The Clean Paper

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

Cryptographic proof tokko simulator dhabame prove gochuun rakkisaa taasisuun iccitii isaa dhoksuu danda'a

Zero-knowledge proofs namni statement tokko witness osoo hin mul'isin prove akka godhu dandeessisu. Classical theory hiika guutuu keessatti ergaa tokko, trusted setup malee fi perfect soundness waliin kana qabaachuun hin danda'amu jedha. Paper Rahul Ilango impossibility sana hin balleessu. Target jijjiira: simulator dhugumaan jiraachuu gaafachuu mannaa, proof system filatame tokko simulator akka hin jirre efficiently prove gochuu akka hin dandeenye gaafata. Assumptions guguddoo proof-complexity fi cryptography jalatti, kun consequences falsifiable, game-based zero-knowledge property tokkoon tokkoon isaanii deebisuuf gaha. Point isaa internet primitive plug-in tokko miti. Mathematical unprovability cryptographic cover gochuuf karaa proof-theoretic dha.

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

Mala keessaa dhoksuuf ragaa kennuun osoo hin taane, fakkeessituu dhabame akka mirkanaa'u rakkisaa gochuu dha

Zero-knowledge keessaa gosa salphaa irraa haa jalqabnu.

Alice Sudoku puzzle tokko furmaata qabaachuu Bob amansiisuu barbaaddi. Furmaata yoo ergite, Bob ni amana, garuu puzzle sun iccitii isaa dhaba. Alice wanti barbaaddu kana caalaa ajaa'iba: furmaata akka jiru ragaa kennuu, furmaata sana osoo hin mul'isin.

Kun waadaa **zero-knowledge ragaa** ti. Prover (Alice) statement tokko dhugaa ta'uu verifier (Bob) amansiisa, garuu dhugummaa statement sanaa alatti homaa hin saaxilu.

Rakkoon isaa waadaan kun kaffaltii qaba. Ragaan herregaa idilee amaloota mijataa lama qaba. Inni **ergaa tokko** dha: barreessita, namaaf kennita, deemta. Akkasumas **perfectly sound** dha: statement sobaa ragaa sirrii homaa hin qabu. Kilaasikaalaa impossibility bu'aawwan zero-knowledge amaloota lamaan kana dhiisuu akka qabu jedhu — lamaan walitti qofa miti; tokkoon tokkoon isaanii addaan illee daangaa keessaa ala.

Tokkoffaa, zero-knowledge ragaa marii barbaada. Alice ergaa tokko qofa ergee, trusted setup dursee qophaa'e yoo hin jirre, zero-knowledge guarantee kufa — soundness hammam akka gadi buusuuf fedhii qabaattus kun ni jiraata.

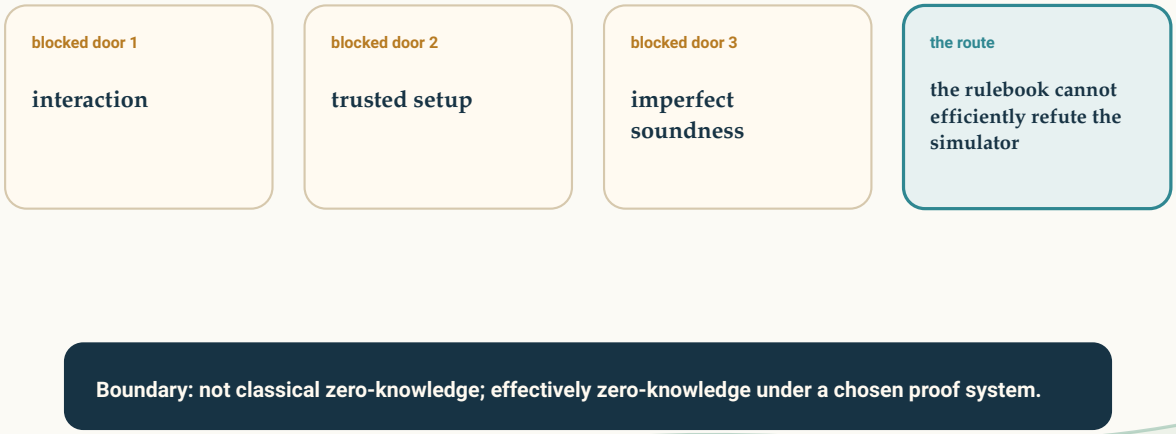
Lammaffaa, zero-knowledge ragaa dogoggora xiqqoo obsuu qaba. Perfect soundness gaafachuun interaction illee callisee balleessa: verifier tasaa choices inni godhu kamiyyuu irratti matumaa gowwoomfamuu hin danda'u yoo ta'e, choices sana dursee sirreessu danda'a; verifier predictable taanaan Alice waan hunda ergaa tokko keessatti deebisuu danda'a, kun immoo haala duraan rakkoo keessa seene sana dha.

Barruu Rahul Ilango daangaa lamaa kana irraa karaa biraatiin darbuu ilaala. Daangaan akka hin jirre fakkeessuun miti; impossible setting keessatti kilaasikaalaa zero-knowledge oomishuunis miti. Sochiin isaa subtle dha: "homaa hin saaxilu" jechuun maal akka ta'e laaffisa, garuu security amaloota cryptographers dhugumaan qorachuu danda'an akka hafanitti laaffisa.

Bu'aan kun **effectively zero-knowledge** jedhama.

A proof without leaking the witness

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



Zero-knowledge karra sadii irratti cufama — interaction, trusted setup fi imperfect soundness. Ilango karaa biraatiin seena: kitaaba seeraa sun fakkeessituu akka hin jirre efficiently refute gochuu hin danda'u.

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.

Kilaasikaalaa zero-knowledge fakkeessituu dhugumaan jira moo jedha; "effectively zero-knowledge" immoo kitaaba seeraa ati filatte fakkeessituu akka hin jirre efficiently mirkaneessuu gochuu danda'a moo qofa gaafata.

Gaaffiin laafaan kun ergaa tokko, setup dhabuu fi perfect soundness waliin akka turu taasisa.

