Szakdolgozat kivonat

Némileg és teljesen homomorf titkosítás

Szögi Viktória Rózsa

Témavezető: Wettl Ferenc, Matematika Intézet, Algebra Tanszék

A kriptográfiában néhány éve kialakult egy új kutatási terület, ami a teljesen homomorf titkosítás köré épül. Napjainkban is nagyon sokan dolgoznak rajta, hogy használható eljárássá váljon.

A teljesen homomorf titkosítás fogalma már korábban is ismert volt, de 2009-ig nem sikerült megvalósítani. Craig Gentry doktori munkájában ért el áttörést a témában, és azóta is rengeteg fejlesztést hoztak létre, hogy minél hatékonyabban és biztonságosabban működjön.

A teljesen homomorf titkosítás során műveleteket végezhetünk a rejtjelezett szövegeken úgy, hogy ezek az eredeti üzeneten is végbemennek. Számos alkalmazása lehet, hiszen sok helyen fontos szempont, hogy ne kerüljenek információk az illetéktelenek kezébe. Ez a titkosítási eljárás pedig pont ezt teszi lehetővé, hiszen csak a titkosított adatokkal kell dolgoznunk, és eközben nem nyerünk információkat az eredeti üzenetekről.

A szakdolgozatom az ilyen módszerekről szól, ahol először az eljárás általános tulajdonságait és a megértéshez tartozó alapfogalmakat ismertetem. Majd mélyebben is megnézzük, hogy milyen a némileg homomorf séma, mivel ez átalakítható teljesen homomorffá. A későbbiekben tekintjük Craig Gentry és Shai Halevi némileg homomorf módszerét, aminek részletesen megnézzük a működését. Konstruálunk hozzá egy példát, ami segítheti a fogalmak megértését is.

Az utolsó fejezetben az első hatékonynak tekinthető teljesen homomorf titkosítási eljárást vizsgáljuk. Először Niegel P. Smart és Frederik Vercauteren némileg homomorf sémáját vizsgáljuk, amire szintén készítettünk egy szemléltető példát. Később átalakítjuk teljesen homomorffá, és megnézzük, hogy miért csak kis kódszövegre és kis kulcsra működik megfelelően.

Igyekeztünk egy átfogó képet adni erről az érdekes és friss titkosítási eljárásról. Bízunk benne, hogy a jövőben sikerül tökéletesíteni a módszert, és ezáltal hétköznapivá válhat a felhasználási területe, ezzel is segítve sokak munkáját, védelmét.

Budapest, 2015. május 22.