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

Μια κρυπτογραφική απόδειξη μπορεί να κρύψει το μυστικό της κάνοντας δύσκολο να αποδειχθεί ότι λείπει ο προσομοιωτής

Οι αποδείξεις μηδενικής γνώσης επιτρέπουν σε κάποιον να αποδείξει μια πρόταση χωρίς να αποκαλύψει τον witness. Η κλασική θεωρία λέει ότι αυτό, με την πλήρη έννοια, δεν μπορεί να συνδυαστεί με ένα μόνο μήνυμα, χωρίς trusted setup και με τέλεια soundness. Η εργασία του Rahul Ilango δεν εξαφανίζει αυτή την αδυνατότητα. Αλλάζει τον στόχο: αντί να απαιτεί ότι ένας simulator υπάρχει πραγματικά, ζητά κανένα επιλεγμένο proof system να μην μπορεί να αποδείξει αποτελεσματικά ότι ο simulator δεν υπάρχει. Υπό σημαντικές υποθέσεις από την πολυπλοκότητα αποδείξεων και την κρυπτογραφία, αυτό αρκεί για να ανακτηθούν, μία προς μία, διαψεύσιμες συνέπειες της zero-knowledge που βασίζονται σε παιχνίδια. Το νόημα δεν είναι ένα έτοιμο primitive για το διαδίκτυο. Είναι ένας proof-theoretic τρόπος να μετατραπεί η μαθηματική αναποδειξιμότητα σε κρυπτογραφική κάλυψη.

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

Το τέχνασμα δεν είναι να αποδείξεις ότι το μυστικό είναι κρυμμένο

Ας ξεκινήσουμε από την απλούστερη εκδοχή της μηδενικής γνώσης.

Η Alice θέλει να πείσει τον Bob ότι ένα Sudoku έχει λύση. Αν του στείλει τη λύση, ο Bob πείθεται, αλλά το παζλ καταστρέφεται. Αυτό που θέλει είναι κάτι πιο παράξενο: μια απόδειξη ότι υπάρχει λύση, χωρίς να αποκαλύψει τη λύση.

Αυτή είναι η υπόσχεση μιας απόδειξης μηδενικής γνώσης (zero-knowledge proof). Ο αποδεικνύων, η Alice, πείθει τον επαληθευτή, τον Bob, ότι μια πρόταση είναι αληθής, χωρίς να αποκαλύπτει τίποτε πέρα από το ότι η πρόταση είναι αληθής.

Το πρόβλημα είναι ότι αυτή η υπόσχεση έχει κόστος. Μια συνηθισμένη μαθηματική απόδειξη έχει δύο άνετα χαρακτηριστικά. Είναι **ένα μήνυμα**: τη γράφεις, την παραδίδεις και φεύγεις. Και έχει **τέλεια ορθότητα ως προς ψευδείς προτάσεις (perfect soundness)**: μια ψευδής πρόταση δεν έχει καμία έγκυρη απόδειξη. Κλασικά θεωρήματα αδυνατότητας λένε ότι η μηδενική γνώση πρέπει να εγκαταλείψει και τα δύο χαρακτηριστικά — και όχι απλώς τον συνδυασμό τους· καθένα ξεχωριστά είναι απαγορευμένο.

Πρώτον, μια απόδειξη μηδενικής γνώσης χρειάζεται διάλογο. Αν η Alice στείλει ένα μόνο μήνυμα, χωρίς κάποια έμπιστη αρχικοποίηση (trusted setup) που έχει συμφωνηθεί εκ των προτέρων, η εγγύηση μηδενικής γνώσης καταρρέει — ανεξάρτητα από το πόση soundness είσαι διατεθειμένος να θυσιάσεις ως αντάλλαγμα.

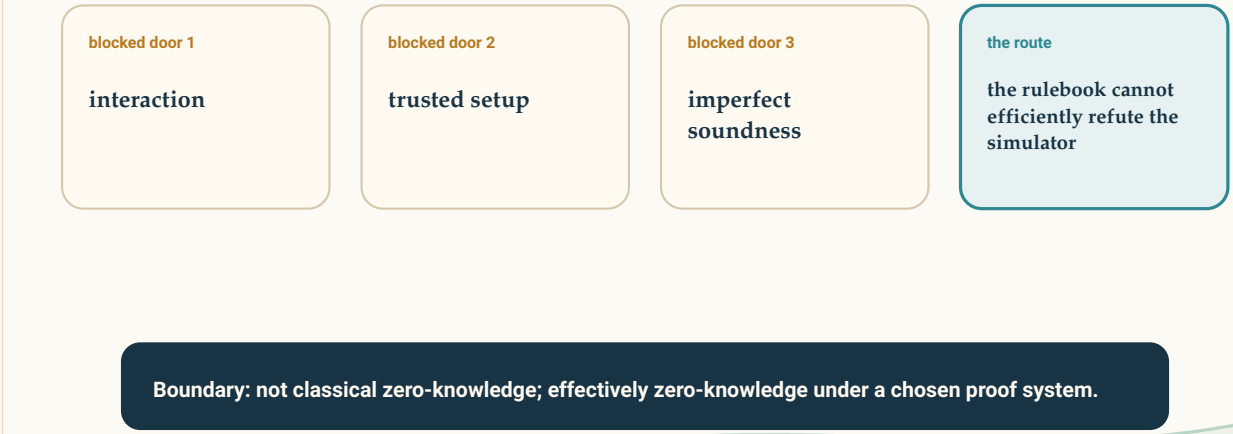
Δεύτερον, μια απόδειξη μηδενικής γνώσης χρειάζεται μια μικρή ανοχή σε σφάλμα. Η απαίτηση για τέλεια soundness αποδεικνύεται ότι καταστρέφει σιωπηρά και την αλληλεπίδραση: ένας επαληθευτής που δεν μπορεί ποτέ να ξεγελαστεί, όποιες τυχαίες επιλογές κι αν κάνει, θα μπορούσε εξίσου καλά να καθορίσει αυτές τις επιλογές από πριν — και μόλις ο επαληθευτής γίνει προβλέψιμος, η Alice μπορεί να απαντήσει σε όλα με ένα μόνο μήνυμα, δηλαδή ακριβώς στην περίπτωση που ήδη ξέρουμε ότι αποτυγχάνει.

Η εργασία του Rahul Ilango αφορά έναν τρόπο να παρακαμφθεί αυτός ο διπλός τοίχος. Όχι προσποιούμενη ότι ο τοίχος δεν υπάρχει και όχι κατασκευάζοντας κλασική μηδενική γνώση στο αδύνατο καθεστώς. Η κίνηση είναι λεπτότερη: αποδυναμώνει το τι σημαίνει «δεν αποκαλύπτει τίποτε», αλλά το αποδυναμώνει με τρόπο που διατηρεί τις ιδιότητες ασφάλειας τις οποίες οι κρυπτογράφοι μπορούν πράγματι να ελέγξουν.

Το αποτέλεσμα ονομάζεται **effectively zero-knowledge**, δηλαδή «αποτελεσματικά μηδενική γνώση».

