Cryptology ePrint Archive: Report 2011/294

Small Public Keys and Fast Verification for Multivariate Quadratic Public Key Systems

Albrecht Petzoldt and Enrico Thomae and Stanislav Bulygin and Christopher Wolf

Abstract: Security of public key schemes in a post-quantum world is a challenging task---as both RSA and ECC will be broken then. In this paper, we show how post-quantum signature systems based on Multivariate Quadratic (MQ) polynomials can be improved up by about 9/10, and 3/4, respectively, in terms of public key size and verification time. The exact figures are 88% and 73%. This is particularly important for small-scale devices with restricted energy, memory, or computational power. In addition, we show that this reduction does not affect security and that it is also optimal in terms of possible attacks. We do so by combining the priory unrelated concepts of reduced and equivalent keys. Our new scheme is based on the so-called Unbalanced Oil and Vinegar class of MQ-schemes. We have derived our results mathematically and verified the speed-ups through a C++ implementation.

Category / Keywords: implementation / MQ, Multivariate Quadratic, UOV, Unbalanced Oil and Vinegar

Date: received 3 Jun 2011, last revised 3 Jun 2011

Contact author: chris at Christopher-Wolf de

Available formats: PDF | BibTeX Citation

Version: 20110603:172134 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]