Posudek oponenta k bakalářské práci
Cube Attacks
Josefa Bárty

Předložená práce rozvíjí techniku takzvaných krychlových útoků, které představili I. Dinur a A. Shamir. Cílem útoku je odhalit pomocí různých voleb inicializačního vektoru tajný klíč proudové šifry nebo jeho část. Základní myšlenkou je převést booleovské funkce reprezentující výstup proudové šifry chápané jako polynomy ve veřejných a tajných proměnných na polynom, který bude lineární v tajných proměnných. Autor navrhl nový postup pro tuto linearizaci a experimentálně ho otestoval na zkrácené verzi šifry Trivium. Verze linearizace označená jako TC2 se v určitém ohledu ukázala lepší než původní postup.

Práce je sepsána velmi srozumitelně, nepochopil jsem ale sekci 3.2. Předpokládám, že pro Trivium 8 lze spočítat polynomy $p_i(X, Y)$ explicitně a s touto reprezentací se při experimentu pracuje. Zdá se mi, že cílem této sekce bylo vysvětlit, jak by vypadal útok, pokud polynom $p_i(X, Y)$ neznáme, pouze lze získat funkční hodnoty různými volbami Y, jak je tomu u klasického Trivia.

Práce dále obsahuje několik drobných nedostatků.

- V Definici 2.3.1. není jasné, co znamená $p_J(X, Y = (1, \ldots, 1))$
- Důkaz Tvrzení 2.4.2. by se měl napsat pečlivěji. Představme si polynom $x_1y_1 + x_1y_1y_2$ pro $J = \{1, 2\}$. Pokud bychom dosadili $y_1 = y_2 = 1$, jak navrhuje důkaz, dostaneme nulový polynom.
- Důkaz Tvrzení 2.4.6. Logická formule je poněkud podezřelá - je kvantifikována proměnná J, která se ve zbylé části formule nevyskytuje. Tvrzení 2.4.6. vede k tomu, že pro T-linearizovatelný polynom p existuje $a \in \mathbb{F}_2^m$ tak, že $p|_a$ je lineární polynom z $\mathbb{F}_2[X]$. Zdá se tedy, že Definici 2.4.1 by šlo zjednodušit.
- V Příkladu 2.5.3 vypadla pro T-linearizaci podmínka $y_1 = 0$.
- Optimalizační část 2.5.1. by bylo podle mě potřeba ještě promyslet. U Tvrzení 2.5.10. se mi zdá, že člen, který proklouzne do superpolynomu při zmenšení J na J', by ještě nutně nemusel zkazit $T1$-linearizovatelnost superpolynomu. Dále pokud máme $T2$-maxterm kandidáta a zmenšíme J na J' (jako v definici 2.5.14), automaticky se zvětší stupně členů $y_{J''}x_I$ v $H_{p_{s(J')}}$ (přibude $y^{J \setminus J'}$), což často povede ke ztrátě $T2$-linearizovatelnosti.

Celkově se mi práce líbí, považuji ji za zajímavou a přínosnou. Práci doporučuji uznat jako bakalářskou s hodnocením *výborně*.

V Hradci Králové, 28. 8. 2014

Pavel Příhoda