

Thomas Debris-Alazard

BORN IN PARIS, FRANCE, MAY 1, 1991 · RESEARCHER SCIENTIST AT INRIA

58 rue du ruisseau, Paris 75018

☎ (+33) 631053595 | ✉ thomas.debris@inria.fr | 🌐 <http://tdalazard.io/>

Research Interests

Research Area: *Public-Key Cryptography (theory, designs, cryptanalysis, standardization) with a focus on code and lattice-based cryptography*

- **Cryptographic Designs,**
- **Cryptanalysis,**
- **Security estimates,** study of the generic decoding problem
- **Security proof,** in the classical or quantum model
- **Algorithms, Reduction** classical and quantum

Employment

Inria Saclay

RESEARCHER SCIENTIST (CHARGÉ DE RECHERCHE)

Project-Team: Grace

Saclay, France

Sept. 2020 - Present

Royal Holloway, University of London, UK

POSTDOC IN THE INFORMATION SECURITY GROUP DEPARTMENT

Advisor: Pr Martin R. Albrecht

London, UK

Sept. 2019 - Sept. 2020

Education

Inria Paris

PH.D., CODE-BASED CRYPTOGRAPHY: NEW APPROACHES FOR DESIGN AND PROOF ; CONTRIBUTION TO

CRYPTANALYSIS

Advisor: Pr Jean-Pierre Tillich

Paris, France

Sept. 2016 - Sept. 2019

École Normale Supérieure de Cachan (ENS)

THESIS, CODE-BASED CRYPTOGRAPHY: STUDY OF A GENERIC DECODING ALGORITHM, STATISTICAL DECODING

Advisor: Pr Jean-Pierre Tillich

Paris, France

Mar. 2016 - Sept. 2016

MASTER MPRI (PARISIAN MASTER OF RESEARCH IN COMPUTER SCIENCE).

Main Topics: Cryptography, Complexity, Security reductions, Gröebner basis, Quantum algorithms

Sept. 2015 - Sept. 2016

AGRÉGATION DE MATHÉMATIQUES OPTION INFORMATIQUE.

Sept. 2014 - Sept. 2015

Honors and Awards

2021-2024 **ANR JCJ**

COLA: AN INTERFACE BETWEEN CODE AND LATTICE-BASED CRYPTOGRAPHY

200 000 €

2021 **Finalist for the Cor Baayen Young Researcher Award**

ERCIM

2020 **Gilles Kahn Thesis Award**

THOMAS DEBRIS-ALAZARD UNDER THE SUPERVISION OF JEAN-PIERRE TILlich

Société Informatique de France

2019

Best Paper Award, Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes

THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILlich

Asiacrypt '19

Scientific Publications

- 2022 **An Algorithmic Reduction Theory for Binary Codes: LLL and more** *IEEE Information Theory '22*
THOMAS DEBRIS-ALAZARD, LÉO DUCAS AND WESSEL P.J. VAN WOERDEN
- 2021 **Classical and Quantum algorithms for generic Syndrome Decoding problems and applications to the Lee metric** *PQCrypto '21*
ANDRÉ CHAILLOUX, THOMAS DEBRIS-ALAZARD AND SIMONA ETINSKI
- 2020 **Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures** *PKC '20*
ANDRÉ CHAILLOUX AND THOMAS DEBRIS-ALAZARD
- 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes** *Asiacrypt '19*
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH
- 2019 **Ternary syndrome decoding with large weights** *SAC '19*
RÉMI BRICOUT, ANDRÉ CHAILLOUX, THOMAS DEBRIS-ALAZARD AND MATTHIEU LEQUESNE
- 2018 **Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme** *Asiacrypt '18*
THOMAS DEBRIS-ALAZARD AND JEAN-PIERRE TILICH
- 2017 **Statistical Decoding** *ISIT '17*
THOMAS DEBRIS-ALAZARD AND JEAN-PIERRE TILICH

Preprints

- 2022 **On Codes and Learning with Errors over Function Fields** *iacr.org*
MAXIME BOMBAR, ALAIN COUVREUR AND THOMAS DEBRIS-ALAZARD
- 2021 **Wavelet: Code-based postquantum signatures with fast verification on microcontrollers** *iacr.org*
GUSTAVO BANEGAS, THOMAS DEBRIS-ALAZARD, MILENA NEDELJKOVIĆ AND BENJAMIN SMITH
- 2021 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem** *arxiv.org*
THOMAS DEBRIS-ALAZARD, MAXIME REMAUX AND JEAN-PIERRE TILICH
- 2020 **On the Hardness of Code Equivalence Problems in Rank Metric** *arxiv.org*
ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT
- 2019 **About Wave Implementation and its Leakage Immunity** *iacr.org*
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH
- 2017 **The problem with the SURF scheme** *arxiv.org*
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH

Teaching

MPRI (2021-2022)

- **Error-correcting codes and applications to cryptography (with Anne Canteaut and Alain Couvreur)**, introduction to code-based cryptography

ENS Lyon (2021-2022)

- **Post-quantum cryptography (with Damien Stehlé and Benjamin Wesolowski)**, introduction to code-based cryptography

Polytechnique (2021-2022)

