Avant-propos

David POINTCHEVAL
DIENS, CNRS, ENS, Inria, Paris, France

L'article pionnier de Diffie et Hellman (1976)[1], qui a introduit la *cryptographie à clé publique*, a conduit à l'émergence d'un vaste domaine de recherche. La cryptographie à clé publique inclut non seulement les variantes asymétriques de chiffrement et d'authentification, c'est-à-dire le chiffrement à clé publique et les schémas de signature, mais également de nombreux autres outils innovants et extrêmement puissants.

Cet ouvrage a pour but de présenter les principales primitives cryptographiques ayant été proposées ces 40 dernières années, *via* des chapitres écrits par des cryptographes de renom, spécialistes du domaine, avec de nombreuses publications internationales à leur actif. Je suis très honoré qu'ils aient accepté mon invitation et rendu ce livre aussi complet que possible.

Cet ouvrage commence par la présentation des principales primitives de la cryptographie à clé publique, soit les *signatures* et le *chiffrement à clé publique*, incluant les définitions et les modèles de sécurité. Le chapitre 1 donne également un avant-goût de la sécurité prouvable, en expliquant ce que signifie « être sûr » ou « sécurisé » pour un schéma cryptographique.

Dans le chapitre 2, nous présentons les *preuves à divulgation nulle de connaissance*. Il s'agit d'un outil magique utilisé dans de nombreux autres protocoles. Les preuves à divulgation nulle de connaissance permettent de convaincre tout vérificateur

1. *IEEE Transactions on Information Theory*. 22(6), 644–654, 1976.

Cryptographie asymétrique,
coordonné par David POINTCHEVAL. © ISTE Editions 2024.

de la véracité de n'importe quel énoncé valide, sans révéler d'informations supplémentaires. Dans la même lignée, le *calcul multipartite sécurisé* permet à deux joueurs ou plus, avec des entrées privées, de calculer la sortie d'une fonction bien définie sur les entrées jointes des joueurs, sans pour autant révéler d'autres informations que ladite sortie.

Après de nombreuses utilisations pour attaquer le problème du logarithme discret sur les courbes elliptiques, les couplages ont été largement appliqués à la construction de nouvelles primitives, principalement pour proposer de nouveaux types de chiffrement et de schémas de signature. Par conséquent, nous commencerons par une introduction générale à la *cryptographie à base de couplages* puis nous présenterons des schémas cryptographiques avancés de confidentialité et d'authentification, qui satisfont des propriétés supplémentaires. Le premier schéma que nous présenterons est la *diffusion chiffrée* (ou chiffrement *broadcast*) qui améliore le chiffrement usuel en ciblant plusieurs destinataires lors de l'envoi d'informations privées. Il serait évidemment possible de donner la même clé de déchiffrement à plusieurs utilisateurs, mais lorsque l'on veut changer dynamiquement de groupe cible, différentes clés de déchiffrement sont requises. Avec le *traçage de traîtres* (*traitor tracing*), il est alors possible de tracer les traîtres ayant transmis leurs clés de déchiffrement à des utilisateurs non légitimes. Le *chiffrement par attributs* est une généralisation de la diffusion chiffrée, dans laquelle le groupe cible peut être spécifié par une politique d'accès et des attributs. Il est alors possible de décrire le groupe cible de manière précise pour chaque nouveau texte chiffré. Les *signatures avancées* ajoutent des propriétés d'anonymisation à la signature et à l'authentification. Grâce aux couplages, il est en effet possible de s'authentifier efficacement auprès d'un service en minimisant les données personnelles divulguées.

En plus du chiffrement et des schémas de signature, *l'échange de clés* est un outil important en situation réelle car il permet à deux participants, ou plus, de se mettre d'accord sur une clé de session commune, qui peut alors être utilisée pour établir un canal de communication sûr. Bien que la tâche semble simple et bien définie, les protocoles d'échange de clés sont complexes et plusieurs notions de sécurité sont à prendre en compte. Il existe également de nombreuses façons d'authentifier les utilisateurs, soit en signant les messages soit en montrant sa capacité à déchiffrer. L'utilisation d'une clé symétrique partagée est également possible. Cependant, la configuration d'authentification la plus pratique, mais aussi la plus ardue, est celle dans laquelle les parties détiennent une *courte* clé symétrique. Cette dernière information commune est appelée *mot de passe* et la solution réside dans un *échange de clés authentifié par mot de passe*.

L'externalisation massive du stockage et des calculs a fait du *calcul vérifiable*, dans lequel on souhaite de fortes garanties sur la sortie des calculs externes, un domaine très

actif. Évidemment, l'objectif est que la vérification du calcul soit plus efficace que son évaluation, d'où le développement des *arguments succincts non interactifs* (*succinct non-interactive arguments* ou SNARGS).

Les différents chapitres offrent une vue d'ensemble des quelques avancées récentes en cryptographie à clé publique. Cela ne se veut pas exhaustif et chaque présentation reflète le point de vue de l'auteur sur le domaine. On y trouve des descriptions générales et parfois des exemples plus spécifiques pour illustrer l'objectif. Ils conviennent à un large public désireux de découvrir ou d'approfondir la cryptographie à clé publique.