Enhanced Digital Signature using Splitted Digit Exponent Representation

Christophe Nègre, Thomas Plantard, J.M. ROBERT

WRAC'H submission, first of march, 2019

Abstract :

Digital Signature Algorithm (DSA) involves modular exponentiation, of a public and known base by a random one-time exponent. In order to speed-up this operation, well-known methods take advantage of the memorization of base powers. However, due to the cost of the memory, to its small size and to the latency of access, previous research sought for minimization of the storage. In this paper, taking into account the modern processor features and the growing size of the cache memory, we improve the storage/efficiency trade-off, by using a RNS Digit exponent representation. We then propose algorithms for modular exponentiation. The storage is lower for equivalent complexities for modular exponentiation computation. The implementation performances show significant memory saving, up to 3 times for the largest NIST standardized key sizes compared to state of the art approaches. This work has been presented at WAIFI 2016 conference. We extend this approach to the Elliptic Curve Scalar Multiplication with another multiplicative digit approach we call R-splitting, providing side-channel resistance.