Posudek

❑oponenta
❑bakalářské práce
Autor: Jakub Töpfer
Název práce: Rotační kryptoanalýza ARX šifer
Jméno oponenta: doc. RNDr. Jiří Tůma, DrSc

Matematická úroveň:
❑vynikající

Grafická, jazyková a formální úroveň:
❑vynikající

Výsledky:
❑původní i převzaté

Použité metody:
❑standardní

Aplikovatelnost:
❑přínos pro teorii

Věcné chyby:
❑téměř žádné

Tiskové chyby:
❑téměř žádné

Celková úroveň práce:
❑velmi dobrá

Práci
❑doporučuji
uznat jako bakalářskou. Návrh klasifikace přikládám na zvláštním papíru.

Připomínky a vyjádření vedoucího/oponenta:
V práci jsou studovány ARX šifry, tj. šifry, které jsou postavené na kombinaci modulárního sčítání, rotací, xorů a konstantních binárních vektorů. V první kapitole jsou uvedené základní výsledky o tom, kdy lze pomocí těchto funkcí vyjádřit jakoukoliv booleovskou funkci. Ve druhé kapitole je uvedena myšlenka rotační kryptoanalýzy takových šifer. Tato metoda je pak použita ve třetí kapitole na šifru Treefish a na šifry TEA a XTEA. V případě posledních dvou šifer je založena na vlastních výsledcích autora. V poslední kapitole je uvedena myšlenka rotačního rozpínavého útoku a její použité na Treefish.

Práce je napsána přesným matematickým jazykem prakticky bez jakýchkoliv chyb nebo překlepů. Prokazuje výborné matematické schopnosti autora. Jediným důvodem, proč práci celkově nehodnotím jako vynikající, je absence výrazného vlastního přínosu.

K výsledkům první kapitoly mám pouze jeden dotaz. Do jaké míry jsou výsledky první kapitoly závislé na charakteristice 2?

Místo, datum, podpis oponenta: Praha 14.6.2012.

Jiří Tůma