Fabien Laguillaumie

Laboratoire d'Informatique, de Robotique et
de Microélectronique de Montpellier
Université de Montpellier
161, rue Ada
34095 Montpellier cedex
fabien.laguillaumie@lirmm.fr

Guilhem Castagnos

Institut de Mathématiques de Bordeaux
Université de Bordeaux
351 cours de la Libération
33405 Talence cedex
guilhem.castagnos@math.u-bordeaux.fr

Objet : Soutien à la candidature d'Ida Tucker au prix de thèse du GDR Sécurité Informatique 2021

Nous avons co-dirigé la thèse d'Ida Tucker entre octobre 2017 et octobre 2020 au LIP à l'ÉNS de Lyon. Nous l'avions identifiée dès la première année de son master *Cryptologie & Sécurité Informatique* à Bordeaux comme une excellente candidate, à la double culture mathématique et informatique, aussi lui avons nous proposé un stage de M2, qu'elle a brillamment réussi. Elle a accepté de poursuivre en thèse avec nous, sur un support ANR, et ces trois années de thèse allèrent bien au delà de nos attentes, révélant Ida comme une jeune chercheuse exceptionnelle.

La thèse d'Ida s'inscrit dans le contexte de la sécurisation de données extrêmement volatiles, dont la quantité explose, et qui sont stockées sur des plates-formes de plus en plus hétérogènes. Ce ne sont plus seulement les données qui sont protégées, mais leur traitement ou l'accès fin à celles-ci.

Dans sa thèse, Ida a créé un cadre générique et modulaire pour concevoir des systèmes cryptographiques avancés, à partir de briques élémentaires non triviales, les fonctions de hachage projectives, pour répondre aux défis précédemment mentionnés. Grâce à son approche, Ida a exploré deux axes de recherche. Premièrement, elle a pu concevoir des protocoles de chiffrement permettant un traitement des données à partir de leurs chiffrés, appelés *chiffrement fonctionnel*. Ce type de protocole permet de contrôler la quantité d'information sur le message que l'on peut obtenir à l'exécution du déchiffrement (par exemple à partir d'un email chiffré, une clé de déchiffrement peut permettre de savoir si l'email est un spam ou non, et *rien* d'autre). La découverte de cette primitive fut une percée fondamentale en cryptographie, et les progrès théoriques sont extrêmement prometteurs. Néanmoins, elle est très loin d'un déploiement en grandeur réelle. Ida s'est donc restreinte à une fonctionnalité particulière, qui consiste à calculer des statistiques linéaires sur des données chiffrées (pour des statistiques sur des données médicales qu'on souhaite garder anonyme par exemple), et

a obtenu les algorithmes les plus efficaces en terme de bande passante et de temps de calculs. Elle a réussi notamment à rendre efficaces et pratiques des protocoles qui atteignent le plus haut niveau de sécurité possible. Une partie de ce travail a été publiée à la conférence ASIACRYPT en 2018, qui est considérée comme la troisième conférence la plus importante du domaine. Une autre partie est actuellement en cours de soumission.

Deuxièmement, Ida a démontré que son approche s'appliquait au calcul distribué sécurisé, et plus particulièrement pour le calcul distribué du standard de signature ECDSA, qui est largement déployé, et au cœur de nombreuses cryptomonnaies. Le design assez atypique de ce protocole rend complexe sa distribution entre plusieurs parties. Faire un calcul partagé de ces signatures est un sujet actuellement très animé, notamment par les meilleurs chercheurs en cryptographie (comme Rosario Gennaro - City University of New York, Ran Canetti - Boston University, ou Yehuda Lindell - Bar Ilan University). Dans ce contexte hautement compétitif, Ida a obtenu des avancées majeures notamment en spécialisant son cadre par un outil mathématique original, le groupe de classes d'idéaux de corps quadratiques imaginaires. Ida a ainsi pu partager la signature de façon la plus efficace en terme de bande passante, qui est une mesure cruciale en pratique. Ainsi, elle a obtenu dans un article paru à CRYPTO en 2019 (première conférence de cryptographie), le calcul entre deux parties d'une signature ECDSA le plus efficace. Elle a également amélioré le calcul à seuil (un quorum est nécessaire pour réaliser le calcul) d'une signature ECDSA dans un travail paru à PKC en 2020, qui est une excellente conférence du domaine. Elle a été en contact avec des chercheurs de la start-up israélienne Zengo qui développe un porte-monnaie électronique avec clé partagée, qui a implémenté sa solution. Ida a donc pu valoriser ainsi une partie de ces travaux, en prouvant que des solutions théoriques pouvaient avoir un impact pratique.

Ida a toujours pris une part fondamentale et prépondérante dans tous ses travaux : elle a notamment assimilé des modèles de sécurité très complexes et réalisé toutes les preuves de sécurité. Elle a également une facilité de rédaction remarquable. Son mémoire de thèse reflète son goût pour une présentation de qualité. Plutôt que de suivre ses articles, Ida a pris le parti d'une réorganisation complète de ses travaux en unifiant ses résultats ce qui permet une lecture fluide et synthétique.

Tout au long de son doctorat, Ida a su nouer des relations avec des collègues en dehors de sa zone de confort, démontrant son indépendance et sa maturité scientifiques ainsi que sa facilité d'intégrer de petits groupes de chercheurs.

Les riches travaux d'Ida lui ont permis d'obtenir de nombreuses expertises précieuses. D'une part, elle participe au renouveau de la cryptographie utilisant les groupes de classe de corps quadratiques imaginaires. Cet outil connaît un fort regain d'intérêt ces dernières années car il se prête bien aux protocoles décentralisés sans tiers de confiance, tels que les

blockchains. D'autre part, ses travaux autour de la signature ECDSA lui ont permis d'acquérir une expertise en calcul distribué sécurisé, domaine qui se développe très rapidement avec l'émergence de nombreuses startups mais qui est très peu représenté dans la communauté cryptographique française.

En plus de ces qualités scientifiques admirables, Ida participe à l'animation, organisant des séminaires et journées locales pour les doctorants, ainsi que des conférences nationales et internationales. Elles contribue à des actions scientifiques vers les jeunes, et particulièrement vers les jeunes filles. Très active et impliquée, elle assure des responsabilités collectives : elle a par exemple été membre élue du conseil de laboratoire du LIP.

Elle fait l'effort de constituer des dossiers pour obtenir des financements : elle a obtenu une bourse du labex MiLyon afin de financer un séjour à l'ETH Zurich (malheureusement annulé par la pandémie).

Elle a été lauréate de la prestigieuse bourse jeunes talents l'Oréal Unesco pour les femmes et la science, en octobre 2020, récompensant l'excellence de ses travaux et son engagement.

Pour résumer, Ida se positionne actuellement comme une cryptologue prometteuse, qui s'est déjà constitué un réseau de collaborateurs extrêmement solide. Elle est parvenue à obtenir 3 articles dans les conférences les plus prestigieuses de cryptographie, ce qui est remarquable. Ses qualités humaines font d'elle une collègue exceptionnelle : dans un groupe, sa créativité est un catalyseur qui crée une dynamique toujours positive. Elle est investie et n'hésite pas à repousser ses limites. Elle va nous manquer.

Nous soutenons donc avec le plus grand enthousiasme la candidature d'Ida au prix de thèse du GDR Sécurité Informatique.

Fabien Laguillaumie

Guilhem Castagnos