Zero Knowledge Proofs

Bitó Tamás, Regenye Dávid Kristóf

2015.11.05.

Bevezető

- Ki?
- Mikor?
- Miért?
- Mire jó?
- Hogyan?

Nulla-ismeretű bizonyítások motivációja

Tegyük fel, hogy két szereplő közül egyikük szeretné bizonyítani a másiknak, hogy rendelkezik egy bizonyos információval, viszont nem szeretné átadni az információ egy apró részét sem.

Képzeljük el, hogy szeretnénk megvásárolni egy nehéz feladat megoldását, de nem szeretnénk, hogy becsapjanak. Aki rendelkezik a feladat megoldásával, hogyan bizonyíthatja, hogy rendelkezik az információval, anélkül hogy megadná magát a megoldást?

Add előbb a pénzt! Nem! Te add előbb az árút …

Az ilyen típusú rendszerek két szereplőből állnak. A bizonyító és az ellenőrző.

Az ellenőrző kérdéseket tesz fel a bizonyítónak, melyekre a bizonyító csak akkor tudhatja a választ, ha valóban rendelkezik azzal a tudással amit bizonyítani akar.

A bizonyító válszol ezekre a kérdésekre.

Az ellenőrző addíg tesz fel kérdéseket, mígnem elég biztos abban, hogy a bizonyító rendelkezik az információval.

- Teljesség (Completeness):
  - ❖ Amennyiben a bizonyító és az ellenőrző is igazat mond, kielégítő biztonsággal lehet igazolni a bizonyító állítását.
- Megalapozottság (Soundness):
  - ❖ Aki nem ismeri a bizonyító titkát, nem tudja meggyőzni az ellenőrzőt, arról, hogy ismeri a titkot. (A bizonyító nem tud hamis állítást igazolni.)
- Nulla-ismeret (Zero-Knowledge):
  - ❖ A bizonyítási folyamat során a titok nem derülhet ki.

Shafrira Goldwasser

1958-ban New York-ban született, Izraeli származású informatikus. Informatikai és villamosmérnöki professzor az MIT-n, valamint matematika professzor a Weizmann tudomány intézetnél.

Főként számítási komplexitással, kriptográfiával és számítógépes számelmélettel foglalkozik. Nulla-ismeretű bizonyítások egyik megalkotója, melyért Gödel díjat kapott 1993-ban. 2001-ben ismét Gödel díjjal jutalmazták. Sikerült bebizonyítania, hogy bizonyos NP teljes problémák akkor is NP teljesek maradnak, ha csupán közelítő eredményt szeretnénk elérni.

1958

New York

Silvio Micali

1954-ben az Olaszországi Palmeroban született. MIT Villamosmérnöki és Informatikai kar professzora, az MIT Informatikai és Mesterséges intelligenciával foglalkozó laboratórium kutatója.

Nyílt kulcsú titkosítási rendszerek, álvéletlen számgenerátorok, digitális aláírások, feledékeny átvitelek és biztonságos többszereplős algoritmusok kutatása sorolhatók munkásságához. Ezen felül a nulla-ismeretű bizonyítások egyik megalkotója, melyért 1993-ban Gödel díjat kapott.

1954

Palmermo

Charles Rackoff

1948-ban New York-ban született, amerikai kriptográfus. MIT-n szerzett diplomát, majd egy évet a Franciaországi INRIA-nál töltött.

Torontói egyetemen algoritmusok komplexitását kutatja. Leginkább kriptográfiával és biztonságos protokollok fejlesztésén dolgozik. 1988-ban Michael Lubyval megalkotta a Feistel kódolót. 1993-ban Gödel díjat kapott a Nulla-ismeretű bizonyítások kutatásáért.

1948

New York

Shlomo Moran

1947-ben született izraeli informatikus. A haifai Technion egyetem oktatója.

Disszertávióját az "NP Optimization Problems and their Approximation" címmel íródott. Arthur-Merlin protokollok egyik megalkotója, melyért 1993-ban megosztott Gödel-díjat kapott.

