Eötvös Loránd Tudományegyetem
Informatikai Kar

Ligeti Péter

K2: Kombinatorika és Kriptográfia

Habilitációs tézisfüzet

1. Bevezető

A dolgozat célja a szerzőnek a PhD fokozat megszerzését követően elért tudományos eredményeinek rövid, velős összefoglalása, tézisfüzete. Az eredményeket több szerzőtársammal közösen dolgoztuk ki, majd a [4, 5, 13, 14, 15, 19, 21, 22, 25, 26] publikációkban tettük közzé. A szerteágazó témák, valamint terjedelmi korlátok következményeként az újabb, egy témakörbe illeszkedő eredmények bemutatásánál törekedtem pontosabb, részletesebb képet adni, a többi témánál elsősorban a motiváció és az alapötlet "dallamának" átadására szorítkoztam.

A matematika különböző területeinek találkozása gyakran érdekes problémákat és megoldásokat szül. A kriptográfiának első pillantásra nem sok köze van a kombinatorikához, mivel a hagyományos kriptográfiában elsősorban számelméleti, algebrai vagy statisztikai ötleteket használnak. Azonban számos kombinatorikai módszernek és struktúrának lehet fontos szerepe az elméleti és alkalmazott kriptográfia különböző területein. Kutatásaim során tisztán kriptográfiai problémák vizsgálatán túl az ilyen metszéspontok felfedezése és kiaknázása volt a cél. Több témakörrel foglalkoztam kutatásaim során, melyek alapvetően két nagyobb csoportba sorolhatóak: tisztán kriptográfiai problémák (2. fejezet), valamint kombinatorikai módszerek a kriptográfiában (3. fejezet).

A dolgozat felépítése a következő. A bevezetést követően témakörönként a lényegesebb elért eredmények prezentációja következik. Ezen fejezetek túlnyomó hányadában az alapfogalmakat és a megoldandó problémát csak informálisan érzékeltetem, míg a részletesebben tárgyalt titokmegosztások problémakör (3.2 alfejezet) esetében szükséges fogalmakat precízebben is ismertetem. Végül, de nem utolsó sorban a jelenlegi kutatásokról is szót ejtek. Az alábbiakban bemutatott eredmények többszerzős publikációkban jelentek meg, mind közös munka gyümölcse, ezért nehéz lenne valamely protokollt vagy tételt egyetlen személyhez kötni. A dolgozatban azokat az eredményeket fogom téziseknek nevezni, amik egyrészt lényeges hozzáadott értéket

képviselőnek gondolok az adott témában, másrészt amelyek keletkezésében jelentős szerepem volt.

2. Kriptográfiai problémák

2.1. Ebédelő kriptográfusok

Egyrészt kevés résztvevős, kriptográfiailag biztonságos algoritmusok kidolgozásával foglalkoztam. A témakörhöz kapcsolódó egyik eredmény egy biztonságos kevés résztvevős protokoll javítása, illetve erre épülő alkalmazások kidolgozása. A feladat az úgynevezett *ebédelő kriptográfusok* problémára adott megoldás [11], az *anonim broadcast csatorna*, amely arra ad eljárást, hogyan lehetséges több résztvevőnek egyetlen bitet anonim módon elküldeni kizárólag broadcast üzenetek segítségével. Az eredeti cikkben ismertetett brilliáns alapötletnek vannak azonban hátrányai is, elsősorban a teljes anonimitásnak köszönhetően.

Az eredeti protokoll hiányosságait egy újfajta megközelítéssel sikerült javítani és felhasználni több alkalmazás (szavazás, illetve árverés) esetén is. A kidolgozott protokoll alapötlete szerint egy helyett három különböző csoportban is lejátsszuk az ebédelő kriptográfus alap-protokollt, ezzel meggátolva a lehetséges visszaéléseket. Először egy kisebb méretű csoportban számolunk, ami mindössze arra szolgál, hogy a résztvevők lefoglalják a későbbiekben általuk használt "rekeszeket", vagyis azt a részét az üzenetnek, ahová a saját inputjaikat tehetik majd. A második kör egy elköteleződést valósít meg, ahol a tényleges üzenet (és a megfelelő csoport) egyirányű homomorf képével számolnak a résztvevők. Végezetül egy közönséges ebédelő kriptográfus protokollt futtatnak, immáron a tényleges üzenettel, ami a homomorf képek alapján ellenőrizhető is. A protokoll segítségével tetszőleges üzenet anonim küldésére lehetőség nyílik, aminek egyik nem-triviális alkalmazásaként kevés résztvevős szavazási protokollt dolgoztunk ki. A Bárász Mihállyal, Lója

Krisztinával, Mérai Lászlóval és Nagy Dániellel közös munkát folyóiratcikként [4], illetve magyar szabadalomként [3] publikáltuk.

A javított protokoll másik alkalmazása egy speciális árverezőrendszernek, az úgynevezett borítékos versenytárgyalás biztonságos megvalósítására ad megoldást. Ebben a változatban anonim módon licitálnak a résztvevők úgy, hogy az árverés végén a liciteknek minden külső és belső résztvevő számára összehasonlíthatónak kell lenniük. Csalások elkerülésének érdekében megköveteljük azt is, hogy a nyertes személye az összes többi résztvevő összefogásával kideríthető legyen, erre adott megoldásunk az úgynevezett *mérges tömeg protokoll*, ami további alkalmazásokban is hasznos lehet. A Bárász Mihállyal, Mérai Lászlóval és Nagy Dániellel közös munkából publikáció [5], valamint magyar szabadalom [2] készült.

