High Performance Computing - List 4

Deadline for the list: your laboratory classes between 09.04.2018 and 15.04.2018.

Task 1 (15 pts) In C/C++ implement the parallel version of the kangaroo method for solving the interval discrete logarithm problem. Let the interval be shorter than $(\pi/8) \cdot \mathrm{ord} g$. Use OpenMP. For big integers use NTL library. As an instance choose p being 40-60 bit number, random $g \in \mathbb{F}_p \setminus \{0\}$ such that $\mathrm{ord} g$ is prime, and $y \in \langle g \rangle$ (hint: a strong prime is the least troublesome choice of p, for such a prime it is easy to choose g of prime order – consider the trick from the lecture).

Task 2 (5 pts) Install PGI Compilers & Tools - Community Edition. Demonstrate how to use pgdbg on one of your solutions from any of the HPC lists.