# Thibauld Feneuil

PARIS, Ile-de-France
France

thibauld.feneuil@cryptoexperts.com
Website: https://www.thibauld-feneuil.fr

## Experience

**2023-...** **Cryptography Expert in CryptoExperts**
I am a researcher at CryptoExperts, a service and technology company in cryptography.
*Research Topics:* Zero-knowledge proofs and post-quantum signature Schemes.

**2020-2023** **Cryptography Engineer in CryptoExperts**
I worked on my Ph.D. while completing several missions for CryptoExperts' clients.

**2020** **Research Internship into cryptography field in CryptoExperts**
*From March 2020 to August 2020.* I studied lattice-based key encapsulation mechanisms, their security and their reduction-based attacks. And more precisely, I studied the impact of side-channel leakages on the security of these schemes.

**2018-2019** **Head of the IT System Department in Telecom Etude**
*From May 2018 to May 2019.* I managed a team of 3-7 members devoted to perform maintenance of servers and digital tools (LDAP, Web, Samba, ...) for a student-run company which develops and manages links between Télécom Paris and firms. Moreover, I developed and set up new tools (intranet...).

**2018** ***Summer*** **Internship in I-Tracing, company in cybersecurity services**
I implemented an audit tool checking automatically the various recommendations of ANSSI (French national agency in cybersecurity) on GNU/Linux configuration (Bash, Python, Django).

**2016** ***Summer*** **Creation of a software for Sainte-Geneviève High School**
I invented in pairs a software to manage oral examinations (C++, Qt). 500-hour project.
Project URL: https://projects.aprilas.fr/spark/

## Education

**2020-2023** **Ph.D. – Sorbonne University, France**
*Topic*: Post-Quantum Signatures from Secure Multiparty Computation
*Supervisors*: Jean-Claude Bajard, Antoine Joux, and Matthieu Rivain
*Website*: https://www.thibauld-feneuil.fr/phd-defense.html

**2017-2020** **Télécom Paris, one of France's top engineering schools**
*2019-2020* : Master M2 MPRI - Cryptography, quantum computing
*2018-2019* : Theoretical computer science, applied mathematics
*2017-2018* : Broad-based education in computer science

**2015-2017** **French preparatory classes in Mathematics & Computer Science**
Preparation for the competitive entrance examinations to French Engineering Schools in the "Grandes Ecoles" system, at Sainte-Geneviève High School, Versailles, France.

**2012-2015** **French Scientific Baccalaureat with highest honors**
Mathematics speciality. At Louis Rascol High School, Albi, France.

## Spoken languages & Computer skills

*French* Native language
*English* Upper-Intermediate B2

*Programming*
*Software:* C, C++ (Qt), Java (Android), Python (Django), Caml
*Web:* PHP 5 (MySQL), HTML, Javascript (JQuery)
*Math:* SageMath, R

**Peer-Reviewed Publications:**

- **RYDE: a digital signature scheme based on rank syndrome decoding problem with MPC-in-the-Head paradigm.** Loïc Bidoux, Jesús-Javier Chi-Domínguez, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain and Adrien Vinçotte. *Designs, Codes and Cryptography – 2025.*
- **Dual Support Decomposition in the Head: Shorter Signatures from Rank SD and MinRank.** Loïc Bidoux, Thibauld Feneuil, Philippe Gaborit, Romaric Neveu, and Matthieu Rivain. *Asiacrypt 2024.*
- **MQ on my Mind: Post-Quantum Signatures from the Non-Structured Multivariate Quadratic Problem.** Ryad Benadjila, Thibauld Feneuil, and Matthieu Rivain. *Euro&P 2024.*
- **Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP.** Thibauld Feneuil. *ACNS 2024.*
- **Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head.** Thibauld Feneuil, and Matthieu Rivain. *Asiacrypt 2023.*
- **Shared Permutation for Syndrome Decoding: New Zero-Knowledge Protocol and Code-Based Signature.** Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. *Designs, Codes and Cryptography – 2023.*
- **Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection.** Thibauld Feneuil, Jules Maire, Matthieu Rivain, and Damien Vergnaud. *Asiacrypt 2022.*
- **Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.** Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. *Crypto 2022.*

**Pre-Prints:**

- **CAPSS: A Framework for SNARK-Friendly Post-Quantum Signatures.** Thibauld Feneuil, and Matthieu Rivain. Available at `https://eprint.iacr.org/2025/061`.
- **Threshold Computation in the Head: Improved Framework for Post-Quantum Signatures and Zero-Knowledge Arguments.** Thibauld Feneuil, and Matthieu Rivain. Available at `https://eprint.iacr.org/2023/1573`.



