Kévin Carrier

Born in Châteaubriant, France, on May 18, 1991

Associate Professor at École Polytechnique

+33 6 87 45 75 57 • kevin.carrier@polytechnique.edu

https://kevincarrier.fr/ • Kévin Carrier • kevin-carrier

Research Interests

Blind reconstruction of error-correcting codes
Reverse engineering of telecommunication

Post-quantum cryptography
Code and Lattice based cryptography, NIST standardization process

Nearest-Neighbors Search problem
in various metric, application to decoding and lattice problems

Error-Correcting Codes
LDPC codes, Polar Codes

Employments

École Polytechnique — **Palaiseau – France**
Associate Professor at LIX (UMR7161) and DIX — *Sept. 2025 – Now*
Member of GRACE team-project

CY Cergy-Paris Université — **Cergy-Pontoise – France**
Associate Professor at ETIS (UMR8051) and CY Tech — *Aug. 2021 – Aug. 2025*
Member of ICI team

Ministère des Armées — **Paris – France**
R&D Engineer — *March 2020 – Aug. 2021*
Reverse engineering of telecommunication and error-correcting codes

Ministère des Armées / Inria de Paris — **Paris – France**
PhD Student, Member of the team-project SECRET at Inria de Paris. — *Sept. 2016 – Feb. 2020*

Ministère des Armées — **Paris – France**
Apprenticeship on "Blind LDPC Code Recognition" — *Sept. 2015 – Sept. 2016*

Orange Labs — **Issy-Les-Moulineaux – France**
Internship on "Obfuscation of symmetric cryptographic primitives" — *June 2014 – Sept. 2014*

Collège René Cassin — **Paray-Le-Monial – France**
Mathematics teacher — *Jan. 2013 – Jul. 2013*
Mathematics teacher in a middle school.

Education

Qualifications for the position of *Maître de Conférence* — **France**
from the Conseil National des Universités *(CNU)* — *2021 (valid until 2026)*

- Section 25 - Mathematics (N° 21225340720);
- Section 26 - Applied Mathematics and Applications of Mathematics (N° 21226340720);
- Section 27 - Computer Sciences (N° 21227340720).

Orsys formation and Telecom Evolution — **Paris – France**
Professional Training — *Sept. 2020 – Dec. 2020*
advanced C/C++, advanced Python 3, 1G to 5G, satellite communications

Ministère des Armées / Inria de Paris / Sorbonne Université / EDITE — **Paris – France**
PhD Student, Member of the team-project SECRET at Inria de Paris. — *Sept. 2016 – Dec. 2019*

- **Title:** "Near-Collision Search for Decoding and Code Recognition"
- **Supervisors:** Jean-Pierre Tillich and Nicolas Sendrier (Inria de Paris).
- **Jury:** Daniel Augot (president), Sébastien Houcke, Pierre Loidreau (reviewer), Nicolas Sendrier, Jean-Pierre Tillich, Annick Valibouze, and Gilles Zémor (reviewer).
- **Defense date:** June 19, 2020

Université Paris Diderot — **Paris – France**
Master MIC – With honours — *Sept. 2014 – Sept. 2016*
Mathematics and Computer Science applied to Cryptography

- Apprenticeship at the Ministère des Armées on "Blind LDPC Code Recognition"
- Master's thesis: "List Decoding of Reed-Solomon Codes"

Université Paris Diderot — **Paris – France**
Bachelor's Degree – With honours — *Sept. 2013 – Jul. 2014*
Applied Mathematics and Computer Science

- Internship at Orange Lab on "Obfuscation of symmetric cryptographic primitives"
- End-of-year project on "Integer Factorization using Lenstra Algorithm"

Ashford Adult Education Centre — **Ashford – England**
English courses — *Sept. 2012 – Dec. 2012*

Université de Nantes — **Nantes – France**
Bachelor's Degree – With honours — *Sept. 2009 – Jul. 2012*
Fundamental Mathematics

Lycée Guy Moquet — **Châteaubriant – France**
Baccalauréat – With honours — *June 2009*
Sciences, Mathematics, Engineering sciences

Skills

Languages: French (native), English
Programming: C/C++, Java, Python, SageMath
Driving Licenses: Car, Motorcycle, Boat

