MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

1. června 2022

Věc: Posudek vedoucího práce Bc. Tomáše Krňáka "Verifiable Delay Functions z Lucasových posloupností"

Práce kolegy Krňáka přináší nové konstrukce pro delay functions (DFs) a verifiable delay functions (VDFs). VDFs nalezly v nedávné době mnoho zajímavých aplikací v kontextu distribuovaných kryptoměn. Palčivým problémem při využití VDFs je však momentální nedostatek kandidátů pro inherentně sekvenční funkce, které by bylo možné veřejně efektivně verifikovat.

Jako první výsledek kolega Krňák ve své práci navrhuje novou heuristiku pro konstrukce inherentně sekvenčních funkcí založenou na modulárních Lucasových posloupnostech. Je známé, že modulární Lucasovy posloupnosti v grupě neznámého řádu lze vyhodnocovat pomocí iterovaného mocnění ve vhodném tělesovém rozšíření. Kolega Krňák ukazuje, že sekvenčnost odpovídající DF je alespoň taková jako sekvenčnost iterovaného mocnění ve stejné grupě - první DF navržená Rivestem, Shamirem a Wagnerem v roce 1996. Vzhledem k rekurentní struktuře Lucasových posloupností však není zřejmé, zda existuje i redukce opačným směrem. Kolega Krňák proto postuluje domněnku, že sekvenčnost modulárních Lucasových posloupností v grupě neznámého řádu je striktně slabší předpoklad než předpoklad sekvenčnosti modulárního mocnění v grupě neznámého řádu.

Jako druhý výsledek práce autor ukazuje, že, podobně jako pro iterované modulární mocnění, i modulární Lucasovy posloupnosti lze efektivně veřejně verifikovat bez znalosti řádu grupy. Autor tak předkládá novou konstrukci VDF. Tato část práce přenáší metody z konstrukcí VDFs založených na iterovaném modulárním mocnění do kontextu modulárních Lucasových posloupností.

Práce kolegy Krňáka rozšiřuje naše porozumění VDFs a přináší zajímavý přístup ke konstrukcím delay functions a verifiable delay functions. Předložené výsledky jsou rozhodně publikovatelné v oborové konferenci se zaměřením na kryptografii. Vzhledem k aplikacím VDFs očekávám, že na dosažené výsledky naváže další výzkum studující domněnku o sekvenčnosti modulárních Lucasových posloupností. Práce je napsána přístupným stylem a dobře vysvětluje kontext studovaného problému i dosažené výsledky. Doporučuji proto práci k obhájení jako diplomovou.

Mgr. Pavel Hubáček, Ph.D.

Informatický ústav Univerzity Karlovy
Malostranské nám. 2/25, 118 00 Praha 1
telefon: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz