Cryptology ePrint Archive: Report 2011/196

Acceleration of Composite Order Bilinear Pairing on Graphics Hardware

Ye Zhang and Chun Jason Xue and Duncan S. Wong and Nikos Mamoulis and S.M. Yiu

Abstract: Recently, composite-order bilinear pairing has been shown to be useful in many cryptographic constructions. However, it is time-costly to evaluate. This is because the composite order should be at least 1024bit and, hence, the elliptic curve group order n and base field become too large, rendering the bilinear pairing algorithm itself too slow to be practical (e.g., the Miller loop is $\Omega(n)$). Thus, composite-order computation easily becomes the bottleneck of a cryptographic construction, especially, in the case where many pairings need to be evaluated at the same time. The existing solution to this problem that converts composite-order pairings to prime-order ones is only valid for certain constructions. In this paper, we leverage the huge number of threads available on Graphics Processing Units (GPUs) to speed up composite-order pairing computation. We investigate suitable SIMD algorithms for base field, extension field, elliptic curve and bilinear pairing computation as well as mapping these algorithms into GPUs with careful considerations. Experimental results show that our method achieves a record of 8.7ms per pairing on a 1024bit security level, which is a 20-fold speedup compared to state-of-the-art CPU implementation. This result also opens the road to adopting higher security levels and using rich-resource parallel platforms, which for example are available in cloud computing. In fact, we can achieve more than 24 times speedup on a 2048bit security level and a record of 7×10^{-6} USD per pairing on the Amazon cloud computing environment.

Category / Keywords: implementation /

Date: received 17 Apr 2011

Contact author: yzhang4 at cs hku hk