Harnessing Graphics Processors for High Speed Cryptography

Lee Wai Kong
Gachon University, South Korea

Abstract:

Graphics Processing Units (GPU) is originally developed for graphics and video applications, but nowadays it is widely used in many applications beyond graphics. The booming of blockchain technology invited many "miners" to develop efficient hashing software to perform high performance proof-of-work consensus (mining). GPU also accounted for the success of deep learning applications, wherein the massively parallel GPU architecture is turned into an efficient machine for neural networks training and inference. In this talk, an overview of the GPU architecture and programming model will be given, followed by some successful development of GPU-based implementation techniques for lattice-based cryptographic schemes. Some potential research directions of GPU-based cryptographic engineering will also be discussed.