1947

Izrael

Babai László

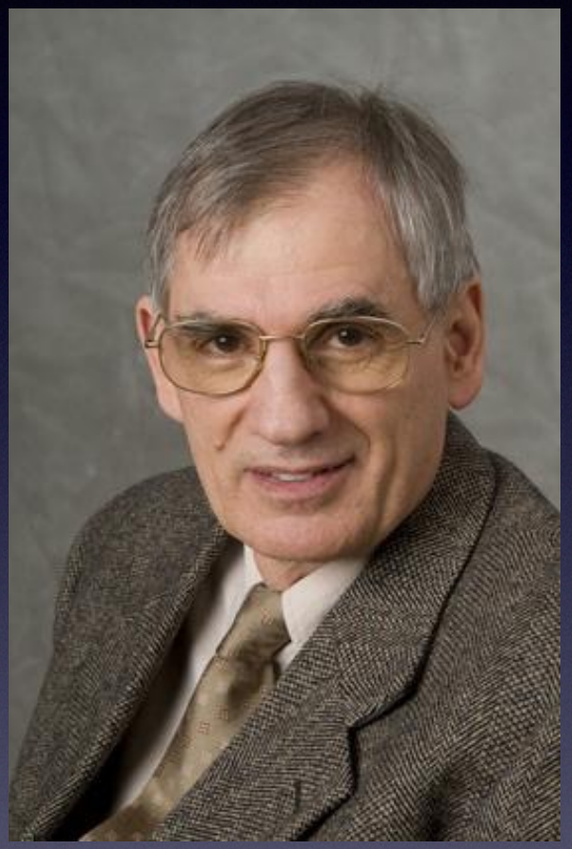
Kutatási területe a kombinatorika, a csoportelmélet és a komplexitáselmélet. Több mint száznyolcvan kombinatorikával, algebrával és számítástudománnyal foglalkozó tudományos publikációja jelent meg, amelyeket jelentős részben angol nyelven adott ki. Erdős-száma 1.

1950-ben Budapesten született. 1968-ban érettségizett, majd felvették az Eötvös Loránd Tudományegyetem matematika szakára, ahol diplomáját 1973-ban szerezte meg. Diplomájának megszerzése után az egyetem algebra és számelmélet tanszékén kezdett el dolgozni.

1985-ben Lovász Lászlóval létrehozta a Budapest Semesters in Mathematics-t, ahol az igazgatótanács elnöke lett. 1987-ben kapott egyetemi tanári kinevezést. Szintén ebben az évben a Chicagói Egyetem Számítástudományi Intézetében kapott professzori állást, előbb félállásban, majd 1994-ben főállásban oktat.

1987 és 1989 között a Budapesti Műszaki Egyetem Villamosmérnöki Karán volt vendégtanár. 1975-ben védte meg a matematikai tudományok kandidátusi, 1984-ben akadémiai doktori értekezését. A Magyar Tudományos Akadémia Matematikai Bizottságának tagja lett.

1990-ben megválasztották az MTA levelező, 1995-ben rendes tagjává.

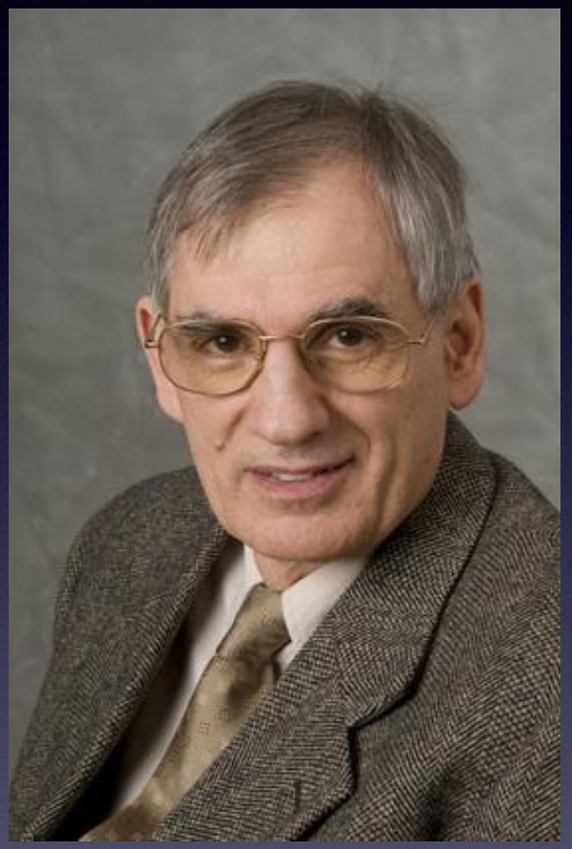


1950

Budapest

Díjak

- Grünwald Géza-díj (1972)
- MTA Matematikai Díj (1983)
- Állami Díj (1988)
- Gödel-díj (1993)
- Szele Tibor-emlékérem (1993)
- Budapesti Műszaki és Gazdaságtudományi Egyetem díszdoktora (1999)
- Llewellyn John and Harriet Manchester Quantrell Award (2005)
- Knuth-díj (2015)



