

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 Interest

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

- **Cryptographic Designs**, Wave, Surf
- **Cryptanalysis**, a signature and an IBE in rank metric
- **Security estimates**, study of the generic decoding problem
- **Security proof**, in the classical or quantum model
- **Algorithmic, Reduction** classical and quantum

Employment

Inria Saclay

RESEARCHER SCIENTIST (CHARGÉ DE RECHERCHE)

Project-Team: Grace

Saclay, France

Sept. 2020 - Present

Education

Royal Holloway, University of London, UK

POSTDOC IN THE INFORMATION SECURITY GROUP DEPARTMENT

Advisor: Pr Martin R. Albrecht

London, UK

Sept. 2019 - Sept. 2020

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

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

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

AGRÉGATION DE MATHÉMATIQUES OPTION INFORMATIQUE.

Paris, France

Mar. 2016 - Sept. 2016

Sept. 2015 - Sept. 2016

Sept. 2014 - Sept. 2015

Awards

2021-2024 **ANR JCJ**

COLA: AN INTERFACE BETWEEN CODE AND LATTICE-BASED CRYPTOGRAPHY

200 000 €

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

- 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

Eprints

- 2021 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem** *arxiv.org*
ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT
- 2020 **On the Hardness of Code Equivalence Problems in Rank Metric** *arxiv.org*
ALAIN COUVREUR, THOMAS DEBRIS-ALAZARD AND PHILIPPE GABORIT
- 2020 **An Algorithmic Reduction Theory for Binary Codes: LLL and more** *iacr.org*
THOMAS DEBRIS-ALAZARD, LÉO DUCAS AND WESSEL P.J. VAN WOERDEN
- 2019 **About Wave Implementation and its Leakage Immunity** *iacr.org*
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH
- 2017 **Surf: a new code-based signature scheme** *arXiv*
THOMAS DEBRIS-ALAZARD, NICOLAS SENDRIER AND JEAN-PIERRE TILICH

Teaching

Polytechnique (2020-2021)

- **Introduction à l'informatique**, under the supervision of Philippe Chassignet and François Morain
- **Introduction to Cryptology**, 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
- **Environment and Development in Linux**, 2nd year Bachelor
- **Programming in C**, 1st year Bachelor

Presentations

Seminars and Conferences

Sept, 2021	Quantum Reduction of Finding Short Code Vectors to the Decoding Problem , ENS LYON, RHUL AND CWI	Online
June, 2020	Tight and Optimal Reductions for Signatures based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures , PKC	Online
Dec, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , ASIACRYPT 19'	Kobe
Oct, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR LIP6	Université Jussieu, Paris
Oct, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR, RESEARCH TEAM GRACE	Inria, Paris-Saclay
Sept, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , LONDON-ISH LATTICE CODING AND CRYPTO MEETINGS	Imperial College, London
June, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CBC 19'	Darmstadt
June, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CCA SEMINAR	Université Jussieu, Paris
May, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTO MEETING	ENS, Lyon
Feb, 2019	Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes , CRYPTOGRAPHY SEMINAR	PQShield, Oxford
Jan, 2019	Wave: A New Code-Based Signature Scheme , CRYPTOGRAPHY SEMINAR	Research Institute, Rennes
Dec, 2018	Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme , ASIACRYPT 18'	Brisbane
Nov, 2018	WAVE: A New Code-Based Signature Scheme , ACROCRYPT	Research Institute, Caen
Oct, 2018	Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme , JOURNÉES C2	Aussois
June, 2017	Statistical Decoding , ISIT 17'	Aachen
June, 2017	Statistical Decoding and Surf : a new code-based signature scheme , CBC 2017	Tenerife
Apr, 2017	Statistical Decoding , JOURNÉES C2	La Bresse

Workshops

Mar. 2016 -	Workshop “code-based cryptography” , ORGANIZED BY JEAN-PIERRE TILlich	Inria Paris
	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	
Sept. 2020-	Workshop on Transference , ORGANIZED BY LÉO DUCAS	CWI
	PRESENTATION: SMOOTHING BOUNDS FOR CODES AND LATTICES	

Scientific Mediation

2021	Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)
2018	International Tournament of Young Mathematicians (Jury Member)
2018	Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (Jury Member)
2018	Les Rendez-vous des Jeunes Mathématiciennes et Informaticiennes

Skills

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

Reviews

2021	Eurocrypt, Crypto, CTRSA, DCC, ISIT, PQCrypto, ANR
2020	Advances in Mathematics of Communications, ITW, IEEE
2019	Eurocrypt, ISIT, DCC, PKC
2018	PQCrypto, WCC
2017	C2SI