Project Description

Advanced Encryption Standard (AES) is a worldwide block cipher, which is used in many modern cryptosystems. For example, AES is a part of Wi-Fi, SSL/TLS, IPSec, VPN, etc. Up to date this block cipher is secure against all known attacks from practical point of view. Despite this, in 2011 a theoretical attack on the block cipher was presented, which is not more 4 times faster than brute force.

In cryptology data, memory and time complexities are usually considered. It is well known that the exhaustive search attack can always be applied to any of present-day ciphers with only time complexities. All other cryptanalytical attacks are compared with brute force. Therefore, optimization and obtaining data of exhaustive search attack on modern computers and clusters are one of priority tasks.

During this project it is proposed to implement several versions of AES oriented on cluster systems using open source libraries (e.g. MPI and OpenMP) and compare performance on UoB's Hexagon high performance computer.

Prerequisites

Programming, compile and run code in Linux/BSD-based operation systems, and experience in C/C++. Knowledge of MPI will be an advantage.

Working Language

English

Course Completion

After completing the project students will be able to explain the main principles lying in AES, work with existent open source libraries, write parallel programs oriented on high performance, write scientific reports.