A proof without leaking the witness

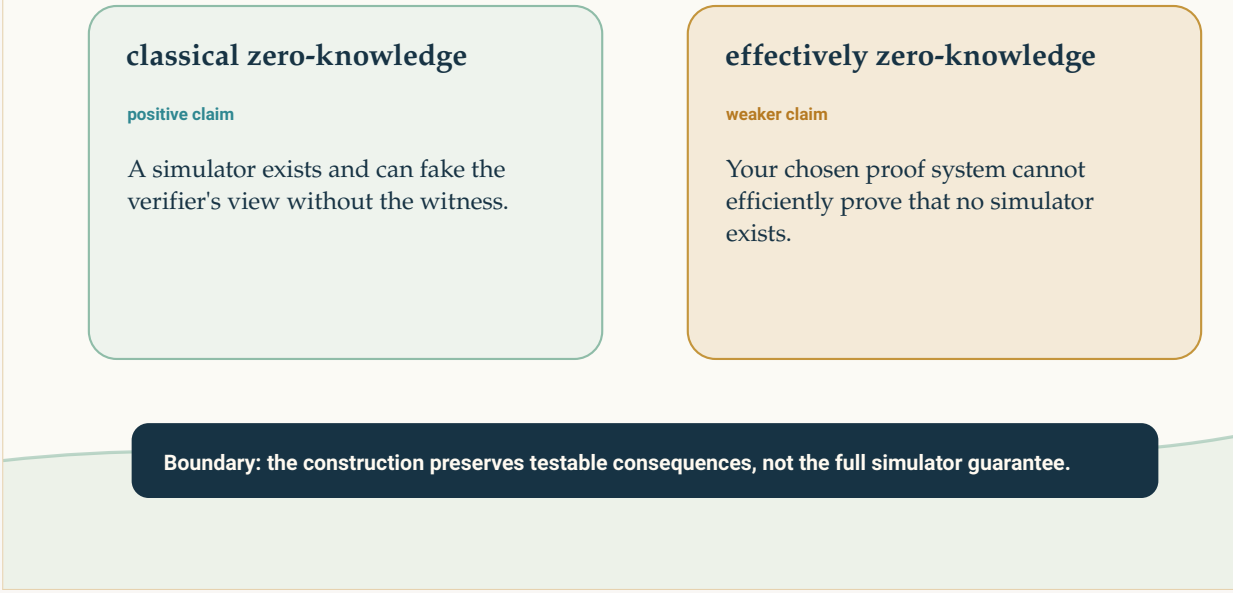
The paper keeps the ordinary-proof shape by weakening what privacy must prove.



Η μηδενική γνώση βρίσκει κλειστές τρεις πόρτες — αλληλεπίδραση, trusted setup και μη τέλεια soundness. Η κατασκευή του Ilango περνά από μια διαφορετική: το επιλεγμένο τυπικό σύστημα δεν μπορεί να αντικρούσει αποτελεσματικά την ύπαρξη του προσομοιωτή.

Classical privacy vs effective privacy

The relaxation is the point: the paper changes what the privacy claim has to establish.



Η κλασική μηδενική γνώση ρωτά αν υπάρχει προσομοιωτής· η «effectively zero-knowledge» ρωτά μόνο αν

το επιλεγμένο τυπικό σύστημα μπορεί να αποδείξει αποτελεσματικά ότι δεν μπορεί να υπάρχει. Αυτή η ασθενέστερη ερώτηση είναι που επιτρέπει στην κατασκευή να κρατήσει ένα μήνυμα, καθόλου setup και τέλεια soundness.

Το παλιό κριτήριο: υπάρχει προσομοιωτής

Ο κλασικός τρόπος να διατυπωθεί μαθηματικά η μηδενική γνώση χρησιμοποιεί έναν υποθετικό βοηθό που ονομάζεται **προσομοιωτής (simulator)**.

Η ιδέα είναι η εξής: φανταστείτε την Jane, η οποία **δεν** γνωρίζει το μυστικό της Alice. Αν η Jane μπορεί, ολομόναχη, να δημιουργήσει αποδείξεις που μοιάζουν ακριβώς με εκείνες που θα είχε λάβει ο Bob από την Alice, τότε οι αποδείξεις της Alice δεν δίδαξαν στον Bob τίποτε καινούργιο. Η Jane μπορούσε ήδη να αναπαράγει την εμπειρία χωρίς το μυστικό της Alice.

Άρα η κλασική μηδενική γνώση απαιτεί έναν πραγματικό προσομοιωτή. Πρέπει να υπάρχει ένας αποδοτικός αλγόριθμος που μπορεί να παράγει πειστικές ψεύτικες αποδείξεις χωρίς να γνωρίζει το μυστικό — τον **μάρτυρα (witness)**, στην ορολογία· για το Sudoku, ο μάρτυρας είναι απλώς το συμπληρωμένο πλέγμα.

Ο ορισμός είναι ισχυρός, αλλά ακριβώς εκεί δαγκώνει και η παλιά αδυναμία. Η διαίσθηση είναι η εξής. Μια πραγματικά μη διαδραστική απόδειξη είναι απλώς μια συμβολοσειρά. Μόλις ο Bob έχει αυτή τη συμβολοσειρά, μπορεί να τη δείξει σε κάποιον άλλο: απέκτησε την ικανότητα να αποδεικνύει την πρόταση και σε άλλους, κάτι που ήδη ακούγεται σαν περισσότερο από «τίποτε». Τα κλασικά θεωρήματα μετατρέπουν αυτή τη διαίσθηση στις παραπάνω αδυναμίες.

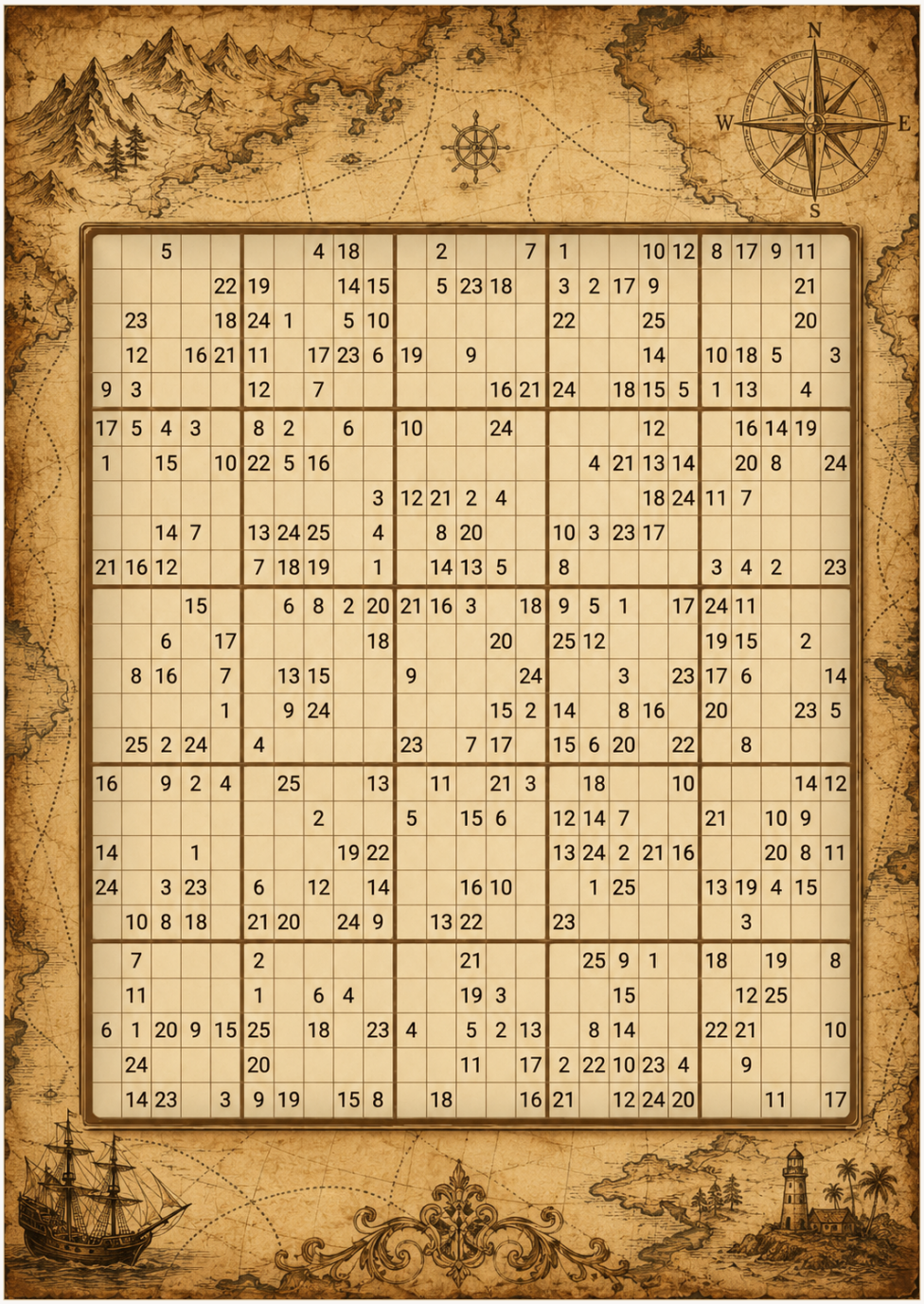
Οι τρεις ιδιότητες στις οποίες επιμένει αυτή η εργασία

Ο τίτλος της εργασίας κατονομάζει τρεις περιορισμούς:
Καμία αλληλεπίδραση: Η Alice στέλνει μία συμβολοσειρά απόδειξης. Δεν υπάρχει πρωτόκολλο με πήγαινε-έλα.
Καθόλου setup: Η Alice και ο Bob δεν βασίζονται σε μια έμπιστη κοινή συμβολοσειρά αναφοράς ή σε άλλη δημόσια τυχαιότητα που έχει κανονιστεί εκ των προτέρων. Πολλά συστήματα που ονομάζονται «μη διαδραστική μηδενική γνώση» εξακολουθούν να βασίζονται σε setup· εδώ εννοείται μηδενικό setup.
Τέλεια soundness: μια ψευδής πρόταση δεν έχει έγκυρη απόδειξη. Όχι «σχεδόν ποτέ δεν γίνεται δεκτή»· δεν υπάρχει έγκυρη απόδειξη.
Αυτές είναι ακριβώς οι τρεις ιδιότητες που έχει η συνηθισμένη γραπτή μαθηματική απόδειξη — και, όπως εξηγήθηκε παραπάνω, η κλασική μηδενική γνώση δεν μπορεί να τις διατηρήσει.

