Posudek vedoucího diplomové práce
Důkazy bezpečnosti hashovacích funkcí
Marka Zpěváčka

Důležitým aspektem mřížové kryptografie je možnost dokazovat bezpečnost některých kryptografických konstrukcí pomocí obtížnosti nejtěžších instancí určitých výpočetních problémů. První takovou konstrukci publikoval M. Ajtai v roce 1996, když ukázal, že pomocí orákula hledajícího kolize v určité množině hashovacích funkcí by bylo možno sestrojit efektivní algoritmus pro hledání krátké báze mříže (viz Věta 19 a sekce 3.2 předložené práce). Tento výsledek ještě nelze považovat za optimální, protože aproximační faktory pro problém krátké báze vyjdou příliš velké, respektive o odpovídajícím problému krátké báze není známo, zda je NP-těžký.

Na Ajtaiův článek navazuje řada prací, které vylepšují aproximační faktory nebo dávají efektivnější kryptografické konstrukce. Vlastní článek je ale obtížně srozumitelný. Prvním úkolem kolegy Zpěváčka měla být detailnější a matematicky korektní prezentace tohoto článku. Na ni měla navázat rešerše existujících konstrukcí hashovacích funkcí s uvedeným typem důkazu bezpečnosti a případně pokus o nějaký vlastní návrh.

Ukázalo se, že vlastní přepsání Ajtaiova výsledku je poměrně náročný úkol. Přestože bylo možné sledovat hlavní myšlenky důkazu, jednotlivé detaily bylo třeba často výrazně upravit či celé vymyslet. Z tohoto důvodu je kapitolka o hashovacích funkcích velice stručná, přesto považuji odvedené množství práce za dostatečné.

Zkontrolovat korektnost všech detailů v práci není úplně snadné, zejména odhad pravděpodobnosti selhání Algoritmu 5 se obtížně čte. Závažnějších nedostatků jsem si ale nevšimnul. K úplné spokojenosti s důkazem by bylo ještě třeba dořešit 'bez újmy na obecnosti $k = m$' na straně 28 a aplikaci lemmatu 14 na straně 31. Dále se mi zdají některé pasáže týkající se odhadů složitosti dost stručné (minimálně ve srovnání se zbytkem práce). Kromě toho, některé formulace by měly být pečlivější: definice postupných minim na straně 9, kolmost vektorů $\mathbf{d}_i$ na straně 12, omezení M v algoritmu 3, aby byl polynomiální.

Celkově si ale myslím, že student splnil zadání práce, kromě projasnění Ajtaiova článku též provedl diskusi aproximačních faktorů, které tato metoda poskytuje. Předloženou práci proto navrhuji uznat jako práci diplomovou.

V Praze, 5. 6. 2019

Pavel Příhoda