Qormaata durii: fakkeessituu tokko jira

Kilaasikaalaa zero-knowledge formalize gochuuf gargaaraa yaadame tokko **fakkeessituu** jedhamee waamama.

Yaadni isaa kana: Jane jechuun nama iccitii Alice **hin beekne** yaadi. Jane ofuma isaatiin proofs Bob Alice irraa argatu fakkaatan uumuu yoo dandeesse, proofs Alice Bob waan haaraa hin barsiifne jechuu dha. Jane iccitii Alice malee experience sana duraanuu fake gochuu dandeessi.

Kanaaf kilaasikaalaa zero-knowledge fakkeessituu dhugaa gaafata. Algorithm efficient tokko iccitii — jargon keessatti *witness* — osoo hin beekin proofs fakkeessuu danda'u jiraachuu qaba. Sudoku keessatti witness grid furame qofa dha.

Hiika kun cimaa dha, garuu impossibility durii itti ciniinu bakka kana. Intuition isaa: ragaa dhugumaan non-interactive ta'e string tokko qofa dha. Bob string sana erga qabaatee booda nama biraatti agarsiisuu danda'a: statement sana namoota biraatti mirkaneessuu gochuu dandeettii argateera, kun immoo "homaa" caalaa waan argate fakkaata. Kilaasikaalaa theorems intuition sana impossibilities armaan oliitti jabeessu.

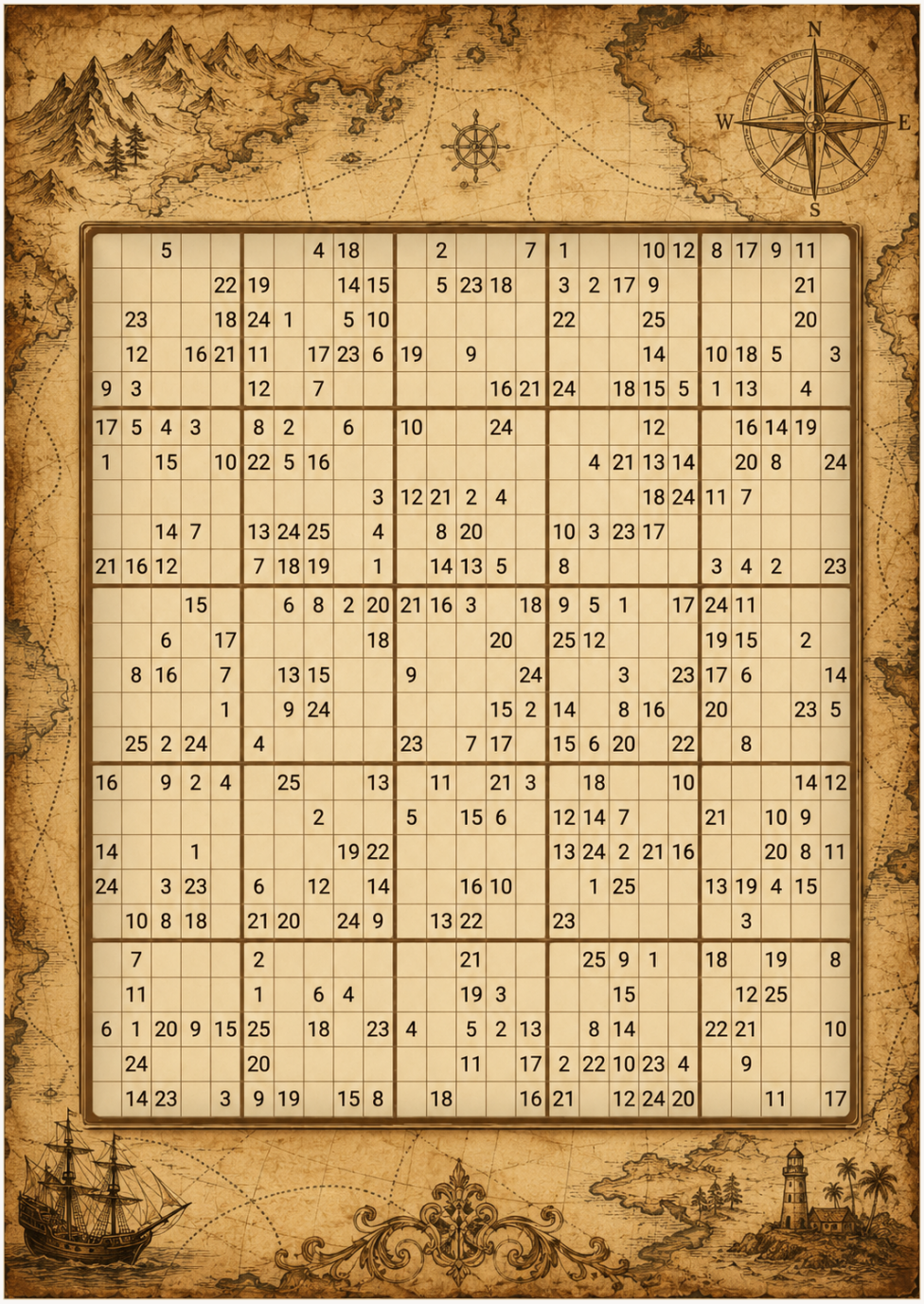
> **Barruu kun amaloota sadii irratti cicha**
>
> Maqaan barruu kanaa constraints sadii kaasa:
> **Interaction hin jiru:** Alice ragaa string tokko erga. Protocol deebi'anii wal-dubbachuu hin qabu.
> **Setup hin jiru:** Alice fi Bob trusted baramaa wabii string yookaan ummataaf banaa carraa tasaa dursee qophaa'e irratti hin hirkatan. Sirnoota "non-interactive zero-knowledge" jedhaman hedduun setup irratti hirkatu; barruu kun setup zero jechuu dha.
> **Perfect soundness:** statement sobaa ragaa valid homaa hin qabu. "Jechuun ni danda'ama never accepted" miti; ragaa valid tokko illee hin jiru.
> Amaloota sadan kun wantoota ragaan herregaa barreeffamaa idilee qabu dha — kilaasikaalaa zero-knowledge immoo, akka olitti ibsame, isaan eeguu hin danda'u.

