Ida Tucker

IMDEA Software Institute

Campus de Montegancedo, s/n
28223 Pozuelo de Alarcón, Madrid
Espagne
+33 (0)6.44.72.98.51
ida.tucker@imdea.org
https://idatucker.github.io
Nationalité: Française & Britannique

Intérêts de recherche : cryptographie à clé publique, systèmes cryptographiques avancés, calculs distribués sécurisés.

Diplômes et Études

2009–2012 **Classe Préparatoire aux Grandes Écoles (MPSI puis MP)**, *Lycée Michel Montaigne*, Bordeaux, France.

2012–2013 **Licence (L3) de Mathématiques parcours Mathématiques et Informatique**, *Université de Bordeaux*, France, Mention Bien.

2015–2017 **Master Cryptologie et Sécurité Informatique**, *Université de Bordeaux*, France, Mention Très Bien.
Projet M1 : Étude et implantation de l'algorithme SHA-3, comparaison à la construction de Merkle Damgård. Encadré par Emmanuel FLEURY.
Projet M2 : État de l'art en preuves à divulgation nulle de connaissances basées sur les réseaux Euclidiens. Encadré par Guilhem CASTAGNOS.

Stage de Recherche

Mars-Sept 2017 **Stage de Recherche**, *Chiffrement vérifiable de données à faible entropie pour le stockage dédupliqué*, sous la direction de Fabien LAGUILLAUMIE, Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM), Université de Montpellier, Montpellier, France.

Thèse de doctorat

Titre Chiffrement fonctionnel et signatures distribuées fondés sur des fonctions de hachage à projection, l'apport des groupes de classes.

Financement Projet ANR ALAMBIC.

Spécialité Informatique.

Dates Du 1er Octobre 2017 au 19 Octobre 2020.

Laboratoire Laboratoire de l'Informatique et du Parallélisme (LIP) à l'ENS de Lyon.

Affiliation Membre de l'équipe Inria AriC du LIP, de l'équipe Théorie des nombres et de l'équipe Inria LFANT de l'Institut Mathématique de Bordeaux (IMB).

Directeur Fabien LAGUILLAUMIE – Professeur à l'Université de Montpellier, LIRMM (au cours du doctorat : Professeur à l'Université Claude Bernard Lyon 1, LIP).

Co-directeur Guilhem CASTAGNOS – Maître de Conférences HDR à l'Université de Bordeaux, IMB.

Rapporteurs Michel ABDALLA – Directeur de Recherche CNRS, DI ENS, Paris.
Ivan DAMGÅRD – Professeur à Aarhus University au Danemark.

Examinateur·rices Shweta AGRAWAL – Associate Professor à I.I.T. Madras en Inde.
Pierre-Alain FOUQUE – Professeur à l'Université Rennes 1.
Carla RÀFOLS – Lectora Tenure Track à l'Universitat Pompeu Fabra en Espagne.

Libre accès `http://www.theses.fr/2020LYSEN054`

Expérience Professionnelle

Situation actuelle

Depuis 01/10/20 **Post-doctorante**, IMDEA Software Institute, Madrid, Espagne.
Sous la direction de Dario FIORE, Associate Research Professor à l'IMDEA Software Institute.

Développement de Logiciel

2013 - 2015 **Ingénieure Logiciel (CDI)**, *RDT Ltd., Kings Hill, Royaume Uni.*
Implantation en C# et maintenance d'une application permettant aux compagnies d'assurance de gérer leur activité. Travail d'équipe, respect des délais de réalisation des projets, gestion de projet Agile et méthodologie Scrum. Communication directe avec des clients exigeants et influents. Prise de décision.

Articles

Dans mon domaine de recherche (cryptographie), les articles sont publiés essentiellement dans des actes de conférences avec comité de lecture. Par défaut, les auteurs sont ordonnés par ordre alphabétique. Toutes les versions publiées dans des actes font 30 pages, par conséquent je spécifie uniquement le nombre de pages des versions longues (en libre accès).

Acceptés

2020 Bandwidth-efficient threshold EC-DSA. Avec Guilhem CASTAGNOS, Dario CATALANO, Fabien LAGUILLAUMIE et Federico SAVASTA.
- Dans les actes de PKC 2020 (`https://link.springer.com/chapter/10.1007/978-3-030-45388-6_10`).
- Conférence internationale de rang B.
- Sélectionné pour la *Curated list of talks* du séminaire international 'Workshop on Elliptic Curve Cryptography (ECC) 2020' (`https://eccworkshop.org/2020/talks.html`).
- L'article (version longue de 45 p.) est en libre accès : `https://hal.inria.fr/hal-02944825/?`
- Contributrice principale.
- Joint au dossier.