Mind a szavazó, mind az árverezőrendszer esetében több biztonsági kritériumot kellett teljesítenie a rendszereknek. A résztvevők anonimitásán felül minden résztvevőnek és külső megfigyelőnek egymástól függetlenül meg kell tudnia győződni a protokoll eredményének a helyességéről, továbbá senkinek ne legyen módja megsérteni a szavazás/árverés titkosságát, viszont ki lehessen deríteni a nem szabályos résztvevők kilétét. Ezeken felül lényeges feltétel volt, hogy a protokollok működéséhez ne legyen szükség megbízható harmadik félre, minden számítást a résztvevőknél lévő korlátozott erőforrású eszköz végez. A javasolt protokollokra sikerült megmutatni, hogy kielégítik a fenti követelményrednszert sztenderd biztonsági feltevések teljesülés esetén, úgymint a *random orákulum*, illetve a *számítási Diffie-Hellman* feltevések. Mivel minden egyes biztonsági kritérium teljesítésére vonatkozó állítást itt nem kívánok felsorolni, így az alábbi összefolgaló téziseket mondhatjuk ki:

1. Tézis (Szavazó rendszer biztonsága [4]). *A [4] szavazó rendszer teljesíti a felsorolt biztonsági kritériumokat, feltéve, hogy a random orákulum feltevés, valamint a megfelelő csoportban a számítási Diffie-Hellman feltevés teljesül.*

2. Tézis (Árverező rendszer biztonsága [5]). *Az [5] árverező rendszer teljesíti a felsorolt biztonsági kritériumokat, feltéve, hogy a random orákulum feltevés, valamint a megfelelő csoportban a számítási Diffie-Hellman feltevés teljesül.*

2.2. Egy alkalmazás: SIREN

Másodikként nyílt hálózatokat használó biztonságos adatmegosztással foglalkoztam. Ide kapcsolódó eredmény egy titokmegosztásokra épülő eljárás, amelyben a felhasználók eltitkosított érzékeny adatait csak az általuk meghatározott felhasználói csoportok képesek visszafejteni szükség esetén. A Kasza Péterrel és Nagy Ádámmal közös eredményeket publikáltuk [25], [26].

Az alkalmazás célja érzékeny adatok biztonságos szétosztása a rendszer felhasználói között oly módon, hogy az adatokat csak előre meghatározott jogosult résztvevők (illetve azok valamely koalíciói) tudják visszaállıtani, amennyiben az adat küldőjétől egy további, ún. "riasztás" üzentet kapnak. Példák ilyen riasztásra extrém értékek valamely okoseszköz által mért egészségügyi adatban (vércukorszint, vérnyomás, stb.), vagy egy egyszerű segélyhívás fizikai támadás vagy roham esetén. Az adatok tárolása elosztottan történik, nem egy központi szerveren, a rendszer biztonsága nem függ semmilyen megbızható harmadik féltől. A rendszer fő kommunikációs csatornái a *peer-to-peer* (P2P) és *friend-to-friend* (F2F) hálózatok, fő kriptográfiai építőelemei a *titokmegosztás* és szimmetrikus titkosítási primitívek.

Kommunikációs oldalról egyrészt a P2P hálózatok decentralizált, elosztott hálózati architektúráját használtuk fel az adatmegosztásra, üzenetek fel/letöltésére és keresésére. A F2F hálózat egy speciális privát P2P hálózat, amelyben a felhasználók csak az általuk ténylegesen ismert résztvevőkkel („barátokkal") vannak közvetlen kapcsolatban. A F2F hálózatok további lényeges tulajdonsága, hogy senkinek nincs információja arról, hogy a barátainak a körén túl kik vesznek részt a hálózatban, így a hálózat mérete az anonimitás megsértése nélkül növekedhet.

Titokmegosztásokról részletesen és precízen lesz szó a 3.2 alfejezetben, így itt csak az általunk használt speciális esetnek, az úgynevezett *t-küszöb titokmegosztásnak* az informális leírását adjuk meg. A feladatunk valamely titkos információt szétosztani a rendszert használó n résztvevő között oly módon, hogy t vagy annál több felhasználó képes legyen visszaállítani a titok az általa ismert információ-részekből, míg t-nél kevesebben ne legyenek erre képesek. Ha a második feltételnek a lehető legerősebb változata is igaz, jelesül a résztvevők bármely, t-nél kisebb méretű részhalmaza által birtokolt összes információ független a titoktól, akkor *tökéletes t-küszöb titokmegosztásról* beszélünk.

A protokoll három fő fázisból áll. Elsőként az adatküldő felhasználó egy ideiglenes kulcs segítségével eltitkosított üzeneteket tölt fel a P2P hálózatba, majd az ideiglenes kulcsnak a barátokkal vett páronkénti közös kulcsokkal eltitkosított példányait szétosztja a F2F hálózatban egy titokmegosztás alapján (itt a t küszöb a konkrét alkalmazástól függő, változtatható paraméter). Második körben a riasztást követően mindenki feltölti a P2P hálózatba a saját titokrészeket és letölti a többi hiányzót. Végezetül a letöltött adatokból a közös kulcs segítségével visszafejtik az ideiglenes kulcsot, majd az eredeti üzenetet.

A rendszertől megkövetlünk több biztonsági kritériumot is. Egyrészt legalább t megbízható barát esetén minden barát vissza tudja állítani az eredeti titkosítatlan üzenetet. Másrészt a riasztást megelőzően semmilyen t-nél kisebb méretű koalíció ne tudjon meg semmit az ideiglenes kulcsról. Végezetül azon felhasználóknak semmilyen részhalmaza ne tudjon meg semmi információt az eredeti üzenetről, akik nem barátai a küldőnek a F2F hálózatban. A kidolgozott rendszer a megfelelő feltevések mellett kielégíti a követelményeket:

3. Tézis (SIREN biztonsága [25, 26]). *Ha az üzenetküldő fél a protokollban tökéletes t-küszöb titokmegosztást, valamint biztonságos titkosítást*

használ, akkor a SIREN rendszer [25, 26] teljesíti a felsorolt biztonsági kritériumokat.