Garaagarummaa kana MegaSudoku'n yaaduu

Garaagarummaa kana ittiin hubatan karaa salphaa ta'e tokko kana.

Analogy serious keessatti Sudoku 9×9 idilee hin fayyadamin. Baay'ee xiqqaa fi daangeffame dha: kompiitara salphaatti furuu, yookaan furmaata akka hin qabne mirkaneessuu gochuu danda'a. Bakka isaa maatii puzzles **MegaSudoku(n)** jedhamu yaadi. Rule idilee guddifadhu: block hammamtaa n

filadhu, $N = n^2$ godhi, grid N by N block n by n irraa ijaarame, symbols N qabu. Sudoku idilee haala xiqqaa $n = 3$, $N = 9$ qofa: grid 9×9, blocks 3-by-3 fi symbols sagal. Seenaa proof-complexity n guddataa deemuu yeroo eegaluu fi grid gadgets dabalataa SAT formula akka Sudoku uffateetti hojjachiisan yeroo baatu qofa jalqaba. SAT formula jechuun constraints eeyyee/lakkii tarree qofa: variables'f true/-false gatiiwwan kennuun constraints hunda satisfy gochuu dandeessaa?



Sudoku 25x25: rules isaa grid guutuu osoo hin mul'isin sakatta'uun ni danda'ama — furmaata dhokataa, witness, mirkaneessuu gochuuf fakkeenya mul'ataa.

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

Sudoku fi SAT: puzzle tokko uffata lama keessa

Sudoku "SAT formula akka ta'etti hojjachuu danda'a" jechuun metaphor miti. Translation kallattii lamaan deema, kallattii salphaa immoo guutuutti barreessuun ni danda'ama.

Sudoku irraa gara SAT. SAT true/false qofa dubbata, kanaaf (row, column, gatii) triple tokkoon tokkoof boolean jijjiiramaa tokko kenni: *x(r,c,v)* jechuun "seelii row *r*, column *c* keessa gatii *v* qaba" jechuu dha. Sudoku 4-by-4 (blocks 2-by-2, gatiiwwan 1–4) variables 4·4·4 = 64 barbaada; kilaasikaalaa 9 × 9 variables 729 barbaada. Rule Sudoku tokkoon tokkoon isaa clauses hedduutti jijjiirama. (Clause jechuun variables yookaan negations isaanii Yookaan godhuu dha; formula guutuun clauses hunda Fi godha.)

Seelii hundi gatii tokko yoo xiqqaate qaba — seelii tokkoof clause tokko:

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

Seelii hundi gatii tokko caalaa hin qabu — gatiiwwan lama lamaaf clause "lamaan waliin miti" jedhu:

$$\neg x(1,1,1) \vee \neg x(1,1,2) \quad \neg x(1,1,1) \vee \neg x(1,1,3)$$ ... fi pairs ja'a hundaaf itti fufa.

Row hundi gatii hunda qaba — row 1 fi gatii 3'f: yoo xiqqaate yeroo tokko,

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

fi yeroo tokko caalaa miti: $\neg x(1,1,3) \vee \neg x(1,2,3)$, akkasuma seelota row keessaa pairs hundaaf.

Columns fi blocks — batches wal-fakkaataa; garee seelota qofa jijjiirama. Block gubbaa-bitaa fi gatii 2'f:

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

itti aansuun pairwise "lamaan waliin miti" clauses.

Clues maxxanfaman — kutaa salphaa: clue tokkoon tokko clause jijjiiramaa tokko qofa qabu. 3 top-left irratti maxxanfame clause kana ta'a:

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

Fi wantoota kana hunda satisfiable ta'a exactly yeroo Sudoku furmaata qabu — satisfying assignment *ofuma isaa* furmaata dha: x(r,c,v) keessaa kam true akka ta'e dubbisiitii grid guuti. 9 × 9 tokkoof variables 729 fi clauses kumaatama muraasa ta'a, ammayyaa SAT solver milliseconds keessatti fura. Clue clause x(1,1,3) hubadhu: "seelii kun exactly 3 dha" jedha, "seelota kun hundi adda" miti — asymmetry wal fakkaatu kun protocol note gadi keessatti clue seelota'f trick dabalataa akka barbaachisu taasisa.

SAT irraa gara Sudoku. Barruu kun kallattii faallaa, rakkisaa, barbaada: SAT formula *arbitrary* tokko fudhattee, mega-Sudoku furmaata qaba exactly yeroo formula sun furmaata qabu ijaari. Rules native Sudoku "seelota kun hundi adda" qofa jechuu danda'u, kanaaf arbitrary loojikaalaa constraints *ijaaramuu* qabu — kunis gadgets dha. Gadget cluster seelota xiqqaa dursee qophaa'e, formula clause tokko tokkoof tokko, bakka seelota murtaa'an gahee variables taphatan (symbol isaan qaban true yookaan false koodessaa) fi constraints cluster keessaa

fillings legal qofa clause sana satisfy godhan akka ta'anitti qophaa'e. Kun hojii istaandaardii NP-completeness proofs keessatti; generalized Sudoku'f Yato fi Seta 2003 keessatti hojjetan. Kallattii lamaan walitti, N-by-N Sudoku fi SAT rakkoo tokko uffata lama keessatti jedhu. Kun article kana — fi barruu kana — grids fi symbols fayyadamuun NP hunda irratti seenaa dubbachuuf hayyama.

Witness ammallee suura yaaduuf salphaa dha. Alice mega-Sudoku guutuu sirrii tokko beekti. Bob filling akkasii akka jiru amanuu barbaada, garuu Alice isa mul'isuu hin barbaaddu. Filling guutuu yoo ergite Bob ni amana, iccitiin garuu bade.

