Cryptology ePrint Archive: Report 2011/540

Efficient Implementation of the η_T Pairing on GPU

Yosuke Katoh and Yun-Ju Huang and Chen-Mou Cheng and Tsuyoshi Takagi

Abstract: Recently, efficient implementation of cryptographic algorithms on graphics processing units (GPUs) has attracted a lot of attention in the cryptologic research community. In this paper, we deal with efficient implementation of the η_T pairing on supersingular curves over finite fields of characteristics 3. We report the performance results of implementations on NVIDIA GTX 285, GTX 480, Tesla C1060, and Tesla C2050 graphics cards. We have implemented η_T pairing in three different ways, namely, one pairing by one thread (Implementation~\Rmnum{1}), one pairing by multiple threads (Implementation~\Rmnum{2}), and multiple pairings by multiple threads in a bitsliced fashion (Implementation~\Rmnum{3}). The timing for Implementation~\Rmnum{3} on a single GTX 285 is 1.47, 8.15, and 140.7~milliseconds for η_T pairing over $\mathbb{F}_{3^{97}}$, $\mathbb{F}_{3^{193}}$, and $\mathbb{F}_{3^{509}}$, respectively. On a single GTX 480, the throughput performance of Implementation~\Rmnum{3} is 33710, 4970, and 332 η_T pairings per second over $\mathbb{F}_{3^{97}}$, $\mathbb{F}_{3^{193}}$, and $\mathbb{F}_{3^{509}}$, respectively. To the best of our knowledge, this is the first implementation of η_T pairing on GPU. Furthermore, it is currently the software implementation that achieves the highest single-chip throughput for η_T pairing.

Category / Keywords: implementation / public-key cryptography

Publication Info: This technical report is a full version of our earlier report that appeared in ACNS '11 Industrial Track

Date: received 1 Oct 2011

Contact author: ccheng at cc ee ntu edu tw