Η διαφορά σε μια εκδοχή MegaSudoku

Ακολουθεί ένας σκόπιμα απλουστευμένος τρόπος να νιώσει κανείς τη διαφορά.

Μη χρησιμοποιήσετε ένα συνηθισμένο Sudoku 9 επί 9 για το σοβαρό μέρος της αναλογίας. Είναι υπερβολικά μικρό και πεπερασμένο: ένας υπολογιστής μπορεί απλώς να το λύσει ή να αποδείξει ότι δεν έχει λύση. Φανταστείτε αντί γι' αυτό μια οικογένεια παζλ **MegaSudoku(n)**. Μεγεθύνετε τον συνηθισμένο κανόνα: επιλέξτε μέγεθος μπλοκ *n*, θέστε *N* = *n^2* και κατασκευάστε ένα πλέγμα *N* επί *N*, χωρισμένο σε μπλοκ *n* επί *n*, με *N* σύμβολα. Το συνηθισμένο Sudoku είναι απλώς η μικροσκοπική περίπτωση *n* = *3*, *N* = *9*: πλέγμα 9 επί 9, μπλοκ 3 επί 3 και εννέα σύμβολα. Η ιστορία της πολυπλοκότητας αποδείξεων αρχίζει μόνο όταν επιτρέπουμε στο *n* να μεγαλώνει και όταν το πλέγμα μπορεί να περιέχει πρόσθετα gadgets που το κάνουν να συμπεριφέρεται σαν τύπος SAT ντυμένος Sudoku. Ένας τύπος SAT είναι απλώς μια λίστα περιορισμών ναι/όχι: μπορείς να αντιστοιχίσεις τιμές αληθές/ψευδές στις μεταβλητές έτσι ώστε να ικανοποιούνται όλοι οι περιορισμοί;



Ένα Sudoku 25x25: οι κανόνες του μπορούν να ελεγχθούν χωρίς να αποκαλυφθεί το ολοκληρωμένο πλέγμα — ένα οπτικό υποκατάστατο για μια απόδειξη που επαληθεύει μια κρυφή λύση, τον witness.

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

Sudoku και SAT: το ίδιο παζλ με δύο μεταμφιέσεις

Ο ισχυρισμός ότι ένα Sudoku μπορεί «να συμπεριφέρεται σαν τύπος SAT» δεν είναι μεταφορά. Η μετάφραση λειτουργεί και προς τις δύο κατευθύνσεις, και η εύκολη κατεύθυνση μπορεί να γραφτεί ολόκληρη.

Από Sudoku σε SAT. Το SAT μιλά μόνο σε αληθές/ψευδές, οπότε του δίνουμε μία δυαδική

μεταβλητή για κάθε τριάδα (γραμμή, στήλη, τιμή): *x(r,c,v)* σημαίνει «το κελί στη γραμμή *r*, στήλη *c* περιέχει την τιμή *v*.» Ένα Sudoku 4 επί 4 (μπλοκ 2 επί 2, τιμές 1–4) χρειάζεται 4·4·4 = 64 μεταβλητές· το κλασικό 9 επί 9 χρειάζεται 729. Κάθε κανόνας Sudoku γίνεται στη συνέχεια μια δέσμη από ρήτρες. (Μια ρήτρα είναι OR μεταβλητών ή αρνήσεών τους· ολόκληρος ο τύπος είναι το AND όλων των ρητρών.)
Κάθε κελί περιέχει τουλάχιστον μία τιμή — μία ρήτρα ανά κελί:

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

Κάθε κελί περιέχει το πολύ μία τιμή — μία ρήτρα «όχι και τα δύο» για κάθε ζεύγος τιμών:

¬x(1,1,1) ∨ ¬x(1,1,2) ¬x(1,1,1) ∨ ¬x(1,1,3) … και ούτω καθεξής για όλα τα έξι ζεύγη.

Κάθε γραμμή περιέχει κάθε τιμή — για τη γραμμή 1 και την τιμή 3: τουλάχιστον μία φορά,

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

και το πολύ μία φορά: ¬x(1,1,3) ∨ ¬x(1,2,3), και ούτω καθεξής για κάθε ζεύγος κελιών στη γραμμή.
Στήλες και μπλοκ — ίδιες δέσμες· αλλάζει μόνο η ομάδα κελιών. Για το πάνω αριστερό μπλοκ και την τιμή 2:

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

συν τις ανά ζεύγη ρήτρες «όχι και τα δύο».
Οι τυπωμένες ενδείξεις — το απλούστερο μέρος: κάθε ένδειξη είναι μια ρήτρα με μία μόνο μεταβλητή. Ένα τυπωμένο 3 στην πάνω αριστερή γωνία γίνεται η ρήτρα

x(1,1,3)

Το AND όλων αυτών είναι ικανοποιήσιμο ακριβώς όταν το Sudoku έχει λύση — και μια ικανοποιούσα ανάθεση *είναι* η λύση: διαβάζουμε ποιες x(r,c,v) είναι αληθείς και συμπληρώνουμε το πλέγμα. Για ένα 9 επί 9 αυτό σημαίνει 729 μεταβλητές και μερικές χιλιάδες ρήτρες, τις οποίες ένας σύγχρονος SAT solver λύνει σε χιλιοστά του δευτερολέπτου. Προσέξτε τη ρήτρα της ένδειξης x(1,1,3): λέει «αυτό το κελί ισούται ακριβώς με 3», όχι «αυτά τα κελιά είναι όλα διαφορετικά» — η ίδια ασυμμετρία που θα απαιτήσει το επιπλέον τέχνασμα για τα κελιά με ενδείξεις στη σημείωση του πρωτοκόλλου παρακάτω.
Από SAT σε Sudoku. Η εργασία χρειάζεται την αντίθετη, δυσκολότερη κατεύθυνση: δοθέντος ενός αυθαίρετου τύπου SAT, να κατασκευαστεί ένα mega-Sudoku που έχει λύση ακριβώς όταν ο τύπος είναι ικανοποιήσιμος. Οι εγγενείς κανόνες του Sudoku μπορούν μόνο να πουν «αυτά τα κελιά είναι όλα διαφορετικά», οπότε οι αυθαίρετοι λογικοί περιορισμοί πρέπει να κατασκευαστούν — και ακριβώς αυτό είναι τα gadgets. Ένα gadget είναι μια μικρή προκατασκευασμένη συστάδα κελιών, μία για κάθε ρήτρα του τύπου, όπου ορισμένα κελιά παίζουν τον ρόλο μεταβλητών (το σύμβολο που

περιέχουν κωδικοποιεί αληθές ή ψευδές) και οι εσωτερικοί περιορισμοί της συστάδας έχουν σχεδιαστεί έτσι ώστε τα μόνα νόμιμα συμπληρώματα να αντιστοιχούν σε αναθέσεις που ικανοποιούν τη ρήτρα. Πρόκειται για τυπική τεχνική από αποδείξεις NP-πληρότητας· για το γενικευμένο Sudoku υλοποιήθηκε από τους Yato και Seta το 2003. Μαζί, οι δύο κατευθύνσεις λένε ότι το Sudoku N επί N και το SAT είναι το ίδιο πρόβλημα με δύο διαφορετικές μεταμφιέσεις. Αυτό είναι που επιτρέπει σε αυτό το άρθρο — και στην εργασία — να αφηγείται μια ιστορία για ολόκληρη την NP χρησιμοποιώντας πλέγματα και σύμβολα.

