The Clean Paper

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

Uthibitisho wa kriptografia unaweza kuficha siri kwa kufanya ukosefu wa kiigaji kuwa mgumu kuthibitisha

Uthibitisho wa zero-knowledge humruhusu mtu kuthibitisha dai bila kufichua shahidi. Nadharia ya kawaida inasema huwezi kupata hilo kwa maana kamili kwa ujumbe mmoja, bila setup ya kuaminika na kwa soundness kamili. Paper ya Rahul Ilango haifuti kutowezekana huko. Inabadilisha lengo: badala ya kudai kwamba kiigaji kipo kwa kweli, inauliza kama proof system iliyochaguliwa inaweza kuthibitisha kwa ufanisi kwamba kiigaji hakipo. Chini ya assumptions kubwa za proof complexity na cryptography, hilo linatosha kurejesha, property kwa property, consequences za zero-knowledge zinazoweza kufalsifiwa na kujaribiwa katika game. Hii si primitive ya mtandao ya kuingiza moja kwa moja. Ni njia ya proof theory ya kubadilisha unprovability ya kihisabati kuwa kifuniko cha kriptografia.

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

Ujanja si kuthibitisha kwamba siri imefichwa

Anza na toleo rahisi zaidi la zero-knowledge.

Alice anataka kumshawishi Bob kwamba fumbo la Sudoku lina suluhisho. Akimtumia suluhisho, Bob atasadiki, lakini fumbo lenyewe litakuwa limeharibika. Anachotaka ni kitu cha ajabu zaidi: uthibitisho kwamba suluhisho lipo, bila kufichua suluhisho hilo.

Hiyo ndiyo ahadi ya **uthibitisho wa zero-knowledge**. Mtoa-uthibitisho (Alice) anamshawishi mkaguzi (Bob) kwamba dai ni la kweli huku hafichui chochote zaidi ya ukweli wa dai hilo.

Tatizo ni kwamba ahadi hiyo ina gharama. Uthibitisho wa kawaida wa kihisabati una sifa mbili zinazofaa. Ni **ujumbe mmoja**: unauandika, unaukabidhi, kisha unaondoka. Na una **soundness kamili**: dai la uongo halina uthibitisho halali hata mmoja. Matokeo ya kawaida ya kutowezekana yanasema zero-knowledge lazima iachane na sifa zote mbili — na si kwamba tu haiwezi kuwa nazo kwa pamoja; kila moja peke yake pia hairuhusiwi katika mpangilio huo.

Kwanza, uthibitisho wa zero-knowledge unahitaji mazungumzo. Alice akituma ujumbe mmoja tu, bila setup ya kuaminika iliyopangwa mapema, dhamana ya zero-knowledge huanguka — na hili hubaki kweli bila kujali ni kiasi gani cha soundness uko tayari kutoa kama badala.

Pili, uthibitisho wa zero-knowledge unahitaji kuvumilia uwezekano mdogo wa kosa. Kudai soundness kamili kunageuka pia kuondoa mwingiliano kimya kimya: mkaguzi ambaye hawezi kudanganywa kamwe, bila kujali uchaguzi wake wa nasibu, anaweza tu kufunga chaguo hizo mapema — na mkaguzi akishatabirika, Alice anaweza kujibu kila kitu katika ujumbe mmoja, yaani kesi ileile ambayo tayari ilivunja zero-knowledge.

makala ya Rahul Ilango inatafuta njia ya kuzunguka ukuta huo wa pande mbili. Si kwa kujifanya ukuta haupo, wala kwa kuzalisha zero-knowledge ya kawaida katika mazingira yaliyothibitishwa kuwa hayawezekani. Hatua yake ni laini zaidi: kulegeza maana ya “hafichui chochote”, lakini kwa namna inayohifadhi mali za usalama ambazo wanakryptografia wanaweza kuzijaribu kwa kweli.

Matokeo hayo yanaitwa **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 imezuiwa katika milango mitatu — mwingiliano, setup ya kuaminika, na soundness isiyo kamili. Ujenzi wa llango unapita kupitia mlango tofauti: mfumo wa kanuni hauwezi kwa ufanisi kubatilisha kiigaji.

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.

Zero-knowledge ya kawaida huuliza kama kiigaji kipo; “effectively zero-knowledge” huuliza tu kama mfumo wa kanuni uliochaguliwa unaweza kuthibitisha kwa ufanisi kwamba kiigaji hakiwezi kuwepo. Swali hili dhaifu ndilo

linaloruhusu ujenzi kuhifadhi ujumbe mmoja, kutokuwa na setup, na soundness kamili.

Original diagram — The Clean Paper CC BY 4.0

Jaribio la zamani: kiigaji kipo

Njia ya kawaida ya kufafanua zero-knowledge hutumia msaidizi wa kufikirika anayeitwa **kiigaji (simulator)**.

Wazo ni hili: fikiria Jane, ambaye **hajui** siri ya Alice. Ikiwa Jane anaweza kuzalisha peke yake uthibitisho unaoonekana kama ule ambao Bob angepokea kutoka kwa Alice, basi uthibitisho wa Alice haukumfundisha Bob jambo jipya. Jane angeweza kuiga uzoefu huo hata bila siri ya Alice.

Kwa hiyo zero-knowledge ya kawaida hudai kiigaji halisi. Lazima kuwe na algoriti yenye ufanisi inayoweza kuzalisha uthibitisho wa kuiga bila kujua siri — kwa jargon, **shahidi (witness)**; katika Sudoku, shahidi ni gridi iliyotatuliwa.

Ufafanuzi huo una nguvu, lakini pia ndipo matokeo ya zamani ya kutowezekana yanapouma. Huu ndio mtazamo wa msingi. Uthibitisho usioingiliana kabisa ni mfuatano wa data tu. Bob akishaupokea, anaweza kumuonyesha mtu mwingine: sasa ana uwezo wa kuwathibitishia wengine dai hilo, jambo ambalo tayari linaonekana kuwa zaidi ya “hakuna alichojifunza.” Teorema za kawaida hufanya intuition hiyo kuwa matokeo rasmi ya kutowezekana yaliyoelezwa juu.

