Implementation of DES cryptographic algorithm using NVIDIA GPU for a brute-force attack

Miroslav Monok and Robert Lorencz

Abstract

In our work we describe a software implementation of DES cryptographic algorithm using NVIDIA GPU, and its use in a brute-force attack. The main purpose of the work was to design and implement DES algorithm in the CUDA architecture. We have achieved a great throughput with the so called ”bitslicing” technique. The achieved results were compared with FPGA loaded key-cracker called COPACOBANA (Guneysu, T.et al.: Cryptanalysis with COPACOBANA, IEEE TRANSACTIONS ON COMPUTERS, VOL. 57, NO. 11, NOVEMBER 2008).