Jan Krhovják
Fakulta informatiky
Masarykova univerzita
Botanická 68a, 602 00 Brno

POSUDEK DIPLOMOVÉ PRÁCE

Datum: 14.9.2012

Student: Bc. Jakub Skalický
Vedoucí DP: Mgr. et Mgr. Jan Krhovják, Ph.D.
Oponent DP: prof. RNDr. Aleš Drápal, CSc., DSc.
Název: Efektivní aritmetika eliptických křivek nad konečnými tělesy

Zpráva:

Úvodem tohoto posudku bych rád poznamenal, že jakožto formální vedoucí práce (hlavním konzultantem byl Dr. Paul C. Leyland) jsem se k práci během jejího vytváření dostával až v posledních měsících. První ucelené verze textu také vznikly až na přelomu dubna/května 2012. S obsahem práce jsem i přesto po několika pročteních dobře obeznámen. Pro účely objektivního posouzení práce však poznamenávám, že detailní posouzení některých techničtějších důkazů stejně jako posouzení množství obsahu práce, které musel student nově nastudovat (ve srovnání s látkou standardně přednášenou na MFF UK), ponechávám plně v kompetenci oponenta práce.

Student se v diplomové práci zabývá efektivní aritmetikou eliptických křivek nad konečnými tělesy. První kapitola práce je věnována definicím základních algebraických pojmů vedoucích až k definici eliptických křivek. V samotném závěru kapitoly se student také (okrajově) dostává k aplikaci eliptických křivek v kryptografii a k případným dopadům použitých (konečných) těles na rychlost aritmetiky s eliptickými křivkami. V následující kapitole je popsán přechod od afinních k projektivním souřadnicím – student zde jasně demonstruje dopad takovýchto reprezentací bodů na rychlost základních operací s nimi. Závěrečná část práce je zaměřena na Edwardsovy křivky (obecné i binární) a zvláštní pozornost je věnována opět efektivitě základních operací s body na těchto křivkách.

K samotnému obsahu práce nemám mnoho zásadních výhrad – celkově je text dobře strukturován, jednotlivé kapitoly jsou dobře provázány, a je patrné, že student dané látce rozumí. Přínosem diplomanta je v práci zejména shromáždění poznatků o tématu z různých zdrojů a vzájemné srovnání efektivity jednotlivých základních (např. sčítání dvou bodů) a kryptografických (např. ECDSA-384) algoritmů pro různé reprezentace křivek. Práce s literaturou v první kapitole zpočátku sice pokulhává (na prvních 3–4 stránkách zde chybí zdroje odkud student základní definice a důkazy čerpal), avšak tento nedostatek je dále již napraven. Po gramatické a typografické stránce je práce jinak na výborné úrovni.

Dle mého názoru by však práci rozhodně prospěla i praktičtěji orientovaná část – např. kapitola věnovaná kryptografickým aplikacím (zaměřená více na problém diskrétního logaritmu, vybrané kryptosystémy atp.). V práci o eliptických křivkách bych pak také ocenil (alespoň v závěru) i explicitní zmínění hypereliptických křivek.

Hodnocení:

Předloženou práci i přes výše uvedené výtky doporučuji uznat jako diplomovou a navrhuji hodnocení stupněm **velmi dobře**.

Jan Krhovják