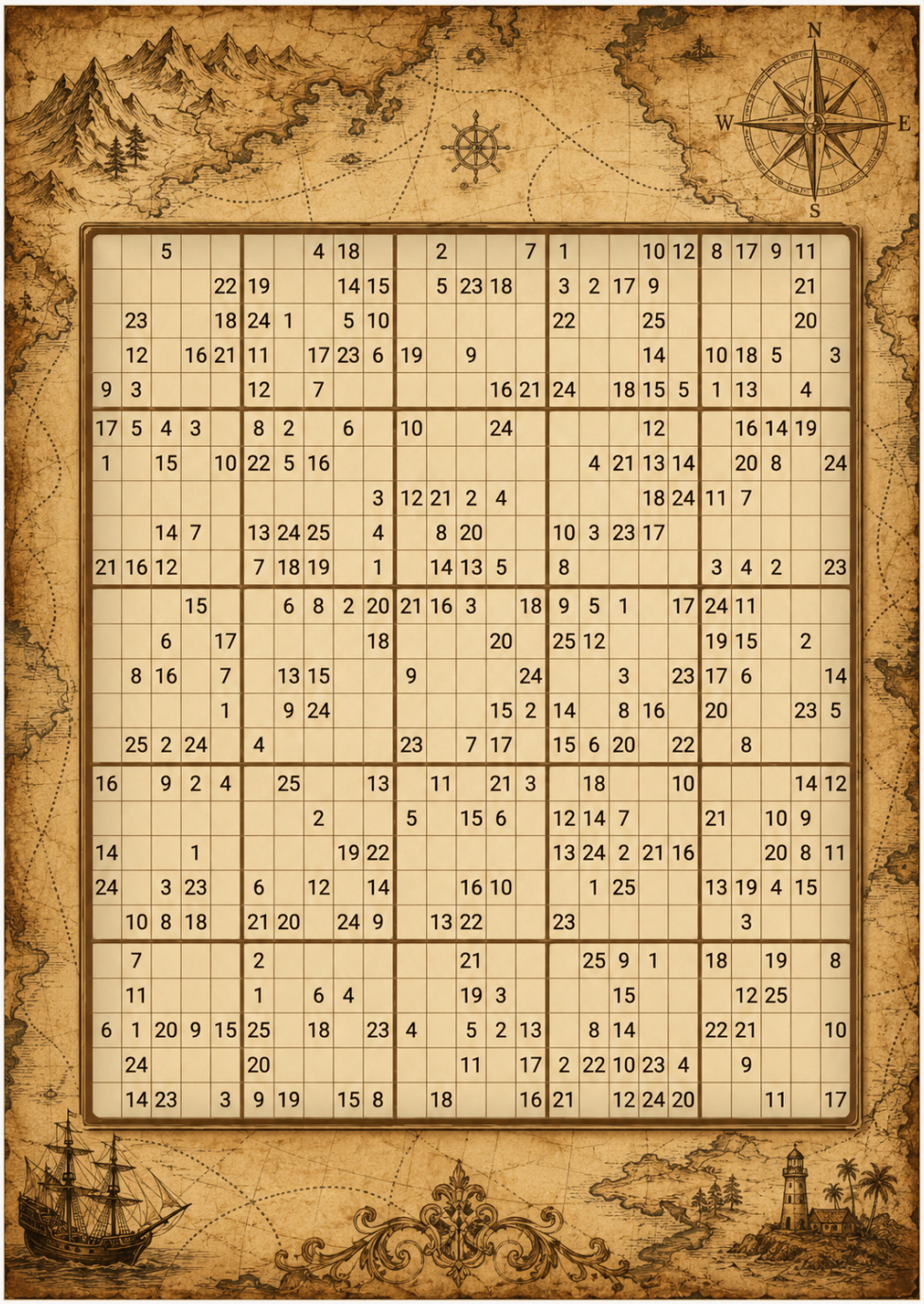
> **Sifa tatu ambazo makala hii inasisitiza**
>
> Kichwa cha makala kinataja vikwazo vitatu:
> **Hakuna mwingiliano:** Alice anatuma mfuatano mmoja wa uthibitisho. Hakuna mazungumzo ya kurudi na kurudi.
> **Hakuna setup:** Alice na Bob hawategemei common reference string ya kuaminika wala randomness nyingine ya umma iliyopangwa mapema. Mifumo mingi inayoitwa “non-interactive zero-knowledge” bado hutegemea setup; hapa maana ni setup sifuri.
> **Soundness kamili:** dai la uongo halina uthibitisho halali. Si “karibu kamwe halikubaliwi”; uthibitisho halali haupo kabisa.
> Hizo ndizo sifa tatu ambazo hisabati ya kawaida iliyoandikwa huwa nazo — na, kama ilivyoelezwa hapo juu, zero-knowledge ya kawaida haiwezi kuzihifadhi zote katika mpangilio huu.

Mega-Sudoku kama njia ya kuona tofauti

Hapa kuna njia iliyarahisishwa kwa makusudi ya kuhisi tofauti hiyo.

Usitumie Sudoku ya kawaida ya 9 kwa 9 kwa sehemu nzito ya mfano huu. Ni ndogo sana na finite sana: kompyuta inaweza kuitatua tu, au kuthibitisha kwamba haina suluhisho. Badala yake fikiria

familia ya mafumbo ya **MegaSudoku(n)**. Panua sheria ya kawaida: chagua ukubwa wa block *n*, weka *N = n^2*, kisha jenga gridi ya *N* kwa *N* iliyogawanywa katika block za *n* kwa *n*, ikiwa na alama *N*. Sudoku ya kawaida ni kesi ndogo ya *n = 3*, *N = 9*: gridi ya 9 kwa 9, block za 3 kwa 3 na alama tisa. Hadithi ya utata wa uthibitisho huanza tu *n* inaporuhusiwa kukua, na gridi inapoweza kubeba gadgets za ziada zinazoifanya itende kama formula ya SAT iliyovishwa mavazi ya Sudoku. Formula ya SAT ni orodha ya vikwazo vya ndiyo/hapana: je, unaweza kuwapa variables thamani true/false ili kila kikwazo kitimizwe?



