Posudek vedoucího bakalářské práce

Název: Korelační útoky
Autor: David Mařák

Shrnutí obsahu práce

Práce pojednává o korelačních útocích na proudové šifry. Po stručném úvodu následuje popis jednoduchých korelačních útoků na kombinační generátor uvádějící také jejich interpretaci pomocí lineárních kódů. Třetí kapitola za zabývá rychlými korelačními útoky a představuje algoritmy A a B z původního článku, ve kterém byly tyto útoky popsány. Závěrečná kapitola velice stručně zmiňuje některé vylepšení těchto útoků.

Celkové hodnocení práce

Téma práce. Téma práce a její náročnost jsou přiměřené pro bakalářskou práci. Zpracování vyžadovalo nastudování původních článků s využitím přehledu z dizertační práce F. Jönssona. Zadání práce bylo splněno, i když na detailnější popis modifikací rychlých korelačních útoků již nedošlo.

Vlastní příspěvek. Práce přehledová a neobsahuje vlastní příspěvek studenta.

Matematická úroveň. Dobrá.

Práce se zdroji. Všechny zdroje jsou správně citovány.

Formální úprava. Dobrá.

Závěr

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

Michal Hojsík
Katedra algebry
1.9.2015