MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

21. června 2021

Posudek vedoucího bakalářské práce Petra Sedláčka

Práce kolegy Sedláčka s názvem „Limitace nekomprimovatelných kódování“ se zabývá následující otázkou v teoretické kryptografii: *Lze konstruovat netriviální schémata pro nekomprimovatelná kódování s bezpečností proti výpočetně neomezeným útočníkům?* Tento problém byl zdánlivě vyřešen v práci Morana a Wichse (Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference), jež nekomprimovatelná kódování definovala. Moran a Wichs v jejich článku přednesli ideu důkazu, kterou se snaží zdůvodnit, že netriviální nekomprimovatelná kódování s takto silnou bezpečnostní zárukou neexistují. Tímto negativním výsledkem pak zdůvodňují nutnost použití výpočetních předpokladů v jejich konstrukcích nekomprimovatelných kódování.

Kolega Sedláček však nalezl v argumentu Morana a Wichse zásadní nedostatky, které ve své práci explicitně popisuje. Ve zbytku práce poté předkládá úplný formální důkaz tohoto výsledku. Ukazuje tedy, že netriviální nekomprimovatelná kódování nemůžou být bezpečná, pokud je útočník výpočetně neomezený.

Hlavní silné stránky práce jsou zejména:

1. Práce řeší přirozený otevřený problém o novém typu kryptografických schémat. Hlavní výsledek pokrývá širokou třídu schémat pro nekomprimovatelná kódování, která jsou pravděpodobnostní a mohou také chybovat. Autor tedy řeší otázku, kterou se práce zabývá, v obecnosti pro všechny zajímavé parametry uvažovaných schémat.

2. Práce je formálně na velice kvalitní úrovni. Vzhledem k tomu, že kolega Sedláček dokazuje negativní výsledek pro tento typ schémat, je formální stránka práce zásadní. Práce však nutnou úroveň formálnosti rozhodně splňuje.

3. Důkaz hlavního tvrzení je představen v sérii kroků, které vylučují postupně se zvětšující třídy uvažovaných schémat. Tento rozvoj myšlenek důkazu činí práci přístupnější čtenářům, kteří nejsou nutně s oblastí práce detailně seznámeni. Formální definice bezpečnostních experimentů a použitou notaci autor také doplnil ilustracemi, které čtenáři značně ulehčují orientaci v myšlenkách důkazu.

Jako menší nedostatek bych uvedl, že je text práce v poslední kapitole značně lakonický. Obzvláště v kapitole 4.3 prezentující důkaz nejobecnější verze uvažovaného negativního výsledku by mohla posloupnost technických lemmat být více okomentována s důkladnějším vyzdvižením hlavních myšlenek důkazu.

Kolega Sedláček s prací získal třetí místo v letošním ročníku soutěže SVOČ, kde byla hodnocena mezi dalšími bakalářskými i diplomovými pracemi. I přes zmíněné drobné nedostatky v prezentaci práci považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Mgr. Pavel Hubáček, Ph.D.

Informatický ústav Univerzity Karlovy
Malostranské nám. 2/25, 118 00 Praha 1
telefon: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz