Semestrální práce z předmětu KIV/PPR

Prolomení šifry SkipJack

Zdeněk Valeš

22.11. 2018

1 Zadání

Vaším úkolem bude prolomit šifru SkipJack. Tuto šifru je výpočetně náročné prolomit hrubou silou, nicméně lze zkusit i sofistikovanější metody např. genetické a evoluční algoritmy. Abyste prolomení urychlili, lze referenční kód přepsat a vektorizovat na úrovni instrukcí, pomocí GPU, případně ho distribuovat pomocí MPI.

Samostatná práce využije alespoň dvě z celkem tří možných technologií:

- Paralelní program pro systém se sdílenou pamětí - C++, popř. WinAPI
- Program využívající asymetrický multiprocesor - konkrétně x86 CPU a OpenCL kompatibilní GPGPU - C++ AMP
- Paralelní program pro systém s distribuovanou pamětí - C++ MPI

2 Popis řešení

Cenová fce, jak to přibližně funguje

2.1 Diferenciální evoluce

Jak to cca funguje, který typ mutace jsem použil, hodnoty parametrů

2.2 Paralelizace

Vektory na mutaci ne-e. Použito TBB + OpenCL, popis paralelizace evoluce (parallel_for)

3 Výsledky

4 Závěr