:

Under standard cryptographic assumption — existence of **non-interactive witness indistinguishable proofs**, well-studied objects tí follow láti several established assumption packages — àti lábẹ proof-complexity conjecture pé **no (infinitely often) optimal proof ètò exists**, ìwé ìwádìí construct, fún every choice of rulebook, one-message prover àti verifier fún NP/SAT pèlú **perfect soundness** àti no setup tí effectively zero-knowledge relative sí rulebook yẹn. (NP/SAT ni standard “hardest common denominator” ti puzzle-like ẹ̀dò; mega-Sudoku jẹ costume kan tí ó wò.)

Fún broader claim nípa preserving falsifiable security properties, ìwé ìwádìí add ọkan sí i standard assumption, derandomization belief **P = BPP** (roughly: randomness kò fún algorithms ní essential extra power).

Ní èdè tí kì í ẹ theorem:

- Proof nàà jẹ ọkan message.
- Kò sí trusted setup.
- False statements kò lè be fi ẹrí múlẹ.
- Prover nàà kì í ẹ classical zero-knowledge — kò ní simulator.
- Sùgbọn every falsifiable, game-based security consequence of classical zero-knowledge lè achieved nínú setting yíí.

“Falsifiable” ẹ pàtàkì. Ó túmọ sí pé security ìkùnà lè idánwò nípa running adversary nínú game. Ọpọ cryptographic security definitions ní form yíí: lè adversary distinguish méjì encryptions, invert a function, recover a witness, tàbí win specified idánwò? Theorem nàà give prover kan fún each falsifiable property, ọkan at a àkókò. Single prover tó enjoy every falsifiable property at once likely impossible — old reusability ìkọlù (“Bob lè fi hàn the proof to others”) fúnra rẹ jẹ falsifiable property, ó sì genuinely fail níbí. Proposal iwé iwádíí ni pé single prover kan plausibly lè cover gbogbo *natural* falsifiable properties — ones tí actually occur nínú cryptographic practice — sùgbọn apá yẹn jẹ conditional theorem tó rest lórí informal notion of “natural,” plus explicit conjecture. Guarantee aimed at observable ìkùnà, kì í ẹ every philosophical tàbí simulation-based meaning of secrecy.

Concrete corollary kan tó láti name: construction yields first non-interactive *witness hiding* proofs pẹlú uniform prover — “proof of a puzzle does not help you rí its solution,” pẹlú no interaction àti no setup — object tó sound modest sùgbọn tí construction rẹ resisted fún decades.

Ohun tí èyí kò sọ

Section yíí ni tó keep piece honest.

Kò sọ pé old impossibility theorems wrong. Construction avoids wọn nípa changing definition.

Kò give ordinary, classical zero-knowledge pẹlú no interaction, no setup àti perfect soundness. iwé iwádíí explicitly sọ pé constructed prover kò ní simulator.

Kò mean proof kò lè be reused. One-message proof sì lè fi hàn fún ẹlòmíràn; iwé iwádíí kò preserve deniability-style properties. (Non-interactive zero-knowledge pẹlú trusted setup ní limitation kan nàà.)

Kò mean pé practical protocol ready fún deployment ni. Èyí jẹ complexity àbá-ẹkọ àti cryptographic foundations. èsì depend lórí major assumptions láti proof complexity àti cryptography, construction nàà sì nípa ohun tó ẹẹ ẹ in principle.

Kò make “Gödel” magic security primitive. Gödel connection wá nípasẹ proof ètò, optimal proof ètò àti finite analogues of incompleteness. Useful intuition kì í ẹ “incompleteness protects your password.” Ó jẹ: bí rulebook kò lè efficiently fi ẹrí múlẹ pé simulator impossible, ìkọlù tí yóò require proof yẹn lè blocked at ìpele of security definitions.

Kí ló dé tí ó fi interesting síbè?

Cryptography sáà turn hardness sínú ààbò. Factoring hard, torí RSA-style assumptions useful. Lattice ìṣòro hard, torí lattice cryptography useful. Ní here hardness stranger: kì í ṣe “hard to compute a secret,” ṣùgbón “hard to fi ẹ́rí múlẹ̀ that a certain proof object kò lè exist.”

Ìdí nìyẹn tí ìwé ìwádíí fi feel unusual. Ó treat axioms àti rulebooks almost like cryptographic resources. Usual impossibility sọ pé tension wà láàárín soundness àti simulation. Move Ilango ni láti place tension nàà behind proof-theoretic curtain: simulator absent, ṣùgbón formal ètò kò lè efficiently expose absence nàà.

Fún reader, surprising part kì í ṣe pé èyí máa replace today’s zero-knowledge ètò. Probably kò ní, at least not taara. Surprising part ni pé limitation láti mathematical logic lè be lò constructively: kì í ṣe wall nìkan, ṣùgbón kind of cover.

Báwo ni ẹ́rí ṣe lágbára tó?

Èyí jẹ́ theorem ìwé ìwádíí, torí nàà “ẹ́rí” tùmọ̀ sí nìkan yàtò sí biology tàbí astronomy ìwé ìwádíí. Ìbéèrè kì í ṣe bóyá ìdánwò replicated. Ìbéèrè ni bóyá definitions, assumptions àti proof chain ṣe àtílẹ̀yìn fún claim nàà.

Proof nàà formal, ìwé ìwádíí sì explicit nípa assumptions rẹ̀. Assumptions nàà kì í casual. Non-interactive witness indistinguishable proofs jẹ́ standard objects nínú cryptography, wọn sì follow láti several established assumption packages. No-optimal-proof-system conjecture jẹ́ central conjecture nínú proof complexity. $P = BPP$ jẹ́ standard derandomization belief tí a lo nìkan fún broader falsifiable-property theorem.

