Oponentský posudek diplomové práce

**Autorka práce: Bc. Romana Linkeová**
**Název: Problém batohu a jeho aplikace**
**Vedoucí: doc. Mgr. Pavel Příhoda, Ph.D.**

V předložené práci Romany Linkeové je představeno několik asymetrických kryptosystémů založených na různých variantách $\mathcal{NP}$-úplného problému, který je znám pod názvem problém batohu.

Práce vedle stručného úvodu a závěru sestává ze čtyř částí. Zatímco první kapitola zavádí potřebnou terminologii teorie grafů a teorie složitosti, druhá kapitola představuje několik variant samotného problému batohu včetně důkazu jeho $\mathcal{NP}$-úplnosti. Centrální místo zaujímá v práci rozsáhlá třetí část, která je věnována analýze Merkleova-Hellmanova kryptosystému a především analýze kryptosystému založenému na problému maticového 0-1 batohu. Poslední, čtvrtá část práce podává podrobný přehled dalších kryptosystémů založených na problému batohu, konkrétně kryptosystém založený na problému kvadratického batohu, kryptosystém s pravděpodobnostním šifrováním, které nahrazuje zadní vrátka, a hybridní kryptosystém, který vedle problému batohu využívá problému diskrétního logaritmu.

Jak dosvědčuje rozsáhlý seznam použité literatury, nezanedbatelnou část textu tvoří podrobná a důkladně zpracovaná kompilace rozsáhlého souboru literatury. Hlavním výsledkem práce je ovšem návrh a kryptoanalýza kryptosystému, který se opírá o maticovou verzi problému 0-1 batohu. Kvalitu tohoto výsledku nesnižuje ani fakt, že byly využity vesměs známé či analogické postupy.

Text je napsán přehledně a velmi pečlivě. Po matematické ani jazykové stránce se mu nedá nic podstatného vytknout a velmi dobře se čte. Jak již bylo zmíněno, práce obsahuje vedle velmi kvalitní kompilační části zajímavé původní výsledky a zjevně svědčí o autorčině vhledu do zkoumané problematiky i o její schopnosti samostatné odborné práce.

Práce Romany Linkeové *Problém batohu a jeho aplikace* bez pochyby naplnila zadání a doporučuji ji uznat jako diplomovou.

v Praze 5.9.2017 Jan Žemlička