# Posudek

❑vedoucího ❑**oponenta**
❑**diplomové** ❑bakalářské práce
Autor/Autorka: Rudolf Barczi
Název práce: Důvěryhodnost prokazatelně bezpečné kryptografie
Jméno oponenta: Daniel Joščák

Matematická úroveň:
❑vynikající ❑**velmi dobrá** ❑průměrná ❑podprůměrná ❑nevyhovující

Grafická, jazyková a formální úroveň:
❑**vynikající** ❑velmi dobrá ❑průměrná ❑podprůměrná ❑nevyhovující

Výsledky:
❑originální ❑původní i převzaté ❑**netriviální kompilace** ❑citované z literatury ❑opsané

Použité metody:
❑nestandardní ❑**standardní** ❑obojí

Aplikovatelnost:
❑**přínos pro teorii** ❑přínos pro praxi ❑přínos pro praxi i teorii ❑bez přínosu ❑nedovedu posoudit

Věcné chyby:
❑**téměř žádné** ❑vzhledem k rozsahu a pojednávanému tématu přiměřený počet ❑méně podstatné četné ❑závažné

Tiskové chyby:
❑**téměř žádné** ❑vzhledem k rozsahu a pojednávanému tématu přiměřený počet ❑četné

Celková úroveň práce:
❑**vynikající** ❑velmi dobrá ❑průměrná ❑podprůměrná ❑nevyhovující

Práci
❑**doporučuji** ❑nedoporučuji
uznat jako diplomovou. Navrhuji ohodnocení známkou: výborně.

Připomínky a vyjádření vedoucího/oponenta:

Diplomová práca sa zaoberá problémom dokázateľnej bezpečnosti v kryptografii na názornom príklade dôkazu bezpečnosti schémy RSA-OAEP.

Po úvodných definíciách autor v druhej časti podrobne rozoberá a vysvetľuje kontroverzný pôvodný dôkaz z roku 1994 a opravený dôkaz z roku 2004. Ukazuje v čom spočívajú argumenty proti používaniu (resp. používaniu nesprávnym spôsobom) ideálnych prvkov ako sú náhodné orákulá v dôkazoch. Zároveň ukazuje, že takýto dôkaz má predsa istú

vypovedaciu hodnotu. Predovšetkým opravený dôkaz bezpečnosti RSA-OAEP považujem za mimoriadne technicky náročný a oceňujem autorovu snahu o čo najpochopiteľnejšie a najpresnejšie vysvetlenie a podanie. To sa mu z môjho pohľadu podarilo dosiahnuť.

V tretej časti práce autor popisuje praktické aspekty bezpečnosti a vysvetľuje problém nedostatočnej priliehavej redukcie a teda faktu, že uvedený dôkaz bezpečnosti RSA-OAEP je praktický až od istého rádu (4096). Pre najčastejšie používané RSA s modulom dĺžky 1024 a 2048 bitov nemá dôkaz žiadny vypovedajúci charakter vďaka odhadom zložitosti efektívnych algoritmov pre faktorizáciu takýchto modulov. V tejto časti autor správne upozorňuje aj na reálne problémy spojené s implementáciou RSA-OAEP.

Predposledná štvrtá časť práce podáva problematiku bezpečnosti RSA-OAEP v štandardnom modeli. Spracováva nedávny dôkaz z práce [12] o nemožnosti existencie dokázateľne bezpečného kryptosystému s verejným kľúčom a náhodným dopĺňaním v štandardnom modeli. Následne prezentuje pozitívny dôkaz o slabej neohybnosti pseudonáhodnými generátormi inštancializovanej varianty OAEP v štandardnom modeli a techniku nahrádzania náhodných orákulí za pseudonáhodné generátory. Túto časť práce a autorovu snahu o čo najjasnejšie vysvetlenie hodnotím veľmi kladne vzhľadom na rozsiahlosť, náročnosť a rôznorodosť prác, z ktorých autor čerpal.

V závere autor výstižne sumarizuje problémy dôkazov v oboch modeloch a uvádza ich klady a zápory.

Prácu ako celok hodnotím veľmi pozitívne. Dá sa jej vytknúť absencia vlastných výsledkov a zriedkavé preklepy, ktoré však nijak nebránia čitateľnosti a pochopeniu textu. Autor v práci ukázal schopnosť naštudovania technicky náročných odborných článkov a dôkazov ako aj orientáciu v problematike dokazovania bezpečnosti v štandardnom modeli aj v modeli s náhodným orákulom. Práca je výbornou kompiláciou článkov z odboru dokázateľnosti bezpečnosti, ktorá v českej či slovenskej literatúre, podľa mojich znalostí, nemá obdobu a napomáha pochopeniu danej problematiky.

V Praze, 14. 9. 2009