PMNS revisited for efficiency and better memory cost

Fangan Yssouf Dosso*[1], Jean-Marc Robert[2], and Pascal Véron[3]

[1]Laboratoire SAS, EMSE – Ecole Nationale Supérieure des Mines de Saint-Etienne – France
[2]IMath, Université de Toulon – Université Sud Toulon Var – France
[3]IMath, Université de Toulon – Université Sud Toulon Var – France

Résumé

The Polynomial Modular Number System (PMNS) is an integer number system that aims to speed up arithmetic operations modulo a prime number p. Such a system is defined by a tuple (p, n, g, r, E), where p, n, g and r are positive integers, E is a monic polynomial with integer coefficients, having g as a root modulo p. Many works have shown that the PMNS can be an efficient alternative to the classical representation for modular arithmetic and cryptographic size integers. It has also been shown how to
randomise operations using this system, by exploiting its redundancy property. In this presentation, we present some properties and a process to generate PMNS with small memory cost and efficient reduction capabilities.

*Intervenant