Algèbre linéaire exacte pour le retrait privé d'informations.

Calcul scientifique, calcul exact, protection de la vie privée.

Contact :	Jean-Guillaume.Dumas@imag.fr, tél : 04 76 51 48 66.
Laboratoire :	Jean Kuntzmann (LJK), tour IRMA, BP 53 X 51, av. des Mathématiques, 38041 Grenoble. http://ljk.imag.fr
Rémunération :	Standard par le laboratoire ou dans le cadre du projet NSF-ANR HPAC High Performance Algebraic Computations, http://hpac.gforge.inria.fr.
Poursuites :	Thèse en lien avec le projet HPAC ; mobilité partielle possible aux USA North Carolina State U., U. of Delaware, etc.

Les protocoles de retrait privé d'information (*Private Information Retrieval*) permettent de récupérer des éléments d'une base de données sans révéler à la base de quels éléments il s'agit. La problématique voisine du filtre à mots-clefs secrets (*Private Searching*) permet de demander à un serveur d'extraire d'une base de documents ceux qui correspondent à un ensemble de critères eux aussi gardés secrets [1].

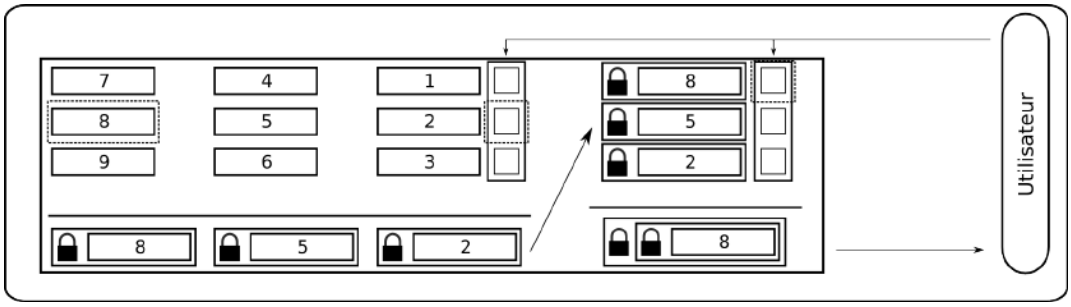

Figure 1: Retrait privé avec récursion (base de taille 9 vue comme 3×3): la requête sélectionne d'abord la ligne, puis la bonne colonne dans cette ligne, à chaque fois par un produit de matrices effectué en aveugle par le serveur.

Une base de donnée étant un ensemble discret, il est nécessaire d'utiliser des méthodes d'algèbre linéaire exacte afin de traiter les requêtes. Sur des corps finis de la taille du mot machine, les méthodes exactes sont dorénavant plus rapides que les méthodes approchées [2]. Néanmoins, dans le cadre du retrait privé d'information, la taille des bases de données envisagées nécessite d'augmenter la taille des corps considérés.
La première partie du sujet du stage consiste ainsi à combiner efficacement méthodes matricielles rapides, méthodes modulaires, méthodes rapides sur les entiers à précision arbitraire, afin d'étendre les routines d'algèbre linéaire à des corps finis de taille quelconque dans un environnement multi-cœurs.
La seconde partie consiste à comparer les différentes approches possibles de chiffrement homorphique (voir par exemple http://crypto.stanford.edu/pir-library/ ou la litterature sur le chiffrement homomorphe, http://www.cs.ut.ee/~lipmaa/crypto/link/public/fhe.php) afin de réaliser un retrait d'information privé efficace.

References

[1] Carlos Aguilar, Laurent Fousse et Philippe Gaborit : Filtres à mots-clefs secrets et réseaux euclidiens. *In Atelier Protection de la Vie Privée, Annecy, France*, mai 2010. http://www-verimag.imag.fr/~async/CCIS/talks_09/Laurent_Fousse.pdf.

[2] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet : Dense linear algebra over prime fields. *ACM Transactions on Mathematical Software*, 35(3):1–42, novembre 2008.

[3] Sergey Yekhanin : Private information retrieval. *Communication of the ACM*, 53(4):68–73, avril 2010.