A Binomial Family for Practical Polynomial Modular Number Systems

Thomas Plantard*[1]

[1]Nokia Bell Labs – États-Unis

Résumé

Polynomial Modular Number System have became a powerful tool to implement safely and efficiently modular arithmetic for cryptographic protocols. A long list of type of Polynomial Modular Number Systems have been proposed to operate practically on different prime field. However, to this day, there was no guarantee that there exists a practical Polynomial Modular Number System for any prime p.
In this work, we propose a new family of Polynomial Modular Number System based on Binomial. Using this family, we prove that there exist for any prime p and any system size n a Polynomial Modular Number System both compact and efficient.

*Intervenant