Posudek oponenta bakalářské práce

Název: Útok na Wieschebrinkovu verziu Niederreiterovho systému
Autor: Miloslav Homer

Shrnutí obsahu práce

Cílem práce bylo vysvětlit a implementovat útok na Wieschebrinkovu modifikaci už dříve prolomeného Niederreiterova kryptosystému. Text práce je rozdělen do čtyř kapitol. Zatímco první část zavádí potřebné pojmy z teorie samoopravných kódů, je druhá kapitola věnována postupně popisu McEliecova, Niederreiterova a Wieschebrinkovu schématu. Těžiště textu představuje třetí kapitola, která se zabývá samotným útokem založeným na odstranění náhodných sloupců z generující matice použitého kódu a Sidelnikova-Šestakovova útoku na Niederreiterův kryptosystém. Poslední kapitola obsahuje výsledky měření na implementaci útoku.

Celkové hodnocení práce

Téma práce. Vybudování matematického aparátu umožňující popis kryptosystému a vysvětlení útoku na něj i samotná jeho implementace byly značně netriviální úlohy, z nichž každá by podle oponentova mínění vystačila na bakalářskou práci. Zadání bylo studentem bezpochyby naplněno.

Vlastní příspěvek. Vedle implementace a měření, která na ní byla provedena, je nezpochybnitelným studentovým příspěvkem i pečlivé vysvětlení fungování algoritmu. Student se rovněž neúspěšně pokusil o exaktní důkaz pouze experimentálně potvrzovaného předpokladu, svoje úvahy na toto téma prezentoval alespoň ve formě rozsáhlého komentáře k hypotéze.

Matematická úroveň. Matematická úroveň práce je velmi dobrá, formulace jsou korektní a snadno srozumitelné.

Práce se zdroji. Text práce je harmonizovanou kompilací několika zdrojů, na nichž zjevně není formulačně příliš závislý.

Formální úprava. Text se velmi dobře čte a množství jazykových a stylistických nepřesností je zanedbatelné.

Připomínky a otázky

Žádné závažnější připomínky k předložené práci oponent nemá.

Závěr

Práci považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
1.9.2015