3. Kombinatorikai módszerek a kriptográfiában

3.1. Biztonságos hálózati kódolás és véges geometria

Itt az alapfeladatunk, hogy egy kommunikációs hálózatban egy forrásból több nyelőhöz egyszerre elküldött információ mennyiségét maximalizáljuk. Ezt egy Ahlswede és társai [1] által javasolt ötlet alapján úgy lehet elérni, hogy a köztes csúcsok egyszerű lineáris műveleteket végezhetnek a bejövő adatokon, majd azt küldik tovább. Egy ilyen kódolást akkor nevezünk *k-biztonságosnak*, ha az ellenség bármely, k méretű élhalmaz lehallgatásával nem jut semmi információhoz. Cai és Yeung [10] megoldásában a forrásnál véletlen zajt kevernek az üzenethez lineáris operátorok segítségével, ezzel garantálható a biztonság kellően nagy méretű test felett:

1. Tétel (Cai és Yeung [10]). *$G = (V, E)$ hálózatra létezik $\mathbb{F}$ test feletti k-biztonságos lineáris hálózati kódolás, ha $|\mathbb{F}| > \binom{|E|}{k}$.*

Adódik a kérdés, hogy lehetséges-e ezen javítani, akár nemlineáris, akár szofisztikáltabb lineáris konstrukciók segítségével. A probléma véges geometriai átfogalmazásával, valamint affin egyenesekre vonatkozó összefüggések felhasználásával sikerült megmutatni, hogy nem lehet elérni az úgynevezett *univerzális biztonságot*, azaz tetszőleges (de lineáris) hálózat esetén k-biztonságos módon elrejteni az eredeti üzenetet a forrásnál. Ennek az egyszerűbb esete, hogy lineáris operátorokkal nem lehet megoldani, az izgalmasabb eset a nemlineáris operátorok kérdése, ami szintén nem lehetséges:

4. Tézis ([19]). *Nem létezik univerzális $k-$biztonságos hálózati kódolás.*

Ezen felül a létező lineáris konstrukciókon javítottunk, lefogó halmazok keresésével sikerült a fenti korlátot [10] feljebb tornászni:

5. Tézis ([19]). *$G = (V, E)$ hálózatra létezik $\mathbb{F}$ test feletti k-biztonságos lineáris hálózati kódolás, ha $|\mathbb{F}| > \binom{|E|}{k} - k + 1$.*

Végezetül ismert hálózat esetében megadtunk egy algoritmust, ami előállítja a biztonságos hálózati kódolást. A Fancsali Szabolccsal közös eredményekből nemzetközi folyóiratcikk született [19].

3.2. Titokmegosztás gráfokon

3.2.1. Alapfogalmak

Egy általános titokmegosztási séma esetében valamely titkos információt kell szétosztani a rendszer résztvevői között oly módon, hogy azt csak bizonyos meghatározott részhalmazaik tudják visszaállítani. Precízebben, adott a résztvevőknek egy $\mathcal{P}$ véges halmaza, valamint egy *hozzáférési struktúrának* nevezett $\mathcal{A} \subseteq 2^{\mathcal{P}}$ felszálló részhalmazrendszer (azaz $A \in \mathcal{A}$ és $A \subseteq B$ esetén $B \in \mathcal{A}$). $\mathcal{A}$ elemeit *kvalifikált részhalmazoknak* nevezzük. Egy adott hozzáférési struktúrához tartozó titokmegosztástól megköveteljük, hogy a kvalifikált részvevők együtt vissza tudják állítani az eredeti titkot a saját titokrészeikből, míg a nem-kvalifikáltak ne legyenek erre képesek. A továbbiakban kizárólag *tökéletes titokmegosztásokkal* foglalkozunk, ahol a nem-kvalifikált részhalmazok résztvevői semmilyen valódi információt nem tudhatnak meg a titokról:

1. Definíció. *Az $\mathcal{A}$ hozzáférési struktúrát megvalósító $\mathcal{S}$ tökéletes titokmegosztás közös eloszlású $\xi_i : \forall i \in \mathcal{P}$ és ξ_s véletlen valószínűségi változók együttese, amire*

(i) ha $A \in \mathcal{A}$, akkor $\{\xi_i : i \in A\}$ meghatározza ξ_s-t;

(ii) ha $B \notin \mathcal{A}$, akkor $\{\xi_i : i \in B\}$ független ξ_s-től.

(Itt a triviális esetek elkerülése érdekében feltesszük, hogy az ξ_s titok 1 valószínűséggel nem konstans.)

A titokmegosztást először két független cikkben vezették be, mindkét esetben a 2.2 fejezetben említett t-küszöb titokmegosztásokat vizsgálták, ahol $\mathcal{A} = \{A \subseteq \mathcal{P} : |A| \geq t\}$. Shamir [27] egyszerű konstrukciója Lagrange interpolációra épül, Blakley [6] megoldása véges dimenziós vektorterek hipersíkjainak metszési tulajdonságait használja.

Egy titokmegosztási séma bonyolultságát azzal mérjük, hogy a legjobban terhelt résztvevőnek mennyi információt kell megjegyeznie a titokhoz képest. Ezt a mennyiséget a szakirodalom *információs hányados* vagy *komplexitás* néven tárgyalja. A témakör egyik legizgalmasabb és legnehezebb kérdése ennek a hányadosnak a meghatározása vagy legalább becslése adott halmazrendszer esetén. Legyenek a ξ diszkrét véletlen változó m lehetséges értéke $x_1, \ldots, x_m$ a megfelelő valószínűségek pedig $p_i = P(\xi = x_i)$. A ξ méretét hagyományosan az információtartalmával, avagy a *Shannon entrópiájával* mérjük: $\mathbf{H}(\xi) = \sum p_i \log p_i$, . Ezek alapján az alábbi precíz definíciót adhatjuk:

2. Definíció. *Az $\mathcal{A}$ hozzáférési struktúra információs hányadosa*

$$\sigma(\mathcal{A}) = \inf_{\mathcal{S}} \max_{i \in \mathcal{P}} \frac{\mathbf{H}(\xi_i)}{\mathbf{H}(\xi_s)},$$

ahol az infumumot az $\mathcal{A}$-t megvalósító összes $\mathcal{S}$ tökéletes titokmegosztásra kell nézni.