- **Introduction to cryptology (INF558)**, under the supervision of François Morain

Polytechnique (2020-2021)

- **Introduction à l'informatique (INF361)**, under the supervision of Philippe Chassignet and François Morain
- **Introduction to cryptology (INF558)**, under the supervision of François Morain

ENSTA (2020-2021)

- **Mathématiques discrètes pour la protection de l'information**, under the supervision of Françoise Levy-Dit-Vehel

University Paris-Sorbonne (2016-2019)

- **Advanced Cryptography**, Master 1 under the supervision of Damien Vergnaud
- **Introduction of Cryptography**, 3rd year Bachelor under the supervision of Valérie Ménéssier-Morain
- **Environment and Development in Linux**, 2nd year Bachelor under the supervision of Valérie Ménéssier-Morain
- **Programming in C**, 1st year Bachelor

Program Committees

2022 **Journées Codage & Cryptographie (JC2)**

Presentations

Seminars and Conferences

Oct, 2021	Quantum Reduction of Finding Short Code Vectors to the Decoding Problem , DAGSTUHL SEMINAR, QUANTUM CRYPTANALYSIS	<i>Dagstuhl</i>
Sept, 2021	Quantum Reduction of Finding Short Code Vectors to the Decoding Problem , ENS LYON, RHUL AND CWI	<i>Online</i>
June, 2020	Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures , PKC	<i>Online</i>
Dec, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , ASIACRYPT 19'	<i>Kobe</i>
Oct, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR LIP6	<i>Université Jussieu, Paris</i>
Oct, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR, RESEARCH TEAM GRACE	<i>Inria, Paris-Saclay</i>
Sept, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , LONDON-ISH LATTICE CODING AND CRYPTO MEETINGS	<i>Imperial College, London</i>
June, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CBC 19'	<i>Darmstadt</i>
June, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CCA SEMINAR	<i>Université Jussieu, Paris</i>
May, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTO MEETING	<i>ENS, Lyon</i>
Feb, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR	<i>PQShield, Oxford</i>
Jan, 2019	Wave: A New Code-Based Signature Scheme , CRYPTOGRAPHY SEMINAR	<i>Research Institute, Rennes</i>

Dec, 2018	Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme , ASIACRYPT 18'	<i>Brisbane</i>
Nov, 2018	WAVE: A New Code-Based Signature Scheme , ACROCRYPT	<i>Research Institute, Caen</i>
Oct, 2018	Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme , JOURNÉES C2	<i>Aussois</i>
June, 2017	Statistical Decoding , ISIT 17'	<i>Aachen</i>
June, 2017	Statistical Decoding and Surf : a new code-based signature scheme , CBC 2017	<i>Tenerife</i>
Apr, 2017	Statistical Decoding , JOURNÉES C2	<i>La Bresse</i>

Workshops

Sept. 2020-	Organization of the team Grace Seminar , PRESENTATIONS: HERE	<i>Inria Saclay</i>
Sept. 2020-	Workshop on Transference , ORGANIZED BY LÉO DUCAS PRESENTATION: SMOOTHING BOUNDS FOR CODES AND LATTICES	<i>CWI</i>
Sept. 2019-2020	Workshop “yet another crypto reading group” , ORGANIZED BY MARTIN R. ALBRECHT PRESENTATION: WORST-CASE HARDNESS FOR LPN AND CRYPTOGRAPHIC HASHING VIA CODE SMOOTHING	<i>Royal Holloway University of London</i>
Mar. 2016 -	Workshop “code-based cryptography” , ORGANIZED BY JEAN-PIERRE TILlich PRESENTATIONS: STATISTICAL DECODING, SURF : A NEW CODE-BASED SIGNATURE SCHEME, TWO ATTACKS AGAINST SCHEMES BASED ON RANK METRIC, NEW RESULTS ABOUT SIGNATURES BASED ON CODES, WAVE, WORST-CASE HARDNESS FOR LPN AND CRYPTOGRAPHIC HASHING VIA CODE SMOOTHING, AN ALGORITHMIC REDUCTION THEORY FOR BINARY CODES: LLL AND MORE, QUANTUM REDUCTION OF FINDING SHORT CODE VECTORS TO THE DECODING PROBLEM, SMOOTHING BOUNDS: FROM LATTICES TO CODES AND BACK TO LATTICES	<i>Inria Paris</i>

Scientific Popularization

2021	Rendez-vous des Jeunes Mathématiciennes et Informatiennes, Fête de la science à l'école Polytechnique, Olympiades de Mathématiques de l'Académie de Créteil
2018	International Tournament of Young Mathematicians (Jury Member)
2018	Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)
2018	Rendez-vous des Jeunes Mathématiciennes et Informatiennes

Skills

Programming	C, Java, Python, jkiloMagma, SageMath
Languages	French (native), English (fluent)

Reviews

2022	DCC, AMC
2021	Eurocrypt, Crypto, CTRSA, DCC, ISIT, PQCrypto, ANR, IMACC, AMC, Latincrypt
2020	AMC, ITW, IEEE
2019	Eurocrypt, ISIT, DCC, PKC
2018	PQCrypto, WCC
2017	C2SI