# Posudek vedoucího na diplomovou práci Jana Oupického nazvanou Teoretické základy kryptosystémů využívajících isogenie supersingulárních eliptických křivek

Cíl prácem bylo podat koherentní výklad systému CSIDH, který by přiblížil jak teoretická východiska, tak ryze kryptografické aspekty. Jde o nelehkou látku, která jde daleko za obsah přednášek o eliptických křivkách kursovní výuky.

Teoretické zdůvodnění účinnosti kryptosystému CSIDH se opírá o korespondenci mezi supersingulárními eliptickými křivkami nad prvočíselným tělesem a eliptickými křivkami nad komplexními čísly, jejichž okruh endomorfismů koresponduje s imaginárním kvadratickým číselným tělesem indukovaným daným prvočíslem. Tato korespondence poskytuje vzájemně jednoznačný vztah separabilních izogenií daného stupně.

Díky této korespondenci je možné využít klasické výsledky z teorie komplexních eliptických křivek popisující regulární působení třídové grupy daného celooboru (tedy řádu, anglicky order) na křivkách, jejichž okruh endomorfismů je tomuto celooboru roven. (Jde o křivky až na izomorfii, takže je lze reprezentovat $j$-invariantem.)

Na prvních padesáti stranách práce je shrnuto množství výsledků týkajících se kvadratických číselných těles, izogenií křivek, (včetně vlastností duálních izogenií, normy a stopy), a dále vztahu komplexních křivek a mříží. Zvláštní pozornost je věnována vlastnostem a charakterizacím supersingulárních křivek.

Mnohá tvrzení jsou podána i s důkazy, a mnohá bez důkazů. Víceméně je to tak, že zásadní tvrzení s obtížnými důkazy jsou citována, zatímco jejich vzájemné propojení je většinou dokázáno. Pro práci daného charakteru to považuji za správné řešení.

Samostatná kapitola je věnována teorii, o kterou se opírá Deuringova věta o zvedání (Deuring lifting theorem).

Kapitola pátá popisuje grafy isogenií. Je vysvětleno, proč jsou potřeba prvočísla $\equiv 11 \bmod 12$ a jaké jsou důvody toho, že z horizontálních izogenií lze sestavovat regulární grafy, které vykazují prvky náhodného chování. Poté je vyloženo, jak lze v případě konečných těles určitých charakteristik pro daný celoobor získat jeho regulární akci horizontálními izogeniemi, a to jak v případě obyčejných křivek, tak v případě supesingulárních křivek.

Tím se uzavírá teoretická část. Na 12 následujících stranách (kapitola šestá) je celkem zdařile vyložen systém CSIDH, včetně rozsáhlého příkladu a diskuse bezpečnosti jak klasické, tak kvantové. Posledních 5 stran, pokud nepočítáme závěr, je věnováno systému SIDH. Zde je výklad poněkud hutnější, ale věcně správný.

Hlavní přínos práce vidím v integraci výsledků z různých zdrojů, v jejich uspořádání a srozumitelné interpretaci. Autor práce doplnil některá tvrzení, která jsou snad špičkovým odborníkům zřejmá, ale bez kterých je pro ostatní porozumění funkčnosti systému velmi obtížné, například Tvrzení 42. Rozsah práce považuji za přiměřený. Sestupovat na další rovinu detailu by učinilo práci příliš rozsáhlou. V práci nejsou hluchá místa, organizace textu je příkladná, angličtina velmi dobrá, byť ne perfektní. Pokud by někdo plánoval poučenou implementaci jednoho z obou systémů, tak je předkládaná práce ideálním východiskem. Samostatný fakt, že autor zjevně teorii, kterou předkládá, porozuměl a je schopen ji poučeně reprodukovat, považuji za nadstandardní výkon.

Proto navrhuji, aby práce byla přijata a hodnocena stupněm *výborně,* třebaže neobsahuje výsledky, které bylo možno označit za nové.

Práce není bez chyb, ale chyb není mnoho. V počátečních kapitolách se vyskytují nejasnosti, kdy určitý pojem se definuje, ale pak se pojednává ve zúžené podobě, takže není jasné, co v danou chvíli platí. Třeba Theorem 6 je zjevně třeba chápat vzhledem ke krátkému tvaru Weierstrassovy rovnice, z kontextu to však úplně jasně nevyplývá.

Prohřešky proti angličtině jsou řídké. Poněkud kuriósní je obrat ‘This theorem completes our doubts about the correspondence between elliptic curves over $\mathbb{C}$ and lattices.’

V tvrzení označeném Claim 37 vypadl předpoklad, že jde o supersingulární křivku.

V kapitole 6 mi vadilo, že autor mluví o komponentě grafu, ale nemyslí tím souvislou komponentu. Snad proto jsem nepochopil, co přesně mínil posledním odstavcem podkapitoly 6.6. Budu rád, když toto během prezentace objasní.

Aleš Drápal

V Praze 4. února 2022