Faster PMNS Multi-precision Multiplications UsingTruncated Montgomery Technique

Laurent-Stéphane Didier[1], Alexy Dutois-Ruiz*[1], and Jean-Marc Robert[1]

[1]Université de Toulon - UFR Sciences et Techniques – Université de Toulon – France

Résumé

The Polynomial Modular Number Systems (**PMNS**) aim to represent elements of fields or rings of large characteristics using polynomials satisfying bounds on some parameters (degree, absolute values of the coefficients). Those PMNS, while some conditions are fulfilled, using convenient parameters and implementation features, allow some speed-ups in cryptographic computations. Recent works propose better speed-ups by improving the parameter generation of the system, and by using **multiprecision polynomial coefficents** *i.e.* coefficients stored using several machine words. In this work, we present a new improvement on the PMNS, applying to the *internal reduction* an approach similar to the *truncated Montgomery reduction* technique presented by Didier *et al.* In the context of software implementations using *AVX512* instruction set extension, and modulo size up to 8192 bits, this new approach allows speed-ups up to 15% in modular multiplication computation, in comparison with conventional approaches.

*Intervenant