Calcul Sécurisé sur Réseaux Chiffrés

SCENE

Appel : AAPG

Année : 2021

Instrument : ANR JCJC

Contact : couteau@irif.fr

COORDINATEUR : Geoffroy Couteau

PARTENAIRES : IRIF

Résumé (3 lignes max) : Les promesses de l'apprentissage machine sont immenses, mais requièrent la manipulation de données souvent sensibles. Ce projet vise à développer des méthodes cryptographiques efficaces pour manipuler des données dans de telles applications, sans compromettre leur sécurité.

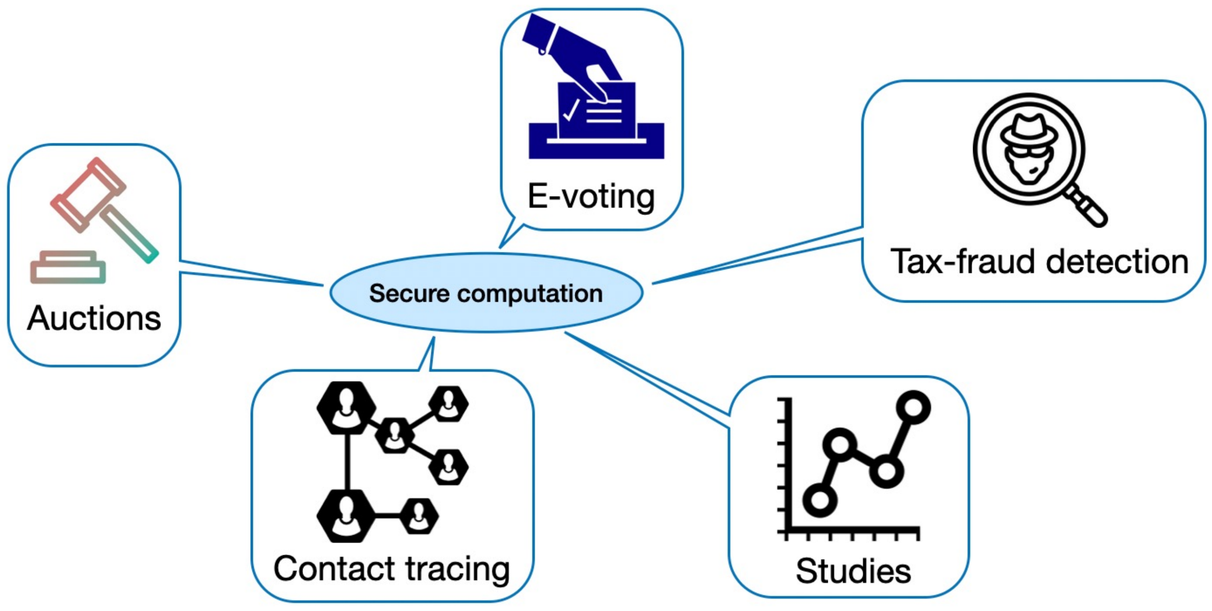
CONTEXTE ET OBJECTIFS

Nos communications en ligne sont aujourd'hui très majoritairement chiffrées, assurant la protection des données sensibles que nous transmettons. Cependant, il devient de plus en plus courant d'utiliser nos données dans un cadre plus large, où une entité externe doit pouvoir les donner en entrée à des algorithmes : c'est le cas lorsque nous utilisons des service en ligne (Cloud, réseaux sociaux, applications comme Google Photo, etc) ou lorsque des entreprises ou laboratoires entraînent des algorithmes sur de grandes bases de données privées, par exemple pour la recherche médicale. Hélas, les méthodes usuelles d'anonymisation des données sont aujourd'hui largement reconnues comme inefficaces. Il devient donc urgent de réinventer la protection des données, en trouvant des méthodes réconciliant ce besoin crucial avec leur usage dans les applications sus-mentionnées.