Sudoku ya 25x25: sheria zake zinaweza kukaguliwa bila kufichua gridi iliyokamilishwa — mfano wa kuona wa uthibitisho unaothibitisha suluhisho lililofichwa, yaani shahidi.

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

Sudoku na SAT: fumbo lilelile katika mavazi mawili

Dai kwamba Sudoku inaweza “kutenda kama formula ya SAT” si tashbihi tu. Tafsiri inaenda pande zote mbili, na upande rahisi unaweza kuandikwa kikamilifu.

Kutoka Sudoku kwenda SAT. SAT huzungumza kwa true/false tu, kwa hiyo mpe variable moja ya boolean kwa kila utatu wa (mstari, safu, thamani): *x(r,c,v)* inamaanisha “kisanduku katika mstari *r*, safu *c* kina thamani *v*.” Sudoku ya 4 kwa 4 (block za 2 kwa 2, thamani 1–4) inahitaji 4·4·4 = variables 64; Sudoku ya kawaida ya 9 kwa 9 inahitaji 729. Kila sheria ya Sudoku kisha hubadilishwa kuwa kundi la clauses. (Clause ni OR ya variables au negations zake; formula nzima ni AND ya clauses zake zote.)

Kila kisanduku kina angalau thamani moja — clause moja kwa kila kisanduku:

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

Kila kisanduku kina si zaidi ya thamani moja — clause ya “si zote mbili” kwa kila jozi ya thamani:

$$\neg x(1,1,1) \lor \neg x(1,1,2) \quad \neg x(1,1,1) \lor \neg x(1,1,3) \quad \ldots \text{ na kadhalika kwa jozi zote sita.}$$

Kila mstari una kila thamani — kwa mstari wa 1 na thamani 3: angalau mara moja,

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

na si zaidi ya mara moja: $\neg x(1,1,3) \lor \neg x(1,2,3)$, na kadhalika kwa kila jozi ya visanduku katika mstari.

Safu na block — makundi yaleyale; kinachobadilika ni kundi la visanduku. Kwa block ya juu kushoto na thamani 2:

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

pamoja na clauses za jozi za “si zote mbili”.

Vidokezo vilivyochapishwa — sehemu rahisi zaidi: kila kidokezo ni clause yenye variable moja tu. Namba 3 iliyochapishwa katika kona ya juu kushoto inakuwa clause

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

AND ya yote haya inaweza kutimizwa ikiwa na tu ikiwa Sudoku ina suluhisho — na assignment inayotimiza formula **ndiyo** suluhisho: soma ni x(r,c,v) zipi ni true na ujaze gridi. Kwa Sudoku ya 9 kwa 9 hii ni variables 729 na clauses elfu chache, ambazo SAT solver ya kisasa huzishughulikia kwa milliseconds. Angalia clause ya kidokezo x(1,1,3): inasema “kisanduku hiki ni 3 hasa,” si “visanduku hivi vyote ni tofauti” — asymmetry hiyo hiyo ndiyo italazimisha ujanja wa ziada kwa visanduku vya vidokezo katika note iliyo chini.

Kutoka SAT kwenda Sudoku. makala inahitaji upande wa pili, mgumu zaidi: ukipewa formula yoyote ya SAT, jenga mega-Sudoku yenye suluhisho ikiwa na tu ikiwa formula hiyo inaweza kutimizwa. Sheria asili za Sudoku zinaweza kusema tu “visanduku hivi vyote ni tofauti,” kwa hiyo vikwazo vya kimantiki vya aina yoyote lazima **vijengwe** — na hapa ndipo gadgets zinapoingia. Gadget ni kundi dogo la visanduku lililotengenezwa mapema, moja kwa kila clause ya formula, ambapo visanduku maalum vinawakilisha variables (alama inayoshikiliwa

huencode true au false) na vikwazo vya ndani vimeundwa ili fillings zake halali tu zilingane na assignments zinazotimiza clause hiyo. Huu ni ufundi wa kawaida kutoka uthibitisho za NP-completeness; kwa generalized Sudoku ulifanywa na Yato na Seta mwaka 2003.
Kwa pamoja, pande hizo mbili zinasema Sudoku ya N kwa N na SAT ni tatizo lilelile katika mavazi tofauti. Hilo ndilo linaloruhusu makala hii — na makala — kusimulia hadithi kuhusu NP yote kwa kutumia gridi na alama.

Shahidi bado ni rahisi kuiona. Alice anajua filling kamili na halali ya mega-Sudoku. Bob anataka kushawishika kwamba filling kama hiyo ipo, lakini Alice hataki kuifichua. Akituma filling yote, Bob atasadiki, lakini siri imekwisha.

Katika toleo la kawaida la zero-knowledge, Alice na Bob huingiliana. Mental modeli ya zamani hutumia vigae vilivyofunikwa. Alice anaficha gridi iliyotatuliwa, anabadilisha majina ya alama kwa siri kabla ya kila round, kisha anamruhusu Bob kukagua constraint moja ya eneo iliyochaguliwa kwa nasibu: mstari, safu, box au gadget. Visanduku vilivyofunguliwa vikionyesha alama zote tofauti, Bob anaongeza imani. Kisha kila kitu kinafunikwa tena na alama zinapewa majina mapya. (Kuna tatizo moja: clues zilizotolewa kwenye fumbo zinahitaji ujanja wa ziada, kwa sababu kubadilisha majina ya alama huzificha pia. Note inayofuata inaeleza jinsi protocol za kawaida zinavyolitatua; picha hii rahisi inatosha kwa yanayofuata.)

