Posudek k bakalářské práci
Bezpečné sdílené počítání modulo p^k
Martina Struka

Cílem předložené práce je popis protokolu pro sdílené počítání termu v Galoisově okruhu $GR(p^k, d)$ spolu s výkladem části teorie využívané v protokolu.

Práce je rozdělena do tří kapitol, v první kapitole je látka běžně probíraná na přednáškch doplněna do tvaru, ve kterém se dále v práci využívá. Kromě toho je zaveden pojem Galoisova okruhu.

Druhá kapitola je věnována pojmu hyperinvertibilní matice a je dokázáno Tvrzení 9 o konstrukci hyperinvertibilní matice z výjimečné posloupnosti.

Třetí kapitola se pak věnuje popisu protokolu pro MPC v $GR(p^k, d)$. Postupně jsou předvedeny algoritmy pro privátní rekonstrukci, veřejnou rekonstrukci, sdílení náhodných vektorů, sdílení tajného nebo náhodného vstupu, výpočet součtu a součinu.

Práce je sepsána pečlivě, má dobrou matematickou úroveň a po formální stránce téměř bezchybná. V prvních dvou kapitolách se autor snaží vyjadřovat maximálně korektně, což místy působí trošku těžkopádně.

Ve třetí kapitole naopak autor popisuje poměrně komplikovaný protokol. Bezpečnost ani korektnost protokolu není diskutována nad rámec citovaných tvrzení, což trochu ztěžuje srozumitelnost textu (například není jasné, co protokol očekává od útočníků). Osobně bych spíš volil představení protokolu v nějaké odlehčené variantě, kterou by bylo možné demonstrovat konkrétním příkladem.

Jinak se mi ale práce líbí. Autor dle mého názoru splnil zadání a práci proto doporučuji uznat jako práci bakalářskou.

V Praze, 5. 9. 2023

Pavel Příhoda

Věcné připomínky k práci

- str. 7: jak je definováno $\deg(f(x) + (h(x)))$?
- Definice na straně 9 obsahuje tvrzení, že izotřída R nezávisí na volbě h, pouze jeho stupni. Takové (netriviální) tvrzení by mělo být formulováno samostatně.
- V Tvrzení 9 by mělo být vysvětleno, co je f.
- Lemma 10: Důkaz Lemmatu by měl být proveden lépe: Přesně definovat, jak zobrazení φ vypadá na celém R^n a pak ověřit, že se jedná o modulový izomorfismus. Pokud je $\overline{a} \in R^n$ a $\overline{b} = \overline{a}M$, je $(\overline{a}, \overline{b}) \in R^{2n}$.

- Je Definice na straně 16 v pořádku? Intuitivně bych čekal, že existenci více polynomů, pro které je velikost uvedené množiny alespoň $n' - t'$ a zároveň mají různou hodnotu v α_0, nechceme.
- Algoritmus 3: Mělo by být zdůrazněno , že $[s_0]_D$ je distribuován mezi jednotlivé účastníky.