Ο witness παραμένει εύκολο να απεικονιστεί. Η Alice γνωρίζει ένα πλήρες έγκυρο συμπλήρωμα του mega-Sudoku. Ο Bob θέλει να πειστεί ότι υπάρχει τέτοιο συμπλήρωμα, αλλά η Alice δεν θέλει να το αποκαλύψει. Αν στείλει ολόκληρο το συμπλήρωμα, ο Bob πείθεται, αλλά το μυστικό χάνεται.

Στην κλασική εκδοχή μηδενικής γνώσης, η Alice και ο Bob αλληλεπιδρούν. Ένα παλιό νοητικό μοντέλο χρησιμοποιεί καλυμμένα πλακίδια. Η Alice κρύβει το λυμένο πλέγμα, μετονομάζει κρυφά τα σύμβολα πριν από κάθε γύρο και αφήνει τον Bob να επιθεωρήσει έναν τυχαία επιλεγμένο τοπικό περιορισμό: μια γραμμή, μια στήλη, ένα μπλοκ ή ένα gadget. Αν τα ανοιγμένα κελιά δείχνουν όλα διαφορετικά σύμβολα, ο Bob αποκτά περισσότερη εμπιστοσύνη. Μετά όλα καλύπτονται ξανά και τα σύμβολα μετονομάζονται εκ νέου. (Υπάρχει μια λεπτομέρεια: οι δοσμένες ενδείξεις του παζλ χρειάζονται επιπλέον τέχνασμα, επειδή η μετονομασία των συμβόλων τις κρύβει κι αυτές. Η σημείωση παρακάτω εξηγεί πώς το λύνουν τα κλασικά πρωτόκολλα· για όσα ακολουθούν αρκεί αυτή η απλοποιημένη εικόνα.)

Πώς χειρίζονται πραγματικά τα κλασικά πρωτόκολλα τα κελιά με ενδείξεις

Το τέχνασμα της μετονομασίας έχει ένα τυφλό σημείο. Οι κανόνες γραμμής, στήλης και μπλοκ λένε όλοι «αυτά τα κελιά είναι όλα διαφορετικά», και το *όλα διαφορετικά* επιβιώνει από οποιαδήποτε μετονομασία των συμβόλων. Όμως μια ένδειξη λέει «αυτό το κελί περιέχει ακριβώς 5», και μετά τη μετονομασία ο Bob βλέπει μόνο σ(5) — κάποιο καλυμμένο σύμβολο — χωρίς να γνωρίζει τη μετονομασία σ. Δεν μπορεί να ελέγξει τίποτε. Αν δεν διορθωθεί αυτό, η Alice θα μπορούσε να αποδείξει ότι υπάρχει *κάποιο* έγκυρο πλέγμα αγνοώντας εντελώς τις τυπωμένες ενδείξεις, πράγμα που δεν αποδεικνύει τίποτε για *αυτό* το παζλ. Η κλασική βιβλιογραφία έχει δύο τυπικές λύσεις. **Η παλέτα.** Προσθέστε μία επιπλέον γραμμή N κελιών στο κρυφό πλέγμα — μια παλέτα που η Alice γεμίζει με τα σύμβολα 1…N σε σταθερή δημόσια σειρά και στη συνέχεια μετονομάζει μαζί με όλα τα υπόλοιπα, ώστε να περιέχει σ(1)…σ(N). Η τυχαία πρόκληση του Bob έχει τώρα μία επιπλέον επιλογή. Εκτός από το να διαλέξει μια γραμμή, στήλη, μπλοκ ή gadget για άνοιγμα, μπορεί να επιλέξει **την παλέτα μαζί με ένα κελί ένδειξης**. Η Alice αποκαλύπτει και τα δύο· η παλέτα αποκαλύπτει τη μετονομασία εκείνου του γύρου και ο Bob ελέγχει ότι το κελί της ένδειξης δείχνει ακριβώς τη μετονομασμένη μορφή της τυπωμένης ένδειξης. Αυτό παραμένει zero-knowledge επειδή ο Bob μαθαίνει μόνο το σ — το οποίο επιλέγεται ξανά τυχαία σε κάθε γύρο και από μόνο του είναι

άχρηστο — και την τιμή ενός κελιού που ήδη γνώριζε από το παζλ. Τίποτε για τα μυστικά κελιά δεν διαρρέει και ένας simulator μπορεί να αναπαράγει την εικόνα επιλέγοντας ένα τυχαίο σ. Είναι sound επειδή μια Alice που κλέβει έχει σταθερή πιθανότητα να πιαστεί σε κάθε γύρο και οι γύροι επαναλαμβάνονται μέχρι η αμφιβολία να γίνει αμελητέα.

Μεταγλώττιση των ενδείξεων. Μια πιο δομική παραλλαγή αφαιρεί την ειδική πρόκληση αντί να την προσθέσει. Αντί να *επαληθεύσουμε* την τιμή της ένδειξης, την επιβάλλουμε με περιορισμούς ανισότητας: συνδέουμε το κελί της ένδειξης με κάθε κελί της παλέτας εκτός από εκείνο που φέρει τη δική του τιμή — «διαφορετικό από σ(1), διαφορετικό από σ(2), …, διαφορετικό από όλα εκτός από σ(5)». Το μόνο σύμβολο που μπορεί νόμιμα να περιέχει το κελί είναι εκείνο της ένδειξης. Κάθε περιορισμός είναι πάλι του τύπου «αυτά τα δύο διαφέρουν» — αμετάβλητος στη μετονομασία και ελέγξιμος ακριβώς όπως μια γραμμή. Είναι η ίδια κίνηση που χρησιμοποιείται για προχρωματισμένες κορυφές στο κλασικό πρωτόκολλο χρωματισμού γράφων και βρίσκεται στο πνεύμα της λέξης *gadgets* παραπάνω: στην εικόνα MegaSudoku-ως-SAT, οι ενδείξεις μεταγλωττίζονται σε gadgets ανισότητας όπως κάθε άλλος περιορισμός.

Το φυσικό πρωτόκολλο. Το πραγματικό πρωτόκολλο με κάρτες για Sudoku (Gradwohl, Naor, Pinkas και Rothblum, 2007) δεν χρησιμοποιεί καθόλου μετονομασία και τακτοποιεί τις ενδείξεις πριν καν αρχίσει η απόκρυψη. Για κάθε κελί, η Alice τοποθετεί τρεις ίδιες κάρτες με την τιμή του κελιού — κλειστές για τα μυστικά κελιά, αλλά ανοιχτές για τα **κελιά με ενδείξεις**, ώστε ο Bob να δει με τα ίδια του τα μάτια ότι οι ενδείξεις τηρούνται πριν γυρίσουν οι κάρτες. Μετά μία κάρτα από κάθε κελί πηγαίνει στο πακέτο της γραμμής του, μία στο πακέτο της στήλης του και μία στο πακέτο του μπλοκ του· κάθε πακέτο ανακατεύεται και αποκαλύπτεται, και ο Bob ελέγχει ότι περιέχει και τα N σύμβολα. Το ανακάτεμα καταστρέφει την πληροφορία θέσης (αυτό είναι το zero-knowledge), αλλά οι ενδείξεις είχαν ήδη σταθεροποιηθεί κατά τη μοιρασιά. Σε κάθε περίπτωση, το μάθημα είναι το ίδιο στο οποίο επιστρέφει συνεχώς αυτό το άρθρο: ένα πρωτόκολλο μηδενικής γνώσης είναι προσεκτική λογιστική του ποια γεγονότα επιβιώνουν από την απόκρυψη. Η μετονομασία διατηρεί το «όλα διαφορετικά» και σβήνει το «ισούται με 5» — άρα το «ισούται με 5» πρέπει να επανεισαχθεί με άλλο τρόπο.