Jinsi protocol za kawaida zinavyoshughulikia visanduku vya clue

Ujanja wa kubadilisha majina una sehemu isiyoonekana. Sheria za mstari, safu na box zote zinasema “visanduku hivi vyote ni tofauti,” na **all different** hubaki kweli chini ya renaming yoyote ya alama. Lakini clue inasema “kisanduku hiki kina 5 hasa,” na baada ya renaming Bob anaona tu $\sigma(5)$ — alama iliyofichwa — bila kujua renaming σ. Hawezi kukagua chochote. Isipotatuliwa, Alice angeweza kuthibitisha kwamba *gridi fulani* halali ipo huku akipuuza kabisa clues zilizochapishwa, jambo lisilothibitisha chochote kuhusu *fumbo hili*. Fasihi ya kawaida ina marekebisho mawili ya msingi.
Palette. Ongeza mstari mmoja wa ziada wenye visanduku N kwenye gridi iliyofichwa — palette ambayo Alice hujaza kwa alama 1…N katika mpangilio wa umma uliowekwa, kisha huzibadilisha majina pamoja na kila kitu kingine, hivyo ina $\sigma(1)\ldots\sigma(N)$. changamoto ya nasibu ya Bob sasa ina chaguo la ziada. Mbali na kuchagua mstari, safu, box au gadget ya kufungua, anaweza kuchagua **palette pamoja na kisanduku kimoja cha clue**. Alice hufungua vyote; palette inaonyesha renaming ya round hiyo, na Bob hukagua kwamba kisanduku cha clue kina toleo lililobadilishwa jina la clue iliyochapishwa. Hii hubaki zero-knowledge kwa sababu Bob anajifunza tu σ — ambayo huchaguliwa upya kila round na haina thamani peke yake — pamoja na thamani ya kisanduku ambacho tayari alikijua kutoka kwenye fumbo. Hakuna kitu kuhusu visanduku vya siri kinachovuja, na kiigaji kinaweza kuiga mtazamo huo kwa kuchagua σ ya nasibu. Ina soundness kwa sababu Alice anayadanganya anakamatwa kwa probability isiyobadilika katika kila round, na rounds hurudiwa hadi shaka iwe ndogo sana.
Kukompail clues ndani ya constraints. Toleo la kimuundo zaidi huondoa changamoto maalum badala ya kuiongeza. Badala ya *kukagua* thamani ya clue, ilazimishe kwa difference

> constraints: unganisha kisanduku cha clue na kila kisanduku cha palette isipokuwa kile kinachobeba thamani yake — "tofauti na $\sigma(1)$, tofauti na $\sigma(2)$, …, tofauti na kila kitu isipokuwa $\sigma(5)$." Alama pekee ambayo kisanduku kinaweza kubeba kihalali ni ya clue yenyewe. Kila constraint sasa tena ni ya aina "hivi viwili vinatofautiana" — invariant chini ya renaming, na inaweza kukaguliwa kama mstari. Huu ni ujanja uleule unaotumiwa kwa vertices zilizopewa rangi mapema katika protocol ya classical graph-coloring, na ndio roho ya neno *gadgets* hapo juu: katika picha ya MegaSudoku-kama-SAT, clues zinakompailiwa kuwa inequality gadgets kama constraint nyingine yoyote.
> **Protocol ya kimwili.** Protocol halisi ya kadi kwa Sudoku (Gradwohl, Naor, Pinkas na Rothblum, 2007) haitumii renaming kabisa na huthibitisha clues kabla hata ya kuficha kuanza. Kwa kila kisanduku, Alice huweka kadi tatu zinazofanana zenye thamani ya kisanduku — face-down kwa visanduku vya siri, lakini **face-up kwa visanduku vya clue**, hivyo Bob anaona mwenyewe kwamba clues zimeheshimiwa kabla kadi hazijageuzwa. Kisha kadi moja kutoka kila kisanduku inaingia katika pakiti ya mstari wake, moja katika pakiti ya safu, moja katika pakiti ya box; kila pakiti huchanganywa na kufunuliwa, na Bob hukagua kwamba ina alama zote N. Kuchanganya huondoa taarifa ya nafasi (hiyo ndiyo zero-knowledge), lakini clues tayari zilikuwa zimefungwa wakati wa kugawa kadi.
> Kwa njia yoyote, somo ni lilelile ambalo makala hii hurudia: protocol ya zero-knowledge ni uhasibu makini wa **ni facts zipi** zinaendelea kuonekana baada ya kuficha. Renaming huhifadhi "zote tofauti" na kufuta "ni 5" — kwa hiyo "ni 5" lazima irudishwe kwa njia nyingine.

Hiyo si protocol ya makala hii. Ni mental modeli ya zero-knowledge ya kawaida:

- Alice na Bob wanabadilishana ujumbe.
- Bob anachagua ukaguzi wa nasibu.
- Alice anafichua consistency ya eneo tu, si suluhisho lote.
- Uthibitisho wa faragha unaonyesha kwamba mtazamo wa Bob ungeweza kuzalishwa bila suluhisho la siri la Alice.

Kwa hiyo zero-knowledge ya kawaida imejengwa juu ya ukweli chanya:

> Kiigaji kipo kwa kweli.

Sasa ondoa sehemu zinazorahisisha mambo. Alice anatuma mfuatano mmoja wa uthibitisho na anaondoka. Hakuna setup ya kuaminika, hakuna shared random string iliyotayarishwa mapema, na Bob lazima asikubali kamwe fumbo la uongo. Hayo ndiyo mazingira ambayo zero-knowledge ya kawaida haiwezi kuishi.

Tunamhitaji mhusika mmoja zaidi kabla ya ujanja. Funga **kitabu cha kanuni (rulebook)**: mfumo rasmi wa uthibitisho kwa maana ya mantiki — seti maalum ya axioms pamoja na sheria za kimakanika za kukagua uthibitisho wa kihisabati ulioandikwa. ZFC, axioms za kawaida za hisabati, ndiyo mfano mkuu. Kuanzia hapa kila dai linafanywa kwa kuhusishwa na rulebook iliyochaguliwa mapema, na uchaguzi unaweza kuwa wowote: ujenzi hufanya kazi kwa rulebook yoyote utakayofunga, ikiwemo ZFC.

