Ida Tucker

Post Doctoral researcher in Cryptography

☎ *06.44.72.98.51*
✉ *ida.tucker@imdea.org*
Nationality: French & British

*Research Interests: advanced cryptographic systems,
public key cryptography, multi-party computation,
zero-knowledge proof systems.*

Education

Oct 2017 - Oct 2020 **PhD Student**, *École Normale Supérieure de Lyon*, France.
Construction of Advanced Cryptographic Systems from Homomorphic Building Blocs. Funded by the ANR project ALAMBIC. Supervised by Guilhem Castagnos and Fabien Laguillaumie.
Focus on the construction of:
- Practical and efficient schemes for functional encryption.
- Generic tools ensuring security against active adversaries.
- Distributed digital signatures.

2015–2017 **Master of Science in Cryptology and IT Security**, *University of Bordeaux*, France, Mention Très Bien.
Included the study of Advanced Cryptography, Cryptanalysis, Elliptic Curves, Computer Algebra, Automata and Complexity, Information Theory, Smart Cards, Software Security, Software Verification, Network Security, Operating Systems, C and Java Programming.

2012–2013 **Bachelor's Degree in Mathematics specialised in Mathematics and Computer Science**, *University of Bordeaux*, France, Mention Bien.

2009–2012 **Preparatory School for entering Top Schools, in Mathematics, Physics and Engineering**, *Lycée Michel Montaigne*, Bordeaux, France.

Projects

2017 Masters' research project (2nd year): "State of the art in lattice based proofs of knowledge".

2016 Masters' research project (1st year): "Study and implementation of the SHA-3 hashing algorithm, and comparison to systems based on the Merkle Damgård construction".

Employment

Research

Oct 2019 - Now **PostDoctoral Researcher**, *IMDEA Software Institute*, Madrid, Spain.

March-Sept 2017 **Research Internship**, *L.I.R.M.M.*, Montpellier, France.
Internship in the field of lattice-based cryptography supervised by Fabien Laguillaumie. Subject: Verifiable encryption of predictable data for deduplicated storage.

Teaching

2020 **Teaching Assistant**.
- Cryptography (M1): 15h at University Claude Bernard Lyon 1
- Computer Algebra (M1): 10h at ENS de Lyon

2019 **Teaching Assistant**, *University Claude Bernard Lyon 1*.
- Cryptography (M1): 15h; Operating Systems (L2): 42h; Networking & Web Programming (L1): 18h; Software Architecture (L1): 58h

2018 **Teaching Assistant**, *University Claude Bernard Lyon 1*.
- Cryptography (M1): 15h; Networking & Web Programming (L1): 36h

2017 **Teaching Assistant**, *University of Bordeaux*, Software Security (M1).

Software Development

Nov 2013 - Aug 2015 **Software Engineer**, *RDT Ltd.*, Kings Hill, UK.
Implementation and customer support.

Publications

G. Castagnos, F. Laguillaumie and I. Tucker. Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p. Proc. of Asiacrypt 2018, Part II, Springer LNCS Vol. 11273, 1-32 (2018) Copyright IACR. `http://eprint.iacr.org/2018/791`

G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta, I. Tucker. Two-Party ECDSA from Hash Proof Systems and Efficient Instantiations. CRYPTO 2019, Part III, LNCS 11694, p. 191–221. Springer, 2019. `http://eprint.iacr.org/2019/503`

G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta, I. Tucker. Bandwidth-efficient threshold EC-DSA. Public-Key Cryptography (PKC) 2020 Part II., LNCS 12111, p. 266-296. Springer 2020 `http://eprint.iacr.org/2020/084`

Talks

Scientific Events

November 2020 **The GT-C2 Days**, *IRISA*, Online.
Bandwith efficient threshold ECDSA.

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

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

January 2020 **Invited Talk**, *IMDEA Software Institute*, Madrid, Spain.
Distributing the elliptic curve digital signature algorithm both securely and efficiently

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

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

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

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

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

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

October 2018 **The GT-C2 Days**, *LIP*, Aussois, France.
Unrestricted Functional Encryption for the Evaluation of Inner Products modulo a prime p.

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

Science Popularisation

November 2019 **Journée Filles et Informatique 2019**, *Maison des Mathematiques et de l'Informatique*, Lyon, France.

April 2018 **Encounters with middle school students**, *Collège Maria Casarès*, Rillieux-la-Pape, France.

Active Involvement in Scientific Events

October 2018 REDOCS 2018, Rencontres Entreprises-DOCtrorants en Sécurité, CNRS event in which PhD students in IT security work for a week on problems set by industries, Gif-sur-Yvette, France.

Volunteering

October 2018 GT-C2 Days, LIP, Aussois, France.

April 2017 IEEE Symposium on Security and Privacy, and EUROCRYPT 2017 Workshops, University Pierre et Marie Curie, Paris, France.

Young Researchers' Schools

August 2018 Swedish Summer School in Computer Science 2018, mini-courses on Quantum Computing by Ronald de Wolf and Lattices and Cryptography by Oded Regev, Stockholm, Sweden.

March 2018 Post-Scryptum Spring school, dedicated to algorithmic methods for post-quantum cryptography, near Grenoble, France.

Training

Jan-March 2018 Science popularisation: communicating one's research to all publics, with Isabelle Bonardi at the University of Lyon, France.

Administrative Responsibilities

2018-2019 Elected representative of non permanent members at the LIP laboratory council.

2018 Organising *PhD Days* social event. Aims to bring together PhD students of the LIP laboratory, to share experience and learn from one another.

Extra-Curricular Activities

Languages Bilingual in French and English. Intermediate level in Spanish. Learning Italian.