POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Název: Moderní aplikace zero-knowledge protokolů
Autor: Tomáš Krňák

Shrnutí obsahu práce

Tato práce seznamuje s kryptografickými protokoly typu zero-knowledge succinct non-interactive argument of knowledge (zkráceně zkSNARK) a jejich aplikacemi v kontextech decentralizovaných kryptografických měn. První část představuje definici protokolů zkSNARK a popisuje specifickou konstrukci z článku Ben-Sasson et al. z konference CRYPTO 2013. Tato konstrukce sestává z několika netriviálních kroků, které kombinují techniky využívané v literatuře o probabilistically checkable proofs a speciální šifrovací schémata s takzvanou linear-only vlastností. Druhá část práce popisuje použití protokolů zkSNARK pro zajištění anonymity transakcí v decentralizovaných kryptografických měnách a navrhuje nový typ elektronického podpisu nazvaný „síťový podpis".

Celkové hodnocení práce

Téma práce. Téma práce vyžadovalo nastudování odborných článků, zkompilování detailů konstrukce z několika článků a doplnění částí detailů důkazů. Text rozhodně pokrývá téma práce, a tak splňuje zadání práce.

Vlastní příspěvek. Hlavním vlastním příspěvkem autora práce je definice „síťového podpisu", který zobecňuje schémata elektronického podpisu známé jako ring signatures. V práci je také nastíněno, jak lze síťový podpis zkonstruovat právě pomocí zkSNARKs a jaké aplikace by tento nový kryptografický objekt mohl mít v kontextu reputačních systémů.
Za další vlastní přínos považuji samostatné nastudování konstrukcí protokolů zkSNARK z článků a jejich přehledné představení. Student dokonce zjednodušil jeden z kroků v popsané konstrukci protokolů zkSNARK z lineárních probabilistically checkable proofs.

Matematická úroveň. Matematická úroveň práce je velmi dobrá a formulace jsou korektní.

Práce se zdroji. Práce jasně odkazuje na použité zdroje a formulace v textu jsou na zdrojích nezávislé.

Formální úprava. Formální úprava práce je na odpovídající úrovni. Drobné jazykové nedostatky jsou přiměřené rozsahu práce.

Připomínky a otázky

Mé připomínky a otázky, které jsem v měl v průběhu konzultací k pracovním verzím textu student úspěšně zapracoval do odevzdané verze práce.

Závěr

Práci považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Mgr. Pavel Hubáček, Ph.D.
Informatický ústav Univerzity Karlovy
12. června 2019