(Note kuhusu maneno, ikifuata makala yenyewe: “mfumo wa uthibitisho” hapa daima inamaanisha **rulebook hii** — mfumo rasmi unaokagua uthibitisho za kihisabati — si ujumbe ambao Alice anatuma. Mashine za Alice na Bob huitwa “prover” na “verifier”, yaani mtoa-uthibitisho na mkaguzi.)

Toleo la mtindo wa Gödel linaendelea na hadithi ya mega-Sudoku lakini linabadilisha aina ya uthibitisho.

Chagua mfumo wa pili wa constraints wenye ukubwa uleule unaoonyeshwa, na uite **D**. Katika hadithi, S na D ni mafumbo mawili ya MegaSudoku(n) katika format ileile. Nyuma ya pazia, D inaweza kuanza kama formula ngumu ya kimantiki yenye ukubwa tofauti; ikihitajika inaweza kuongezewa dummy constraints zisizo na madhara ili iingie kwenye gridi yenye ukubwa huo. D inajengwa kutoka formula ambayo kwa kweli **haiwezi kutimizwa (unsatisfiable)**: hakuna assignment ya values inayoweza kufanya constraints zake zote ziwe true, kama fumbo lililovunjika lisivyo na gridi halali iliyokamilishwa. Mfano mdogo ungekuwa formula inayodai kwa pamoja “X ni true” na “X ni false.” Kwa hiyo D haina filling halali.

Lakini D haipaswi kuwa fumbo lililovunjika ambalo ni **rahisi kufichua**. Mfano mdogo hapo juu haufai: rulebook yoyote inaweza kubatilisha “X na si-X” kwa mstari mmoja. D lazima iwe false kwa namna ambayo rulebook iliyochaguliwa haiwezi kuthibitisha kwa hoja fupi. Ikiwa rulebook ingeweza kubatilisha D kwa uthibitisho fupi, hadithi inayofuata ingeanguka: njia mbadala ambayo ingeweza kuzalisha uthibitisho bila siri ya Alice ingeweza kufungwa rasmi, na dhamana ya faragha ingeanguka nayo. Kwa hiyo D huchaguliwa kutoka familia ambayo rulebook iliyofungwa haiwezi kuirefute kwa ufanisi: **hakuna uthibitisho fupi ndani ya rulebook hiyo kwamba D haina suluhisho**.

Uthibitisho wa ujumbe mmoja wa Alice kisha unahusu dai la ama/au:

> ama mega-Sudoku halisi S ina suluhisho, au decoy D ina suluhisho.

Hiki ndicho kiungo cha kimantiki. D **haizalishwi kwa uchawi** ili kufanya S iwe true. uthibitisho haisemi “D haina suluhisho, kwa hiyo S ina suluhisho.” Inathibitisha disjunction **S au D**. Soundness kamili inasema disjunction ya uongo haiwezi kuwa na uthibitisho halali. Kwa kuwa D ni false katika uhalisia — haina suluhisho — njia pekee ambayo disjunction inaweza kuwa true ni S kuwa true. Kwa hiyo uthibitisho ikikubaliwa, S lazima iwe na suluhisho. Decoy haiwezi kufanya S ya uongo iwe true.

Lakini kwa sehemu inayofanana na zero-knowledge, uliza nini kingetokea kama D *ingekuwa* na suluhisho. Suluhisho hilo la decoy lingekuwa shahidi mbadala. Lingemruhusu mtu kuzalisha uthibitisho bila kujua suluhisho halisi la mega-Sudoku la Alice — yaani, kiigaji. Katika uhalisia D haina suluhisho, kwa hiyo njia hii ya kiigaji imefungwa. Jambo muhimu ni kwamba rulebook haiwezi kuthibitisha kwa ufanisi kwamba imefungwa.

Kwa hiyo D ina kazi mbili. Kwa **soundness**, D ni false, hivyo uthibitisho halali ya “S au D” inalazimisha S iwe true. Kwa **effectively zero-knowledge**, D ni ngumu kurefutiwa, hivyo rulebook haiwezi kwa haraka kufunga njia ya decoy ambayo, kama ingekuwa wazi, ingewezesha uigaji.

Kwa hiyo jaribio la usalama si tena:

> Je, tunaweza kuthibitisha kwamba kiigaji kipo kwa kweli?

Linakuwa:

> Je, rulebook yako inaweza kuthibitisha kwa ufanisi kwamba kiigaji hakiwezekani?

Ikiwa jibu ni hapana, jambo lenye nguvu kwa kushangaza linafuata: kila dhamana ya usalama ambayo (a) inaweza kuonekana kwa kuendesha jaribio, na (b) inaweza kuthibitishwa — ndani ya rulebook hiyo — kufuata kutoka kuwepo kwa kiigaji, kwa kweli hushikilia. Shambulio lililofanikiwa dhidi ya mojawapo ya dhamana hizo lingekuwa lenyewe refutation fupi iliyokosekana, na refutation hiyo fupi haipo. Hiyo ndiyo sehemu ya "effective" katika effectively zero-knowledge.

Kwa hiyo tofauti ya darasani ni:

Zero-knowledge ya kawaida: uthibitisho ni salama kwa sababu kiigaji kipo.

Effectively zero-knowledge ya mtindo wa Gödel: uthibitisho hutendewa kama salama kwa majaribio ya usalama yanayoonekana kwa sababu rulebook haiwezi kwa ufanisi kuthibitisha kwamba kiigaji hakiwezekani.

Dai la pili ni dhaifu zaidi. Na hilo ndilo linaloeleza kwa nini makala inaweza kuhifadhi sifa tatu zilizovunja toleo la kawaida: ujumbe mmoja, hakuna setup, na soundness kamili.

Jaribio jipya: huwezi kuthibitisha kwamba kiigaji hakipo

Relaxation ya Ilango inabadilisha swali.

Zero-knowledge ya kawaida huuliza:

> Je, kiigaji kipo?