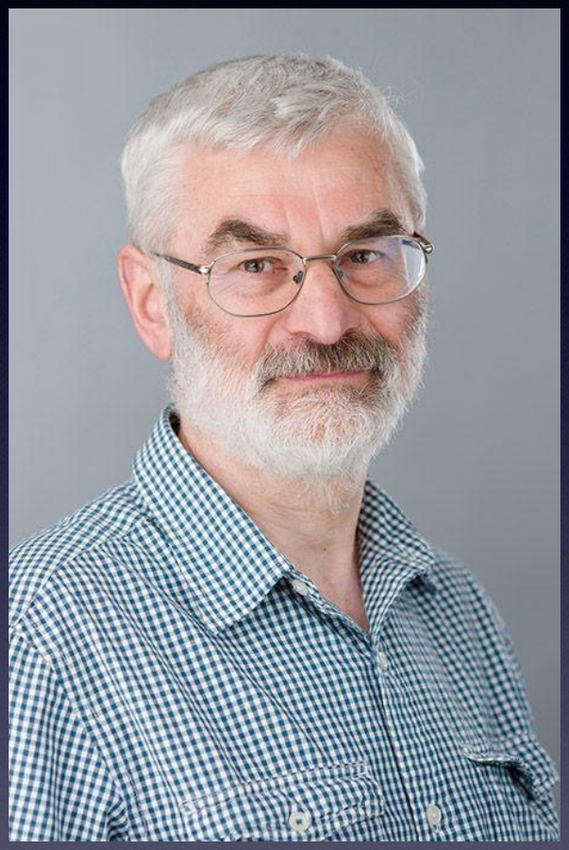
1950

Budapest

Csirmaz László

1951-ben született, magyar matematikus, egyetemi docens, oktató.

1981-ben szerezte meg a PhD fokozatát. Szakterülete a halmazelmélet, a kombinatorika és a matematikai logika, valamint foglalkozik kritpográfiával és számítástudománnyal is. Jelenleg három magyar egyetemen dolgozik és tanít. A Debreceni Egyetemen 1997 óta, a Közép-európai Egyetemen 1996 óta és az Eötvös Loránd Tudományegyetemen 1985 óta.



1951

Története

Elösszőr 1985-ben jelent meg cikk a nulla-ismeretű protokollokról Shafi Goldwasser, Silvio Micali és Charles Rackoff munkálya révén. A publikáció tartalmazta az interaktív bizonyítási rendszerek IP hierarchiáját, valamint a tudás mennyiségének mérését, amikor a bizonyítás eljut a kérdezőtől a válaszadóig.

Tőlük függetlenül fejlesztette ki Babai László és Shlomo Moran az ezzel lényegében ekvivalens Artúr–Merlin játékok tervét. Munkájukért mind az öten Gödel-díjat kaptak.

Goldwasser és Sipser megmutatták, hogy valójában lényegtelen az, hogy a véletlen bit titkos, vagy nyilvános. Tehát az Artúr–Merlin-játékok és az interaktív bizonyítási rendszerek egymással ekvivalensek.

