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

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

Objet : Soutien à la candidature d'Ida Tucker sur les concours de maîtres de conférences

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 Tucker comme une jeune chercheuse exceptionnelle.

Les travaux de thèse d'Ida Tucker participe au renouveau actuel de la cryptographie utilisant les groupes de classes de corps quadratiques imaginaires. La difficulté du calcul de l'ordre de ces groupes en font un outil adapté pour les protocoles décentralisés sans tiers de confiance, tels que les blockchains.

Inspirée par ces groupes, Ida Tucker 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. Grâce à cette approche, Ida Tucker 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 dans la cryptographie, et les progrès théoriques sont extrêmement prometteurs. Néanmoins, elle est très loin d'un déploiement en pratique. Ida Tucker s'est donc restreint à une fonctionnalité particulière, qui consiste à calculer des statistiques linéaires sur des données chiffrées, 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 publié 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 Tucker 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 Tucker a obtenu des avancées majeures notamment en spécialisant son cadre aux groupes de classes d'idéaux de corps quadratiques imaginaires. Ida Tucker 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. D'autre part, Ida Tucker a eu de nombreux contacts avec la startup israélienne ZenGo qui a implanté son protocole bipartite.

Si ces travaux ont été faits avec nous, ainsi qu'avec des collègues de Catania en Italie, Ida Tucker a pris une part fondamentale et prépondérante dans ces collaborations. Elle a notamment réalisé toutes les preuves de sécurité, qui sont très complexes, et liées à des modèles de sécurité sophistiqués. Elle a également une facilité de rédaction remarquable.

Par ailleurs, elle a également obtenu des résultats autour des modules de sécurité matériels actuellement en cours de soumission avec O. Blazy, L. Brouilhet, C. Chevalier, P. Towa et D. Vergnaud. Nous ne participons pas à cette collaboration, au cours de laquelle Ida Tucker a impulsé une dynamique scientifique très positive, aux dires de ses collaborateurs. Tout au long de son doctorat, Ida Tucker 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. Au delà des travaux précédemment mentionnés, Ida Tucker a initié des recherches avec Dennis Hofhein (ETH Zürich) et Claudio Orlandi (Aarhus University). La situation sanitaire a malheureusement ralenti ces opportunités.

Depuis octobre dernier, Ida Tucker a choisi de commencer un post-doctorat à l'IMDEA Software Institute de Madrid, avec Dario Fiore. Ces travaux actuels portent sur la délégation de calculs vérifiables, domaine en plein essor qu'elle projette de développer.

Les riches travaux d'Ida Tucker lui ont permis d'obtenir de nombreuses expertises précieuses. D'une part, autour de la cryptographie utilisant les groupes de classe de corps quadratiques imaginaires, domaine qui a actuellement le vent en poupe et qui compte peu

d'experts à l'échelle mondiale. 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.

Durant sa thèse, Ida Tucker a pu effectuer l'équivalent d'un service d'enseignement d'un enseignant chercheur en tant que vacataire. Elle a enseigné à des publics et des niveaux variés : licence et master à l'université et à l'ENS de Lyon ; ainsi que sur des domaines différents : en informatique et à l'intersection math info (calcul formel, cryptographie). Tous les retours que nous avons eu sont élogieux sur son investissement et ses qualités pédagogiques.

En plus de ces qualités scientifiques et pédagogiques admirables, Ida Tucker 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) et continue cette activité chronophage en Espagne.

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, les travaux d'Ida Tucker lui ont permis d'acquérir une expertise qui serait très précieuse pour les équipes dans lesquelles elle postule. Elle se positionne actuellement comme une cryptologue prometteuse, qui s'est déjà constitué un réseau de collaborateurs extrêmement solide. Ses qualités humaines font d'elle une collègue exceptionnelle : dans un groupe ou une équipe pédagogique, sa créativité est un catalyseur qui crée une dynamique toujours positive. Elle est investie et n'hésite pas à repousser ses limites.

Nous soutenons donc avec grand enthousiasme la candidature d'Ida Tucker au concours de maîtres de conférences.

Guilhem Castagnos

Fabien Laguillaumie