Effectively zero-knowledge huuliza jambo dhaifu zaidi:

> Je, rulebook uliyochagua inaweza kuthibitisha kwa ufanisi kwamba hakuna kiigaji?

Hilo linaweza kusikika kama kukwepa tatizo la kiufundi, lakini ndilo wazo kuu. Ujenzi unaishi katika hali ya ajabu: kiigaji **hakipo kwa kweli** — makala iko wazi kuhusu hilo — lakini rulebook uliyofunga haiwezi kuthibitisha kwa ufanisi kwamba hakipo. Ikiwa kila matokeo mabaya unayojali yangetaka refutation kama hiyo, mfumo bado hutenda kama zero-knowledge kwa matokeo hayo.

Hapa ndipo Gödel anaingia. Si kama mapambo, wala si kwa maana kwamba "Gödel anafanya cryptography iwe salama." Uhusiano uko katika nadharia ya uthibitisho. Mfumo wa uthibitisho huitwa **optimal** ikiwa, kwa maana rasmi, unaweza kuiga mifumo mingine bila ongezeko kubwa sana la urefu wa uthibitisho: ikiwa mfumo mwingine unaweza kukanusha formula fulani kwa uthibitisho mfupi, mfumo optimal unaweza kufanya hivyo pia kwa uthibitisho ambao ni mrefu kwa kiwango cha polynomial tu. Krajíček na Pudlák walikisia mwaka 1989 kwamba **hakuna mfumo optimal wa**

uthibitisho. Kwa mfumo wowote uliowekwa, kunaweza kuwa na mfumo mwingine unaothibitisha familia fulani ya kauli za kweli kwa ufupi zaidi sana. Hii ni mojawapo ya conjectures kuu zilizo wazi katika proof complexity na ina uhusiano wa kifamilia na nadharia ya kutokamilika ya Gödel: katika mfumo uliowekwa, baadhi ya kauli za kweli zinaweza kukosa **uthibitisho mfupi**, si kwa sababu haziwezi kuthibitishwa kabisa, bali kwa sababu mfumo huo hauziwakilishi kwa njia fupi.

makala inachukulia conjecture hiyo kuwa kweli (katika toleo lenye nguvu kidogo la "infinitely often", ambalo ni la kawaida wakati conjectures zinapotumiwa cryptographically). Faida yake, kupitia theorem ya Krajíček na Pudlák, ni ya moja kwa moja: kwa kila rulebook kuna mfuatano wa formulas ambazo kwa kweli ni unsatisfiable lakini rulebook haiwezi kuzirefute kwa uthibitisho fupi — na, muhimu zaidi, algoriti yenye ufanisi inaweza **kuzizalisha**. Sifa hiyo ya mwisho, uniformity, ndiyo inayobadilisha wazo kutoka dai la kuwepo tu kuwa algoriti halisi ambayo Alice anaweza kuendesha: decoys D zake zinatoka kwenye mstari wa uzalishaji, si hewani.

Hatua ya cryptographic ni kutumia upungufu huo wa nguvu ya uthibitisho kama rasilimali.

Ujenzi unafanya nini

Huu ndio umbo la ujenzi wa makala, bila mapambo.

Funga rulebook — tuseme ZFC. Chini ya dhana ya utata wa uthibitisho, kuna mfuatano unaoweza kuzalishwa kwa ufanisi wa formulas ambazo kwa kweli ni unsatisfiable, lakini rulebook haina uthibitisho fupi kwamba ni unsatisfiable.

Sasa jenga uthibitisho ya ujumbe mmoja ya umbo hili:

> ama statement halisi inaweza kutimizwa, au formula hii maalum ngumu inaweza kutimizwa.

Formula maalum ngumu haiwezi kutimizwa. Kwa hiyo, ikiwa machinery ya uthibitisho ina soundness kamili, kukubali ujumbe bado kunamaanisha statement halisi ni true. Hapo ndipo soundness kamili inapotoka.

Lakini kwa usalama unaofanana na zero-knowledge, fikiria formula maalum ngumu *ingeweza* kutimizwa. Shahidi wake basi angeweza kutumiwa kuiga uthibitisho bila kujua shahidi halisi. Formula haiwezi kutimizwa katika uhalisia — lakini rulebook haiwezi kuthibitisha hilo kwa ufanisi. Kwa hiyo haiwezi kuthibitisha kwa ufanisi kwamba kiigaji hakiwezekani.

Huo ndio mhimili. Mfumo haufichi siri kwa kuzalisha kiigaji cha kawaida. Kwa kundi kubwa la majaribio ya usalama yanayoonekana, huficha siri nyuma ya kutokuwa na uwezo wa rulebook kuthibitisha kwamba kiigaji hakipo.

makala inadai nini

Teorema kuu ina tabaka kadhaa. Matokeo ya msingi ni haya:

Chini ya dhana ya kawaida ya cryptography — kuwepo kwa **non-interactive witness indistinguishable uthibitisho**, vitu vilivyochunguzwa sana vinavyofuata kutoka vifurushi kadhaa vya dhana vinavyotumika — na chini ya conjecture ya utata wa uthibitisho kwamba **hakuna (infinitely often) optimal mfumo wa uthibitisho**, makala inajenga, kwa kila chaguo la rulebook, prover na verifier wa ujumbe mmoja kwa NP/SAT wenye **soundness kamili**, bila setup, ambao ni effectively zero-knowledge ukihusishwa na rulebook hiyo. (NP/SAT ni "hardest common denominator" ya kawaida ya matatizo yanayofanana na mafumbo; mega-Sudoku ni mavazi moja tu inayovaa.)

Kwa dai pana zaidi la kuhifadhi mali za usalama zinazoweza kufalsifiwa, makala inaongeza dhana nyingine ya kawaida: imani ya derandomization **P = BPP** (kwa ufupi: randomness haizipi algoriti nguvu ya ziada iliyo ya lazima).