Kilaasikaalaa zero-knowledge gosa keessatti Alice fi Bob wal-interact godhu. Mental moodeela durii tokko covered tiles fayyadama. Alice grid furame dhoksa, round tokkoon tokko dura symbols iccitiin maqaa jijjiirti, Bob immoo naannoo keessaa constraint tasaa filatame tokko — row, column, box, yookaan gadget — akka ilaalu eeyyamti. Seelota banaman symbols hundi adda ta'uu yoo agarsiisan Bob amanamummaa argata. Sana booda hundi deebi'ee haguugama, symbols immoo maqaa haaraan jijjiiramu. (Rakkoo xiqqoo tokko: clues puzzle irratti kennaman trick dabalataa barbaadu, sababni isaa renaming symbols clues illee dhoksa. Note gadi jiru kilaasikaalaa protocols kana akkamitti furatan ibsa; suura toy kun waan itti aanuuf gahaa dha.)

Kilaasikaalaa protocols clue seelota dhugumaan akkamitti qabatu

Renaming trick bakka odeeffannoo garee dhoksee tokko qaba. Rules row, column fi box hundi "seelota kun hundi adda" jedhu, fi *hundi adda* jechuun symbol maqaa kamiyyuu jijjiiruun ni tura. Garuu clue tokko "seelii kun exactly 5 qaba" jedha; renaming booda Bob $\sigma(5)$ qofa arga — symbol masked tokko — renaming σ maal akka ta'e osoo hin beekin. Homaa qorachuu hin danda'u. Yoo hin sirreeffamne, Alice clues maxxanfaman guutumaan ignore gochuun *muraasa* valid grid akka jiru mirkaneessuu gochuu dandeessi; kun *puzzle kana* irratti homaa hin mirkaneessuu godhu. Kilaasikaalaa literature repairs istaandaardii lama qaba.

Palette. Hidden grid irratti row dabalataa seelota N tokko dabaluu — palette Alice symbols 1…N dhaabbataa ummataaf banaa order keessatti guutuu, sana booda waan hunda waliin rename godhu, akka $\sigma(1)$…σ(N) qabu. Tasaa qormaata Bob amma option dabalataa tokko qaba. Row, column, box yookaan gadget banuu qofa osoo hin taane, **palette plus clue seelii tokko** filachuu danda'a. Alice lamaan bana; palette renaming round sanaa mul'isa, Bob immoo clue seelii exactly printed clue gosa renamed akka qabu sakatta'a godha. Kun zero-knowledge ta'ee tura sababni isaa Bob σ qofa barata — round hunda keessatti haaraan draw ta'ee ofumaan gatii hin qabne — fi gatii seelii duraan puzzle irraa beekuu qabu. Secret seelota irratti homaa hin leak godhu, fakkeessituu tasaa σ draw godhuun view sana fake gochuu danda'a. Sound dha sababni isaa Alice cheating carraa dhaabbataa round tokko keessatti qabama, rounds immoo shakkii negligible ta'utti repeat godhamu.

Clues constraints keessa compile gochuu. Variant structural tokko addaa qormaata dabaluu mannaa isa balleessa. Clue gatii *verify* gochuu mannaa garaagarummaa constraints'n dirqisisa: clue seelii palette seelota hunda keessaa gatii isaa mataa isaa baatu tokko malee hunda waliin link godhi — "$\sigma(1)$ irraa adda, $\sigma(2)$ irraa adda, …, $\sigma(5)$ malee waan hunda irraa

adda.” Symbol seelii legally qabaachuu danda’u clue sana qofa. Constraint hundi deebi’ee “lamaan kun adda” gosa — renaming keessatti invariant, row akka sakatta’uun danda’amu. Kun manoeuvre kilaasikaalaa graph-coloring protocol keessatti pre-colored vertices’f fayyadamu waliin wal fakkaata, fi jecha *gadgets* olitti fayyadamne spirit isaa dha: MegaSudoku-as-SAT suura keessatti, clues constraints biroo hunda akka ta’etti inequality gadgets keessa compile godhamu.

Fiizikaalaa protocol. haala addunyaa dhugaa card protocol Sudoku (Gradwohl, Naor, Pinkas fi Rothblum, 2007) renaming hin fayyadamu; clues hiding jalqabuu dura settle godha. Seelii hundaaf Alice cards identical sadii gatii seelii sana qabu kaa’a — secret seelota’f face-down, garuu **clue seelota’f face-up**, kanaaf Bob clues respect ta’uu cards flip godhamu dura ija isaatiin arga. Sana booda seelii tokko irraa card tokko row packet isaatti, tokko column isaatti, tokko box isaatti seena; packet tokkoon tokko shuffle fi reveal godhamee, Bob symbols N hunda qabaachuu sakatta’a godha. Shuffling position odeeffannoo balleessa (kun zero-knowledge dha), clues garuu dealing yeroo irratti duraan nailed down.

Karaa kamiyyuu, barumsi isaa article kana keessatti irra deddeebi’u isuma: zero-knowledge protocol jechuun bookkeeping of-eeggannoo **facts kam** hiding keessatti akka hafan irratti. Renaming “hundi adda” eega, “equals 5” balleessa — kanaaf “equals 5” karaa biraatiin deebi’ee galuu qaba.

Kun protocol barruu keessaa miti. Kilaasikaalaa zero-knowledge’f mental moodeela dha:

- Alice fi Bob wal-deebi’anii dubbatu.
- Bob sakatta’awwan tasaa filata.
- Alice naannoo keessaa consistency qofa mul’isa, furmaata guutuu miti.
- Ragaa iccitii dhuunfaa Bob view isaa Alice secret furmaata malee uumamuu akka danda’u agarsi-isuun hojjata.

Kanaaf kilaasikaalaa zero-knowledge pooziitivii fact tokko irratti ijaarama:

> Fakkeessituu tokko dhugumaan jira.

Amma kutaalee mijataa sana balleessi. Alice ragaa string tokko ergee deema. Trusted setup hin jiru, shared tasaa string dursee qophaa’e hin jiru, Bob immoo puzzle sobaa matumaa accept gochuu hin qabu. Kun setting kilaasikaalaa zero-knowledge keessa jiraachuu hin dandeenye dha.