Αυτό δεν είναι το πρωτόκολλο της εργασίας. Είναι το νοητικό μοντέλο για την κλασική μηδενική γνώση:

- Η Alice και ο Bob πηγαίνουν μπρος-πίσω.
- Ο Bob επιλέγει τυχαίους ελέγχους.
- Η Alice αποκαλύπτει μόνο τοπική συνέπεια, όχι ολόκληρη τη λύση.
- Η απόδειξη ιδιωτικότητας λειτουργεί δείχνοντας ότι η εικόνα που βλέπει ο Bob θα μπορούσε να είχε παραχθεί χωρίς τη μυστική λύση της Alice.

Άρα η κλασική μηδενική γνώση χτίζεται γύρω από ένα θετικό γεγονός:

> Ένας simulator υπάρχει πραγματικά.

Τώρα αφαιρέστε τα βολικά στοιχεία. Η Alice στέλνει μία συμβολοσειρά απόδειξης και φεύγει. Δεν υπάρχει trusted setup, ούτε κοινή τυχαία συμβολοσειρά προετοιμασμένη από πριν, και ο Bob δεν πρέπει ποτέ να αποδέχεται ένα ψευδές παζλ. Αυτό είναι το καθεστώς στο οποίο η κλασική μηδενική γνώση δεν μπορεί να επιβιώσει.

Χρειαζόμαστε έναν ακόμη χαρακτήρα πριν από το τέχνασμα. Καθορίστε ένα **εγχειρίδιο κανόνων**: ένα τυπικό σύστημα αποδείξεων (proof system), με την έννοια της μαθηματικής λογικής — ένα σταθερό σύνολο αξιωμάτων μαζί με μηχανικούς κανόνες για τον έλεγχο γραπτών μαθηματικών αποδείξεων. Το ZFC, τα καθιερωμένα αξιώματα των μαθηματικών, είναι το κανονικό παράδειγμα. Από εδώ και πέρα όλα διατυπώνονται σε σχέση με ένα τέτοιο σύστημα που επιλέγεται εκ των προτέρων, και η επιλογή είναι ευέλικτη: η κατασκευή λειτουργεί για οποιοδήποτε proof system καθορίσετε, συμπεριλαμβανομένου του ZFC.

(Μια σημείωση για τις λέξεις, δανεισμένη από την ίδια την εργασία: εδώ «proof system» σημαίνει πάντα αυτό το εγχειρίδιο κανόνων — το τυπικό σύστημα που ελέγχει μαθηματικές αποδείξεις — και ποτέ τα μηνύματα που στέλνει η Alice. Ο μηχανισμός της Alice και του Bob ονομάζεται «prover και verifier», δηλαδή αποδεικνύων και επαληθευτής.)

Η εκδοχή τύπου Gödel κρατά την ιστορία του mega-Sudoku αλλά αλλάζει την απόδειξη.

Επιλέξτε ένα δεύτερο σύστημα περιορισμών ίδιου εμφανιζόμενου μεγέθους και ονομάστε το **D**. Για την ιστορία, τα S και D είναι δύο παζλ MegaSudoku(n) στην ίδια μορφή. Στο παρασκήνιο, το D μπορεί να ξεκίνησε ως ένας δύσκολος λογικός τύπος διαφορετικού μεγέθους· αν χρειάζεται, μπορεί να συμπληρωθεί με ακίνδυνους εικονικούς περιορισμούς ώστε να χωρά στο ίδιο πλέγμα. Το D κατασκευάζεται από έναν λογικό τύπο που είναι στην πραγματικότητα **μη ικανοποιήσιμος (unsatisfiable)**: δεν υπάρχει καμία ανάθεση τιμών που να κάνει όλους τους περιορισμούς του αληθείς, όπως ένα χαλασμένο παζλ δεν έχει κανένα νόμιμο ολοκληρωμένο πλέγμα. Ένα απλό παράδειγμα θα ήταν ένας τύπος που απαιτεί ταυτόχρονα «το X είναι αληθές» και «το X είναι ψευδές». Άρα το D δεν έχει έγκυρη λύση.

Όμως το D δεν πρέπει να είναι ένα χαλασμένο παζλ που είναι *εύκολο να εκτεθεί*. Το απλό παράδειγμα αποτυγχάνει: οποιοδήποτε proof system αντικρούει το «X και όχι-X» σε μία γραμμή. Το D πρέπει να είναι ψευδές με τρόπο που το επιλεγμένο proof system δεν μπορεί να πιστοποιήσει με σύντομο επιχείρημα. Αν μπορούσε να αντικρούσει το D με σύντομη απόδειξη, η παρακάτω ιστορία θα κατέρρεε: η εναλλακτική διαδρομή που θα μπορούσε να παράγει αποδείξεις χωρίς το μυστικό της Alice θα αποκλειόταν τυπικά, και μαζί της η εγγύηση ιδιωτικότητας. Άρα το D επιλέγεται από μια οικογένεια την οποία το σταθερό proof system δεν μπορεί να αντικρούσει αποτελεσματικά: μέσα σε αυτό το σύστημα δεν υπάρχει σύντομη απόδειξη ότι το D δεν έχει λύση.

Η απόδειξη ενός μηνύματος της Alice αφορά τότε μια πρόταση «είτε/είτε»:

> είτε το πραγματικό mega-Sudoku S έχει λύση, είτε το δόλωμα D έχει λύση.

Αυτός είναι ο λογικός σύνδεσμος. Το D **δεν** παράγεται με κάποιο μαγικό τρόπο που κάνει το S αληθές. Η απόδειξη δεν λέει «το D δεν έχει λύση, άρα το S έχει λύση». Αποδεικνύει τη διάζευξη **S ή D**. Η τέλεια soundness λέει ότι μια ψευδής διάζευξη δεν μπορεί να έχει έγκυρη απόδειξη.

Επειδή το D είναι ψευδές στην πραγματικότητα — δεν έχει λύση — ο μόνος τρόπος να είναι αληθής η διάζευξη είναι να είναι αληθές το S. Άρα, αν η απόδειξη γίνει δεκτή, το S πρέπει να έχει λύση. Το δόλωμα δεν μπορεί να κάνει ένα ψευδές S αληθές.

Για το τμήμα που μοιάζει με zero-knowledge, όμως, ρωτήστε τι θα συνέβαινε αν το D *είχε* λύση. Αυτή η λύση-δόλωμα θα λειτουργούσε ως εναλλακτικός witness. Θα επέτρεπε σε κάποιον να παράγει αποδείξεις χωρίς να γνωρίζει την πραγματική λύση mega-Sudoku της Alice — δηλαδή θα έδινε έναν simulator. Στην πραγματικότητα το D δεν έχει λύση, άρα αυτή η διαδρομή προσομοίωσης είναι κλειστή. Το σημείο είναι ότι το proof system δεν μπορεί να αποδείξει αποτελεσματικά ότι είναι κλειστή.

Το D λοιπόν έχει δύο δουλειές. Για τη **soundness**, το D είναι ψευδές, άρα μια έγκυρη απόδειξη του «S ή D» επιβάλλει το S. Για την **effective zero-knowledge**, το D είναι δύσκολο να αντικρουστεί, οπότε το proof system δεν μπορεί γρήγορα να αποκλείσει τη διαδρομή του δολώματος που θα έκανε δυνατή την προσομοίωση.

Έτσι το τεστ ασφάλειας δεν είναι πια:

> Μπορούμε να αποδείξουμε ότι ένας simulator υπάρχει πραγματικά;

Γίνεται:

> Μπορεί το proof system σου να αποδείξει αποτελεσματικά ότι ο simulator είναι αδύνατος;

Αν η απάντηση είναι όχι, ακολουθεί κάτι εκπληκτικά ισχυρό: κάθε εγγύηση ασφάλειας που (α) μπορεί να παρατηρηθεί εκτελώντας ένα τεστ και (β) αποδεδειγμένα προκύπτει — μέσα σε αυτό το proof system — από την ύπαρξη simulator, πράγματι ισχύει. Μια επιτυχής επίθεση σε οποιαδήποτε από αυτές θα ισοδυναμούσε η ίδια με τη σύντομη αναίρεση που λείπει, και αυτή η σύντομη αναίρεση δεν υπάρχει. Αυτό είναι το «effective» στο effectively zero-knowledge.

Άρα η διδακτική αντίθεση είναι:

Κλασική zero-knowledge: οι αποδείξεις είναι ασφαλείς επειδή υπάρχει simulator.

