Cryptology ePrint Archive: Report 2013/204

Computing Privacy-Preserving Edit Distance and Smith-Waterman Problems on the GPU Architecture

Shi Pu, Jyh-Charn Liu

Abstract: This paper presents privacy-preserving, parallel computing algorithms on a graphic processing unit (GPU) architecture to solve the Edit-Distance (ED) and the Smith-Waterman (SW) problems. The ED and SW problems are formulated into dynamic programming (DP) computing problems, which are solved using the Secure Function Evaluation (SFE) to meet privacy protection requirements, based on the semi-honest security model. Major parallelization techniques include mapping of variables to support collision-free parallel memory access, scheduling and mapping of gate garblers on GPU devices to maximize GPU device utilization, and latency minimization of context switch for computing steps in the DP matrix. A pipelined GPU-CPU interface is developed to mask latency of CPU housekeeping components. The new solutions were tested on a Xeon E5504 at 2GHz plus a GTX-680 GPU (as generator), connecting an i7-3770K at 3.5GHz plus a GTX-680 GPU (as evaluator) via local Internet. A 5000×5000 8-bit alphabet ED problem requires roughly 1.88 billion non-free gates, and the running time of around 26 minutes (roughly 1.209×106 gate/second). A 60×60 SW problem is computed in around 16.79 seconds. Compared to the state of art performance [5], we achieved the acceleration factor of 12.5× for the ED problem, and 24.7× for the SW problem.

Category / Keywords: applications / secure multi-party computing

Date: received 9 Apr 2013

Contact author: shipu at cse tamu edu

Available formats: PDF | BibTeX Citation

Version: 20130414:060048 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]