Tukitafsiri kutoka lugha ya theorem:

- uthibitisho ni ujumbe mmoja.
- Hakuna setup ya kuaminika.
- Statements za uongo haziwezi kuthibitishwa.
- Prover si zero-knowledge ya kawaida — haina kiigaji.
- Lakini kila matokeo ya usalama ya zero-knowledge ya kawaida ambayo yanaweza kufalsifiwa na kujaribiwa katika game linaweza kufikiwa katika mpangilio huu.

Neno "falsifiable" ni muhimu. Linamaanisha failure ya usalama inaweza kujaribiwa kwa kumendesha adversary katika game. Definitions nyingi za usalama wa cryptography zina umbo hili: je, adversary anaweza kutofautisha encryptions mbili, kugeuza function, kupata witness, au kushinda experiment maalum? Teorema inatoa prover kwa kila property inayoweza kufalsifiwa, moja baada ya nyingine. Prover mmoja mwenye **properties zote** zinazoweza kufalsifiwa kwa wakati mmoja huenda haiwezekani — shambulio la zamani la reusability ("Bob anaweza kuwaonyesha wengine uthibitisho") lenyewe ni property inayoweza kufalsifiwa, na kwa kweli linafeli hapa. Proposal ya makala ni kwamba prover mmoja huenda akaweza kufunika properties zote **natural** zinazoweza kufalsifiwa — zile zinazotokea katika matumizi halisi ya cryptography — lakini sehemu hiyo ni teorema ya masharti inayotegemea notion isiyo rasmi ya "natural", pamoja na conjecture iliyo wazi. Dhamana inalenga failures zinazoweza kuonekana, si kila maana ya kifalsafa au uigaji-based ya usiri.

Corollary moja ya moja kwa moja inafaa kutajwa: ujenzi unatoa uthibitisho za kwanza zisizoingiliana za **witness hiding** zenye prover uniform — "uthibitisho wa fumbo haukusaidii kupata suluhisho lake," bila interaction na bila setup — kitu kinachosikika kidogo lakini kilikataa kujengwa kwa miongo kadhaa.

Hii haisemi nini

Hii ndiyo sehemu inayoweka makala katika mipaka yake.

Haisemi teorema za zamani za kutowezekana zilikuwa na makosa. Ujenzi unazikwepa kwa kubadilisha definition.

Haitoi zero-knowledge ya kawaida, ya classical, bila interaction, bila setup na yenye soundness kamili. makala inasema wazi kwamba prover iliyojengwa haina simulator.

Haimaanishi uthibitisho haiwezi kutumika tena. uthibitisho ya ujumbe mmoja bado inaweza kuonyeshwa kwa mtu mwingine; makala haihifadhi properties za aina ya deniability. (Non-interactive zero-knowledge yenye trusted setup ina limitation hiyo hiyo.)

Haimaanishi hii ni protocol ya vitendo iliyo tayari kutumia katika mazingira halisi. Hii ni complexity theory na misingi ya cryptography. Matokeo yanategemea dhana kubwa kutoka utata wa uthibitisho na cryptography, na ujenzi unahusu kinachowezekana kwa kanuni.

Haifanyi "Gödel" kuwa primitive ya kichawi ya usalama. Uhusiano wa Gödel unapitia mifumo ya uthibitisho, optimal mifumo ya uthibitisho na analojia finite za incompleteness. Intuition inayoweza kutumiwa si "incompleteness inalinda password yako." Ni: ikiwa rulebook haiwezi kuthibitisha kwa ufanisi kwamba kiigaji hakiwezekani, basi mashambulio ambayo yangetaka uthibitisho hiyo yanaweza kuzuiwa katika kiwango cha definition za usalama.

Kwa nini bado inavutia

Cryptography mara nyingi hubadilisha ugumu kuwa usalama. Factoring ni ngumu, kwa hiyo dhana za mtindo wa RSA zinafaa. Matatizo ya lattice ni magumu, kwa hiyo lattice cryptography linafaa. Hapa ugumu ni wa ajabu zaidi: si "ni vigumu kukokotoa siri," bali "ni vigumu kuthibitisha kwamba object fulani ya uthibitisho haiwezi kuwepo."

Ndiyo maana makala ina hisia isiyo ya kawaida. Inatendea axioms na rulebooks karibu kama rasilimali za cryptography. Kutowezekana kwa kawaida kunasema kuna mvutano kati ya soundness na uigaji. Hatua ya Ilango ni kuweka mvutano huo nyuma ya pazia la uthibitisho theory: kiigaji hakipo, lakini mfumo rasmi hauwezi kufichua kwa ufanisi kutokuwepo kwake.

Kwa msomaji, jambo la kushangaza si kwamba hii itachukua nafasi ya mifumo ya zero-knowledge ya leo. Huenda haitafanya hivyo, angalau si moja kwa moja. Jambo la kushangaza ni kwamba limitation kutoka logic ya hisabati inaweza kutumiwa kwa kujenga: si kama ukuta tu, bali kama aina ya kifuniko.

Ushahidi una nguvu kiasi gani?

Hii ni makala ya theorem, kwa hiyo “ushahidi” una maana tofauti na katika biology au astronomy. Swali si kama experiment imerudiwa. Swali ni kama definitions, dhana na mlolongo wa uthibitisho vinaunga mkono dai.

uthibitisho ni rasmi, na makala iko wazi kuhusu dhana zake. dhana si za kawaida tu. Non-interactive witness indistinguishable uthibitisho ni objects za kawaida katika cryptography na zinafuata kutoka vifurushi kadhaa vya dhana vinavyotumika. Conjecture kwamba hakuna optimal mfumo wa uthibitisho ni conjecture kuu katika utata wa uthibitisho. **P = BPP** ni imani ya kawaida ya derandomization inayotumiwa tu kwa theorem pana zaidi ya properties zinazoweza kufalsifiwa.

makala pia inatoa hoja kwamba dhana hizo ni gharama inayofaa, si scaffold iliyochaguliwa kiholela: inathibitisha converse inayoonyesha kwamba kwa kiasi kikubwa ni za lazima — ikiwa constructions kama hii zipo kabisa, basi non-interactive witness indistinguishable uthibitisho lazima ziwepo, na (ukikubali one-way functions za kawaida) optimal mfumo wa uthibitisho haiwezi kuwepo. Na dhana ni “win-win”: kukataa yoyote kati yao kungekuwa yenyewe ugunduzi mkubwa katika utata wa uthibitisho, cryptography au complexity theory.