2019 Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations. Avec Guilhem CASTAGNOS, Dario CATALANO, Fabien LAGUILLAUMIE et Federico SAVASTA.
- Dans les actes de CRYPTO 2019 (`https://link.springer.com/chapter/10.1007/978-3-030-26954-8_7`).
- Conférence internationale de rang A*.
- L'article (version longue de 40 p.) est en libre accès : `https://eprint.iacr.org/2019/503.pdf`
- Contributrice principale.
- Joint au dossier.

2018 Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p. Avec Guilhem CASTAGNOS et Fabien LAGUILLAUMIE.
- Dans les actes de ASIACRYPT 2020 (`https://link.springer.com/chapter/10.1007/978-3-030-03329-3_25`).
- Conférence internationale de rang A.
- L'article (version longue de 45 p.) est en libre accès : `https://eprint.iacr.org/2018/791.pdf`
- Contributrice principale.
- Joint au dossier.

Soumissions (en cours de review)

2021 Hardware Security without Secure Hardware: How to Decrypt with a Password and a Server. Avec Olivier BLAZY, Laura BROUILHET, Céline CHEVALIER, Patrick TOWA et Damien VERGNAUD.
- Eprint, version longue de 61 pages : `https://eprint.iacr.org/2020/1571.pdf`

2021 Bandwidth-efficient threshold EC-DSA revisited: Online/Offline Extensions, Identifiable Aborts, Proactive and Adaptive Security. Avec Guilhem CASTAGNOS, Dario CATALANO, Fabien LAGUILLAUMIE et Federico SAVASTA. 46 pages.

2021 A Tighter Proof for CCA Secure Inner Product Functional Encryption: Genericity Meets Efficiency. Avec Guilhem CASTAGNOS et Fabien LAGUILLAUMIE. 47 pages.

Prix et bourses

Octobre 2020 **Lauréate de la bourse jeunes talents l'Oréal Unesco pour les femmes et la science**, *15 000€*.
`https://ins2i.cnrs.fr/cnrsinfo/prix-jeunes-talents-france-2020-loreal-unesco-pour-les-femmes-et-la-science`

Été 2020 **Soutien du labex MiLyon à la mobilité doctorale sortante**, *2 100€*.
Projet de stage de deux mois à l'ETH Zurich avec Denis HOFHEINZ (n'a pas eu lieu du fait de la crise sanitaire).

Exposés

Conférences internationales

Août 2019 **Crypto 2019**, *UCSB*, Santa Barbara, CA, USA.
Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations

Décembre 2018 **Asiacrypt 2018**, *Queensland Université of Technology*, Brisbane, Australia.
Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p

Évènements nationaux

Novembre 2020 **Journées Codage et Cryptographie du GDR IM et du GDR Sécurité Informatique**, *IRISA*.
Bandwith efficient threshold ECDSA.

Octobre 2018 **Journées Codage et Cryptographie du GDR IM et du GDR Sécurité Informatique**, *LIP*, Aussois, France.
Unrestricted Functional Encryption for the Evaluation of Inner Products modulo a prime p.

Exposés Invités

Séminaires

Février 2020 **Séminaire Crypto**, *Aarhus University*, Aarhus, Danemark.
Distributing the elliptic curve digital signature algorithm both securely and efficiently

Janvier 2020 **Séminaire Quarkslab (aka Fridaycon)**, *Quarkslab*, Paris, France.
An introduction to functional encryption and multi-party computation

Janvier 2020 **Séminaire de l'IMDEA Software Institute**, *IMDEA*, Madrid, Espagne.
Bandwidth-efficient threshold EC-DSA

Avril 2019 **Séminaire Crypto**, *ENS de Lyon*, Lyon, France.
Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations

Mars 2019 **Séminaire C2**, *IRMAR*, Rennes, France.
Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo a prime p

Février 2019 **Séminaire AriC**, *ENS de Lyon*, Lyon, France.
Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo a prime p

Novembre 2018 **Séminaire Lfant**, *IMB*, Bordeaux, France.
Inner Product Functional Encryption modulo a prime p.

Juin 2017 **Séminaire ECO**, *LIRMM*, Montpellier, France.
Verifiable Encryption of Predictable Data for Deduplicated Storage.

Expertise

Rapporteuse externe pour des conférences

Rapports d'articles pour les conférences avec comité de programme et actes suivantes : Eurocrypt 2021, Crypto 2019, Asiacrypt 2020, Cryptographers' Track RSA Conference (CT-RSA) 2021, Applied Cryptography and Network Security (ACNS) 2018, Australasian Conference on Information Security and Privacy (ACISP) 2019, International Conference on Security and Cryptography for Networks (SCN) 2018.

Enseignement

2019-2020
- TDs de calcul formel, en M1 à l'ENS de Lyon (10h).
- TPs de cryptographie en M1 à la Faculté des Sciences de l'Université Claude Bernard Lyon 1 (UCBL 1) (15h).
- TDs et TPs de bases de l'architecture pour la programmation en L1 à l'UCBL 1 (34h).