Trick dura character tokko dabalataa barbaachisa. **Kitaaba seeraa** tokko fix godhi: idilee ragaa sirna, logician hiika keessatti — axioms dhaabbataa fi rules mechanical herregaa proofs barreeffaman qo-ratan. ZFC, axioms istaandaardii mathematics, fakkeenya canonical dha. As irraa waan hundi kitaaba seeraa dursee filatame tokko irratti walbira qabamee ta’ee ibsama; filannoon flexible dha: construc-tion kitaaba seeraa ati fix goote kamiyyuu, ZFC dabalatee, irratti hojjata.

(Jecha irratti note, barruu keessaa fudhatame: “ragaa sirna” asitti yeroo hunda kitaaba seeraa kana — herregaa proofs qoratu idilee sirna — jechuu dha; Alice ergaa ergitu miti. Machinery Alice fi Bob “prover fi verifier” jedhama.)

Gödel-style gosa mega-Sudoku seenaa eega, ragaa garuu jijjiira.

Constraint sirna lammaffaa displayed hammamtaa wal-fakkaataa tokko filadhu, **D** jedhii waami. Seenaa keessatti S fi D MegaSudoku(n) puzzles lama format wal-fakkaataa keessa jiru. Behind the mul'atawwan D loojikaalaa formula rakkisaa hammamtaa adda irraa jalqabuu danda'a; yoo barbaachise harmless dummy constraints'n pad godhamee grid wal-fakkaataa keessa galuu danda'a. D loojikaalaa formula dhugumaan **unsatisfiable** irraa ijaarama: gatiiwwan assignment tokko illee constraints hunda true godhu hin jiru, puzzle cabe filling legal hin qabne akka ta'etti. Toy fakkeenya tokko formula "X true dha" fi "X false dha" lamaan gaafatu ta'a. Kanaaf D filling valid hin qabu.

Garuu D puzzle cabe *salphaatti saaxilamu* ta'uu hin qabu. Toy fakkeenya ol jiru kufa: kitaaba seeraa kamiyyuu "X fi not-X" sarara tokko keessatti refute godha. D akka soba ta'eetti kitaaba seeraa filatame argument gabaabaa'n certify gochuu hin dandeenye ta'uu qaba. Kitaaba seeraa D ragaa gabaabaa'n refute gochuu yoo danda'e, seenaa gadi jiru ni kufa: alternative route Alice secret malee proofs uumuu danda'a jedhamu formally ruled out ta'a, iccitii dhuunfaa guarantee illee waliin bada. Kanaaf D family dhaabbataa kitaaba seeraa efficiently refute gochuu hin dandeenye keessaa filatama: kitaaba seeraa sana keessatti D furmaata akka hin qabne ragaa gabaabaa hin jiru.

One-message ragaa Alice sana booda either/yookaan statement irratti:

> either mega-Sudoku dhugaa S furmaata qaba, yookaan decoy D furmaata qaba.

Kun loojikaalaa link dha. D karaa magic S true godhuun hin generated. Ragaa "D furmaata hin qabu, kanaaf S furmaata qaba" jechuun argue hin godhu. Inni disjunction **S yookaan D** mirkaneessuu godha. Perfect soundness disjunction sobaa ragaa valid hin qabaatu jedha. D reality keessatti soba — furmaata hin qabu — kanaaf disjunction true ta'uuf karaa jiru S true ta'uu qofa. Ragaa accepted yoo ta'e S furmaata qabaachuu qaba. Decoy S sobaa true gochuu hin danda'u.

Garuu zero-knowledge-style kutaa'f, D *furmaata qabaatee ture* maal akka ta'u gaafadhu. Decoy furmaata sun alternative witness ta'a. Alice mega-Sudoku furmaata dhugaa osoo hin beekin proofs oomishuuf nama dandeessisa — jechuun fakkeessituu. Reality keessatti D furmaata hin qabu, kanaaf route fakkeessituu kun cufame. Qabxii isaa kitaaba seeraa cufamuu sana efficiently mirkaneessuu gochuu hin danda'u.

Kanaaf D hojii lama qaba. **Soundness** keessatti D soba, kanaaf ragaa valid "S yookaan D" S dirqisiisa. **Effective zero-knowledge** keessatti D refute gochuuf rakkisaa dha, kanaaf kitaaba seeraa decoy route fakkeessuu dandeessisa ture sana saffisaan rule out gochuu hin danda'u.

Kanaaf security qormaata amma kana miti:

> Fakkeessituu dhugumaan jiraachuu mirkaneessuu gochuu dandeenyaa?

Inni gara kanaatti jijjiirama:

> Kitaaba seeraa kee fakkeessituu impossible ta'uu efficiently mirkaneessuu gochuu danda'aa?

Deebiin lakkii yoo ta'e, wanti nama ajaa'ibu tokko hordofa: security guarantee hundi kan (a) qormaata raawwachuun observably ilaalamuu danda'u, fi (b) fakkeessituu jiraachuu irraa — kitaaba seeraa sana keessatti — provably follow godhu, dhugumaan hold godha. haleellaa successful amaloota isaanii kam irratti ta'u ofuma isaatiin gabaabaa refutation dhabame sana ta'a; gabaabaa refutation sun hin jiru. Kun "effective" kutaa effectively zero-knowledge dha.

Kanaaf classroom contrast:

Kilaasikaalaa zero-knowledge: proofs nageenya qabu dha sababni isaa fakkeessituu jira.

Gödel-style effective zero-knowledge: proofs observable security qormaatawwan'f nageenya qabu ta'anii ilaalamu sababni isaa kitaaba seeraa fakkeessituu impossible ta'uu efficiently mirkaneessuu gochuu hin danda'u.

Himannaa lammaffaa laafaa dha. Akkasumas barruu amaloota sadii kilaasikaalaa gosa cabsan — tokko message, lakki setup fi perfect soundness — eeguu akka danda'u sababni isaa kana.