**Signature Schemes:**

- Co-author of **MIRA, a signature scheme relying on the MinRank problem**
  *Submitted to the NIST call for additional post-quantum signatures.*
- Co-author of **MQOM, a signature scheme relying on the multivariate quadratic problem**
  *Submitted to the NIST call for additional post-quantum signatures.*
- Co-author of **RYDE, a signature scheme relying on the rank syndrome decoding problem**
  *Submitted to the NIST call for additional post-quantum signatures.*
- Co-author of **SDitH, a signature scheme relying on the syndrome decoding problem**
  *Submitted to the NIST call for additional post-quantum signatures.*
- $2^{\text{nd}}$-round co-submitter of **PERK, a signature scheme relying on the permuted kernel problem**
  *Submitted to the NIST call for additional post-quantum signatures.*

**Others:**

- Co-author of **CRY.ME, a cryptography challenge about a secure messaging application**

## Program Committees

**Program Committee Member:**

PQCrypto'24, PQCrypto'25, CiC'25

## Teaching

**Master Thesis Supervision:**

- 2024. **Auguste Warmé-Janville**, Master Thesis at Sorbonne University (France)
- 2023. **Ronan Thoraval**, Master Thesis at University of Bordeaux (France)

**Tutorials:**

- **Post-Quantum Signatures from Secure Multiparty Computation.** Winter Research School (Rennes, France). February 2024.
- **Introduction to Zero-Knowledge Proofs.** Winter Research School (Rennes, France). February 2024.

## Presentations

**International Conferences:**

- **MQ on my Mind: Post-Quantum Signatures from the Non-Structured Multivariate Quadratic Problem.** EuroS&P 2024 (Vienna, Austria). July 2024.
- **Building MPCitH-based Signatures from MQ, MinRank, and Rank SD.** ACNS 2024 (Abu Dhabi, UAE). March 2024.
- **Threshold Linear Secret Sharing to the Rescue of MPC-in-the-Head.** Asiacrypt 2023 (presented online). December 2023.
- **Post-Quantum Signatures from Multiparty Computation: Recent Advances (invited talk).** PQCrypto'23 (Maryland, USA). August 2023.
- **Code-Based Signatures from Secure Multiparty Computation.** 2023 SIAM Conference on Applied Algebraic Geometry (Eindhoven, Netherlands). July 2023.
- **Zero-Knowledge Protocols for the Subset Sum Problem from MPC-in-the-Head with Rejection.** Asiacrypt 2022 (presented online). December 2022.
- **Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.** Crypto 2022 (Santa Barbara, USA). August 2022.

**Workshops:**

- **The Polynomial-IOP Vision of the Latest MPCitH Frameworks for Signature Schemes.** Post-Quantum Algebraic Cryptography – Workshop 2 (Paris, France). November 2024.
- **Post-Quantum Signatures from Secure Multiparty Computation.** Workshop ReAdPQC24 at Cifris24 (Rome, Italy). September 2024.
- **Threshold Computation in the Head: More Efficient Signatures from MPCitH.** Workshop NAC (Paris, France). February 2024.
- **Post-Quantum Signatures from Secure Multiparty Computation.** Journées C2 2023 (Najac, France). October 2023.
- **RYDE & MIRA Signature Schemes.** Second Oxford Post-Quantum Cryptography Summit (Oxford, France). September 2023.
- **Post-Quantum Signatures from Secure Multiparty Computation.** Workshop WRACH (Roscoff, France). June 2023.
- **Zero-Knowledge Proofs for Syndrome Decoding from MPC-in-the-Head.** Journées C2 2022 (Hendaye, France). April 2022.

**Seminars:**

- **The Polynomial-IOP Vision of the Latest MPCitH Frameworks for Signature Schemes.** ACCESS Seminar (presented online). October 2024.
- **Constructions for digital signature Part I: Introduction to MPC-in-the-Head.** NIST PQC Seminar (presented online). May 2024.
- **Recent Advances in MPCitH-based Post-Quantum Signatures.** Crypto Seminar Rennes (Rennes, France). March 2024.
- **Post-Quantum Signatures from Secure Multiparty Computation.** Quantum PEPR PQ-TLS project days (Paris, France). June 2023.
- **CRY.ME: a Cryptographic Challenge on a Messaging Application.** Journées Nationales 2023 du GDR Sécurité Informatique (Puteaux, France). June 2023. Joint talk with Abdul Rahman Taleb.
- **Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP.** Code-based Working Group at INRIA (Paris, France). November 2022.
- **Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.** ENSL-CWI-RHUL Joint Seminar (online). November 2022.
- **Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.** Seminar C2 (Rennes, France). June 2022.
- **Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs.** Code-based Working Group at INRIA (Paris, France). Mars 2022.
- **Shared Permutation for Syndrome Decoding: New Zero-Knowledge Protocol and Code-based Signature.** ALMASTY Seminar (Paris, France). December 2021.