# 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

**École Polytechnique** — *Saclay, France*

Teacher Assistant (chargé d'enseignement) — *Sept. 2022 - Present*

Département d'Informatique de l'École Polytechnique (DIX)

**Inria Saclay** — *Saclay, France*

Researcher Scientist (chargé de recherche) — *Sept. 2020 - Present*

Project-Team: Grace

**Royal Holloway, University of London, UK** — *London, UK*

Postdoc in the information security group — *Sept. 2019 - Sept. 2020*

Hosted by Pr Martin R. Albrecht

## Education

**Inria Paris** — *Paris, France*

PH.D., Code-based Cryptography: New Approaches for Design and Proof ; Contribution to Cryptanalysis — *Sept. 2016 - Sept. 2019*

Advisor: Pr Jean-Pierre Tillich

**École Normale Supérieure de Cachan (ENS)** — *Paris, France*

Thesis, Code-Based Cryptography: study of a generic decoding algorithm, statistical decoding — *Mar. 2016 - Sept. 2016*

Advisor: Pr Jean-Pierre Tillich

Master MPRI (Parisian Master of research in computer science). — *Sept. 2015 - Sept. 2016*

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

Agrégation de Mathématiques Option Informatique. — *Sept. 2014 - Sept. 2015*

## Honors and Awards

2021-2024 **ANR JCJ** — *200 000 €*

COLA: An interface between COde and LAttice-based cryptography

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

2020 **Gilles Kahn Thesis Award** — *Société Informatique de France*

Thomas Debris-Alazard under the supervision of Jean-Pierre Tillich

2019 **Best Paper Award, Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes** — *Asiacrypt '19*

Thomas Debris-Alazard, Nicolas Sendrier and Jean-Pierre Tillich

## Scientific Publications

2024 **New Solutions to Delsarte's Dual Linear Programs** *IEEE Information Theory '24*
André Chailloux and Thomas Debris-Alazard

2024 **Exploiting signature leakages: breaking Enhanced pqsigRM** *ISIT '24*
Thomas Debris-Alazard, Pierre Loisel and Valentin Vasseur

2024 **Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs** *STOC '24*
Thomas Debris-Alazard, Pouria Fallahpour and Damien Stehlé

2024 **Reduction from sparse LPN to LPN, Dual Attack 3.0** *Eurocrypt '24*
Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger and Jean-Pierre Tillich

2023 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem** *IEEE Information Theory '23*
Thomas Debris-Alazard, Maxime Remaux and Jean-Pierre Tillich

2023 **On the pseudorandomness of the decoding problem via the Oracle Comparison Problem** *Asiacrypt '23*
Maxime Bombar, Alain Couvreur and Thomas Debris-Alazard

2023 **Smoothing codes and lattices: systematic study and new bounds** *IEEE Information Theory '23*
Thomas Debris-Alazard, Léo Ducas, Nicolas Resch and Jean-Pierre Tillich

2022 **Statistical Decoding 2.0: Reducing Decoding to LPN** *Asiacrypt '22*
Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger and Jean-Pierre Tillich

2022 **On Codes and Learning with Errors over Function Fields** *Crypto '22*
Maxime Bombar, Alain Couvreur and Thomas Debris-Alazard

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 Tillich

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 Tillich

2017 **Statistical Decoding** *ISIT '17*
Thomas Debris-Alazard and Jean-Pierre Tillich

## Preprints

2022 **Worst and Average Case Hardness of Decoding via Smoothing Bounds** *iacr.org*
Thomas Debris-Alazard and Nicolas Resch

2021 **Wavelet: Code-based postquantum signatures with fast verification on microcontrollers** *iacr.org*

Gustavo Banegas, Thomas Debris-Alazard, Milena Nedeljković and Benjamin Smith

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 Tillich

2017 **The problem with the SURF scheme** *arxiv.org*

Thomas Debris-Alazard, Nicolas Sendrier and Jean-Pierre Tillich

# Teaching

## PhD. Supervision

2023- **Pierre Loisel** *with Alain Couvreur*

on code algorithms and cryptanalysis

2020-2023 **Maxime Bombar** *with Alain Couvreur*

on structures codes in cryptography (Defended on december 15, 2023)

## Courses

2023- **Introduction to information theory (INF563)**

École Polytechnique

2022- **Introduction to quantum computing and quantum information (INF587)**

École Polytechnique

2021- **Error-correcting codes and applications to cryptography**

MPRI, with Anne Canteaut and Alain Couvreur

2021-2023 **Post-quantum cryptography, introduction to code-based cryptography**

ENS Lyon, with Damien Stehlé and Benjamin Wesolowski

## Tutorials

Sept. 2024 **Summer School IES Corsica,** introduction to code-based crypotgraphy *Cargèse*

June. 2024 **Introduction to Quantum-Safe Cryptography (IBM Zurich)** introduction to code-based crypotgraphy *Zurich*

Oct. 2023 **CIMPA school: mathematical aspects of post-quantum cryptography,** introduction to code-based crypotgraphy *Rabat*

Aug. 2022 **Summer school in post-quantum cryptography,** introduction to code-based crypotgraphy *Budapest*

June. 2022 **CIMPA: SuSAAN Summer School of Applied Arithmetic,** introduction to research via an open problem in combinatorics *Izmir*

# Invited Talks

2024 **Mathematics for post-quantum cryptanalysis** *Budapest*

2024 **Thirteenth in the series workshop Coding and Cryptography (WCC)** *Perugia*

# Program Committees

2024 **Program committee**

Crypto '25, Eurocrypt '25, PKC '25

2024 **Guest Editor**

Special issue on Code-Based Cryptography in *Designs, Codes and Cryptography*

2021-2023 **Gilles Kahn Award**

Société Informatique de France

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

# Presentations

## Selected Talks at Seminars, Workshops and Conferences

Feb, 2024 **Codes and Lattices in Cryptography: real twins or distant cousins?** Attacc Workshop — *Munich*

Sept, 2023 **Wave: a Code-based Hash and Sign Signature Scheme,** Oxford Post-Quantum Cryptography Summit (PQCS) — *Oxford*

Oct, 2021 **Quantum Reduction of Finding Short Code Vectors to the Decoding Problem,** Dagstuhl Seminar, Quantum Cryptanalysis — *Dagstuhl*

Dec, 2019 **Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes,** Asiacrypt 19' — *Kobe*

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*

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*

Dec, 2018 **Two attacks on rank metric code-based schemes: Ranksign and an identity-based-encryption scheme,** Asiacrypt 18' — *Brisbane*

June, 2017 **Statistical Decoding,** ISIT 17' — *Aachen*

## Workshops

Sept. 2020- **Organization of the team Grace Seminar,** — *Inria Saclay*

Presentations: here

Sept. 2020- **Workshop on Transference,** organized by Léo Ducas — *CWI*

Presentation: Smoothing bounds for codes and lattices

Sept. 2019-2020 **Workshop "yet another crypto reading group",** organized by Martin R. Albrecht — *Royal Holloway University of London*

Presentation: Worst-Case Hardness for LPN and Cryptographic Hashing via Code Smoothing

Mar. 2016 - **Workshop ‘‘code-based cryptography”,** organized by Jean-Pierre Tillich *Inria Paris*

Presentations: On the pseudorandomness of the decoding problem via the Oracle Comparison Problem, 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

## Scientific Popularization

2021 **Rendez-vous des Jeunes Mathématiciennes et Informaticiennes, 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 Informaticiennes**