Cryptology ePrint Archive: Report 2011/334

On the Efficient Implementation of Pairing-Based Protocols

Michael Scott

Abstract: The advent of Pairing-based protocols has had a major impact on the applicability of cryptography to the solution of more complex real-world problems. However there has always been a question mark over the performance of such protocols. In response much work has been done to optimize pairing implementation, and now it is generally accepted that being pairing-based does not preclude a protocol from consideration as a practical proposition. However although a lot of effort has gone into the optimization of the stand-alone pairing, in many protocols the pairing calculation appears in a particular context within which further optimizations may be possible. It is the purpose of this paper to bridge the gap between theory and practise, and to show that even complex protocols may have a surprisingly efficient implementation. We also point out that in some cases the usually recommended pairing friendly curves may not in fact be optimal. We claim a new record with our implementation of a pairing at the AES-256 bit level.

Category / Keywords: implementation /

Date: received 20 Jun 2011, last revised 8 Aug 2011

Contact author: mike at computing dcu ie