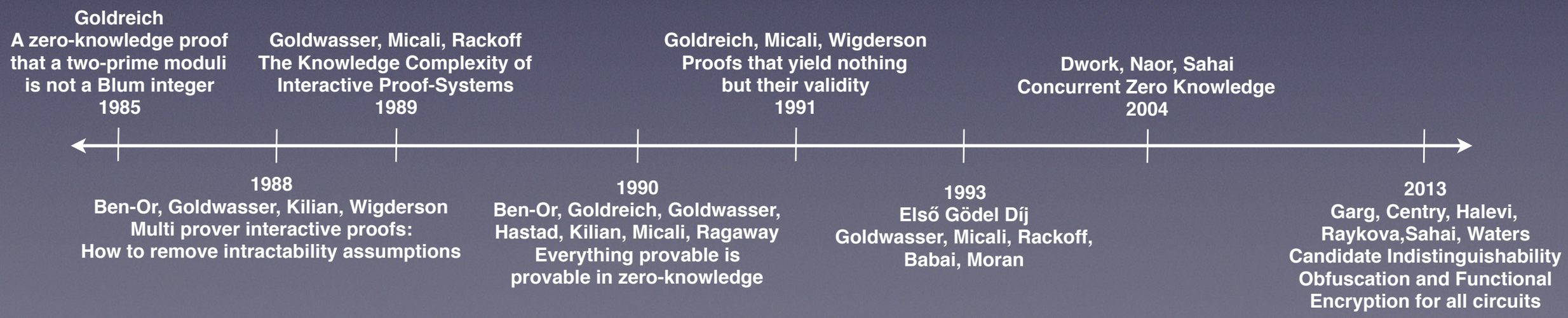
Oded Goldreich, Silvio Micali és Avi Wigderson megmutatta, hogy ha létezik törhetetlen titkosítás, létrehozható nulla ismeretű bizonyítási rendszer az NP-teljes gráf színezési problémára három színnel. Mivel minden probléma NP-ben visszavezethető erre a problémára, ezért minden NP-ben levő problémához létezik nulla-ismeretű bizonyítás. A törhetetlen titkosítás létezésének elégséges feltétele az egyirányú függvények létezése.

Többen próbálták kikerülni az egy-irányú függvények szükségességét. Ennek egyik módja a több bizonyítót tartalmazó interaktív típusú bizonyítási rendszer, mely lehetővé teszi a kérdezőnek a keresztben történő vizsgálatot a bizonyítókkal. A félrevezetés elkerülése érdekében a vizsgálat elszigetelve történik. Belátható tehát, hogy minden NP-beli nyelvnek van nulla-ismeretű bizonyítása az ilyen rendszerekben.

Nyilvánvalóvá vált, hogy egy internethez hasonló környezetben, ahol több protokoll is párhuzamosan felhasználásra kerül, a nulla-ismeretű bizonyítások megalkotása sokkal nehezebb.

Dwork, Naor és Sahai kifejlesztett egy protokollt (witness-indistinguishable proof protocols), melyeknél kiküszöbölték a párhuzamos felhasználás miatt keletkező problémákat. A bemutatott folyamatot megkülönböztethetetlen összezavarásnak (indistinguishability obfuscation) nevezték el. Két nappal később kiegészítették tanulmányukat, így már elméletben megvalósították a kriptográfusok álmát, a feltörhetetlen összezavarást.

Tanulmányuk megjelenése után hat hónappal több témával kapcsolatos cikk jelent meg, mint az elmúlt 17 évben összesen. Ennek ellenére az új technológia még messze van a kereskedelmi használattól: a kicsi, egyszerű programokból az álcázáshoz egyelőre hatalmas monstrumokat készít. Feltörni azonban az első próbálkozók nem tudták. Ez pedig az utóbbi idők legnagyobb előrelépése.



Példa: A Hamilton kör

- Tamás ismer egy Hamilton kört egy nagy G gráfban.
- Dávid ismeri a G gráfot, de a Hamilton kört nem.
- Hamilton kör keresése egy nagy gráfban NP teljes probléma, de Dávidnak sajnos nincs annyi “ideje”, viszont nagyon érdekli a Hamilton kör.
- Ahhoz hogy Tamás bizonyítani tudja hogy ismeri a Hamilton kört a következő párbeszéd hangzik el ...

- Minden kör elején Tamás készít egy új H gráfot ami a G-vel izomorf. Ha Tamás ismer egy Hamilton kört G-ben akkor H-ban is ismernie kell legalább egyet.

- Tamás H minden csúcsát megszámozza, és minden élhez készít egy papírt ami tartalmazza, hogy mely két csúcsot köti össze. Ezeket az asztalra teszi lefordítva. Erre azért van szükség, hogy Tamás ne tudja H-t megváltoztatni, míg Dávidnak nincs információja H-ról.

- Dávid ezután két kérdés közül véletlenszerűen választ. Megkérheti Tamást, hogy bizonyítsa, hogy H és G izomorfak, vagy hogy Tamás mutassa meg H-ban a Hamilton kört.

- Ha Tamásnak H és G izomorfizmusát kell bizonyítani, akkor minden lapot megfordít melyek H éleit írják le, majd megmutatja a két gráf közötti leképezést, Dávid pedig meggyőződhet róla, hogy a két gráf izomorf.