Ìwé ìwádíí tún argue pé assumptions nàà ni right price, kì í ṣe arbitrary scaffold: ó fi ẹ́rí múlẹ̀ converse kan showing pé wọn essentially necessary — bí constructions bí èyí bá exist rárá, non-interactive witness indistinguishable proofs gbòdò exist, àti (granting standard one-way functions) no optimal proof ètò lè exist. Assumptions nàà sì “win-win”: refuting any of them fúnra rẹ̀ yóò jẹ́ landmark discovery nínú proof complexity, cryptography tàbí complexity àbá-ẹ̀kọ̀.

Ṣùgbón torí èsì conditional, ìgbẹ̀kẹ̀lẹ̀ rẹ̀ conditional nàà. Bí assumptions yẹn bá fail, interpretation theorem change. Bí wọn bá hold pàápàá, guarantee nàà kì í ṣe full classical zero-knowledge; ó jẹ́ relaxed, proof-theoretic ẹ̀dà ìwé ìwádíí.

Torí nàà right ìgbẹ̀kẹ̀lẹ̀ ni high pé ìwé ìwádíí establish coherent conditional possibility èsì; moderate pé assumptions rẹ̀ describe cryptographic world tí a ní gbé gidì; low fún any immediate practical consequence.

Kí nìdí tí ó fi ṣe pàtàkì?

Ìwé ìwádíí nàà open route kan tí a ro pé closed.

Classical àbá-ẹ̀kọ̀ sọ pé: full zero-knowledge kò lè be ọ̀kan message láìsì setup, kò sì lè perfectly sound. ìwé ìwádíí Ilango sọ pé: bí a bá ask fún consequences of zero-knowledge tí a lè ìdánwò nínú security games, àti bí a bá allow

security definition to depend lórí ohun tí rulebook lè tàbí kò lè efficiently refute, nígbà náà púpò useful ìhùwàsí lè recovered — pèlú òkan message, no setup àti perfect soundness.

Èyí kì í ẹ small definitional tweak. Ó jẹ way yàtò láti think nípa cryptographic guarantees. Dípò asking nìkan what exists, ask what rulebook rẹ lè òfin out. Dípò treating unprovability bí philosophical nuisance, lò rẹ as ịṣètò.

Practical world lè má change lọla. Ẹ̀gbọ̀n conceptual map change. Formal sense kan wà báyyí níbi tí “no òkan lè efficiently fi ẹrí múlẹ̀ that the secret leaked” lè lágbara tó láti recover many game-based protections tí a fẹ̀ láti “the secret did not leak.”

Ìdí nìyẹn tí Gödel fi belong nínú title.

Àkótán kedere

Zero-knowledge proofs jẹ kí prover convince verifier pé statement true láì reveal witness. Classical impossibility èsì sọ pé zero-knowledge kò lè squeezed sí òkan message láìsí setup, kò sì lè ní perfect soundness. ìwé ìwádíí Rahul Ilango kò refute impossibilities yẹn. Ó define weaker notion, effectively zero-knowledge: dípò requiring pé simulator really exists, ó require pé chosen proof ètò — formal rulebook bí ZFC — kò lè efficiently fi ẹrí múlẹ̀ pé no simulator exists. Under major assumptions láti cryptography (non-interactive witness indistinguishable proofs) àti proof complexity (no optimal proof ètò exists), ìwé ìwádíí construct one-message provers fún NP/SAT pèlú no setup àti perfect soundness tí achieve falsifiable, game-based consequences of zero-knowledge property by property. Single prover tó cover gbogbo “natural” properties bẹ̀ẹ̀ jẹ̀ further, partly conjectural extension — covering literally every falsifiable property likely impossible, torí proofs remain reusable. èsì náà theoretical àti conditional, kì í ẹ deployed primitive, ẹ̀gbọ̀n ó fi hàn tuntun way láti lò proof-theoretic unprovability as cryptographic resource.

Àyèwò láìsí àṣejù

Ohun tí ìwé ìwádíí fi hàn: Under stated assumptions, a lè build one-message, no-setup, perfectly sound provers fún NP/SAT tí effectively zero-knowledge relative sí any chosen proof ètò, tí wọn sì achieve each falsifiable game-based consequence of classical zero-knowledge.

Ohun tó ẹ́ẹ̀ gbà ẹ̀gbọ̀n tí a kò fi ẹrí múlẹ̀ unconditionally: Pé needed proof-complexity àti cryptographic assumptions hold. Wọn serious, well-studied assumptions — ìwé ìwádíí sì fi hàn pé wọn essentially necessary as well as sufficient — ẹ̀gbọ̀n assumptions ni wọn sì jẹ.

Ohun tí kò fi hàn: Classical zero-knowledge pèlú no interaction, no setup àti perfect soundness; practical ètò ready fún deployment; deniability tàbí non-reusability of proofs; tàbí pé Gödel’s incompleteness theorem fúnra rẹ secure cryptography.

Main limitations: Guarantee náà jẹ relaxation of zero-knowledge; broadest ẹ̀dà depend lórí multiple assumptions; single-universal-prover claims remain partly conjectural; èsì náà sì primarily foundational.

Confidence wo ni gbogbogbò reader yẹ kí ó ní? High pé èyí jẹ important conditional àbá-ẹkọ èsì bí a bá accept definitions. Moderate pé assumptions capture reality. Low fún immediate practical deployment. Safe takeaway ni: ìwé ìwádìí nàà kò break zero-knowledge impossibilities; ó rí tuntun proof-theoretic way around parts of them tí matter fún many security games.

Àwọn orísun

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>