Projects and Grants

Honors

ANR JCJC — **France**
DECODE: Generic decoding in various metrics — *Jan. 2023 – Aug. 2026*

- *Jeunes Chercheuses, Jeunes Chercheurs* (JCJC) project
- Granted €184k
- `https://anr.fr/Projet-ANR-22-CE39-0004`

Projects I am Involved In

Submission to the NIST (National Institute of Standards and Technology) — **France – USA**
WAVE, a quantum-resistant signature based on coding theory — *June 2023 – Undefined*

- Coordinated by Thomas Debris-Alazard (Inria Saclay, LIX)
- `https://tdalazard.io/wave.html`

PhD Supervision

Elric Isoardo — **École Polytechnique**
Hybrid Algebraic–Combinatorial Attacks on Post- Quantum Cryptosystems — *Oct. 2023 – Now*

- Co-supervisor: Alain Couvreur (Inria Saclay)

Valérian Hatey — **CY Cergy-Paris Université**
Code and Lattice based Cryptanalysis — *Oct. 2023 – Now*

- As part of the ANR JCJC project DECODE
- Co-supervisor: Laura Luzzi (ENSEA)

Scientific publications

In the cryptography community, authors are always listed in **alphabetical order**. While there are few journals in this field, the most prestigious and selective publications are the proceedings of the annual ranked A* conferences **Crypto**, **Eurocrypt**, and **Asiacrypt**.

International Conferences with Proceedings and Peer Review Committee

[CMST25] Kévin Carrier, Charles Meyer-Hilfiger, Yixin Shen, and Jean-Pierre Tillich. "**Assessing the impact of a variant of the latest dual attack**". In: *Advances in Cryptology – **CRYPTO 2025***. Springer Nature Switzerland, 2025. URL: https://eprint.iacr.org/2022/1750.

[CDMT24] Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. "**Reduction from Sparse LPN to LPN, Dual Attack 3.0**". In: *Advances in Cryptology - **EUROCRYPT 2024** - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. LNCS. Springer, 2024, pp. 286–315. DOI: 10.1007/978-3-031-58754-2_11. URL: https://eprint.iacr.org/2023/1852.

[CHT24] Kévin Carrier, Valerian Hatey, and Jean-Pierre Tillich. "**Projective Space Stern Decoding and Application to SDitH**". In: *Applied Cryptography and Network Security Workshops: **ACNS 2024** Satellite Workshops, AIBlock, AIHWS, AIoTS, SCI, AAC, SiMLA, LLE, and CIMSS, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part II*. Abu Dhabi, United Arab Emirates: Springer-Verlag, 2024, 29–52. ISBN: 978-3-031-61488-0. DOI: 10.1007/978-3-031-61489-7_3. URL: https://eprint.iacr.org/2023/1865.

[CDMT22] Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. "**Statistical Decoding 2.0: Reducing Decoding to LPN**". In: *Advances in Cryptology – **ASIACRYPT 2022**: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*. Taipei, Taiwan: Springer-Verlag, 2022, 477–507. ISBN: 978-3-031-22971-8. DOI: 10.1007/978-3-031-22972-5_17. URL: https://eprint.iacr.org/2022/1000.

[CT17] Kévin Carrier and Jean-Pierre Tillich. "**Identifying an Unknown Code by Partial Gaussian Elimination**". In: ***WCC** Workshop on Coding and Cryptography*. Sept. 2017.

International Journal with Peer Review Committee

[CT19] Kévin Carrier and Jean-Pierre Tillich. "**Identifying an unknown code by partial Gaussian elimination**". In: ***DCC** Designs, Codes and Cryptography* 87.2-3 (2019), pp. 685–713. DOI: 10.1007/s10623-018-00593-7. URL: https://inria.hal.science/hal-02424098/.

Note that as is usual for this journal, the paper [CT19] is an extended version of the WCC paper [CT17], with additional results on the weight enumerators of the parity-checks of LDPC codes.

Pre-print

[CST22] Kévin Carrier, Yixin Shen, and Jean-Pierre Tillich. ***Faster Dual Lattice Attacks by Using Coding Theory***. Cryptology ePrint Archive, Paper 2022/1750. 2022. URL: https://eprint.iacr.org/archive/2022/1750/20221220:184709.

