Přehled kapitol BP

Vojtěch Večeřa
2016

Metody šifrování a hešování

- **Obsah:** 3DES, AES, SHA-1, SHA-256
- **Stav:** mám hotovo 98% – použiji celou kapitolu ze semestrálního projekt, možná odeberu SHA-1 algoritmus

Paralelní výpočty na GPU a OpenCL

- **Obsah:** úvod do problematiky paralelních výpočtů, OpenCL – architektura + modely
- **Stav:** mám hotovo 95% – použiji celou kapitolu ze semestrálního projekt, doplním barevné obrázky

Nástroj Wrathion

- **Obsah:** Popis nástroje a jeho částí
- **Stav:** mám hotovo 90% – použiji celou kapitolu ze semestrálního projekt, doplním barevné obrázky a referenci na clanek o Wrathionu

Analýza formátů .ZIP a .7z

- **Obsah:** Popis formátů a jejich vnitřní struktury, srovnání .ZIP a .7z
- **Stav:** mám hotovo 90% – použiji celou kapitolu ze semestrálního projekt, doplním barevné obrázky, možná doplním nějaké informace, které jsem opomněl nebo nepřesně popsal

Návrh modulů

- **Obsah:** Návrh algoritmů pro ověření hesel formátů .ZIP a .7z
- **Stav:** mám hotovo 95% – použiji celou kapitolu ze semestrálního projekt
  - Chci konzultovat momentální podobu algoritmů a zda není potřeba dodefinovat některé proměnné apod.

Implementace

- **Obsah:** Zmínění co bylo použito za funkce, algoritmy, kde jsem se čím inspiroval a co jsem si, kde půjčil. Popis rozdílu v algoritmech pro ověřování hesel. Shrnutí co přesně bylo naimplementováno.
- **Stav:** Mám hotovo 0% - plánuji začít psát příští týden až doimplementuju a udělám experimenty.

Experimenty a srovnání

- **Obsah:** Vyhodnocení experimentů a srovnáních s dalšími nástroji.
- **Stav:** Mám hotovo 0% – začnu psát po napsání implementace. Experimenty jako takové chci provést po implementaci, výhledově konec tohoto týdne / začátkem příštího.