Megjegyezzük, hogy a szakirodalomban gyakran a fenti mennyiség reciprokát, az úgynevezett *információs rátát* vizsgálják. Jelen műben (valamint a kapcsolódó cikkekben) két főbb ok miatt döntöttünk információs hányados terminológia használata mellett. Egyrészt a legfrissebb, gráfalapú rendszerekre vonatkozó irodalomban ez az elterjedtebb, másrészt a felhasznált módszereknek és ötleteknek sokkal intuitívebb és szemléletesebb bemutatását teszi lehetővé.

Vegyük észre, hogy tetszőleges hozzáférési struktúrát a felszálló tulajdonság miatt a minimális elemei karakterizálnak, ezáltal minden ilyen rendszer leírható egy $H = (\mathcal{P}, \min \mathcal{A})$ hipergráffal. Ha a rendszer minimális elemeinek mérete kettő, akkor *gráf alapú rendszerről* beszélünk. Valóban, ha egy hozzáférési struktúrában csak 2-elemű minimális elemek vannak, annak megfelel egy gráf és fordítva: $G = (V, E)$ véges, egyszerű gráf esetén a csúcsoknak feleltessük meg a titokmegosztás résztvevőit, majd tetszőleges résztvevőhalmaz legyen kvalifikált, ha a megfelelő csúcshalmazban van él. Gráfalapú titokmegosztásoknál a hozzáférési struktúra helyett magára a gráfra hivatkozhatunk, illetve egy adott G gráffal leírható rendszer információs hányadosára a $\sigma(G)$ jelölést használjuk. Érdemes észrevenni, hogy egy adott csúcs elsőfokú szomszédai a titokmegosztás szempontjából egyenrangúan viselkednek (ugyanazt a titokrészt kaphatják), ezért a továbbiakban feltesszük, hogy bármely csúcsra legfeljebb egy levél illeszkedik.

A gráf alapú rendszerek információs hányadosaival kapcsolatos eredmények alapvetően két csoportba sorolhatóak: konkrét, kis gráfokra vonatkozó, illetve általános gráf-osztályokra vonatkozó eredmények. Legfeljebb hat csúcson az összes gráfra meghatározták az információs hányadost [23, 8, 9, 32, 31, 20], míg legfeljebb kilenc csúcsú gráfokra sporadikus eredmények ismertek [33, 29, 17, 28]. Általános eredményből jóval kevesebb van, ilyen Blundo és társai d-reguláris gráfok egy rekurzív családjára [7], Csirmaz hiperkockákra és d-dimenziós rácsokra [12], valamint Csirmaz és Tardos fákra [16] vonatkozó eredményei. A következőkben az információs hányados meghatározására felhasznált főbb módszerek ismertetése következik.

3.2.2. Módszerek: entrópiák és felbontások

Egy rendszer információs hányadosának pontos kiszámítása akkor lehetséges, ha olyan alsó és felső becsléseket tudunk bizonyítani, amelyek egybeesnek. A két irányú becsléshez teljesen eltérő eljárások használhatóak.

Az információs hányados alsó becslésének egyetlen, jelenleg ismert módja a Blundo és társai által bevezetett, úgynevezett *entrópia módszer* [8]. A módszer a Shannon entrópia és a tikokmegosztás néhány alaptulajdonságán alapul és a következőképpen foglalható össze. Definiáljuk a résztvevők minden A részhalmazára az alábbi f valósértékű függvényt:

$$f(A) = \frac{H(\{\xi_i \,:\, i \in A\})}{H(\xi_s)} \tag{1}$$

Ezzel a jelöléssel az infomációs hányados az $\{f(i) \,:\, i \in \mathcal{P}\}$ maximális értéke. Az entrópia függvény sztenderd tulajdonságait felhasználva könnyen megmutatható, hogy az alábbi, úgynevezett *Shannon egyenlőtlenségek* minden résztvevő-halmazra igazak:

1. Állítás (Shannon egyelnőtlenségek). *Legyen $f : 2^{\mathcal{P}} \longrightarrow \mathbb{R}$ az 1-ben definiált függvény. Ekkor minden $A, B \subseteq \mathcal{P}$ esetén igazak az alábbiak:*

(a) $f(\emptyset) = 0$, valamint általában $f(A) \geq 0$ (pozitivitás);

(b) ha $A \subseteq B \subseteq V$, akkor $f(A) \leq f(B)$ (monotonitás);

(c) $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$ (szubmodularitás).

(d) ha $A \subseteq B$, A független csúcshalmaz, de B nem, akkor $f(A)+1 \leq f(B)$ (erős monotonitás);

(e) ha sem A, sem B nem független csúcshalmaz, de $A \cap B$ már az, akkor $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$ (erős szubmodularitás).

Most az a cél, hogy belássuk, hogy *bármely* f valós értékű függvényre, amely teljesíti az (a)–(e) tulajdonságokat, létezik egy i résztvevő, akire $f(i) \geq r$. Mivel a titokmegosztásból kapott függvények is teljesítik ezeket, ezért az információs hányados is legalább r. Eme általános módszer nagy hátránya, hogy a Shannon egyenlőtlenségekből felírt LP feladat már kis méretű

gráfok esetén (8-9 csúcs) is gyakorlatban megoldhatatlan. Általános korlátok bizonyításához ezért a konkrét rendszerben szimmetriákat vagy egyéb struktúrális tulajdonságokat kell keresni, amivel a feladat mérete lényegesen redukálható.

