# OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Autor práce: Petr Vácha
Název: Kryptografické využití grupy kvadratických residuí
Vedoucí: Štěpán Holub

Předložená práce zkoumá strukturu grupy kvadratických zbytků, tedy grupy invertibilních prvků v $\mathbb{Z}_n$, které jsou modulo $n$ druhou mocninou, a následně strukturu z ní odvozené grupu znaménkových kvadratických zbytků. Získané strukturní výsledky jsou využity pro popis dvou asymetrických šifrovacích systémů. Pro každé 3-složené přirozené číslo $n$, které je součinem dvou různých prvočísel, je nejprve popsán jednoduchý kryptosystém na grupě kvadratických zbytků modulo $n$ a poté sice složitější, ale v praxi použitelnější ElGamalův kryptosystén na znaménkové grupě kvadratických zbytků modulo $n$. Obsahem závěrečné části práce je formalizace otázky bezpečnosti ElGamalova kryptosystému a následně důkaz, že se jedná o dostatečně bezpečný šifrovacího systému.

Text, který vychází z nedávného článku, je po jazykové a stylistické stránce pěkně zpracován. Číselně teoretické důkazy v druhé kapitole jsou velmi elegantní, výtku ovšem zaslouží, že z textu není jasné, odkud autor teorii čerpal, případně do jaké míry jsou prezentované důkazy výsledkem jeho vlastní práce. Je trochu škoda, že méně péče je při budování teorie věnováno řidčeji zkoumané avšak pro samotnou práci důležitější konstrukce grupy znaménkových kvadratických zbytků, výsledný text ovšem bezpochyby prokazuje autorovu schopnost samostatné práce s literaturou. Množství věcných chyb, nepřesností či překlepů, které oponent v textu postřehl, je přiměřené rozsahu textu (viz seznam níže).

Přes uvedené drobné výhrady doporučuji práci Petra Váchy *Kryptografické využití grupy kvadratických residuí* uznat jako bakalářskou a navrhuji ji ohodnotit známkou výborně.

v Praze 1.9.2010 Jan Žemlička

Seznam matematických nepřesností:

- s.10, ř.-10 - $0 + 1 \equiv 1$ (nikoli 0);
- s.16, ř.-2 - $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ (nikoli dvakrát $p$);
- s.18, Definice 2.5.1 - slova „odpovídá" a „reprezentujeme" jsou velmi vágní, bylo by mnohem jasnější, kdyby bylo uvedeno (buď v definici či následném komentáři), jak přesně prvky v dané množině reprezentujeme, resp. přesný předpis jak je zaváděná absolutní hodnota definována (tedy např. $|x| = x$ pro $x < \frac{n}{2}$ a $|x| = n - x$ pro $x > \frac{n}{2}$);
- s.18, ř.-5 - $G^+$ je sice podmnožinou, ale nikoli podgrupou $Z_n^*$ (operace násobení na $G^+$ a na $Z_n^*$ se neshodují), proto bychom měli ještě uvážit, že je operace na $G^+$ asociativní;
- s.20, ř.2 - zobrazení $\gamma$ není (multiplikativním) grupovým automorfismem, což nepotřebujeme, ani nedokazujeme, jedná se jen o bijekci.