Posudek vedoucího na bakalářskou práci Petra Váchy
Kryptografické využití grupy kvadratických residuí

Práce má dvě části. První představuje pasáže z teorie čísel potřebné pro kryptografický systém popsaný v části druhé.

Jazyková i matematická úroveň práce je vysoká, překlepů je málo (konkrétní výtky níže). Autor netriviální látku zjevně zvládl, oceňuji zejména samostatné řešení nejasnosti ohledně korekčního faktoru v odhadu pravděpodobnosti úspěchu útoku. Na pozadí tohoto celkově příznivého dojmu je možné formulovat následující výtky:

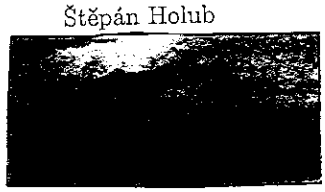
- Pasáž o Gaussových číslech v jednu chvíli – bod (v) Lemmatu 2.1.5 – začne používat isomorfie komplexních čísel a čísel komplexně sdružených, aniž by tato technika byla výslovně zmíněna a ospravedlněna. Bylo by přitom vhodné a užitečné již u definice normy upozornit, že $N(\alpha) = \alpha\overline{\alpha}$.
- Jak přesně z $p|(x-i)(x+i)$ plyne $p|i$? Argument se mi zdá příliš rychlý, je několik možností, jak implikaci odvodit.
- V Lemmatu 2.1.9 není vysvětleno, proč je řešení l rovnice $u + lx \equiv 0$ sudé.
- Práce obsahuje typické nadužívání důkazu sporem. Např. důkaz Lemmatu 2.3.1., kde jde o to ukázat, že $n = 1$, má strukturu

  Nechť $n > 1$.
  Přímý důkaz, že $n = 1$.
  Spor.
- Tvrzení 2.4.4 zamlčuje, že uvažujeme pravděpodobnostní algoritmy (což plyne pouze implicitně, jinak by tvrzení nedávalo smysl).
- Klíčový výklad o grupě znaménkových kvadratických zbytků je bohužel zamlžen přílišnou neformálností. Hlavní potíž je v tom, že se jasně nerozlišuje mezi běžnou absolutní hodnotou v $\mathbb{Z}$ a nově definovanou absolutní hodnotou v $\mathbb{Z}_n$. O ní by bylo především třeba dokázat, že je homomorfismem vůči násobení, což se předpokládá jako samozřejmost, zřejmě opět díky analogii k $\mathbb{Z}$.
- Násobení zleva není automorfismus, pouze bijekce (důkaz Lemmatu 2.5.7).
- Důkazu Tvrzení 3.3.3 by slušelo méně věrné kopírování článku, a více komentářů umožňujících vyvstat ideji důkazu.
- Zkratky jako RSA je třeba sázet pomocí makra, jinak se v matematickém textu "rozsypou".

Celkově považuji práci za zdařilou a plně splňující požadavky na bakalářskou práci.

Praha 5. září 2010

Štěpán Holub



Navrhuji výborně.