Effective zero-knowledge τύπου Gödel: οι αποδείξεις αντιμετωπίζονται ως ασφαλείς για παρατηρήσιμα τεστ ασφάλειας επειδή το proof system δεν μπορεί να αποδείξει αποτελεσματικά ότι ο simulator είναι αδύνατος.

Ο δεύτερος ισχυρισμός είναι ασθενέστερος. Είναι επίσης ο λόγος που η εργασία μπορεί να κρατήσει τα τρία χαρακτηριστικά που κατέρρεαν στην κλασική εκδοχή: ένα μήνυμα, καθόλου setup και τέλεια soundness.

Το νέο κριτήριο: δεν μπορείς να αποδείξεις ότι ο simulator απουσιάζει

Η χαλάρωση του Ilango αλλάζει την ερώτηση.

Η κλασική zero-knowledge ρωτά:

> Υπάρχει simulator;

Η effectively zero-knowledge ρωτά κάτι ασθενέστερο:

> Μπορεί το επιλεγμένο proof system σου να αποδείξει αποτελεσματικά ότι δεν υπάρχει simulator;

Αυτό ακούγεται σαν τεχνικό τέχνασμα, αλλά είναι η κεντρική ιδέα. Η κατασκευή βρίσκεται σε μια παράξενη κατάσταση: **simulator στην πραγματικότητα δεν υπάρχει** — η εργασία το λέει ρητά — αλλά το proof system που καθόρισες δεν μπορεί να αποδείξει αποτελεσματικά ότι δεν υπάρχει. Αν κάθε κακή συνέπεια που σε ενδιαφέρει απαιτούσε μια τέτοια αναίρεση, το σύστημα εξακολουθεί να συμπεριφέρεται σαν zero-knowledge ως προς αυτές τις συνέπειες.

Εδώ μπαίνει ο Gödel. Όχι ως διακόσμηση και όχι ως «ο Gödel κάνει την κρυπτογραφία ασφαλή». Η σύνδεση είναι θεωρία αποδείξεων. Ένα proof system ονομάζεται **βέλτιστο (optimal)** αν είναι, με ακριβή έννοια, το καλύτερο δυνατό: όποτε οποιοδήποτε proof system μπορεί να αντικρούσει έναν τύπο του σχετικού είδους με σύντομη απόδειξη, το βέλτιστο σύστημα μπορεί επίσης, με απόδειξη το πολύ πολυωνυμικά μεγαλύτερη. Οι Krajíček και Pudlák διατύπωσαν το 1989 την εικασία ότι **δεν υπάρχει βέλτιστο proof system**: όποιο σύστημα κι αν καθορίσεις, κάποιο άλλο σύστημα αποδεικνύει κάποια οικογένεια αληθών προτάσεων πολύ πιο συνοπτικά. Πρόκειται για μία από τις κεντρικές ανοικτές εικασίες της πολυπλοκότητας αποδείξεων και είναι ο περασμένος, θεωρητικο-πολυπλοκοτικός συγγενής του θεωρήματος μη πληρότητας του Gödel: ορισμένες αληθείς προτάσεις δεν έχουν σύντομη απόδειξη στο proof system που επέλεξες — όχι επειδή είναι κατ' αρχήν αναπόδεικτες, αλλά επειδή κάθε σταθερό proof system αφήνει κάποιες σύντομες αλήθειες χωρίς σύντομες αποδείξεις.

Η εργασία υποθέτει αυτή την εικασία (σε μια ελαφρώς ισχυρότερη μορφή «infinitely often», όπως συνηθίζεται όταν εικασίες χρησιμοποιούνται κρυπτογραφικά). Το κέρδος, μέσω θεωρήματος των Krajíček και Pudlák, είναι συγκεκριμένο: για κάθε proof system υπάρχει μια ακολουθία τύπων που είναι πραγματικά μη ικανοποιήσιμοι, αλλά το σύστημα δεν μπορεί να τους αντικρούσει με σύντομες αποδείξεις — και, κρίσιμα, ένας αποδοτικός αλγόριθμος μπορεί να τους *παράγει*. Αυτή η τελευταία ιδιότητα, η ομοιομορφία (uniformity), μετατρέπει όλη την ιδέα από ισχυρισμό ύπαρξης σε πραγματικό αλγόριθμο που μπορεί να εκτελέσει η Alice: τα δολώματα D βγαίνουν από γραμμή παραγωγής, δεν εμφανίζονται από το πουθενά.

Η κρυπτογραφική κίνηση είναι να αξιοποιηθεί αυτή η έλλειψη αποδεικτικής ισχύος.

Τι κάνει η κατασκευή

Ακολουθεί η κατασκευή της εργασίας, απογυμνωμένη στη βασική της μορφή.

Καθορίστε ένα proof system — ας πούμε ZFC. Υπό την υπόθεση της πολυπλοκότητας αποδείξεων, υπάρχει μια ακολουθία τύπων που μπορεί να παραχθεί αποδοτικά και οι οποίοι στην πραγματικότητα είναι μη ικανοποιήσιμοι, αλλά το proof system δεν έχει σύντομη απόδειξη της μη ικανοποιησιμότητάς τους.

Τώρα κατασκευάστε μια απόδειξη ενός μηνύματος της μορφής:

> είτε η πραγματική πρόταση είναι ικανοποιήσιμη, είτε αυτός ο ειδικός δύσκολος τύπος είναι ικανοποιήσιμος.

Ο ειδικός δύσκολος τύπος δεν είναι ικανοποιήσιμος. Άρα, αν ο υποκείμενος μηχανισμός απόδειξης έχει τέλεια soundness, η αποδοχή του μηνύματος εξακολουθεί να σημαίνει ότι η πραγματική πρόταση είναι αληθής. Αυτό δίνει τέλεια soundness.

Για την ασφάλεια που μοιάζει με zero-knowledge, όμως, φανταστείτε ότι ο ειδικός δύσκολος τύπος *ήταν* ικανοποιήσιμος. Τότε ο witness του θα μπορούσε να χρησιμοποιηθεί για την προσομοίωση αποδείξεων χωρίς γνώση του πραγματικού witness. Ο τύπος δεν είναι ικανοποιήσιμος στην πραγματικότητα — αλλά το proof system δεν μπορεί να το αποδείξει αποτελεσματικά. Άρα δεν μπορεί να αποδείξει αποτελεσματικά ότι ο simulator είναι αδύνατος.

Αυτός είναι ο μεντεσές της ιδέας. Το σύστημα δεν κρύβει το μυστικό κατασκευάζοντας έναν κλασικό simulator. Κρύβει το μυστικό, για μια μεγάλη κλάση παρατηρήσιμων τεστ ασφάλειας, πίσω από την αδυναμία του proof system να πιστοποιήσει ότι ο simulator απουσιάζει.

Τι ισχυρίζεται η εργασία

Το κύριο θεώρημα έρχεται σε επίπεδα. Το βασικό αποτέλεσμα είναι το εξής:

Υπό μια καθιερωμένη κρυπτογραφική υπόθεση — την ύπαρξη **μη διαδραστικών αποδείξεων με μη διακριτούς witnesses (non-interactive witness indistinguishable proofs)**, καλά μελετημένων αντικειμένων που προκύπτουν από αρκετά καθιερωμένα σύνολα υποθέσεων — και υπό την εικασία της πολυπλοκότητας αποδείξεων ότι **δεν υπάρχει (infinitely often) optimal proof system**, η εργασία κατασκευάζει, για κάθε επιλογή proof system, έναν prover και verifier ενός μηνύματος για NP/SAT, με **τέλεια soundness** και χωρίς setup, που είναι effectively zero-knowledge σε σχέση με αυτό το proof system. (Το NP/SAT είναι ο τυπικός «σκληρότερος κοινός παρονομαστής» προβλημάτων που μοιάζουν με παζλ· το mega-Sudoku είναι μία από τις μεταμφιέσεις του.)

Για τον ευρύτερο ισχυρισμό σχετικά με τη διατήρηση διαψεύσιμων ιδιοτήτων ασφάλειας,

η εργασία προσθέτει άλλη μία τυπική υπόθεση, την πεποίθηση αποτυχαιοποίησης **P = BPP** (χονδρικά: η τυχαιότητα δεν δίνει στους αλγορίθμους καμία ουσιώδη επιπλέον ισχύ).

