Posudek vedoucího diplomové práce
Problém batohu a jeho aplikace
Romany Linkeové

Problémem batohu rozumíme následující problém. Pro danou posloupnost přirozených čísel $a_1, \ldots, a_n$ a $s \in \mathbb{N}$ chceme najít $s_1, \ldots, s_n \in \{0, 1\}$ tak, aby $\sum_{i=1}^{n} s_i a_i = s$. O rozhodovací verzi tohoto problému (tj. chceme zjistit, zda má tato úloha řešení) je známo, že je NP-úplný. Tento fakt vedl řadu autorů k návrhu kryptografických schémat, která by byla na problému batohu založena. Nejznámější je asi Merkle-Hellmanův kryptosystém, jehož základní varianta byla prolomena Shamirem již v roce 1984. Z matematického hlediska jsou útoky na Merkle-Hellmanův systém zajímavé, zejména pak pozdější útoky A. Odlyzka a dalších, které využívají LLL redukci mřížky.

Předložená práce má 4 kapitoly, první z nich je soupis používaných pojmů a vět. Druhou kapitolu tvoří důkaz NP-úplnosti rozhodovacího problému batohu, přesněji redukce problému obarvitelnosti grafu na problém batohu.

Třetí kapitola se zabývá zejména maticovou obdobou Merkle-Hellmanova kryptosystému. Původní motivace pro tuto variantu byla snaha navrhnout kryptosystém, který by mohl být teoreticky bezpečný v tom smyslu, že pokud bychom uměli generovat těžké problémy batohu, uměli bychom vyrobit bezpečný kryptosystém. Později jsme si uvědomili, že maticový problém batohu nelze (z hlediska bezpečnosti) uvažovat jako 4 oddělené problémy batohu.

V práci je provedena kryptoanalýza základního (nezmoduleného) kryptosystému převedením problému maticového batohu na problém hledání vnitřku kužele v $\mathbb{R}^4$ (sekce 3.4.1), o kterém je známo, že jde o úlohu řešitelnou v polynomiálním čase.

Hlavní část práce je pak sekce 3.4.2, kde je adaptován útok Lagariase a Odlyzka na problém batohu s nízkou hustotou na maticový kryptosystém. Přestože se jedná o poměrně přímočarou modifikaci, studentka musela pochopit práci Lagariase a Odlyzka poměrně do hloubky, také si všimla dvou drobných nesrovnalostí v původním článku.

Kromě toho je v této kapitole představen útok na Merkle-Helmanův kryptosystém s velice nevhodnými parametry. Touto metodou je odhlalen soukromý klíč z příkladu uvedeného v knize N.P. Smart: The Algorithmic Resolution of Diophantine Equations, str. 81.

Čtvrtá kapitola měla být matematicky nejzajímavější, bohužel na konstrukci hashovacích funkcí z kompaktních batohů již nezbyl čas. Místo toho byl zařazen přehled několika publikovaných kryptosystémů a útoků na ně.

Práci považuji za zdařilou, první tři kapitoly mají vysokou kvalitu i po formální stránce, čtvrtá by ještě potřebovala trochu vylepšit. Studentka zpracovala velké množství literatury, takže z práce se lze dozvědět i řadu zajímavých informací o problému batohu, které nejsou pro tuto práci potřeba, ale při pokusech o návrh kryptosystému je o nich dobré vědět.

Určité výhrady bych kromě Algoritmu 3 a důkazu konvergence na straně 33 měl ještě sekci 3.4.1. Vzhledem k podrobnosti, s jakou je kapitola 3 napsána, by neškodilo rozebrat, jak přesně Větu 11 využijeme. Podobně by asi bylo vhodné doplnit nějaký závěr k Větě 16 v sekci 3.4.2.

Předložená práce splnila zadání, doporučuji ji proto uznat jako práci diplomovou.

V Praze, 6. 9. 2017

Pavel Příhoda