Zárójelentés a PD100712 számú, "K2, avagy kombinatorika és kriptográfia" című OTKA pályázat kutatási eredményeiről

1. Motiváció

A projekt keretén belül tisztán kombinatorikai és kriptográfiai problémák vizsgálatán túl a két nagy terület metszéspontjainak felfedezése és kiaknázása volt a cél. Több témakörrel foglalkoztam kutatásaim során, melynek eredményei alapvetően három csoportba sorolhatóak.

2. Kombinatorikai problémák

Tisztán kombinatorika témában mátrixok különböző részmátrixokból való rekonstruálásával foglalkoztam. A részmátrixokat jelen esetben ugyanannyi sor, illetve oszlop törlésével származtatjuk. Megmutattam, hogy egy törlés után helyreállítható az eredeti mátrix, valamint ennek alkalmazásaként sikerült meghatározni a részmátrixokból képzett részbenrendezett halmaz automorfizmus-csoportját is. Az derült ki, hogy egy bizonyos mérettől kezdve néhány kézenfekvő automorfizmuson kívül nincs is több. A kapcsolódó eredményeket konferencián ismertettem (8th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications), majd publikáltam [6].

3. Kriptográfiai problémák

Egyrészt kevés résztvevős, kriptográfiailag biztonságos algoritmusok kidolgozásával foglalkoztam. A témakörhöz kapcsolódó egyik eredmény egy kevés résztvevős szavazási protokoll, amely több különböző biztonsági feltételnek eleget tesz. Fő építőköve az úgynevezett anonim broadcast csatorna, amelynek hiányosságait egy újfajta megközelítéssel sikerült javítani és felhasználni. A Bárász Mihállyal, Lója Krisztinával, Mérai Lászlóval és Nagy Dániellel

közös munkából publikáció készült [2]. A másik az úgynevezett elsőáras árverésnek egy általánosítására ad megoldást, ahol több egyforma árura licitálnak a résztvevők, de a nyertesét kivéve mindenkinek a licitjei titokban maradnak. A Mérai Lászlóval közös munkából publikáció készült [8].

Másrészt nyílt hálózatokat használó biztonságos adatmegosztással foglalkoztam. Ide kapcsolódó eredmények egy titokmegosztásokra épülő eljárás, amelyben a felhasználók eltitkosított érzékeny adatait csak az általuk meghatározott felhasználói csoportok képesek visszafejteni szükség esetén. A rendszerben az adatok tárolása elosztottan történik, nyílt és titkosított kommunikációs csatornákat egyaránt használ. Ide kapcsolódik még egy elosztott adattároló rendszer elméleti kidolgozása, amelyben a felhasználók a többiek eszközein titkosítva tárolják adataikat, az önző felhasználói viselkedés megelőzése pedig páronkénti kölcsönös könyvelés segítségével történik. A kapcsolódó eredmények konferenciákon kerültek ismertetésre (9th International Conference on Applied Informatics, 14th Central European Conference on Cryptology), konferencia-kötetben [1], folyóiratban publikálásukra sor került [4], [5].

4. Kombinatorikai módszerek a kriptográfiában

Ezen felül hipergráfokon alapuló titokmegosztásokkal foglalkoztam. Ebben a témakörben már korábbról ismert, gráfalapú titokmegosztásokra vonatkozó eredmények általánosítását vizsgáltam, abban az esetben, ha minden minimális kvalifikált halmaz méretét legfeljebb 3-nak választjuk. Az ideális sémák vizsgálatában Seymour egy korábbi, matroidelmélethez kötődő, tiltott minor karakterizációs eredményére mutattam újabb alkalmazásokat. Az eredményeket konferencián ismertettem (12th Central European Conference on Cryptology) [7]. Ide kapcsolódik továbbá egy tisztán kombinatorikai hátterű feladat általánosítása, amelynek kriptográfiai alkalmazásai is vannak. A hipergráfok uniform teljes rész-hipergráfokkal történő particionálásáról szóló eredmény Erdős és Pyber egy gráfos eredményére ad új, konstruktív bizonyítást, valamint általánosítja azt. Ezen felül "sűrű" hipergráfokra egy erősebb állítást is bizonyít. Ezek felhasználásával új, az eddig ismerteknél jobb általános korlátokat adhatunk gráf és hipergráf alapú titokmegosztások hatékonyságára. A Csirmaz Lászlóval és Tardos Gáborral közös munka publikációként megjelent [3].

5. Utánpótlás-kutatóbázis

A kutatási feladatokon felül tevékenyen részt vettem az utánpótlás nevelésben is. Kettő, kriptográfiai témájú elektronikus jegyzet megírásában segédkeztem (Advanced Cryptography és Applied Cryptography Projects címmel), öt szakdolgozat témevezetője voltam/vagyok. A hallgatók egyike szeptembertől kezdi doktori tanulmányait a témavezetésemmel.

Hivatkozások

[1] B. Bakondi, P. Burcsi, P. Györgyi, D. Herskovics, P. Ligeti, D. A. Nagy, V. Villányi *A P2P Based Storage System with Reputation Points and Simulation Results*, Proc. of ICAI14, International Conference on Applied Informatics, megjelenés alatt.

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

[3] L. Csirmaz, P. Ligeti, G. Tardos *Erdős-Pyber theorem for hypergraphs and secret sharing*, Graphs and Combinatorics, (2014).

[4] P. Kasza, P. Ligeti, Á. Nagy *Siren: Secure Data Sharing Over P2P and F2F Networks*, Studia Math. Sci. Hun., elbírálás alatt

[5] P. Kasza, P. Ligeti, Á. Nagy *On a Secure Distributed Data Sharing System and its Implementation*, Annales Math. Inf., megjelenés alatt

[6] P. Ligeti *Matrix posets and automorphisms*, Discrete Mathematics, elbírálás alatt.

[7] P. Ligeti *On secret sharing and 3-uniform hypergraphs*, kézirat

[8] P. Ligeti, L. Mérai *Biztonságos árverező protokoll*, Alkalmazott Matematikai Lapok, elbírálás alatt.