ABSTRACT

MD5 is a hash function that mostly used as a digital signature or an encryption when passwords being stored in a database. One way to decrypt a hash function is by doing an exhaustive key search attack. This kind of attack is relatively easy to implement, but requires some hardware with high computational performance. To do this cryptanalysis, two high-end GPUs is proposed to run a parallel approach with the use of two programming languages, CUDA and OpenCL.

1 to 9 digits of random string/random password that based on 65 kind of characters, is used to do experiments in this research. Experiment results showed that a single high-end GPU can handle cryptanalysis for at most 9 digits of random password, with the longest running time reached 1 week or more. In terms of performance comparisons, OpenCL on AMD GPU gave the best performance when being compared to CUDA and OpenCL on NVIDIA GPU.

Keywords: MD5, Cryptanalysis, CUDA, OpenCL, GPU.