Izogénia Alapú Kriptográfia

Varga Dóra Kinga
Témavezető: Kiss Sándor

Az izogénia alapú kriptográfia viszonylag új és izgalmas területet jelent a tudományban, amely az elmúlt évtizedben kezdett terjedni és folyamatosan fejlődik napjainkban. Ezen terület jelentős előrelépést kínál a hagyományos kriptográfiai rendszerekhez képest, nagyobb biztonságot és hatékonyságot nyújtva. Gyakorlati alkalmazása egyre elterjedtebbé válik, és ígérete továbbfejlődést tartogat a jövőben. Diplomamunkám célja az volt, hogy részletesebben megismertessem és feltárjam ezt a területet.

Az első fejezetben bemutattam a fontosabb mérföldköveket és matematikai eredményeket, amelyek elengedhetetlenek voltak ahhoz, hogy az izogénia alapú kriptográfia létrejöhessen. Ezáltal áttekintést nyújtottam a terület fejlődéséről és az ahhoz vezető kulcsfontosságú lépésekről.

A következő lépésben a protokollok matematikai hátterének megértéséhez ismertettem a fontos definíciókat és tételeket. Ez segített megérteni a kriptográfiai protokollok alapját, és felkészíteni az ezekkel kapcsolatos elméleti részletek megértését.

A harmadik fejezetben bemutattam az elliptikus görbén alapuló Diffie-Hellman (ECDH), valamint az izogénia alapú Diffie-Hellman (SIDH) protokollt, mely kifejezetten szuperszinguláris görbéken alapul. Emellett bemutattam főbb, különböző változatait is ezen protokollnak, hogy átfogó képet kapjunk a lehetőségekről és alkalmazási területeiről. Ezen túlmenően, bemutattam egy új digitális aláírási sémát, mely az izogéniákra épül, ez pedig az SQISign protokoll, mely hatékony és biztonságos módszer az adatvédelem szempontjából.

Az utolsó fejezetben a prímgenerálás és prímkeresés módszereivel foglalkoztam. Az izogénia alapú kriptográfia területén az egyik kulcsfontosságú lépés a megfelelő prímek megtalálása és generálása. Ezek a prímek olyan speciális tulajdonságokkal rendelkeznek, amelyek lehetővé teszik a hatékony titkosítási és aláírási protokollok működését. Ebben a fejezetben bemutattam a Maurer-algoritmust, a PTE problémát, illetve annak megoldásaival való szita módszert, valamint a Dirichlet-tétel általi prímkeresést. Emellett ismertettem saját eredményeimet, amelyek magukban foglalják Maurer algoritmusát és a Dirichlet-féle prímkeresés programozását. Célom, hogy rávilágítsak ezeknek az algoritmusoknak a hatékonyságára és alkalmazhatóságára az izogénia alapú kriptográfiában.