Qormaata haaraa: fakkeessituu akka hin jirre mirkaneessuu gochuu hin dandeessu

Relaxation Ilango gaaffii jijjiira.

Kilaasikaalaa zero-knowledge gaafata:

> Fakkeessituu tokko jiraa?

Effectively zero-knowledge waan laafaa gaafata:

> Kitaaba seeraa ati filatte fakkeessituu akka hin jirre efficiently mirkaneessuu gochuu danda'aa?

Kun teknikaa dodge fakkaachuu danda'a, garuu yaada core dha. Construction haala ajaa'ibaa keessa jira: fakkeessituu dhugumaan hin jiru — barruu ifatti kana jedha — garuu kitaaba seeraa ati fix goote fakkeessituu akka hin jirre efficiently mirkaneessuu gochuu hin danda'u. Consequences hamaa ati sodaattu hundaaf refutation akkasii barbaachisa yoo ta'e, sirna consequences sanaaf zero-knowledge fakkaatee behave godha.

Asitti Gödel seena. Decoration ta'ee miti, "Gödel crypto nageenya qabu godha" ta'ees miti. Connection proof-theoretic dha. Kitaaba seeraa tokko **optimal** jedhama yoo hiika sirrii keessatti kan caalu ta'e: kitaaba seeraa kamiyyuu formula gosa barbaachisu ragaa gabaabaa'n refute gochuu yoo danda'e, optimal kitaaba seeraa illee ragaa polynomially longer caalaa hin taaneen refute gochuu danda'a. Krajíček fi Pudlák 1989 keessatti **optimal ragaa sirna tokko illee hin jiru** jechuun conjecture godhan: kitaaba seeraa kam fix gootus, kitaaba seeraa biraa family statements dhugaa tokko baay'ee gabaabinaan mirkaneessuu godha. Kun banaa conjectures ragaa complexity keessaa central tokko

dha, fi Gödel incompleteness theorem'f daangeffame, complexity-theoretic cousin: statements dhugaa tokko tokko kitaaba seeraa ati fix goote keessatti ragaa gabaabaa hin qaban — principle keessatti unprovable waan ta'aniif miti, garuu dhaabbataa kitaaba seeraa kamiyyuu truths gabaabaa tokko ragaa gabaabaa malee waan dhiisuuf.

Barruu conjecture kana (mildly stronger "infinitely often" boca, cryptography keessatti conjectures fayyadamuun istaandaardii) assume godha. Payoff, theorem Krajíček fi Pudlák irraa, ifa ta'e dha: kitaaba seeraa hundaaf formulas dhugumaan unsatisfiable ta'an sequence tokko jira, kitaaba seeraa sun ragaa gabaabaa'n refute gochuu hin danda'u — fi murteessaa ta'ee, efficient algorithm sequence sana *generate* gochuu danda'a. Amaloota last kun, uniformity, yaada guutuu existence himannaa irraa algorithm Alice dhugumaan raawwachuu dandeessutti jijjiira: decoys D assembly sarara irraa dhufu, haphii air irraa miti.

Cryptographic move shortage ragaa humna sana hojii irra oolchuu dha.

Construction maal hojjechaa jira

Construction barruu, shape isaa qofa irraa stripped, kana.

Kitaaba seeraa tokko fix godhi — fakkeenyaaf ZFC. Proof-complexity yaada bu'uuraa jalatti formulas efficiently generatable ta'an sequence tokko jira; isaan dhugumaan unsatisfiable, garuu kitaaba seeraa sun unsatisfiable ta'uu isaanii ragaa gabaabaa hin qabu.

Amma one-message ragaa boca kana ijaari:

> either statement dhugaa satisfiable dha, yookaan addaa hard formula kun satisfiable dha.

Addaa hard formula satisfiable miti. Kanaaf underlying ragaa machinery perfectly sound yoo ta'e, message accept gochuun statement dhugaa true jechuu dha. Kun perfect soundness kenna.

Garuu zero-knowledge-like security'f, addaa hard formula *satisfiable ta'ee ture* yaadi. Witness isaa witness dhugaa osoo hin beekin proofs fakkeessuuf fayyadamuu danda'ama ture. Formula reality keessatti satisfiable miti — garuu kitaaba seeraa efficiently kana mirkaneessuu gochuu hin danda'u. Kanaaf fakkeessituu impossible ta'uu efficiently mirkaneessuu gochuu hin danda'u.

Kun hinge dha. Sirna iccitii kilaasikaalaa fakkeessituu uumuu dhaan hin dhoksu. Observable security qormaatawwan hedduuf, kitaaba seeraa fakkeessituu dhabamuu certify gochuu dadhabuu duuba iccitii dhoksa.

Barruu maal himannaa godha

Ijoo theorem layers qaba. Core bu'aa kana:

Istaandaardii cryptographic yaada bu'uuraa tokko — **non-interactive witness indistinguishable proofs** jiraachuu, objects cryptography keessatti sirriitti qo'ataman fi yaada bu'uuraa packages established hedduu irraa hordofan — fi proof-complexity conjecture **lakki (infinitely often) optimal ragaa sirna exists** jedhu jalatti, barruu kitaaba seeraa filannoo hundaaf one-message prover fi verifier NP/SAT irratti **perfect soundness** fi setup hin qabne, kitaaba seeraa sana walbira qabamee ta'ee effectively zero-knowledge, ijaara. (NP/SAT puzzle-like rakkoowwan'f istaandaardii "hardest baramaa denominator" dha; mega-Sudoku uffata isaa keessaa tokko.)

Himannaa bal'aa falsifiable security amaloota preserve gochuu irratti barruu yaada bu'uuraa istaandaardii dabalataa tokko dabala: derandomization belief **P = BPP** (gara: carraa tasaa algorithms'f essential extra humna hin kennu).

