

# Basic Pollard Rho Algorithm Implementation On CUDA Device

Martin Beránek

*Faculty of Information – Technology Czech Technical University*

2. května 2017

## **1 Introduction**

Factorisation problem of a huge number resolved into massive parallel solutions. Large number of algorithms are currently state-of-art and are continuously developed into better forms. This short article is focused on implementation of Pollard-Rho algorithm on **CUDA** device. In first part there is a definition of algorithm. Next the article focuses on options of parallelism on **CUDA** device. Results are measured in multiple instances and compared in graphs.

## **2 Definition of the algorithm**

## **3 CUDA Solution**

## **4 Conclusion**