Design and Implementation of Lattice-Based Cryptography

Tancrède Lepoint

La cryptographie à base de réseaux Euclidiens est aujourd'hui un domaine scientifique en pleine expansion et connait une évolution rapide et accélérée par l'attractivité du chiffrement complètement homomorphe ou des applications multilinéaires cryptographiques. Ses propriétés sont très attractives : une sécurité pouvant être réduite à la difficulté des pires cas de problèmes sur les réseaux Euclidiens, une efficacité asymptotique quasi-optimale et une résistance présupposée aux ordinateurs quantiques. Cependant, on dénombre encore peu de résultats de recherche sur les constructions à visée pratique pour un niveau de sécurité fixé. Cette thèse s'inscrit dans cette direction et travaille à réduire l'écart entre la théorie et la pratique de la cryptographie à clé publique récente.

Dans une première partie, nous concevons et implémentation une signature numérique ultra-performante basée sur les réseaux Euclidiens. Toutes les instanciations jusqu'alors connues de cryptographie à base de réseaux utilisaient des paramètres trop grands pour envisager leur utilisation pratique (en particulier sur petite architecture). Notre contribution principale consiste alors à décrire une nouvelle signature numérique compacte (avec des signatures de l'ordre de 5000 bits), performante, sûre et adaptée aux environnements contraints. Les améliorations théoriques ont été combinées avec des optimisations pratiques et ont permis d'obtenir une signature numérique basée sur les réseaux plus efficace que celles reposant sur RSA ou sur les courbes elliptiques. L'efficacité obtenue fait de cette primitive la signature numérique la plus efficace à ce jour capable de résister aux ordinateurs quantiques. Nos travaux ouvrent la voie au déploiement de celle-ci en pratique dans un futur proche.

Dans une seconde partie, nous avons conçu, amélioré et implémenté plusieurs schémas de chiffrement complètement homomorphes (considéré comme le Saint Graal de la cryptographie). Ce dernier permet d'effectuer (de façon publique) des calculs arbitraires sur des messages chiffrés. Les premières instanciations de cette surprenante primitive ne peuvent être considérées comme pratiques, chaque multiplication de deux bits chiffrés nécessitant d'être suivie par une procédure de plusieurs dizaines de minutes. Notre contribution principale consiste à améliorer les schémas complètement homomorphes sur les entiers afin d'évaluer de façon chiffrée un circuit non trivial (nous avons choisi l'AES). Une telle évaluation de l'AES avec nos schémas nécessite une centaine heures mais permet de traiter 1875 blocs de 128 bits en parallèle, ce qui donne un temps relatif (par bloc) de trois minutes. Nos schémas se révèlent ainsi très compétitifs dans un environnement concurrentiel.

Dans une dernière partie, nous construisons des applications multilinéaires cryptographiques. Cette primitive, généralisant les couplages (applications bilinéaires), admet une première construction basée sur les réseaux depuis fin 2012 et ses conséquences sont nombreuses, inattendues et à très fort potentiel (comme l'existence d'obfuscation indistinguable). Nous proposons une nouvelle construction, une des deux existantes à ce jour, qui permet de donner une primitive alternative plus résistante que l'initiale. Finalement, nous en décrivons la première implémentation (la construction initiale n'étant que théorique) et montrons qu'un échange de clé entre 26 participants nécessite moins de cinq minutes sur un processeur classique actuel en utilisant nos applications multilinéaires cryptographiques.