POSUDEK VEDOUCÍHO NA BAKALÁŘSKOU PRÁCI
MONIKY SAYEDOVÉ
NOVÁ VARIANTA DIFFIE-HELLMANOVA PROBLÉMU

Práce popisuje kryptografické protokoly založené na zdvojeném Diffie-Hellmanovu problému. Tato úprava standardního primitivu byla navržena v článku z roku 2009 a díky elegantnímu „trapdoor testu“ zesiluje jeho bezpečnost. Podstatou zesílení je možnost simulovat rozhodovací orákulum, takže protokoly jsou automaticky bezpečné i proti útočníkům s rozhodovacím orákulem, zatímco v případě jednoduchého Diffie-Hellmanovu problému je odolnost vůči takovému útočníkovi (tzv. silný DH předpoklad) za současného stavu vědomostí nutné považovat za silnější než odolnost proti útočníkovi bez rozhodovacího orákula (obyčejný DH předpoklad).

Je škoda, že studentka tuto základní myšlenku celého článku, a tím i celé své práce, nedokázala dostatečně jasně zdůraznit ani v abstraktu, ani v úvodu a závěru své práce. Bylo by proto žádoucí, aby se to podařilo při obhajobě.

Jinak je ovšem práce srozumitelná a kultivovaná jazykově i matematicky a ukazuje, že studentka problematice porozuměla. Charakter práce je kompilační, k plné rekonstrukci důkazů bylo ale nutné srovnat dvě varianty původního článku, ve kterých autoři sami zjevně hledají nejvhodnější formu výkladu, a doplnit některá vysvětlení nebo nevyslovené předpoklady.

Práce splňuje požadavky kladené na bakalářskou práci a doporučuji ji k obhajobě.

Praha 15. června 2012 Štěpán Holub