- Ha Tamásnak a H-ban található Hamilton kört kell megmutatnia, akkor elvégzi a G-ben található Hamilton kör leképezését H-ra és ezután megfordítja azokat a lapokat az asztalon melyek részei a Hamilton körnek. Ezáltal Dávid meggyőződhet, hogy H-ban van Hamilton kör.

- Ezt ismétlik, míg Dávid elég biztossá nem válik Tamás tudásában.

- Teljesség (Completeness):

  Ha Tamás tényleg ismer egy Hamilton kört akkor könnyedén tud válaszolni Dávid kérdéseire.

- Nulla-ismeret (Zero-Knowledge):

  Tamás válaszai nem fedik fel a Hamilton kört G-ben. Dávid minden körben csak annyit tud meg, hogy az aktuális gráf izomorf G-vel vagy egy Hamilton kört az akutális gráfban. Mindkét válaszra szüksége lenne ugyanazon H gráfhoz, hogy megtudhassa a G-ben található Hamilton kört. Mindaddíg míg Tamás tud az előző köröktől eltérő H-t létrehozni, a titka biztonságban van. Ha Tamás mégsem ismer Hamilton kört G-ben, de valahogyan minden kör előtt tudná Dávid mit fog kérdezni, akkor lényegében Dávid egyedül is tudná szimulálni a protokollt, tehát semmilyen többlet információt nem szerez G-ről.

- Megalapozottság (Soundness):

  Ha Tamás nem ismeri a Hamilton kört, megpróbálhatja kitalálni, milyen kérdést fog kapni. Vagy készít egy G-vel izomorf gráfot, vagy egy független gráfban ad egy Hamilton kört. Mivel nem ismeri a Hamilton kört, nem tudja egyszerre mindkettőt. Ezzel a próbálgatással annak esélye hogy sikerül becsapnia Dávidot 2^{-n}, ahol “n” a körök száma. Így ha Dávid elegendő kérdést tesz fel, megbizonyosodhat róla, hogy Tamás nem ismeri a Hamilton kört G-ben.

Példa: Feige-Fiat-Shamir azonosítási séma

- V. választ egy *m* összetett számot és néhány *r1*, *r2*, ... *rk* számot, melyet titokban tart (PIN kód) nyilvánosságra hozzá viszont a következőt:

$$s_i :\equiv (r_i)^2 \pmod{m}$$

- V. bizonyíthatja azonosságát, ha be tudja bizonyítani, hogy ismeri az *si*-hez tartozó titkos *ri* kódot

- V. választ egy titkos *v* számot és *w*-t átadja K.-nak:

$$w :\equiv v^2 \pmod{m}$$

- K. felteszi kérdését (*e1*, *e2*, ... *ek*) formában, ahol *ei* =1 vagy 0.

- V. válaszként átadja *b*-t:

$$b :\equiv v \cdot \prod_{i=1}^{k} (r_i)^{e_i} \pmod{m}$$

- K. könnyen ellenőrzi V. állítását:

$$b^2 \stackrel{?}{\equiv} w \cdot \prod_{i=1}^{k} s^{e_i} \pmod{m}$$

- További részletek Szalkai, Dósa: Algoritmikus számelmélet c. könyvében

Modern titkosítási eljárások

- SHA
- RSA
- MD5

Felhasznált irodalom

- https://en.wikipedia.org/wiki/Zero-knowledge_proof
- http://index.hu/tech/2014/02/05/johet_a_feltorhetetlen_titkositas/
- http://www.wired.com/2014/02/cryptography-breakthrough/
- http://www.inf.unideb.hu/~pethoe/Jegyzet_PA_20110508.pdf
- https://en.wikipedia.org/wiki/Feige%E2%80%93Fiat%E2%80%93Shamir_identification_scheme
- https://en.wikipedia.org/wiki/Shafi_Goldwasser
- https://en.wikipedia.org/wiki/Silvio_Micali
- https://en.wikipedia.org/wiki/Charles_Rackoff
- https://en.wikipedia.org/wiki/L%C3%A1szl%C3%B3_Babai
- https://en.wikipedia.org/wiki/Shlomo_Moran
- http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html#intro
- https://lucatrevisan.wordpress.com/2009/05/11/cs276-lecture-24/
- http://www.renyi.hu/~csirmaz/zk.html
- http://people.ceu.edu/laszlo_csirmaz
- https://hu.wikipedia.org/wiki/Csirmaz_László
- http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/Szalkai_Dosa_Alg_szamelm.pdf

Kérdések?