2018-2019
- TDs et TPs de systèmes d'exploitation en L2 à l'UCBL 1 (42h).
- TPs de cryptographie en M1 à la Faculté des Sciences de l'UCBL 1 (15h).
- TPs de réseaux et programmation web en L1 à l'UCBL 1 (18h).

2017-2018
- TPs de cryptographie en M1 à la Faculté des Sciences de l'UCBL 1 (15h).
- TPs de réseaux et programmation web en L1 à l'UCBL 1 (36h).

2017 Assistante TP de sécurité des logiciels en M1 à l'Université de Bordeaux.

2016-2017 Tutorats Mathématiques : soutien scolaire ponctuel en mathématiques aux élèves de licence de l'Université de Bordeaux.

Responsabilités Administratives

2018-2020 **Membre élue au conseil de laboratoire**, *ENS de Lyon.*
Représentente des membres non-permanents (un conseil d'environ 3h par mois).

2019-2020 **Organisation du séminaire des doctorants.**, *ENS de Lyon.*
Séminaire de 30 minutes, organisé une fois par mois. L'objectif étant d'offrir aux doctorants du LIP une vue (relativement haut niveau) des sujets de recherches abordés dans les autres équipes.

2019 **Organisation des journées des doctorants du LIP**, *ENS de Lyon.*
Séjour de deux jours avec des formations scientifiques/transversales et des activités ludiques. L'objectif est de créer une cohésion parmi les doctorants du laboratoire.

Octobre 2018 Participation à l'organisation des Journées Codage et Cryptographie du GDR Informatique-Mathématique (IM) et du GDR Sécurité Informatique, LIP, Aussois, France.

Avril 2017 Bénévole à la conférence internationale IEEE S & P, et aux Workshops Eurocrypt 2017, Université Pierre et Marie Curie, Paris, France.

Diffusion

Janvier-Juin 2021 **Plan soutien scolaire pour lycéennes**, *2h par semaine*, Dématérialisé, Organisé par la Fondation d'Entreprise L'Oréal, et les associations Institut Télémaque et Banlieue School.

Novembre 2020 **Inscription sur la liste *Skype a Scientist***, Dématérialisé, Organisation éducative à but non lucratif qui permet aux scientifiques d'organiser des vidéoconférences avec des classes d'étudiants.
`https://www.skypeascientist.com`

2020 et 2017 **Journée Emploi Maths**, *Université de Bordeaux*, Rencontre entre étudiants, chercheurs et entreprises.
`https://uf-mi.u-bordeaux.fr/sites/jemi/`

Octobre, Novembre 2020 **Entretiens avec Médias Régionaux**, *Pays Basque, Bordeaux, Lyon et Montpellier.*, Radio (NRJ, RTL2), Magazine (Cosmopolitan), journaux régionaux, Diffusion de ma recherche (médiation liée au prix L'Oréal).

Juin 2019 **Exposé de vulgarisation scientifique pour des collégiens et lycéens ayant participé au concours Alkindi**, *École Normale Supérieure de Lyon*, Lyon, France.
`https://concours-alkindi.fr/main.html`

Avril 2018 **Rencontre collégiens-chercheurs**, *Collège Maria Casarès*, Rillieux-la-Pape, France.

Participation à des Évènements Scientifiques

Octobre 2018 **REDOCS 2018, Rencontres Entreprises-DOCtrorants en Sécurité**, *Gif-sur-Yvette, France*, Évènement CNRS dans lequel des doctorants en sécurité informatique travaillent pendant une semaine sur des problèmes posés par des industries.

Avec Chloé HÉBANT, Cédric LEFEBVRE, Étienne LOUBOUTIN et Elie NOUMON ALLINI nous avons travaillé sur un sujet proposé par Worldline (groupe Atos). Le problème est le suivant : lors des transactions bancaires, il est courant d'utiliser des algorithmes de détection de fraude. Pour fonctionner, ces algorithmes utilisent actuellement les données confidentielles des clients en clair, ce qui peut constituer une infraction au règlement général sur la protection des données (RGPD). Pour pallier à ce problème, nous avons proposé deux protocoles basés sur le chiffrement homomorphe permettant de détecter ces tentatives de fraude sur des données chiffrées. Nous avons démontré que ces protocoles calculent bien la fonction exacte requise, et qu'ils sont sûrs dans le modèle honnête mais curieux.

Écoles Jeunes Chercheurs

Août 2018 Swedish Summer School in Computer Science 2018 : mini-cours sur l'informatique quantique par Ronald de Wolf et sur les réseaux Euclidiens en cryptographie par Oded Regev, Stockholm, Suède.

Mars 2018 Post-Scryptum Spring school : méthodes algorithmiques pour la cryptographie post-quantique, Grenoble, France.