THINKING IN CRYPTOGRAPHY WITH CUDA
ALGORITHMS OF THE NUMBER THEORY

JONATHAN S. PRIETO C.
SERGIO ARBOLEDA UNIVERSITY
DEPARTAMENT OF MATHEMATICS
MAIL: JONATHAN.PRIETO@CORREO.USA.EDU.CO

1. Abstract

This poster competition aims to give an example of the importance of the concepts and algorithms of number theory to cryptography implementations, more specifically in processes parallelizable. For this occasion I will give theoretical and technical guidelines to start with an implementation of RSA algorithm components (for example), showing some processes and optimized specifically for the block cipher, modular exponentiation by the method of Montgomery and other necessary algorithms. This time, using the Nvidia API 4.0. Hope will be helpful as I try to invite mathematicians interested in computers like me to explore new technologies with classic study in number theory and algorithm design.For in the future implement elliptic curve cryptography for these new platforms.