Généralisations du chiffrement classique en cas multi-utilisateur

Duong Hieu PHAN, duong-hieu.phan@unilim.fr
Tél : 0659139197
Olivier Blazy, olivier.blazy@unilim.fr
Tél : 0

Equipe : CRYPTIS, XLIM

Mots clés : cryptographie, communications multi-utilisateurs

Résumé de la thèse :

L'objectif est de proposer de nouvelles techniques mathématiques de construction des schémas cryptographiques dans le contexte des communications multi-utilisateurs.

The objective is to propose new mathematical method to construct provably secure cryptographic schemes in the contexte of multi-user such as broadcast encryption, attribute-based encryption and signature, and functional encryption.

Objectifs :

Proposer de nouveaux algorithmes et de nouvelles méthodes de preuve de sécurité.

Description complète du sujet de thèse :

Nous sommes dans une ère de développement très rapide des technologies où de nouvelles applications apparaissent régulièrement pour traiter des données de taille de plus en plus massive, liés au développement du cloud. Le cloud permet de stocker des données de taille très importante sur les serveurs et la question essentielle est de savoir comment on peut exploiter ces données de façon sécurisée. Afin d'atteindre cette sécurité, les fonctionnalités cryptographiques qu'il faut obtenir sont à titre d'exemple : la sécurité des calculs sur les données (au sens le plus fort, les calculs sur les données chiffrées), l'anonymat et le contrôle de l'accès aux données. Les primitives cryptographiques classiques "one-to-one" ne sont pas bien adaptées à ces nouveaux usages ; il est donc naturel de considérer des nouvelles primitives dans des communications multi-utilisateurs où les notions de corruptions, collusions, révocation et traçabilités jouent un rôle aussi important que les notions classiques de la confidentialité, de l'authentification et de l'intégrité.

L'objectif est de proposer de nouvelles techniques de construction des schémas cryptographiques dans le contexte des communications multi-utilisateurs :

- D'une part, au niveau des primitives, le but est de travailler sur la diffusion de données chiffrées, la signature du groupe, le chiffrement par attributs, le chiffrement fonctionnel, la cryptographie distribuée ainsi que les applications qui combinent différentes primitives, notamment le vote électronique, la recherche sur des base de données chiffrées.
- D'autre part, nous cherchons à assurer la sécurité dans plusieurs scénarios : contre des attaques puissantes disposant de machines quantiques ; ou contre des attaques plus faibles mais plus pratiques (celles qui peuvent être efficacement implémentées). Pour ce faire, il nous faut formaliser les notions de sécurité, construire des schémas efficaces et fournir des preuves

de sécurité en réduisant la sécurité des schémas à des hypothèses algorithmiques reconnues difficiles ou à d'éventuelles nouvelles hypothèses algorithmiques ; et dans ce dernier cas, étudier la difficulté de ces nouvelles hypothèses.

Compétences à l'issue de la thèse :

Les aspects mathématiques de la cryptographie, en particulier les preuves de sécurité; la conception de protocole dans de nouveaux contextes de communications multi-utilisateus.

Présentation de l'équipe d'accueil :

The Cryptis team is included in the Mathematics, Information Security (MIS) research axis of XLIM. The team is specialized in cryptology and information security. It contains 12 permanent researchers and 11 Ph.D. students, including a mixture of computer scientists and mathematicians. The research group is organized in 4 research projects related to Cryptology (Provable security, quantum and post-quantum cryptology), Physical attacks and cryptology for embedded systems, Systems and network security and Discrete mathematics, coding, effective arithmetic and applications.

Members are involved in several French national projects funded by ANR and other institutions (CNRS, …) and in partnership research projects with major companies (Thales, Worldline, …). Members of the team publish the research results in the best journals (IEEE Inf. Theory, Information Sciences, Algorithmica, …) and conferences (Eurocrypt, Asiacrypt, Crypto, PKC, TrustCom, …). The team members are also involved in organization of major conferences (Asiacrypt, PQCrypto, …).

Financement : Lot 2: Sujet avec demande de financement institutionnel en cours

Spécialité de Doctorat : Mathématiques et leurs Interactions

Domaine de compétences principal: Mathématiques

Domaine de compétences secondaire: Informatique-Electronique

Candidat :
Compétences souhaitées : Master en cryptographie, mathématiques et avec une bonne maitrise en informatique théorique.

Conditions restrictives de candidature : Aucune

Date Limite de candidature : 8 juin 2017 - 18H