**POSUDEK OPONENTA NA DIPLOMOVOU PRÁCI**
**ĽUBICE JANČOVÉ**
***EFFECTIVITY AND LIMITATIONS OF HOMOMORPHIC SECRET SHARING SCHEMES***

Práce se zabývá homomorfním sdílením tajemství založeném na problému distruovaného diskrétního logaritmu. Kromě popisu tématu obsahuje modifikaci dvou výsledků z existujících literatury. Prvním z nich je adaptace odhadu pravděpodobnosti úspěšného útoku na problém distribuovaného diskrétní logaritmu s přípravným výpočtem, což je adaptace analogického výsledku pro nedistribuovanou verzi problému. Druhým výsledkem je podobná adaptace kryptografického schématu Joyeho a Liberta na homomorfní sdílení tajemství.

Práce je napsána dobrou angličtinou a velmi pečlivě, prakticky bez překlepů. Ocenit je možné zejména přehledné zavedení kryptografických pojmů, tradičně značně náročných na rigorózní zápis. Styl prezentace je podobný odborným článkům, na studentskou práci je až neobvykle neosobní. Uvedené modifikace výsledků z literatury jsou poměrně přímočaré, nicméně jsou netriviální. Potvrzují suverénní zvládnutí obsahu modifikované látky a formulačně jsou samostatné a na předloze nezávislé.

Matematická a kryptografická úroveň odpovídá magisterské práci. Zadání bylo splněno.

Náměty k obhajobě:

- Na str. 9 se říká, že oběma hráčům je známa reprezentace grupy. Jak může taková reprezentace vypadat, ve srovnání s generickým modelem?
- Je možné nějak okomentovat bezpečnost modifikovaných bezpečnostních předpokladů `k-QRm`, `k-SJSm` a `k-dRI` ve vztahu k předpokladům původním.

Jedná se o kvalitní práci, kterou doporučuji přijmout jako diplomovou.

Praha 5. února 2022 Štěpán Holub