Theorem afaan irraa baafnee:

- Ragaa ergaa tokko dha.
- Trusted setup hin jiru.
- Statements sobaa mirkaneessuu gochuun hin danda'amu.
- Prover kilaasikaalaa zero-knowledge miti — fakkeessituu hin qabu.
- Garuu falsifiable, game-based security consequence kilaasikaalaa zero-knowledge tokkoon tokkoon isaa setting kana keessatti argamuu danda'a.

"Falsifiable" barbaachisaa dha. Security kufaatii adversary game tokko keessatti raawwachuun qorachuu dandeessu jechuu dha. Cryptographic security definitions hedduun boca kana qabu: adversary encryptions lama distinguish gochuu danda'aa, function invert gochuu danda'aa, witness argachuu danda'aa, yookaan yaalii specified tokko win gochuu danda'aa? Theorem amaloota falsifiable tokkoon tokkoof prover tokko kenna, yeroo tokko tokkoon. Prover tokko *every* falsifiable amaloota yeroo tokko keessatti qabaachuun carraan isaa guddaa impossible — reusability haleellaa durii ("Bob ragaa namoota biraatti agarsiisuu danda'a") ofuma isaatii falsifiable amaloota dha, fi as keessatti dhugumaan fail godha. Barruu yaada dhihaate prover tokko *natural* falsifiable amaloota hunda — cryptographic practice keessatti dhugumaan mul'atan — hammatu plausibly danda'a jedhu; garuu kutaan sun theorem conditional dha, "natural" jechuun informal notion irratti, conjecture explicit dabalataan hirkata. Guarantee observable failures irratti xiyyeeffata, philosophical yookaan simulation-based meaning secrecy hunda irratti miti.

Corollary ifa ta'e tokko maqaa kaasuuf gatii qaba: construction kun proofs non-interactive *witness hiding* kan uniform prover qabu jalqabaa kenna — "ragaa puzzle tokko furmaata isaa argachuuf si hin gargaaru," interaction fi setup malee — object xiqqaa fakkaatu garuu waggoota dheeraaf construction didaa ture.

Kun maal hin jedhu

Kutaan kun article kana honest godha.

Impossibility theorems durii dogoggora turan **hin** jedhu. Construction hiika jijjiiruun isaan irraa

darba.

Interaction hin qabne, setup hin qabne, perfect soundness qabu idilee kilaasikaalaa zero-knowledge **hin** kennu. Barruu explicit ta'ee constructed prover fakkeessituu hin qabu jedha.

Ragaa refayyadamuun hin danda'amu jechuu **miti**. One-message ragaa nama biraatti agarsiisamuu danda'a; barruu deniability-style amaloota hin preserve godhu. (Non-interactive zero-knowledge trusted setup qabu illee limitation wal-fakkaataa qaba.)

Protocol hojiirra oolu hojiirra oolmaa'f qophaa'e jechuu **miti**. Kun complexity tiyoorii fi cryptographic foundations dha. Bu'aan ragaa complexity fi cryptography yaadota bu'uuraa guguddoo irratti hirkata, construction immoo principle keessatti maal danda'amaa akka ta'e irratti.

"Gödel" magic security primitive godha jechuu **miti**. Gödel connection ragaa sirnoota, optimal ragaa sirnoota fi daangeffame analogues incompleteness karaa. Intuition fayyadu "incompleteness password kee eega" miti. Inni: kitaaba seeraa fakkeessituu impossible ta'uu efficiently mirkaneessuu gochuu yoo hin dandeenye, attacks ragaa sana barbaadan security definitions sadarkaa irratti block gochuun danda'ama.

Maaliif ta'us nama hawwata

Cryptography yeroo baay'ee hardness nageenya godha. Factoring rakkisaa dha, kanaaf RSA-style yaadota bu'uuraa faayidaa qabu ta'u. Lattice rakkoowwan rakkisaa dha, kanaaf lattice cryptography faayidaa qabu ta'a. Asitti hardness isaa caalaatti strange: "secret compute gochuun rakkisaa" miti, "ragaa object tokko jiraachuu hin dandeenye mirkaneessuu gochuun rakkisaa" dha.

Kanaaf barruu unusual fakkaata. Axioms fi rulebooks jechuun ni danda'ama cryptographic resources akka ta'anitti ilaala. Impossibility idilee soundness fi fakkeessuu gidduu tension jira jedha. Sochiin Ilango tension sana proof-theoretic curtain duuba kaa'a: fakkeessituu hin jiru, garuu idilee sirna absence sana efficiently saaxilu hin danda'u.

Dubbisaaf wanti nama ajaa'ibu kun sirnoota zero-knowledge har'aa bakka bu'a jechuu miti. Tarii, kallattiin yoo xiqqaate, hin bakka bu'u. Wanti nama ajaa'ibu limitation herregaa logic irraa dhufu constructively fayyadamuun danda'ama: daangaa qofa osoo hin taane, cover gosa tokko akka ta'etti.

Ragaan hammam cimaa dha?

Kun theorem barruu dha, kanaaf "ragaa" baayoloojii yookaan astronomy barruu irraa hiika adda qaba. Gaaffiin yaalii replicate ta'e moo miti miti. Gaaffiin definitions, yaadota bu'uuraa fi ragaa chain himannaa sana deeggaaru moo miti dha.

Ragaa idilee dha, barruu yaadota bu'uuraa isaa ifatti kaa'a. Yaadota bu'uuraa sun casual miti. Non-interactive witness indistinguishable proofs objects istaandaardii cryptography keessa fi yaada

bu'uuraa packages established hedduu irraa follow godhu. No-optimal-proof-system conjecture ragaa complexity keessatti central conjecture dha. P = BPP derandomization belief istaandaardii dha, broader falsifiable-property theorem qofaaf fayyadama.

Barruu yaadota bu'uuraa price sirrii ta'uu, scaffold arbitrary akka hin taane, illee falma: converse mirkaneessuu godhee essentially necessary ta'uu isaanii agarsiisa — constructions akkasii yoo jiraatan, non-interactive witness indistinguishable proofs jiraachuu qabu, fi (istaandaardii one-way functions fudhachuun) optimal ragaa sirna tokko illee jiraachuu hin danda'u. Yaadota bu'uuraa "win-win" illee dha: isaan keessaa tokko refute gochuun ofuma isaatii ragaa complexity, cryptography yookaan complexity tiyoorii keessatti landmark discovery ta'a.