Μεταφρασμένο από τη γλώσσα των θεωρημάτων:

- Η απόδειξη είναι ένα μήνυμα.
- Δεν υπάρχει trusted setup.
- Ψευδείς προτάσεις δεν μπορούν να αποδειχθούν.
- Ο prover δεν είναι κλασικά zero-knowledge — δεν έχει simulator.
- Όμως κάθε διαψεύσιμη, βασισμένη σε παιχνίδι συνέπεια ασφάλειας της κλασικής zero-knowledge μπορεί να επιτευχθεί σε αυτό το καθεστώς.

Η λέξη «διαψεύσιμη» έχει σημασία. Σημαίνει ότι μια αποτυχία ασφάλειας μπορεί να ελεγχθεί βάζοντας έναν αντίπαλο να παίξει ένα παιχνίδι. Πολλοί κρυπτογραφικοί ορισμοί ασφάλειας έχουν αυτή τη μορφή: μπορεί ο αντίπαλος να διακρίνει δύο κρυπτογραφήσεις, να αντιστρέψει μια συνάρτηση, να ανακτήσει έναν witness ή να κερδίσει κάποιο συγκεκριμένο πείραμα; Το θεώρημα δίνει έναν prover για κάθε διαψεύσιμη ιδιότητα, μία κάθε φορά. Ένας μοναδικός prover που διαθέτει *κάθε* διαψεύσιμη ιδιότητα ταυτόχρονα είναι πιθανότατα αδύνατος — η παλιά επίθεση επαναχρησιμοποίησης («ο Bob μπορεί να δείξει την απόδειξη σε άλλους») είναι η ίδια διαψεύσιμη ιδιότητα, και εδώ πράγματι αποτυγχάνει. Η πρόταση της εργασίας είναι ότι ένας μοναδικός prover μπορεί εύλογα να καλύψει όλες τις *φυσικές* διαψεύσιμες ιδιότητες — εκείνες που εμφανίζονται πράγματι στην κρυπτογραφική πρακτική — αλλά αυτό το μέρος είναι υπό όρους θεώρημα που στηρίζεται σε μια άτυπη έννοια του «φυσικού», μαζί με μια ρητή εικασία. Η εγγύηση στοχεύει σε παρατηρήσιμες αποτυχίες, όχι σε κάθε φιλοσοφική ή βασισμένη σε προσομοίωση έννοια της μυστικότητας.

Ένα συγκεκριμένο πόρισμα αξίζει να κατονομαστεί: η κατασκευή δίνει τις πρώτες μη διαδραστικές αποδείξεις από***κρυψης witness (witness hiding)*** με ομοιόμορφο prover — «μια απόδειξη ότι ένα παζλ λύνεται δεν σε βοηθά να βρεις τη λύση του», χωρίς αλληλεπίδραση και χωρίς setup — ένα αντικείμενο που ακούγεται ταπεινό αλλά αντιστεκόταν στην κατασκευή επί δεκαετίες.

Τι δεν λέει αυτό

Αυτή είναι η ενότητα που κρατά το άρθρο έντιμο.

Δεν λέει ότι τα παλιά θεωρήματα αδυνατότητας ήταν λάθος. Η κατασκευή τα αποφεύγει αλλάζοντας τον ορισμό.

Δεν δίνει συνηθισμένη, κλασική zero-knowledge χωρίς αλληλεπίδραση, χωρίς setup και με τέλεια soundness. Η εργασία λέει ρητά ότι ο prover που κατασκευάζεται δεν έχει simulator.

Δεν σημαίνει ότι η απόδειξη δεν μπορεί να επαναχρησιμοποιηθεί. Μια απόδειξη ενός μηνύματος μπορεί ακόμη να παρουσιαστεί σε κάποιον άλλο· η εργασία δεν διατηρεί ιδιότητες τύπου deniability. (Η μη διαδραστική zero-knowledge με trusted setup έχει τον

ίδιο περιορισμό.)

Δεν σημαίνει ότι πρόκειται για πρακτικό πρωτόκολλο έτοιμο για ανάπτυξη. Εδώ μιλάμε για θεωρία πολυπλοκότητας και θεμέλια της κρυπτογραφίας. Το αποτέλεσμα εξαρτάται από σημαντικές υποθέσεις της πολυπλοκότητας αποδείξεων και της κρυπτογραφίας, και η κατασκευή αφορά το τι είναι δυνατό κατ' αρχήν.

Δεν κάνει τον «Gödel» μαγικό primitive ασφάλειας. Η σύνδεση με τον Gödel περνά από proof systems, optimal proof systems και πεπερασμένα ανάλογα της μη πληρότητας. Η χρήσιμη διαίσθηση δεν είναι «η μη πληρότητα προστατεύει τον κωδικό σου». Είναι: αν ένα proof system δεν μπορεί να αποδείξει αποτελεσματικά ότι ένας simulator είναι αδύνατος, τότε επιθέσεις που θα απαιτούσαν αυτή την απόδειξη μπορούν να αποκλειστούν στο επίπεδο των ορισμών ασφάλειας.

Γιατί είναι ενδιαφέρον παρ' όλα αυτά

Η κρυπτογραφία συχνά μετατρέπει τη δυσκολία σε ασφάλεια. Η παραγοντοποίηση είναι δύσκολη, οπότε οι υποθέσεις τύπου RSA γίνονται χρήσιμες. Τα προβλήματα πλεγμάτων είναι δύσκολα, οπότε η κρυπτογραφία πλεγμάτων γίνεται χρήσιμη. Εδώ η δυσκολία είναι πιο παράξενη: όχι «είναι δύσκολο να υπολογίσεις ένα μυστικό», αλλά «είναι δύσκολο να αποδείξεις ότι ένα συγκεκριμένο αντικείμενο απόδειξης δεν μπορεί να υπάρχει».

Γι' αυτό η εργασία μοιάζει ασυνήθιστη. Αντιμετωπίζει αξιώματα και proof systems σχεδόν σαν κρυπτογραφικούς πόρους. Η συνηθισμένη αδυναμότητα λέει ότι υπάρχει ένταση ανάμεσα στη soundness και την προσομοίωση. Η κίνηση του Ilango τοποθετεί αυτή την ένταση πίσω από μια κουρτίνα θεωρίας αποδείξεων: ο simulator απουσιάζει, αλλά το τυπικό σύστημα δεν μπορεί να εκθέσει αποτελεσματικά αυτή την απουσία.

Για έναν αναγνώστη, το εκπληκτικό δεν είναι ότι αυτό θα αντικαταστήσει τα σημερινά συστήματα zero-knowledge. Πιθανότατα δεν θα το κάνει, τουλάχιστον όχι άμεσα. Το εκπληκτικό είναι ότι ένας περιορισμός της μαθηματικής λογικής μπορεί να χρησιμοποιηθεί κατασκευαστικά: όχι μόνο ως τοίχος, αλλά και ως ένα είδος κάλυψης.

Πόσο ισχυρά είναι τα στοιχεία;

Πρόκειται για εργασία θεωρήματος, άρα «στοιχεία» σημαίνει κάτι διαφορετικό απ' ό,τι σε μια εργασία βιολογίας ή αστρονομίας. Το ερώτημα δεν είναι αν ένα πείραμα αναπαράχθηκε. Είναι αν οι ορισμοί, οι υποθέσεις και η αλυσίδα αποδείξεων στηρίζουν τον ισχυρισμό.

Η απόδειξη είναι τυπική και η εργασία δηλώνει ρητά τις υποθέσεις της. Οι υποθέσεις δεν είναι πρόχειρες. Οι non-interactive witness indistinguishable proofs είναι καθιερωμένα αντικείμενα στην κρυπτογραφία και προκύπτουν από αρκετά αναγνωρισμένα σύνολα υποθέσεων. Η εικασία ότι δεν υπάρχει optimal proof system είναι κεντρική εικασία στην

πολυπλοκότητα αποδείξεων. Η P = BPP είναι μια τυπική πεποίθηση αποτυχαιοποίησης που χρησιμοποιείται μόνο για το ευρύτερο θεώρημα περί διαψεύσιμων ιδιοτήτων.

