MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

4. září 2023

Věc: posudek vedoucího práce Bc. Petra Sedláčka "Security of Trapdoor Permutations under Preimage Leakage"

Kolega Sedláček ve své práci studuje bezpečnost permutací se zadními vrátky v modelu, kde útočník zná kromě hodnoty určené k invertování také nějakou dodatečnou informaci o hledaném předobraze. Tento kryptografický model je motivován heuristickými aplikacemi permutací se zadními vrátky a domněnkou o optimální bezpečnosti RSA permutace v tomto modelu ze článku van Dijka a kol. z ACM CCS 2012.

Po krátkém úvodu a představení základních definic práce představuje aplikace bezpečných permutací v tomto modelu pro konstrukce nekomprimovatelných kódování. Hlavní výsledek práce je popsán v poslední kapitole, kde autor analyzuje bezpečnost náhodných permutací se zadními vrátky. Autor aplikoval techniku Gennara a kol. (SICOMP 2005), jež omezuje invertovatelnost náhodné funkce její komprimovatelností. Důkaz Gennara a kol. autor zobecnil a ukázal, že obdobné výsledky platí i pro invertování s dodatečnou informací o předobraze.

Výsledky práce Petra Sedláčka mě velmi potěšily. Práce předkládá první teoretické zdůvodnění domněnky od van Dijka a kol., což by v budoucnu mohlo vést k praktickým dokazatelně bezpečným protokolům pro replikované ukládání dat ze standardních kryptografických předpokladů. Několik nedávných prací v teoretické kryptografii tento problém intenzivně studovalo, ale aktuální dokazatelně bezpečné protokoly nelze v praxi aplikovat kvůli jejich výpočetní náročnosti. Samotná práce je po formální stránce důkladná a všechny nové výsledky jsou pečlivě dokázány. Styl práce je spíše lakonický a čtenáři, který s oblastí není seznámen, by pravděpodobně pomohlo rozšíření doprovodného textu k hlavním definicím a větám. Vzhledem k tomu, že autor primárně prezentuje nové výsledky, to však není zásadním nedostatkem.

Práci doporučuji k obhájení jako diplomovou.

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