Contribution ID: **7** Type: **not specified**

Preuves Implicites

Wednesday, June 9, 2021 1:00 PM (1h 15m)

Les Smooth Projective Hash Functions ont été introduites en 2002 par Cramer et Shoup pour permettre de faire du chiffrement CC2.
Nous allons montrer comment les classifier, comment en construire et comment étendre le champ des langages pouvant être générés.
Pour celà, nous les étudions tout d'abord sous l'angle classique des courbes elliptiques mais également des réseaux euclidiens, ou même de la cryptographie à base de codes. Ensuite nous proposons de nouvelles méthodologies pour construire et prouver des protocoles d'échanges de clé authentifiés (que nous regroupons derrière le concept de LAKE : Language Based Authenticated Key Exchange, Echange de clé authentifié par un langage), et des protocoles asymétriques (regroupés sous le concept d'OLBE : Oblivious Language-Based Envelope, Enveloppe Inconsciente basée sur un langage). A chaque fois, nous regarderons les
fonctionnalités idéales, des instantiations génériques et montrons comment instantier les diverses briques pour générer des protocoles sûrs et le plus efficaces possibles. Bien que développées de façon générique, nous remarquons que nos instantiations conduisent à des protocoles extrêmement efficaces même en cas de corruptions adaptatives, et que ces constructions se transposent presque naturellement aux hypothèses post-quantiques.

Presenter: BLAZY, Olivier

Session Classification: Cryptographie