Másrészt tetszőleges titokmegosztási konstrukció egyben egy felső korlátot is ad az információs hányadosra. Ide kapcsolódó alapvető eredmény Stinson felbontási tétele [30], ami bár általánosabban is igaz, csak gráfokra vonatkozó speciális eseteit idézzük. A tétel kimondása előtt érdemes meggondolni néhány egyszerűbb állítást. Könnyen láthatóan tetszőleges $\mathcal{A}$ hozzáférési struktúra (speciálisan G gráf) esetén $\sigma(\mathcal{A}) \geq 1$, azokat a rendszereket, amelyekre egyenlőség áll fenn, *ideális rendszereknek* nevezzük. Habár sok esetben az ideális rendszerek karakterizációja megoldatlan (és roppant nehéz) probléma, a gráfok esetében pontosan (és könnyen) megadhatóak az ideális rendszerek. Ezek a *teljes multiparti gráfok* lesznek, amik teljes gráfok diszunkt uniójának a komplementereiként állnak elő.

2. Állítás. *Tetszőleges G véges egyszerű gráf esetén $\sigma(G) = 1 \Longleftrightarrow G$ teljes multiparti gráf.*

A cél egy adott gráf olyan fedéseinek vagy felbontásainak megkonstruálása, ahol a kisebb, felbontásban szereplő gráfok információs hányadosai már kiszámíthatóak. A fenti állítás következményeként érdemes ideálisakkal való fedéseket nézni.

2. Tétel (Stinson dekompozíciós tétele gráfokra [30]). *Tegyük fel, hogy létezik a G gráfnak egy teljes multiparti gráfokkal történő fedése, amelyre minden csúcsot legfeljebb p darab gráf fed, valamint minden élet legalább e darab gráf fed. Ekkor $\sigma(G) \leq \frac{p}{e}$.*

A tétel egy egyszerű következményét, amelyben a gráfot a csúcsokból induló csillagokkal, mint speciális teljes páros gráfokkal fedjük külön is nevesítjük:

3. Állítás (Stinson korlát). *Tetszőleges G véges egyszerű gráf esetén $\sigma(G) \leq \frac{d+1}{2}$, ahol d a gráf maximális fokszáma.*

Sun and Chen [31] később általánosította ezt a technikát súlyozott gráfokra, illetve gráf fedésekre is.

3.2.3. Egy gráfcsalád 2-$1/k$ információs hányadossal

A gráfalapú titokmegosztásokhoz kapcsolódó első eredményben a Stinson korlátban is felhasznált speciális esettel , a csillag-fedésekkel foglalkoztunk. Figyeljük meg, hogy a 2 tételben törtfedéseket használva (azaz nem-egész súlyú részgráfokkal fedve) $p, e \in \mathbb{N}$ helyett feltehető, hogy $e = 1$ és $p \in \mathbb{Q}$. Ezt az észrevételt felhasználva sikerült egy adott gráf csillagokkal történő fedéséből adódó legjobb felső korlát kiszámítását egy lineáris programozási feladatra átfogalmazni:

6. Tézis. *Adott $G = (V, E)$ véges egyszerű gráf. Ekkor az alábbi lineáris programozási feladat megoldása felső korlátja $\sigma(G)$-nek:*
Változók:

- *p globális változó: a maximális csúcsfedési szám*
- *x_{uv}, illetve x_{vu} minden $\{uv\} = e \in E$ esetén az e-t tartalmazó u, illetve v közepű csillagok száma*
- *l_v minden $v \in V$ esetén a v közepű csillagok száma*

LP feladat

$$\min p$$

$x_{uv} + x_{vu} \geq 1$	*minden $uv \in E$ esetén,*
$l_u + \sum_{uv \in E} x_{vu} \leq p$	*minden $u \in V$ esetén,*
$x_{uv} \leq l_u$	*minden $u \in V, uv \in E$ esetén.*

A fenti LP feladatnak kettő fő előnye van: a feladat mérete lineáris az élszámban, így nagyobb gráfokra is megoldható, továbbá az optimális megoldásból könnyen előállítható a csillag-fedés. Ezek a fedések olyan esetekben bizonyultak optimálisnak, ahol a magasabb fokú csúcsok nincsenek összekötve, valamint a gráf nem tartalmaz túl rövid köröket. Egy *gráf kerülete* legyen a legrövidebb körének élszáma. A csillag-fedések lineáris programozási karakterizálása segítségével egy jelentős gráf-osztály információs hányadosát sikerült meghatározni , ami a legnagyobb fokszámtól függ csak:

7. Tézis ([13]). *Legyen G egy legalább 6 kerületű gráf, amelyben nincsenek szomszédos, legalább 3-fokú csúcsok, valamint a maximális fokszám d. Ekkor*

$$\sigma(G) = 2 - \frac{1}{d}.$$

A Csirmaz Lászlóval közös eredményből publikáció készült [13].

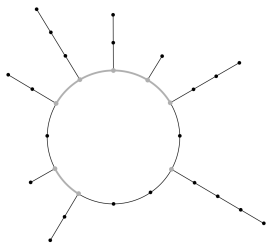
3.2.4. Kis gráfok és általánosított sunletek

Az előzőekben ismertetett fedési eljárásnak, valamint az entrópia módszernek a segítségével további gráf-családok információs hányadosának meghatározása is sikerült, úgymint kevés csúcsú gráfok, illetve legalább öt kerületű gráfok [22].

Kis gráfokra legfeljebb 9 csúcsig néhány gráf információs hányadosa volt ismert csak. A fenti módszerekkel kettő gráf kivételével az összes legfeljebb 9 csúcsú, illetve 10 csúcsú és 10 élű olyan gráfra sikerült pontos értéket kiszámítani, amelyeknek a kerülete legalább 5. Precízebben 202 darab új gráfra kaptunk eredményt, amiből 20 korábban ismert [28], de pontatlan érték javítása volt.

