BaDu primes and applications to cryptography

Sylvain Duquesne*[1]

[1]IRMAR – Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes – France

Résumé

This talk is about a joint work with Jean-Clade Bajard. It deals with BaDu primes (most commonly known as Montgomery-friendly primes) designed for the modular reduction algorithm of Montgomery. These numbers are scattered in the literature and their properties are partially exploited. We exhibit a large family of BaDu primes which give rise to efficient modular reduction algorithms. We will then explain how they can be used in elliptic curve or isogeny-based cryptography but also in finite field arithmetic by proposing families of alternative BNS bases (most commonly known as RNS bases). We show that, for dedicated architectures with word operators, we can reach, for a same or better complexity, larger BNS bases with BaDu pairwise co-primes than the BNS bases generally used in the literature with pseudo-Mersenne numbers.

*Intervenant