Résumé

Les calculs modulaires entrant en jeu dans les applications en cryptographie asymétrique utilisent le plus souvent un modulo premier standardisé, dont le choix n'est pas toujours libre en pratique. L'amélioration des opérations modulaires est centrale pour l'efficacité et la sécurité de ces primitives. Cette thèse propose de fournir une arithmétique modulaire efficace pour le plus grand nombre de premiers possible, tout en la prémunissant contre certains types d'attaques. Pour ce faire, nous nous intéressons au système PMNS utilisé pour l'arithmétique modulaire, et proposons des méthodes afin d'obtenir de nombreux PMNS pour un premier donné, avec une arithmétique efficace sur les représentations. Nous considérons également la randomisation des calculs modulaires via des algorithmes de type Montgomery et Babaï en exploitant la redondance intrinsèque aux PMNS. Les changements induits de représentation des données au cours du calcul empêchent un attaquant d'effectuer des hypothèses utiles sur ces représentations. Nous présentons ensuite un système hybride, HyPoRes, avec un algorithme améliorant les réductions modulaires pour tout modulo premier. Les nombres sont représentés dans un PMNS avec des coefficients en RNS. La réduction modulaire est plus rapide qu'en RNS classique pour les premiers standardisés pour ECC. En parallèle, nous étudions un type de représentation utilisé pour la résolution réelle de systèmes flous. Nous revisitons l'approche globale de résolution faisant appel à des techniques algébriques classiques et la renforçons. Ces résultats incluent un système réel appelé la transformation réelle qui simplifie les calculs, et la gestion des signes des solutions.

Abstract

Modular computations involved in public key cryptography applications most often use a standardized prime modulo, the choice of which is not always free in practice. The improvement of modular operations is fundamental for the efficiency and safety of these primitives. This thesis proposes to provide an efficient modular arithmetic for the largest possible number of primes, while protecting it against certain types of attacks. For this purpose, we are interested in the PMNS system used for modular arithmetic, and propose methods to obtain many PMNS for a given prime, with an efficient arithmetic on the representations. We also consider the randomization of modular computations via algorithms of type Montgomery and Babaï by exploiting the intrinsic redundancy of PMNS. Induced changes of data representation during the calculation prevent an attacker from making useful assumptions about these representations. We then present a hybrid system, HyPoRes, with an algorithm that improves modular reductions for any prime modulo. The numbers are represented in a PMNS with coefficients in RNS. The modular reduction is faster than in conventional RNS for the primes standardized for ECC. In parallel, we are interested in a type of representation used to compute real solutions of fuzzy systems. We revisit the global approach of resolution using classical algebraic techniques and strengthen it. These results include a real system called the real transform that simplifies computations, and the management of the signs of the solutions.