A fenti eredmények segítségével sikerült egy nagyobb gráfosztályra megsejteni, majd bebizonyítani a pontos értéket. Az *általánosított n-sunlet gráfnak* nevezzük egy n hosszú körből és a kör néhány csúcsából induló utakból

álló gráfot. A kör egy összefüggő A csúcshalmazát *ívnek* nevezzük, ha minden A-beli csúcsból indul út, az ív *hossza* pedig az éleinek száma. Szemléltetésként álljon itt egy általánosított 12-sunlet gráf 0, 1 és 4 hosszú (szürke) ívekkel:



Sikerült megmutatni, hogy az információs hányados a maximális ív hosszának függvénye, feltéve, hogy az íven kívül elegendő csúcs van.

8. Tézis ([22]). *Legyen G általánosított n-sunlet gráf, aminek a maximális íve $k \leq n-6$ hosszú. Ekkor*

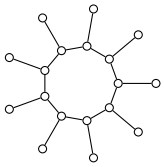
$$\sigma(G) = 2 - \frac{1}{k+3}.$$

A Harsány Károllyal közös eredményekbírálat alatt vannak [22].

3.2.5. Gráfok sok levéllel

Amint azt fentebb említettük, a titokmegosztások szempontjából tetszőleges rögzített csúcs elsőfokú szomszédai megkülönböztethetetlenek, ezért feltettük, hogy a csúcsokra legfeljebb egy levél illeszkedik. A témához kapcsolódó legfrissebb cikkben sok levelet tartalmazó gráfok információs hányadosát vizsgáltuk [21].

Egyrészt entrópia-egyenlőtlenségekkel, valamint egyszerű csillagfedéssel pontos értéket bizonyítottunk az úgynevezett n-sunlet gráfok információs hányadosára, ami egyben megválaszolja a [22] egyik nyitott kérdését is. Jelölje S_n az n-csúcsú körből és a kör csúcsaira illeszkedő n független levélből álló *n-sunlet gráfot*. Az alábbi ábrán az S_9, 9-sunlet gráf látható illusztrációként:

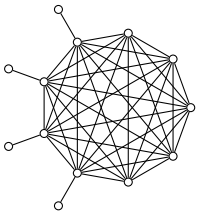


Elég nagy n értékekre az n-sunlet gráfok információs hányadosa konstans lesz.

9. Tézis ([21]). *Legyen* $n \in \mathbb{N}, n \geq 4$. *Ekkor*

$$\sigma(S_n) = 2.$$

Másrészt a K_n^l gráfosztályt vizsgáltuk, ami egy n-csúcsú teljes gráfból, valamint ennek a csúcsaira illesztett l darab levélből áll. Tekintsük a K_9^4 gráfot egyszerű példaként:



Habár itt pontos értékek meghatározása nem sikerült, de rekurzív konstrukciókkal és súlyozott fedésekkel nem-triviális felső korlátot adtunk a K_n^l gráfosztály információs hányadosára.

10. Tézis ([21]). *Legyen* $n, l \in \mathbb{N}, l \leq 4, l \leq n$. *Ekkor*

$\sigma(K_n^l) < 2$.

A Gyarmati Mátéval közös eredmény jelenleg bírálat alatt vann [21].

3.2.6. Kis köröket nem tartalmazó gráfok

Ha néhány korábbi eredményt összevetünk, egy érdekes sejtést fogalmazhatunk meg az információs hányados és a gráf kerülete közötti összefüggésről. Álljon itt az eredmények felsorolása a kerületekkel kiegészítve:

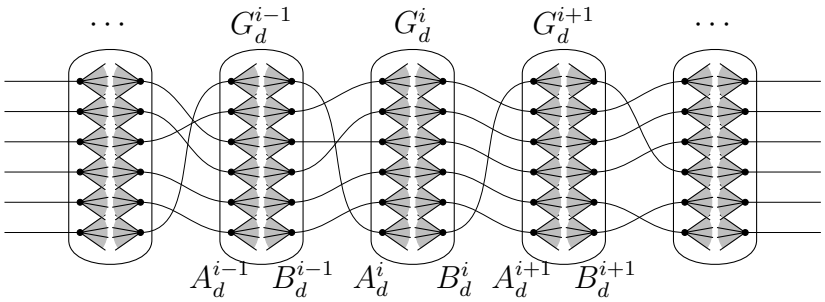
- van Dijk rekurzív gráfcsaládjának [32] információs hányadosa $(d+1)/2$, kerülete 6
- d-dimenziós hiperkocka [12] információs hányadosa $d/2$, kerülete 4
- fák [16] információs hányadosa < 2, kerülete 0
- általánosított n-sunletek információs hányadosa < 2, kerülete > 4
- magasfokú szomszédos csúcsok nélküli gráfok [13] információs hányadosa < 2, kerülete > 5

Mindezek az eredmények azt az intuíciót sugallják, hogy a magas információs hányados következménye korlátos kerület, mivel a csúcsok közötti interakciók csökkenek, ahogy a távolságuk nő. Sikerült ezt a sejtést megcáfolni tetszőlegesen nagy információs hányadosó gráfok konstruálásával, amelyeknek a kerülete is tetszőlegesen nagy lehet [14]. A bizonyítás két nagyobb részre osztható: az első részben entrópia egyenlőtlenségek segítségével d-reguláris páros gráfok egy családjára megmutattuk, hogy eléri a Stinson korlátot 3, azaz az információs hányadosa $(d+1)/2$.

A konstrukció vázlatosan az alábbi lépésekből áll. Legyenek $n_2, n_3, \ldots,$ 4-nél nagyobb egészek és legyen n_2 páros. Megkonstruáljuk páros gráfoknak egy G_2, G_3, ... sorozatát a következőképpen. G_2 az n_2 csúcsú páros hosszú kör A_2 és B_2 független csúcshalmazokkal.

