Posudek oponenta diplomové práce

Název: Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves
Autor: Jan Oupický

Předložená práce prezentuje teorii supersingulárních eliptických křivek potřebnou k porozumění fungování algoritmu varianty Diffie-Hellmanova protokolu založeném na této třídě křivek (CSIDH a SIDH), které patří mezi nadějné kandidáty pro využití v postkvantové kryptografii.

Text kromě motivačního úvodu a závěru sestává ze sedmi sekcí. První dvě části shrnují terminologii a potřebnou teorii eliptických křivek. Zatímco první sekce obsahuje velmi hutný přehled dále využívaných faktů o grupové struktuře eliptických křivek a jejich isogeniích, druhá část detailně popisuje strukturu okruhu endoisogenií $\mathrm{End}(E)$ a (obecně nekomutativního) tělesa $\mathrm{End}^0(E) = \mathbb{Q} \otimes \mathrm{End}(E)$ eliptické křivky E především nad tělesy kladné charakteristiky. Třetí sekce přenáší pozornost čtenáře k okruhu endoisogenií komplexních křivek. K tomu účelu jsou připomenuty některé nástroje komplexní analýzy. Hlavním výsledkem této části práce je objasnění tranzitivní akce třídové grupy řádu v imaginárním kvadratickém tělese na množině j-invariantů, o níž se opírá algoritmus CSIDH. Stručná čtvrtá kapitola odhaluje způsob, kterým lze akci třídové grupy přeložit do situace eliptické křivky nad konečným tělesem. Pátá sekce je věnována konstrukci grafu isogemnií, což je orientovaný multigraf jehož vrcholy tvoří neizomorfní eliptické křivky a hrany jsou neizomorfní isogenie mezi nimi. Poslední dvě kapitoly se zabývají důkladným popisem algoritmů CSIDH a SIDH, diskusí otázky jejich klasické i kvantové bezpečnosti a u první z algoritmů jsou rovněž navržen prakticky použitelné hodnoty parametrů.

Téma je obtížné, třebaže velmi aktuální; algoritmus SIDH patří mezi finalisty třetího kola projektu Post-Quantum Cryptography Standardization, který pořádá NIST, a práce zabývající se primárně oběma algoritmy se do hlubšího vysvětlení jejich teoretického pozadí nepouštějí. Předložená práce vychází z několika zdrojů, první dvě kapitoly a kapitola čtvrtá se opírají především o dvě monografie J.H.Silvermana a lecture notes Andrew Sutherlanda a Aleše Drápala. Třetí sekce využívá vedle Sutherlandova textu rovněž monografii D.A.Coxe a pátá kapitola primárně čerpá z článku D.Jao, S.D.Millera a R.Venkantesana a textu C.Delfsové a S.Galbraitha.

Ačkoli je práce primárně kompilační a část tvrzení je přejata jako fakt bez důkazu, byl student nucen provést značné množství matematické práce, především vybrat tvrzení podstatná pro vysvětlení obou algoritmů a doplnit jejich důkazy o řadu netriviálních detailů. Výsledkem je poměrně rozsáhlý a obtížný, byť čtivý a poměrně dobře srozumitelný text. Po matematické ani jazykové stránce se mu nedá nic podstatného vytknout (drobné komentáře viz níže) a zjevně svědčí o autorově vhledu do zkoumané problematiky i o jeho schopnosti samostatné odborné práce.

Práce Jana Oupického *Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves* podle mého mínění úspěšně naplnila zadání a doporučuji ji uznat jako diplomovou.

Jan Žemlička
Katedra algebry
3.2.2022

Komentáře:

- s.4 - V alternativní definici *řádu* by bylo vhodné vysvětlit ztotožnění $\mathcal{O} \otimes \mathbb{Q} = \mathcal{R}$.

- s.12 - Není mi jasné, jak plyne bezprostředně z Theorem 7, kde se říká, že je $\mathrm{End}(E)$ charakteristiky 0, důsledek, že jde o obor, to vidím až například díky Theorem 11.

- s.19 - Argument důkazu Lemmatu 20, že $(\psi\tau) \otimes (ab) = 0$ implikuje $\psi\tau = 0$ nebo $ab = 0$ se nezdá být korektní (viz například $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$, tedy $1 \otimes_{\mathbb{Z}} 1 = 0$).

- s.73 - Literatura seřazená podle pořadí výskytu v textu je při počtu 23 položek podle mého mínění poněkud nepřehledná.