Η εργασία υποστηρίζει επίσης ότι αυτές οι υποθέσεις είναι το σωστό τίμημα και όχι ένα αυθαίρετο ικρίωμα: αποδεικνύει ένα αντίστροφο αποτέλεσμα που δείχνει ότι είναι ουσιαστικά αναγκαίες — αν υπάρχουν καθόλου τέτοιες κατασκευές, τότε πρέπει να υπάρχουν non-interactive witness indistinguishable proofs και, αν δεχθούμε τις τυπικές μονόδρομες συναρτήσεις, δεν μπορεί να υπάρχει optimal proof system. Και οι υποθέσεις είναι «win-win»: η διάψευση οποιασδήποτε από αυτές θα ήταν από μόνη της ανακάλυψη-ορόσημο στην πολυπλοκότητα αποδείξεων, την κρυπτογραφία ή τη θεωρία πολυπλοκότητας.

Αλλά επειδή το αποτέλεσμα είναι υπό όρους, υπό όρους είναι και η εμπιστοσύνη σε αυτό. Αν οι υποθέσεις αποτύχουν, αλλάζει η ερμηνεία του θεωρήματος. Και ακόμη κι αν ισχύουν, η εγγύηση δεν είναι πλήρης κλασική zero-knowledge· είναι η χαλαρωμένη, proof-theoretic εκδοχή της εργασίας.

Άρα η σωστή εμπιστοσύνη είναι υψηλή ότι η εργασία θεμελιώνει ένα συνεκτικό, υπό όρους αποτέλεσμα δυνατότητας· μέτρια ότι οι υποθέσεις της περιγράφουν τον κρυπτογραφικό κόσμο στον οποίο πράγματι ζούμε· και χαμηλή για οποιαδήποτε άμεση πρακτική συνέπεια.

Γιατί έχει σημασία

Η εργασία ανοίγει μια διαδρομή που υποτίθεται ότι ήταν κλειστή.

Η κλασική θεωρία λέει: η πλήρης zero-knowledge δεν μπορεί να γίνει με ένα μήνυμα χωρίς setup και δεν μπορεί να έχει τέλεια soundness. Η εργασία του Ilango λέει: αν ζητήσουμε τις συνέπειες της zero-knowledge που μπορούν να ελεγχθούν σε παιχνίδια ασφάλειας, και αν επιτρέψουμε στον ορισμό της ασφάλειας να εξαρτάται από το τι ένα proof system μπορεί ή δεν μπορεί να αντικρούσει αποτελεσματικά, τότε μεγάλο μέρος της χρήσιμης συμπεριφοράς μπορεί να ανακτηθεί — με ένα μήνυμα, χωρίς setup και με τέλεια soundness.

Αυτό δεν είναι μικρή αλλαγή ορισμού. Είναι διαφορετικός τρόπος να σκεφτόμαστε τις κρυπτογραφικές εγγυήσεις. Αντί να ρωτάμε μόνο τι υπάρχει, ρωτάμε τι μπορεί να αποκλείσει το proof system μας. Αντί να αντιμετωπίζουμε το αναπόδεικτο ως φιλοσοφική ενόχληση, το χρησιμοποιούμε ως δομή.

Ο πρακτικός κόσμος μπορεί να μη αλλάξει αύριο. Ο εννοιολογικός χάρτης όμως αλλάζει. Υπάρχει πλέον μια τυπική έννοια κατά την οποία το «κανείς δεν μπορεί να αποδείξει αποτελεσματικά ότι το μυστικό διέρρευσε» μπορεί να είναι αρκετά ισχυρό ώστε να ανακτήσει πολλές από τις προστασίες που βασίζονται σε παιχνίδια και τις οποίες θέλαμε από το «το μυστικό δεν διέρρευσε».

Γι’ αυτό ο Gödel ανήκει στον τίτλο.

Καθαρή σύνοψη

Οι αποδείξεις μηδενικής γνώσης επιτρέπουν σε έναν prover να πείσει έναν verifier ότι μια πρόταση είναι αληθής χωρίς να αποκαλύψει τον witness. Κλασικά αποτελέσματα αδυνατότητας λένε ότι η zero-knowledge δεν μπορεί να συμπιεστεί σε ένα μήνυμα χωρίς setup και δεν μπορεί να έχει τέλεια soundness. Η εργασία του Rahul Ilango δεν αναιρεί αυτές τις αδυνατότητες. Ορίζει μια ασθενέστερη έννοια, την effectively zero-knowledge: αντί να απαιτεί ότι ένας simulator υπάρχει πραγματικά, απαιτεί ένα επιλεγμένο proof system — ένα τυπικό εγχειρίδιο κανόνων όπως το ZFC — να μην μπορεί να αποδείξει αποτελεσματικά ότι δεν υπάρχει simulator. Υπό σημαντικές υποθέσεις από την κρυπτογραφία (non-interactive witness indistinguishable proofs) και την πολυπλοκότητα αποδείξεων (δεν υπάρχει optimal proof system), η εργασία κατασκευάζει provers ενός μηνύματος για NP/SAT, χωρίς setup και με τέλεια soundness, οι οποίοι επιτυγχάνουν, μία προς μία, τις διαψεύσιμες συνέπειες της zero-knowledge που βασίζονται σε παιχνίδια. Ένας μοναδικός prover που θα καλύπτει όλες τις «φυσικές» τέτοιες ιδιότητες είναι μια περαιτέρω, εν μέρει εικαστική επέκταση — και η κάλυψη κυριολεκτικά κάθε διαψεύσιμης ιδιότητας είναι πιθανότατα αδύνατη, επειδή οι αποδείξεις παραμένουν επαναχρησιμοποιήσιμες. Το αποτέλεσμα είναι θεωρητικό και υπό όρους, όχι primitive που έχει αναπτυχθεί στην πράξη, αλλά δείχνει έναν νέο τρόπο να χρησιμοποιηθεί η αναποδειξιμότητα από τη θεωρία αποδείξεων ως κρυπτογραφικός πόρος.

Έλεγχος χωρίς υπερβολές

Τι δείχνει η εργασία: Υπό τις δηλωμένες υποθέσεις, μπορούν να κατασκευαστούν provers ενός μηνύματος, χωρίς setup και με τέλεια soundness για NP/SAT, που είναι effectively zero-knowledge σε σχέση με οποιοδήποτε επιλεγμένο proof system και επιτυγχάνουν κάθε διαψεύσιμη, βασισμένη σε παιχνίδι συνέπεια της κλασικής zero-knowledge.

Τι είναι εύλογο αλλά δεν έχει αποδειχθεί άνευ όρων: Ότι ισχύουν οι αναγκαίες υποθέσεις της πολυπλοκότητας αποδείξεων και της κρυπτογραφίας. Είναι σοβαρές, καλά μελετημένες υποθέσεις — και η εργασία δείχνει ότι είναι ουσιαστικά αναγκαίες όσο και επαρκείς — αλλά παραμένουν υποθέσεις.

Τι δεν δείχνει: Κλασική zero-knowledge χωρίς αλληλεπίδραση, χωρίς setup και με τέλεια soundness· πρακτικό σύστημα έτοιμο για ανάπτυξη· deniability ή μη επαναχρησιμοποίηση αποδείξεων· ούτε ότι το θεώρημα μη πληρότητας του Gödel από μόνο του ασφαλίζει την κρυπτογραφία.

Κύριοι περιορισμοί: Η εγγύηση είναι χαλάρωση της zero-knowledge· η ευρύτερη εκδοχή εξαρτάται από πολλαπλές υποθέσεις· οι ισχυρισμοί για έναν μοναδικό καθολικό prover παραμένουν εν μέρει εικαστικοί· και το αποτέλεσμα είναι πρωτίστως θεμελιώδες.

Πόση εμπιστοσύνη πρέπει να έχει ένας γενικός αναγνώστης; Υψηλή ότι πρόκειται για σημαντικό υπό όρους θεωρητικό αποτέλεσμα, εφόσον γίνουν δεκτοί οι ορισμοί. Μέτρια ότι οι υποθέσεις αποτυπώνουν την πραγματικότητα. Χαμηλή για άμεση πρακτική ανάπτυξη.

Το ασφαλές συμπέρασμα είναι: η εργασία δεν καταρρίπτει τις αδυνατότητες της zero-knowledge· βρίσκει έναν νέο, proof-theoretic τρόπο να παρακάμψει τα μέρη τους που έχουν σημασία για πολλά παιχνίδια ασφάλειας.

Πηγές

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