La cryptologie : un exemple d'interdisciplinarité réussie entre informatique et mathématiques

INS2I

Avec l'aide des contributeurs externes : J.-M. Couveignes, P. Elbaz-Vincent, G. Hanrot

La cryptographie est un domaine interdisciplinaire par excellence (voire même transdisciplinaire) qui se situe à la croisée de l'informatique et des mathématiques, mais également du traitement du signal, de la microélectronique, des sciences pour l'ingénieur et des sciences du vivant (avec les aspects biométriques, un domaine de recherche en pleine expansion en cryptographie où se posent également des problèmes de société), et qui a connu ces 20 dernières années un spectaculaire essor. L'interdisciplinarité se joue dans un va-et-vient entre problématiques d'une part, méthodes et outils d'autre part, issus des divers domaines concernés. La cryptographie se pratique de plus avec les acteurs du monde académique, mais aussi des mondes industriel et étatique (agences gouvernementales) avec une grande porosité entre ces trois types d'acteurs.

Les enjeux, essentiellement applicatifs, de la cryptographie sont aussi bien **sociétaux** (outils pour la protection de l'identité et des données personnelles des citoyens, en particulier avec la croissance des réseaux sociaux, lutte contre la cybercriminalité), qu'**industriels** (protection de la propriété intellectuelle et des contenus, sécurisation des architectures réseaux très hauts débits, sécurisation des communications, intégration de la sécurité dans le cadre des maisons intelligentes, des nanotechnologies, des réseaux du futurs et des biotechnologies), et **commerciaux** (les solutions proposées doivent pouvoir être déployées facilement et à faible coût tant financier qu'écologique).

La cryptographie s'organise selon trois niveaux d'intervention (avec des frontières poreuses là encore) : conception de **primitives cryptologiques** (chiffrement, signature, hachage, générateurs d'aléa, etc.), combinaison de ces primitives afin d'obtenir des **protocoles** offrant des propriétés avancées, et enfin, développement de **preuves de sécurité** pour les protocoles.

La conception de primitives cryptologiques est particulièrement demandeuse d'outils mathématiques sophistiqués (arithmétique des congruences, théorie algébrique des nombres, géométrie et cohomologie des groupes algébriques, méthodes p-adiques, probabilités, statistiques, mathématiques discrètes). Le calcul formel, l'arithmétique des ordinateurs et la complexité algorithmique interviennent également naturellement dans ce contexte. Le développement de modèles de sécurité et des preuves formelles de sécurité sur les protocoles font

intervenir la théorie de la complexité mais aussi la théorie des jeux, avec l'automatisation des preuves par jeux dans le cadre de la sécurité prouvée.

Si les problèmes de factorisation et les problématiques relevant du logarithme discret dans les corps finis font l'objet d'un travail de fond sur les 20 dernières années (avec en particulier l'évaluation précise de la sécurité, la veille sur les attaques et les algorithmes probabilistes), l'apparition des **courbes** (elliptiques, hyperelliptiques, calculs de couplages, comptage de points) dans le paysage est un exemple frappant d'interaction entre mathématiques et informatique. Si les méthodes développées font une utilisation remarquable de mathématiques avancées (méthodes p-adiques, cohomologie), il reste à continuer à travailler sur l'efficacité des calculs et sur des implémentations efficaces. L'arithmétique sur les courbes connaît ainsi un grand essor, avec la recherche de nombreux systèmes de coordonnées aboutissant à des opérations performantes et la conception et l'optimisation d'opérateurs arithmétiques associés.

Le développement de la théorie des ordinateurs **quantiques** (machine de Turing quantique) a apporté un dynamisme à la recherche en cryptographie. En effet, pour un ordinateur quantique, factoriser un nombre entier ou résoudre le problème du logarithme discret dans les corps finis ou dans les courbes elliptiques se fait en temps polynomial quantique. On peut donc se demander quelles sont les primitives cryptographiques résistantes à un ordinateur quantique, ce qui implique une compréhension fine des mécanismes de complexité et calculabilité liés aux primitives cryptographiques. Deux sujets trouvent ainsi une actualité et une pertinence dans l'ère de l'algorithmique postquantique : les **codes** (qui ont des propriétés théoriques attrayantes, mais des tailles de clés très grosses), et surtout les **réseaux**, avec des méthodes qui débouchent souvent sur des classes de complexité que l'on sait être difficiles (aussi bien dans un contexte classique que quantique). L'étude des réseaux en cryptographie est ainsi un sujet en plein essor depuis début 2000, qui a donné un regain d'intérêt supplémentaire pour l'algorithme LLL. Si les réseaux ont déjà eu l'occasion de prouver de façon spectaculaire leur efficacité en tant qu'outil de cryptanalyse (NTRU), ce domaine est surtout en pleine explosion depuis 4-5 ans, en particulier grâce aux travaux d'Ajtai (les instances aléatoires sont essentiellement aussi difficiles que les instances difficiles) qui ont conduit à des notions de sécurité beaucoup mieux argumentées que dans bien d'autres systèmes. La forte structure permet en outre de construire des protocoles très avancés comme le chiffrement homomorphe (Gentry). À noter également l'utilisation, comme réseaux sous-jacents, des idéaux d'anneaux d'entiers de corps de nombres. Enfin, les réseaux permettent également de construire des primitives à clé secrète. En particulier, dans le cadre des fonctions de hachage (qui ont récemment fait l'objet d'un appel à propositions international) il est à noter des propositions prometteuses à base de courbes ou de réseaux avec des preuves de sécurité.

Les enjeux applicatifs, avec l'apparition de nouveaux supports et de nouvelles architectures et techniques de programmation, font intervenir de manière naturelle l'**arithmétique des ordinateurs** (conception et optimisation d'opérateurs arithmétiques) et le **calcul formel**. Les efforts d'implémentation de protocoles cryptographiques qui, à l'origine, étaient orientés circuits dédiés (ASIC),

se portent ainsi maintenant vers d'autres supports (comme les cartes programmables FPGA ou les cartes graphiques GPU) et conduisent à de nouveaux problèmes de complexité et de sécurité (attaques par canaux cachés, attaques par fautes). D'autre part, l'aspect cryptanalyse (factorisation, logarithme discret, attaques algébriques etc.) utilise des approches plus larges qui relèvent du calcul intensif utilisant des réseaux de GPU, ou des réseaux de stations homogènes (playstations), voire même hétérogènes (cloud computing). Cette réactivité aux nouvelles technologies est particulièrement visible lorsque l'on considère les implémentations sur les systèmes embarqués légers (cartes à puces, RFID, cartes SIM etc.) aux considérables enjeux sociétaux. L'interdisciplinarité se joue ainsi dans le regard multiple porté sur les objets selon les différents niveaux d'intervention (matériel, logiciel, algorithmique et mathématique), regard qui suscite de multiples questions en retour. Par exemple, quelle complexité considérer en fonction du support matériel choisi (RAM, Turing) ? Quel compromis faire entre sécurité et complexité dans le cas de clients légers ?

Le CNRS a joué un rôle déterminant de structuration pour les communautés concernéees via le GDR Informatique Mathématique dont le groupe de travail C2 (codage et cryptographie) joue un rôle d'animation très structurant, et a su accompagner le développement de cette interface à travers divers PEPS (PEPS ST2I, PEPS Mathématiques-Informatique, PEPS Maths Industrie).