La cryptographie de l'identité et les échanges

Blazy Olivier, olivier.blazy@unilim.fr
Tél : 0587506776
Phan Hieu, duong-hieu.phan@unilim.fr
Tél : 0

Equipe : CRYPTIS, Limoges

Mots clés : Cryptographie, Preuve, Clé publique

Résumé de la thèse :

Cette thèse sera consacrée aux méthode d'authentification et à la cryptographie de l'identité. Le but sera de prendre en compte les protocoles classiques et de proposer des alternatives efficaces, sûrs et justifiées dans un contexte de cryptographie de l'identité.

This PhD aims to improve authentication methods in everyday communication. Usually there is a clash between two worlds at this level, on one hand academic research tends to propose solutions proven secure in some abstract model without real consideration for efficiency, while industrial tends to favor optimization without sufficient concerns for security or the lack thereof, another main issue is that those implementations often tend to consider a Trusted Third Party, and end up relying way too much on its honesty, while no system can be guaranteed no never be corrupted or coerced into evil-doing.

Objectifs :

Proposer de nouveaux algorithmes dans le paradigme de la cryptographie de l'identité

Description complète du sujet de thèse :

Ce sujet s'inscrit dans le cadre de l'ANR JCJC IDFIX
Le projet, et donc la thèse cherche à améliorer les méthodes d'authentification. Il y a souvent une fracture à ce niveau. D'un côté la recherche académique propose généralement des solutions prouvées sures dans un modèle abstrait et sans vraie considération d'efficacité, alors que du milieu industriel émergent des solutions qui favorisent l'efficacité sans forcément beaucoup de considération pour la sécurité. Un autre problème vient du fait que ces implémentations gravitent souvent autour d'une autorité en qui on se retrouve à devoir faire confiance, alors qu'il est impossible de garantir que sous l'effet de pressions, cette dernière ne va pas mal agir.
La thèse visera à exploiter le meilleur des deux mondes, en produisant des protocoles sûrs dans un modèle cohérent avec les applications réelles, des preuves de sécurité, et une efficacité pratique. Pour cela, il faudra revisiter des protocoles classiques, en proposant des alternatives plus sures mais cette fois en faisant de l'ID-Based Crypto.

Compétences à l'issue de la thèse :

- Conception de protocole
- Preuve de sécurité
- Maîtrise des différentes hypothèses de sécurité en cryptographie

Présentation de l'équipe d'accueil :

L'équipe Cryptis allie recherche en cryptographie (traditionnelle, quantique, post-quantique) à des compétences en sécurité.

Financement : Lot3: Sujet financé (organisme - industriel - ...)

Spécialité de Doctorat : Mathématiques et leurs Interactions

Domaine de compétences principal: Informatique-Electronique

Domaine de compétences secondaire: Mathématiques

Candidat :
Compétences souhaitées : Master 2 ou équivalent en mathématiques / informatique.
Stage de recherche dans une équipe / entrerprise sur de la cryptographie

Conditions restrictives de candidature : Aucune

Date Limite de candidature : 8 juin 2017 - 18H