Vyjádření školitele k disertační práci Daniela Joščáka

Využití algebraických a kombinatorických metod při studiu hašovacích funkcí

Daniel Joščák zahájil doktorské studium v roce 2006/07. Na počátku studia se věnoval tehdy velice aktuálnímu výzkumu kolizí v hašovacích funkcích založených na Merkle-Damgardově konstrukci. Výsledkem tohoto výzkumu byly tři články přijaté na významných mezinárodních kryptologických konferencích. Již tyto tři články by bohatě postačily k úspěšné obhajobě doktorské disertace.

Nicméně Daniel Joščák začal brzy pracovat na plný úvazek a doktorskou disertaci tehdy nepředložil. Nakonec ji předkládá až nyní, doplněnou o úvodní teoretickou kapitolu o rovnicích založených na kombinaci modulárního a binárního sčítání vektorů nad dvouprvkovým tělesem, nazývané v práci AX-rovnice. Výsledky této kapitoly sice ještě nebyly publikovány, z dlouhodobé perspektivy je ale považuji za nejpřínosnější. Vytvářejí totiž teoretický rámec pro studium pravděpodobností, se kterou jsou rovnice splněné. Na odhadu a nezávislosti těchto pravděpodobností je založena diferenciální kryptoanalýza často používaných základních kryptologických konstrukcí. Navíc výsledky využívají pouze základní poznatky z lineární algebry a půjdou snadno implementovat za použití existujících knihoven pro lineárně-algebraické výpočty nad dvouprvkovým tělesem.

Samotné výsledky druhé kapitoly jsou již publikovatelné, protože Věta 1.14 pokrývá mnoho v literatuře existujících výsledků o AX-rovnicích založených na ad hoc přístupech, a obsahuje ucelenou metodu, jak tyto výsledky tohoto typu získat pro širokou třídu AX-rovnic. Nicméně v první kapitole je také naznačena řada možných směrů jak teorii AX-rovnic dále rozvíjet a jsem přesvědčen, že další rozvinutí výzkumu v naznačených směrech přinese výsledky, které ovlivní diferenciální kryptoanalýzu v mezinárodním měřítku.

V Praze, 26.8.2015

Jiří Tůma