Lakini kwa kuwa matokeo ni conditional, confidence yake pia ni conditional. Ikiwa dhana hizo ni false, interpretation ya theorem hubadilika. Na hata zikishikilia, dhamana si full classical zero-knowledge; ni toleo lililolegezwa, la uthibitisho-theoretic, la makala.

Kwa hiyo confidence inayofaa ni kubwa kwamba makala inaweka possibility matokeo thabiti ya masharti; ya wastani kwamba dhana zake zinaelezea ulimwengu wa cryptography tunamoishi; na ndogo kwa consequence yoyote ya haraka ya vitendo.

Kwa nini ni muhimu

makala inafungua njia ambayo ilidhaniwa imefungwa.

Nadharia ya kawaida inasema: full zero-knowledge haiwezi kuwa ujumbe mmoja bila setup, na haiwezi kuwa perfectly sound. makala ya Ilango inasema: tukiomba consequences za zero-knowledge zinazoweza kujaribiwa katika security games, na tukiruhusu definition ya usalama kutegemea kile ambacho rulebook inaweza au haiwezi kurefute kwa ufanisi, basi sehemu kubwa ya tabia muhimu inaweza kurejeshwa — kwa ujumbe mmoja, bila setup na soundness kamili.

Hiyo si tweak ndogo ya definition. Ni njia tofauti ya kufikiria dhamana za cryptography. Badala ya kuuliza tu nini kipo, uliza rulebook yako inaweza kuondoa nini. Badala ya kutazama unprovability kama usumbufu wa kifalsafa, itumie kama muundo.

Ulimwengu wa vitendo huenda usibadilike kesho. Lakini ramani ya dhana inabadilika. Sasa kuna maana rasmi ambamo “hakuna mtu anayeweza kuthibitisha kwa ufanisi kwamba siri ilivuja” inaweza kuwa na nguvu ya kutosha kurejesha protections nyingi za game-based ambazo tulitaka kutoka “siri haikuvuja.”

Ndiyo maana Gödel anastahili kuwa kwenye kichwa.

Muhtasari safi

Uthibitisho wa zero-knowledge humruhusu prover kumshawishi verifier kwamba statement ni true bila kufichua witness. Matokeo ya kawaida ya kutowezekana yanasema zero-knowledge haiwezi kubanwa kuwa ujumbe mmoja bila setup, na haiwezi kuwa na soundness kamili. makala ya Rahul Ilango haibatilishi kutowezekana huko. Inafafanua notion dhaifu zaidi, **effectively zero-knowledge**: badala ya kudai kwamba kiigaji kipo kwa kweli, inadai kwamba mfumo wa uthibitisho iliyochaguliwa — rulebook rasmi kama ZFC — haiwezi kuthibitisha kwa ufanisi kwamba hakuna kiigaji. Chini ya dhana kubwa kutoka cryptography (non-interactive witness indistinguishable uthibitisho) na utata wa uthibitisho (hakuna optimal mfumo wa uthibitisho), makala inajenga provers wa ujumbe mmoja kwa NP/SAT bila setup na wenye soundness kamili ambao wanafikia, property kwa property, consequences zinazoweza kufalsifiwa na kujaribiwa katika game za zero-knowledge ya kawaida. Prover mmoja anayefunika properties zote "natural" za aina hiyo ni extension nyingine, yenye sehemu ya conjecture — na kufunika literally kila property inayoweza kufalsifiwa huenda haiwezekani, kwa sababu uthibitisho bado zinaweza kutumiwa tena. Matokeo ni ya kinadharia na conditional, si primitive iliyowekwa kazini, lakini yanaonyesha njia mpya ya kutumia unprovability ya uthibitisho theory kama rasilimali ya cryptography.

Ukaguzi bila kupamba ukweli

makala inaonyesha nini: Chini ya dhana zilizotajwa, inawezekana kujenga provers wa ujumbe mmoja, bila setup, wenye soundness kamili kwa NP/SAT ambao ni effectively zero-knowledge ukihusishwa na mfumo wa uthibitisho yoyote iliyochaguliwa, na ambao wanafikia kila consequence ya classical zero-knowledge inayoweza kufalsifiwa katika game.

Kinachoaminika lakini hakijathibitishwa bila masharti: Kwamba dhana zinazohitajika za utata wa uthibitisho na cryptography ni kweli. Ni dhana nzito na zilizochunguzwa sana — na makala inaonyesha kwa kiasi kikubwa ni za lazima pamoja na kuwa za kutosha — lakini bado ni dhana.

Kisichoonyeshwa: Classical zero-knowledge bila interaction, bila setup na yenye soundness kamili; mfumo wa vitendo ulio tayari kutumia katika mazingira halisi; deniability au kutoweza kutumia uthibitisho tena; wala kwamba theorem ya Gödel ya incompleteness yenyewe inalinda cryptography.

Mapungufu makuu: Dhamana ni relaxation ya zero-knowledge; toleo pana zaidi linategemea dhana kadhaa; madai ya prover mmoja wa universal bado yana sehemu ya conjecture; na matokeo ni ya msingi wa nadharia zaidi kuliko matumizi ya moja kwa moja.

Msomaji wa kawaida awe na confidence kiasi gani? Kubwa kwamba hii ni matokeo muhimu ya theory yenye masharti ikiwa definitions zinakubaliwa. Ya wastani kwamba dhana zinaakisi uhalisia. Ndogo kwa deployment ya haraka ya vitendo. Hitimisho salama ni hili: makala haivunji impossibility

matokeo za zero-knowledge; inapata njia mpya ya uthibitisho theory ya kuzunguka sehemu zake zinazohusika na security games nyingi.

Vyanzo

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