Tegyük fel, hogy a G_d páros gráfot már megkonstruáltuk, A_d és B_d független csúcshalmazokkal. Ezután vegyünk n_{d+1} példányát a G_d-nek ciklikusan, amiket G_d^i-vel jelöljünk, ahol $G_d^{n_{d+1}+1} = G_d^1$. A G_d^i független csúcshalmazai

legyenek A_d^i és $\cup B_d^i$. Ezekből úgy kaphatunk meg egy G_{d+1} gráfot, hogy behúzunk egy-egy (tetszőleges) teljes párosítást a B_d^i és az A_d^{i+1} csúcshalmazok között minden $i = 1, 2, \ldots, n_{d+1}$-re, lásd az alábbi ábrát:



Jelölje $\mathcal{G}_d$ az összes ilyen módon előállítható G_d gráfok halmazát. Entrópia egyenlőtlenségek és konstrukciók segítségével meghatároztuk ezen gráfosztály elemeinek információs hányadosát:

11. Tézis ([14]). *Legyen $3 \leq d \in \mathbb{N}^+$. Ekkor minden $G_d \in \mathcal{G}_d$ esetén*

$$\sigma(G_d) = \frac{d+1}{2}.$$

Második (valójában elég hosszú és nem-nyilvánvaló) lépésben tisztán kombinatorikai ötletek felhasználásával megmutattuk, hogy kellően nagy gráfméret esetén ebben a gráfcsalád tartalmaz tetszőleges kerületű gráfot.

12. Tézis ([14]). *Léteznek tetszőlegesen nagy kerületű gráfok a $\mathcal{G}_d$ osztályban.*

A Csirmaz Lászlóval közös eredményből publikáció született [14].

3.3. Erdős-Pyber tétel hipergráfokra

Ezen felül hipergráfokon alapuló titokmegosztásokkal foglalkoztam. Ebben a témakörben már korábbról ismert, gráfalapú titokmegosztásokra vonatkozó

eredmények általánosítását vizsgáltam. Ide kapcsolódó eredmény a Csirmaz Lászlóval és Tardos Gáborral közös munka [15], amely Erdős és Pyber egy gráfok particionálására vonatkozó eredményét [18] általánosítja uniform hipergráfokra. A tisztán kombinatorikai hátterű feladatnak kriptográfiai alkalmazásai is vannak. Ezek felhasználásával új, az eddig ismerteknél jobb általános felső korlátokat adhatunk gráf és hipergráf alapú titokmegosztások információs hányadosára.

Erdős és Pyber bebizonyították [18], hogy minden n csúcsú G gráf élhalmaza partícionálható teljes páros gráfokra úgy, hogy minden csúcs legfeljebb $O(n/\log n)$ ilyen páros gráfban van benne. Stinson dekompozíciós tétele következtében ebből $\sigma(G) \leq O(n/\log n)$ adódik. Első lépésként egy új, konstruktív bizonyítást adtunk az Erdős-Pyber tételre egy javított, explicit konstans faktorral.

13. Tézis ([15]). *Legyen G egyszerű n csúcsú gráf. Ekkor*

$$\sigma(G) \leq (1/2 + o(1))\frac{n}{\log n}.$$

Másrészt általánosítottuk az eredeti tételt d-uniform hipergráfok (amelyekben minden hiperél d csúcsot tartalmaz) partícióira, 2-nél nagyobb d értékekre. Egy d-uniform hipergráfot *teljes $d-$uniform d-es hipergráfnak* nevezünk, ha a csúcshalmaza partíconálható d részre és a hiperélek pontosan azok, amik minden partícióbeli halmazból tartalmaznak egyetlen elemet. Itt azt mutattuk meg, hogy tetszőleges $\mathcal{H}$ d-uniform hipergráf particionálható teljes $d-$uniform d-es hipergráfokra úgy, hogy minden csúcs legfeljebb $O(n\{d - 1/\log n)$ ilyenben van benne.

14. Tézis ([15]). *Legyen $\mathcal{H}$ egy n csúcsú d-uniform hipergráf által meghatározott hozzáférési struktúra. Ekkor*

$$\sigma(\mathcal{H}) \leq (\frac{1}{d!} + o(1))\frac{n^{d-1}}{\log n}.$$

Sikerült megmutatni azt is, hogy ennél lényegesen jobb korlátot nem lehetséges elérni ezzel a módszerrel, valamint úgynevezett *sűrű* (hiper)gráfokra (amelyekben a csúcsok fokszáma nagy) jobb konstans értékeket is tudtunk adni törtfedések segítségével.

4. Jelenlegi kutatások

Jelen pillanatban, amikor ezeket a sorokat képernyőre vetem, két fő irányban folytatok aktív kutatásokat. Egyrészt a fenti biztonságos adatszétosztó alkalmazás [25, 26] általánosításán, továbbfejlesztésén dolgozunk, ahol a fő probléma egy biztonságos ön-fenntartó elosztott hálózat megvalósítása. Másrészt titokmegosztások témakörben dolgozunk több problémán is: a fákra [16] és az általánosított sunletekre [22] vonatkozó eredmények közös általánosításaként egykörös gráfok információs hányadosait számoljuk, továbbá ígértetes eredményeink vannak aszimptotikusan legkisebb méretű olyan gráfcsalád konstruálására, ahol a Stinson korlát éles. Kicsit messzebre tekintve további hipergráfos illetve ideális rendszerek vizsgálatában kívánok elmélyülni.