Garuu bu'aa conditional waan ta'eef amanamummaa isaa illee conditional dha. Yaadota bu'uuraa sun fail yoo godhan, hiika theorem jijjiirama. Yaadota bu'uuraa hold yoo godhan illee, guarantee guutuu kilaasikaalaa zero-knowledge miti; gosa relaxed, proof-theoretic barruu kanaa dha.

Kanaaf amanamummaa sirrii: barruu coherent conditional possibility bu'aa mirkaneessa irratti olaanaa; yaadota bu'uuraa keenya cryptographic world dhugaa describe godhu irratti moderate; immediate hojiirra oolu consequence irratti gadi-aanaa.

Maaliif barbaachisaa dha

Barruu karaa cufame jedhamee yaadame tokko bana.

Kilaasikaalaa tiyoorii: guutuu zero-knowledge setup malee tokko message ta'uu hin danda'u, perfect soundness illee qabaachuu hin danda'u jedha. Barruu Ilango: zero-knowledge consequences security games keessatti qorachuu dandeenyu gaafanne, fi security hiika kitaaba seeraa maal efficiently refute gochuu danda'a/hin dandeenye irratti depend gochuu eeyyamne, faayidaa qabu amala keessaa baay'ee deebisee argamsiisu dandeenya — tokko message, lakki setup fi perfect soundness waliin.

Kun definitional tweak xiqqaa miti. Cryptographic guarantees akkamitti yaadnu irratti karaa adda dha. Maal jira qofa gaafachuu mannaa, kitaaba seeraa kee maal rule out gochuu danda'a gaafadhu. Unprovability philosophical nuisance qofa akka ta'etti ilaaluu mannaa, caasaa akka ta'etti fayyadami.

Hojiirra oolu world boru hin jijjiiramu ta'a. Conceptual kaartaa garuu jijjiirameera. Amma idilee sense keessatti "namni fakkeessituu impossible ta'uu efficiently mirkaneessuu gochuu hin danda'u" jechuun game-based protections "secret hin leak godhne" irraa barbaadne keessaa hedduu deebisuu gahu ta'uu danda'a.

Kanaaf Gödel title keessa jira.

Cuunfaa gabaabaa

Zero-knowledge proofs prover tokko statement dhugaa ta'uu verifier amansiisuu, witness osoo hin mul'isin, dandeessisu. Kilaasikaalaa impossibility bu'aawwan zero-knowledge setup malee tokko message keessatti cuunfamuu hin danda'u, perfect soundness illee qabaachuu hin danda'u jedhu. Barruu Rahul Ilango impossibilities kana hin refute godhu. Notion laafaa, effectively zero-knowledge, define godha: fakkeessituu dhugumaan jiraachuu gaafachuu mannaa, ragaa sirna filatame — idilee kitaaba seeraa akka ZFC — fakkeessituu akka hin jirre efficiently mirkaneessuu gochuu hin danda'u akka ta'u gaafata. Yaadota bu'uuraa guguddoo cryptography (non-interactive witness indistinguishable proofs) fi ragaa complexity (optimal ragaa sirna hin jiru) jalatti, barruu one-message provers NP/SAT'f lakki setup fi perfect soundness qabu ijaara, kan consequences falsifiable, game-based kilaasikaalaa zero-knowledge amaloota tokkoon tokkoon rehammatu. Prover tokko "natural" amaloota akkasii hunda hammatu extension dabalataa, gariin conjectural dha — literally every falsifiable amaloota cover gochuun carraan isaa guddaa impossible, sababni isaa proofs reusable ta'anii hafan. Bu'aan tiyoorii fi conditional dha, deployed primitive miti, garuu proof-theoretic unprovability cryptographic resource akka ta'etti fayyadamuuf karaa haaraa agarsiisa.

Sakatta'a ifaa

Barruu maal agarsiisa: Yaadota bu'uuraa stated jalatti, one-message, no-setup, perfectly sound provers NP/SAT'f ijaaruun danda'ama; kitaaba seeraa filatame kamiyyuu walbira qabamee ta'ee effectively zero-knowledge, fi falsifiable game-based consequence kilaasikaalaa zero-knowledge tokkoon tokkoon isaanii achieve godhu.

Wanti amansiisaa garuu unconditional hin mirkanoofne: Proof-complexity fi cryptographic yaadota bu'uuraa barbaachisan hold gochuu. Yaadota bu'uuraa serious fi well-studied dha — barruu essentially necessary fi sufficient ta'uu isaanii illee agarsiisa — garuu yaadota bu'uuraa ta'anii hafan.

Wanti hin agarsiifne: Interaction hin qabne, setup hin qabne, perfect soundness qabu kilaasikaalaa zero-knowledge; hojiirra oolu sirna hojiirra oolmaa'f qophaa'e; deniability yookaan non-reusability proofs; yookaan Gödel incompleteness theorem ofuma isaa cryptography secure godha jechuu.

Ijoo limitations: Guarantee zero-knowledge relaxation dha; gosa bal'aan yaadota bu'uuraa hedduu irratti hirkata; single-universal-prover himannoowwan gariin conjectural ta'anii hafan; bu'aan primarily foundational dha.

Waliigalaa reader amanamummaa hammam qabaachuu qaba? Definitions fudhataman yoo ta'e, barbaachisaa conditional tiyoorii bu'aa dha jechuun ol-aanaa. Yaadota bu'uuraa reality capture godhu irratti moderate. Immediate hojiirra oolu hojiirra oolmaa irratti gadi-aanaa. Nageenya qabu ergaa ijoo: barruu zero-knowledge impossibilities hin cabsu; security games hedduuf kutaalee barbaachisan irra darbuu proof-theoretic karaa haaraa argata.

Maddoota

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