Cryptology ePrint Archive: Report 2011/097

Fastplay-A Parallelization Model and Implementation of SMC on CUDA based GPU Cluster Architecture

Shi Pu, Pu Duan, Jyh-Charn Liu

Abstract: We propose a four-tiered parallelization model for acceleration of the secure multiparty computation (SMC) on the CUDA based Graphic Processing Unit (GPU) cluster architecture. Specification layer is the top layer, which adopts the SFDL of Fairplay for specification of secure computations. The SHDL file generated by the SFDL compiler of Fairplay is used as inputs to the function layer, for which we developed both multi-core and GPU based control functions for garbling of various types of Boolean gates, and ECC-based 1-out-of-2 Oblivious Transfer (OT). These high level control functions invoke computation of 3-DGG (3-DES gate garbling), EGG (ECC based gate garbling), and ECC based OT that run at the secure protocol layer. An ECC Arithmetic GPU Library (EAGL), which co-run on the GPU cluster and its host, manages utilization of GPUs in parallel computing of ECC arithmetic. Experimental results show highly linear acceleration of ECC related computations when the system is not overloaded; When running on a GPU cluster consisted of 6 Tesla C870 devices, with GPU devices fully loaded with over 3000 execution threads, Fastplay achieved 35~40 times of acceleration over a serial implementation running on a 2.53GHz duo core CPU and 4GB memory. When the execution thread count exceeds this number, the speed up factor remains fairly constant, yet slightly increased.

Category / Keywords: implementation / secure multiparty computation (SMC), Oblivious Transfer (OT), ECC, Graphic Processing Unit (GPU)

Date: received 24 Feb 2011

Contact author: shipu at cse tamu edu