Posudek oponenta bakalářské práce

Název práce:	Moderní aplikace zero-knowledge protokolů
Autor:	Tomáš Krňák
Rok odevzdání:	2019

Shrnutí obsahu práce

Práce zkoumá konstrukci a aplikace kryptografických protokolů typu zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK). To jsou, zhruba řečeno, neinteraktivní protokoly, v nichž se jedna strana snaží přesvědčit druhou, že zná informaci s nějakou vlastností, aniž by o ní cokoliv dalšího prozradila.

Konstrukce zk-SNARKů vychází z článku Ben-Sasson et al. Je založena na kombinaci několika netriviálních technik, zejména na čistě lineárních pravděpodobnostně ověřitelných důkazech.

Aplikační část práce popisuje použití zk-SNARKů k anonymizaci transakcí v kryptoměnách a v reputačních systémech.

Celkové hodnocení práce

- *Téma práce* patří mezi náročnější a vyžaduje pochopení pokročilých kryptografických konstrukcí a zkombinování výsledků z více zdrojů. Práce splňuje zadání.
- *Vlastní příspěvek* autora spočívá nejen v souhrnném představení zk-SNARKů, ale také v konstrukci „síťového podpisu“ zobecňujícího ring signatures a návrhu jeho použití v reputačních systémech.
- *Matematická úroveň* práce je výborná. Tvrzení jsou exaktně formulována a dokázána.
- *Práce se zdroji.* Použité zdroje jsou správně citovány.
- *Formální úprava.* Práce obsahuje poměrně velké množství překlepů a typografických chyb, které nicméně nekladou vážné překážky pochopení textu. Ocenil bych, kdyby se autor tak striktně nedržel anglické terminologie a pokusil se chybějící české termíny zavést.

Přípomínky a otázky

- V některých definicích (například když se definuje SNARG) není jasné, zda uvažované algoritmy jsou deterministické nebo pravděpodobnostní.
- str. 13: „Značení: Pro x^ℓ je ℓ-složkový vektor $(x, \ldots, x)$.“ nedává smysl, nejspíš tam přebývá „Pro“.
- str. 26: První věta na stránce „První nerovnost protivníkovy úspěšnosti.“ nedává smysl.
- str. 35: Zmiňuje se „silně spojitý graf“, má být „silně souvislý graf“.

Závěr

I přes uvedené nedostatky považuji práci za vynikající a doporučuji ji uznat jako bakalářskou.

V Praze dne 12. června 2019
Martin Mareš, KAM