Köszönetnyilvánítás Szeretném megköszönni minden szerzőtársamnak a közösen elvégzett gyümölcsöző tudományos munkát. Köszönöm kollégáimnak azt a hihetetlenül inspiráló légkört, amit a Komputeralgebra Tanszéken és az Informatikai Karon, valamint a Matematika Intézet ELTECRYPT csoportjában és a Rényi Intézet kripto szemináriumán teremtettek. Végezetül családomnak tartozom végtelen hálával az örömökért és nyugalomért, amit tőlük kapok.

Hivatkozások

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, Network information flow, *IEEE Trans. on Information Theory*, **46** (2000) 1204–1216.

[2] M. Bárász, P. Ligeti, K. Lója, L. Mérai, D. A. Nagy, Árverező rendszer, szabadalmi beadvány **Nr. P0700596** (2007)

[3] M. Bárász, P. Ligeti, K. Lója, L. Mérai, D. A. Nagy, Szavazó rendszer, szabadalmi beadvány **Nr. P0700548** (20076)

[4] M. Bárász, P. Ligeti, K. Lója, L. Mérai, D. A. Nagy, Another Twist in the Dining Cryptographers' Protocol, *Tatra Mountains Mathematical Publications*, **57** (2013) 85–99.

[5] M. Bárász, P. Ligeti, K. L. Mérai, D. A. Nagy, Anonymous sealed bid auction protocol based on a variant of the Dining Cryptographers' Protocol, *Periodica Mathematica Hungarica*, **65** (2) (2012) 167–176.

[6] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the national computer conference*, **48** (1979) 313—317.

[7] C. Blundo, A. De Santis, R. D. Simone and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Des., Codes and Crypt.* **11** (1997), 107–122.

[8] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decomposition and secret sharing schemes, *J. of Crypt.* **8** (1995), 39–64.

[9] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. of Crypt.* **5** (1992), 153–166.

[10] N. Cai and R. W. Yeung, Secure Network Coding, 2002. *Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT 2002)* (2002)

[11] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, *Journal of Cryptology* **1** (1) (1988) 65-–75.

[12] L. Csirmaz, Secret sharing schemes on graphs, *Studia Math. Hung.* **44** (2007), 297–306.

[13] L. Csirmaz, P. Ligeti, On an infinite family of graphs with information ratio $2 - 1/k$, *Computing* **85** (2009), 127–136.

[14] L. Csirmaz, P. Ligeti, Secret sharing on large girth graphs, *Cryptography and Communications* (2018) https://doi.org/10.1007/s12095-018-0338-x.

[15] L. Csirmaz, P. Ligeti, G. Tardos, Erdős-Pyber theorem for hypergraphs and secret sharing, *Graphs and Combinatorics* **31** (5) (2015) 1335–1346.

[16] L. Csirmaz and G. Tardos, Optimal information rate of secret sharing schemes on trees, *IEEE Tr. on Inf. Theory* **59** (2013), 2527–2630.

[17] M. H. Dehkordi, A. Safi, The complexity of the connected graph access structure on seven participants *J. Math. Crypt.* **11** (1) (2017), 25–35.

[18] P. Erdős, L. Pyber, Covering a graph by complete bipartite graphs, *Discrete Mathematics* **170** 1–3 (1997) 249-–251.

[19] Sz. L. Fancsali, P. Ligeti, Some applications of finite geometry for secure network coding, *Journal of Mathematical Cryptology*, **2** (3) (2008) 209–226.

[20] O. Farràs, T. Kaced, S. Martın, C. Padró, Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing, *Cryptology ePrint Archive*, Report 2017/919,2017; available at https://eprint.iacr.org/2017/919

[21] M. Gyarmati, P. Ligeti, On the information ratio of graphs with many leaves, *Tatra Mountains Mathematical Publications*, to appear.

[22] K. Harsányi, P. Ligeti, Exact information ratios for secret sharing on small graphs with girth at least 5, *Journal of Mathematical Cryptology*, to appear

[23] W. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Des., Codes and Crypt.* **9** (1996) 233–250.

[24] S. Jaggi, P. Sanders, Ph. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuisen, Polynomial Time Algorithms for Multicast Network Code Construction, *IEEE Transactions on Information Theory* **51** (2005) 1973–1982.

[25] P. Kasza, P. Ligeti, Á. Nagy, Siren: Secure Data Sharing Over P2P and F2F Network, *Studia Scientarium Mathematicarum Hungarica* **52** (2) (2015) 257–264.

[26] P. Kasza, P. Ligeti, Á. Nagy, On a Secure Distributed Data Sharin System and its Implementation, *Annales Mathematicae et Informaticae* **44** (2015) 111–120.

[27] A. Shamir, How to share a secret, *Communications of the ACM* **22** (1979) 612-–613.

[28] Y. Song, Z. Li, Y. Li and R. Xin, The optimal information rate for graph access structures of nine participants, *Front. Comput. Sci.* **9** (2015) 778–787.

[29] Y. Song, Z. Li and W. Wang, The Information Rate of Secret Sharing Schemes on Seven Participants by Connected Graphs, *Adv. Materials Research* **127** (2012) 637–645.

[30] D.R. Stinson, Decomposition construction for secret sharing schemes, *IEEE Tr. on Inf. Theory* **40** (1994) 118–125.

[31] H.L. Sun and B.L. Chen, Weighted decomposition construction for perfect secret sharing schemes, *Comp. and Math. with Appl.* **43** (2002) 877–887.

[32] M. van Dijk, On the information rate of perfect secret sharing schemes, *Des., Codes and Crypt.* **6** (1995) 143–160.

[33] W. Wang, Z. Li and Y. Song, The optimal information rate of perfect secret sharing schemes, in: *Bus. Man. and Elect. Inf. (BMEI), International Conference*, 2 (2011) 207–212.

[34] D. R. Stinston, New general lower bounds on the information rate of secret sharing schemes, In *Advances in Cryptology – CRYPTO '92, Lecture Notes in Comput. Sci., Vol. 740,* (1993) 168–182.