Cryptology ePrint Archive: Report 2013/218

Comparing the Pairing Efficiency over Composite-Order and Prime-Order Elliptic Curves

Aurore Guillevic

Abstract: We provide software implementation timings for pairings over composite-order and prime-order elliptic curves. Composite orders must be large enough to be infeasible to factor. They are modulus of 2 up to 5 large prime numbers in the literature. There exists size recommendations for two-prime RSA modulus and we extend the results of Lenstra concerning the RSA modulus sizes to multi-prime modulus, for various security levels. We then implement a Tate pairing over a composite order supersingular curve and an optimal ate pairing over a prime-order Barreto-Naehrig curve, both at the 128-bit security level. We use our implementation timings to deduce the total cost of the homomorphic encryption scheme of Boneh, Goh and Nissim and its translation by Freeman in the prime-order setting. We also compare the efficiency of the unbounded Hierarchical Identity Based Encryption protocol of Lewko and Waters and its translation by Lewko in the prime order setting. Our results strengthen the previously observed inefficiency of composite-order bilinear groups and advocate the use of prime-order group whenever possible in protocol design.

Category / Keywords: implementation / Tate pairing, optimal ate pairing, software implementation, composite-order group, supersingular elliptic curve, Barreto-Naehrig curve

Publication Info: This paper will appear at ACNS 2013. This is the full version.

Date: received 13 Apr 2013

Contact author: guillevi at di ens fr