Posudek oponenta k diplomové práci
Verifiable Delay Functions from Lucas sequences
Bc. Tomáše Krňáka

Předložená práce studuje návrh VDF (verifiable delay function) konstruované pomocí Lucasových posloupností. Formální definice VDF je poměrně dlouhá, zhruba řečeno se jedná o funkci f, kterou nelze počítat rychleji než v předepsaném čase, přitom je ale k dispozici algoritmus, který pro dané x spočte ověřitelný důkaz pro tvrzení $y = f(x)$. Ověření důkazu by mělo být podstatně rychlejší než ověření výroku přímým výpočtem. Praktické vužití mají VDF například v návrhu kryptoměn.

Navrhovaná VDF vychází z práce K. Pietrzaka *Simple Verifiable Delay Functions* (2018), který vycházel z funkce $x \mapsto x^{2^T} \bmod N$, kde N je RSA modulus, který je navíc součinem dvou bezpečných prvočísel (RSW delay function). Funkci lze zřejmě spočítat pomocí výpočtů T druhých mocnin v $\mathbb{Z}_N$. Bez znalosti faktorizace N přitom nejsou známy výrazně efektivnější algoritmy pro výpočet této funkce (práce zmiňuje algoritmus Bernsteina a Sorensena, který by udělal $O(T/\text{loglog}(T))$ umocnění).

Autor se zabývá funkcí, která by počítala 2^T-tý člen Lucasových posloupností daných rekurencí $V_k = PV_{k-1} - QV_{k-2}, V_0 = 2, V_1 = P$ a $U_k = PU_{k-1} - QU_{k-2}, U_0 = 0, U_1 = 1$ počítaných modulo N, kde N je vhodný RSA modulus. Tento výpočet lze také chápat jako výpočet 2^T-té mocniny konkrétního prvku v okruhu $\mathbb{Z}_N[x]/(x^2 - Px + Q)$.

Hlavní výsledky práce zahrnují vlastní návrh VDF, redukce sequenciality VDF na sequencialitu RSW (Theorem 1), důkaz odolnosti verifikace proti podvrženému důkazu (Lemma 3, Theorem 2, Theorem 3). Kromě toho jsou navrženy generátory vhodných pseudoprvočísel (sekce 4.4) a v sekci 5 jsou diskutována další možná zobecnění.

Téma práce je zajímavé a aktuální, z textu je patrné, že se autor v problematice velmi dobře orientuje. Práce se poměrně dobře čte, ale výsledné zpracování mohlo být podle mého názoru lepší. Konkrétní připomínky jsou uvedeny níže - vesměs jde o snadno odstranitelné drobnosti.

Celkově si myslím, že práce splnila zadání a doporučuji ji proto uznat jako práci diplomovou.

V Praze, 3. 6. 2022,

Pavel Příhoda

Konkrétní připomínky k práci:

- str. 5, ř. 1: $\mathbb{Z}_N[\sqrt{D}]$ má být $\mathbb{Z}_N[\sqrt{D}]^*$. Kromě toho toto značení může být zavádějící v případě, když D lze v $\mathbb{Z}_N$ odmocnit.

- str. 10, Definice 4: Myslím, že by součástí definice mělo být omezení na složitost algoritmů.
- str. 12, značení U_n, V_n není kompatibliní se značením na str. 3
- str. 13, Conclusion: field by mělo být ring
- str. 13, algoritmus LCS.Gen: Přišlo by mi dobré ověřit, že je ω invertibilní.
- str. 15, Definition 12: $f(x) \in \mathbb{Z}_n$ má být $f(x) \in \mathbb{Z}_n[x]$
- str. 15, Observation 1: potřebujeme $p \neq q$
- str. 16, Definition 15: every *prime* factor of W
- str. 16, ř. -4: $\mathbb{Z}_{p,f}$ má být $\mathbb{Z}^*_{p,f}$
- str. 19, Halving Protocol: Pokud je T liché bude $\lceil \frac{T}{2} \rceil = \frac{T+1}{2}$ a $[\mu] = [\omega^{\frac{T-1}{2}}]$. Pak je $[\mu]^{\lceil \frac{T}{2} \rceil} = [\omega^{2^{\frac{T-1}{2}} 2^{\frac{T+1}{2}}}] = [\omega^{2^T}] = [y]$.
- str. 20, Lemma 3: Tvrzení je zformulováno a dokázáno pro sudá T. Ve znění lemmatu by mělo být $\omega' = \omega^r \mu$. Navíc se mi zdá, že uvedený argument dokazuje pouze neostrou nerovnost $\Pr[...] \leq \frac{1}{2^\lambda}$.
- str. 21, 22: Algoritmy pro generování prvočísel nezohledňují podmínky z Definice 15. Například v Algoritmu 1 hodnota p bude menší než 2^λ.
- str. 23, Construction 2: Hash pouštíme na prvky z množiny $\mathbb{Z} \times \mathbb{Z}^6_N$, dále není vysvětleno, co je t.
- str. 25, Fact 1: Faktory $r_1, \ldots, r_\ell$ by měly být po dvou nesoudělné.
- str. 34, Claim 4.2: Jedná se o poměrně zajímavé tvrzení. O něco podrobnější důkaz by asi nebyl na škodu.
- obecná poznámka: Pro praktické aplikace by asi bylo dobré navrhnout Algoritmy 1,2 tak, aby generovaly opravdová prvočísla. Také by bylo dobré vědět, zda využití pseudoprvočísel v předepsané konstrukci nějak zásadně změní dokazované teoretické výsledky.