Proposition de projet M2 Cybsersécurité IP Paris

Partage de fonction secrète et application à la maintenance sécurisée des données distantes

Mots-clefs :
Function Secret Sharing (FSS), Distributed Point Function (DPF), Private Information Retrieval (PIR), Stockage/recherche/mise à jour dans le nuage.

Laboratoire d'accueil : INRIA Saclay/LIX, équipe Grace

Encadrante: Françoise Levy-dit-Vehel (ENSTA-IP Paris & INRIA Saclay).

Description du sujet :

La problématique est celle d'un client souhaitant récupérer un enregistrement d'une base de données distante, répliquée ou distribuée sur plusieurs serveurs, sans révéler aux serveurs une quelconque information sur le numéro d'enregistrement. Cette problématique est connue sous le nom de "récupération confidentielle d'information", ou "Private Information Retrieval" (PIR). On s'intéressera aussi à la mise à jour confidentielle de bases de données ("private updates").

Les fonctionnalités récentes autour du partage de fonction secrète (FSS), introduites par Ishai et Gilboa en 2014 [1], permettent (notamment) une nouvelle approche des protocoles de PIR.

Soit $\mathcal{F}$ une famille de fonctions $f : \{0,1\}^n \to \mathbb{G}$, où $\mathbb{G}$ est un groupe abélien. Un m-partage FSS pour $\mathcal{F}$ est un moyen de partager (additivement) secrètement n'importe quelle fonction de $\mathcal{F}$.

Un cas particulier important de FSS est constitué des "distributed point functions", qui permettent de partager des fonctions indicatrices (ou "point functions") du type $f_{\alpha,\beta}$, $\alpha \in \{0,1\}^n$, $\beta \in \mathbb{G}$, telles que : $f_{\alpha,\beta}(\alpha) = \beta$, et $f_{\alpha,\beta}(x) = 0$ pour tout $x \neq \alpha$.

Autrement dit, une "distributed point function" (DPF) est un m-FSS pour la classe des fonctions indicatrices. Les DPFs ont été principalement étudiées et construites dans le cas de $m = 2$ parties. Dans ce cas, on note les parts f_0 et f_1.

Dans une phase préliminaire du projet, il s'agit de faire un état de l'art des protocoles de PIR à deux serveurs, pour mettre en évidence les plus performants (en termes de complexité de communication, coût de stockage et complexité de calcul).

Ensuite, l'étudiant mettra en œuvre une DPF avec $m = 2$ en utilisant les algorithmes proposés dans [2], puis un protocole de PIR utilisant cette DPF, comme décrit dans [1]. Egalement, il implantera un PIR avec mise à jour utilisant DPF.

Dans une deuxième phase du projet, il s'agira de considérer qu'un client peut être malicieux. Dans ce contexte, l'étudiant approfondira la notion de "DPF vérifiable", introduite dans [2], qui permet aux serveurs de vérifier que les parts f_0 et f_1 générées par le client et données à ceux-ci sont bien correctes. Il mettra en œuvre une DPF vérifiable avec étude de ses performances, notamment en comparaison avec une DPF simple.

Un dernier volet du travail sera d'envisager l'application de ces schémas de PIR à divers scénarii de recherche/mise à jour confidentielle dans des bases de données distantes.

Bibliographie :

[1] Distributed Point Functions and their Applications - Gilboa, Ishai, Eurocrypt 2014.
[2] Function Secret Sharing : Improvements and Extensions - Boyle, Gilboa, Ishai, CCS2016.

Livrables :
Rapport présentant la problématique du PIR.
Mise en oeuvre de DPF et DPF vérifiable, et tableaux de performances des protocoles de PIR associés.