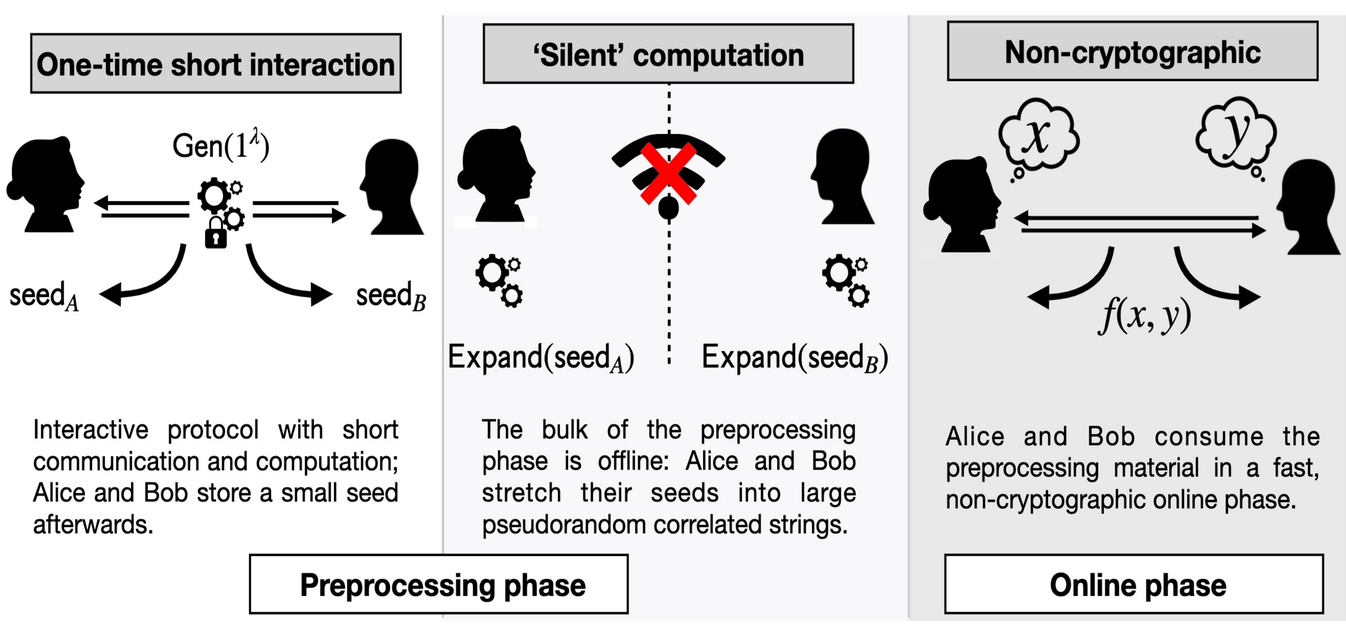
MÉTHODOLOGIE ET RÉSULTATS

Le projet vise à développer de nouvelles méthodes de calcul sécurisé, permettant la manipulation de données dans le cadre de calculs arbitraires, sans compromettre leur sécurité. Si le calcul sécurisé est faisable en théorie, il reste très loin d'être efficace en pratique. Cependant, des méthodes récentes, reposant sur des connexions entre la génération sécurisée d'aléa corrélé, qui est en quelque sorte le « carburant » du calcul sécurisé, et la théorie mathématiques des codes, semblent pouvoir changer la donne. Le projet vise à explorer et améliorer ces connections, avec comme objectifs (1) d'améliorer les protocoles existant de génération sécurisée d'aléa corrélé, (2) d'étudier en profondeur la sécurité des méthodes existantes (un objectif en lien avec la théories des codes et celle des fonctions booléennes) et (3) d'étudier les limites théoriques de cette nouvelle approche.

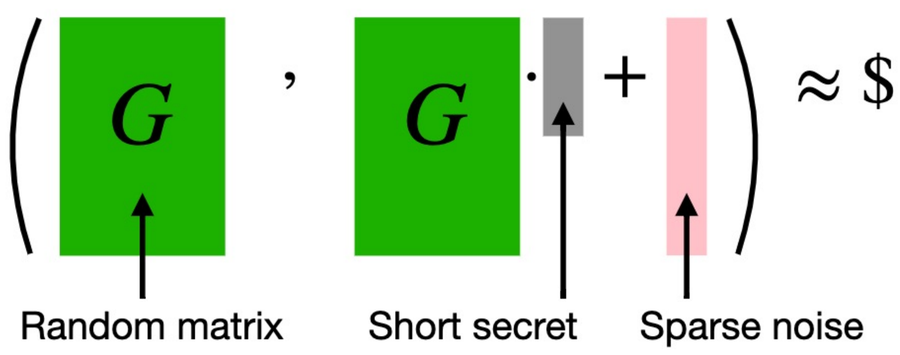
Calcul sécurisé – Applications



Un nouveau modèle de communication



Un outil clé de théorie des codes



RÉSULTATS PRÉLIMINAIRES

- Deux articles de recherches, à EUROCRYPT'21 (avec Pierre Meyer) et à CRYPTO'21 (avec Peter Rindal et Srinivasan Raghamuran) sur les aspects respectivement théoriques et pratiques de la génération efficace d'aléa corrélé
- Plusieurs projets en cours avec les membres du consortium, dont Yann Rotella (cryptanalyse de constructions) et Adi Rosén (limites théoriques de l'aléa corrélé)