PhD thesis

[Car20] Kévin Carrier. "**Recherche de presque-collisions pour le décodage et la reconnaissance de codes correcteurs**". Theses. Sorbonne Université, June 2020. URL: https://tel.archives-ouvertes.fr/tel-03370678v4.

Other

[Ban+23] Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karpman, Johanna Loyer, Ruben Niederhagen, Nicolas Sendrier, Benjamin Smith, and Jean-Pierre Tillich. *Wave*. Round 1 Additional Signatures to the NIST Post-Quantum Cryptography: Digital Signature Schemes Call. June 2023. URL: https://wave-sign.org.

Github projects

- **Coded Dual Attack.**
  - An optimizer to find the best parameters for our coded dual attack presented in [CMST25]. It also provides some simulations to verify our analysis.
  - https://github.com/kevin-carrier/CodedDualAttack
  - Languages: Python (1500 lines), SageMath (2300 lines), C (2000 lines)
  - Contributors : K. Carrier (50%), Y. Shen (10%), C. Meyer-Hilfiger (40%)
- **Analysis dual lattice attack.**
  - An analysis of the distinguisher at the heart of dual lattice attacks. It proves that dual attack can have an impact on lattice-based cryptography. This project supports the paper [CDMT24].
  - https://github.com/kevin-carrier/analysis_dual_lattice_attack
  - Language: SageMath (1300 lines)
  - Contributor : K. Carrier (100%)
- **SDitH security.**
  - This implementation measures the security level of SDitH signature with our attack presented in [CHT24]. It also provides some simulations to verify our analyses.
  - https://github.com/kevin-carrier/SDitH_security
  - Language: SageMath (3170 lines)
  - Contributor : K. Carrier (70%), V. Hatey (30%)
- **Polar codes over $\mathbb{Z}_q$.**
  - An implementation of Polar Codes over the ring $\mathbb{Z}/q\mathbb{Z}$. Study of distortion properties of those codes. This C implementation served as a proof-of-concept for the paper [CMST25].
  - https://github.com/kevin-carrier/PolarCode_over_Zq
  - Language: C (1170 lines)
  - Contributor : K. Carrier (100%)
- **About [BM18].**
  - Simulations demonstrating that the analysis in [BM18] is incorrect, while the one in Appendix B of the paper [CDMT22] is accurate.
  - https://github.com/kevin-carrier/aboutBM18
  - Language: C (811 lines)

- Contributor : K. Carrier (100%)

- **Decoding Cost.**
  - This implementation is carried out as part of the ANR DECODE project. This project include a corrected analysis of [BM18] presented in the Appendix B of the paper [CDMT22].
  - `https://github.com/kevin-carrier/DecodingCost`
  - Language: C++ (2200 lines)
  - Contributor : K. Carrier (100%)

Selected Talks

Tutorials

Eötvös Loránd University — **Budapest – Hungary**
Summer School in Post-Quantum Crypto — *Aug. 2022*
"Introduction to Code-based Cryptography"

Workshops and Conferences

Team Seminaries in Various French Research Labs — **France**
I regularly give talks at various team seminars. — *2017 - Now*

Workshop "Code-based Cryptography" at Inria de Paris — **Paris – France**
Organized by Jean-Pierre Tillich — *2017 - Now*
I regularly participate in and contribute to this workshop.

GDR IFM and Sécurité — **France**
Participation in the Journées Codage et Cryptographie *(JC2),* — *2017 - Now*
which takes place approximately every 18 months

HCERES, Evaluation of the ETIS Lab — **Pontoise – France**
Presentation of Post-Quantum Cryptography Activities at the ETIS Laboratory — *Dec. 11, 2024*

Workshop Interdisciplinaire sur la Sécurité Globale (WISG) 2024 — **Rennes/Marseilles – France**
Presentation of the latest developments in the ANR DECODE Project — *March, 2023 and 2024*

First Modular Code Cryptanalysis Library (MCCL) workshop — **Paris – France**
"The near-collisions finding problem for generic decoding" — *Nov. 23, 2021*

Munich Whorkshop on Coding and Cryptography — **Munich – Germany**
"On the use of Polar Codes for finding Near-Collisions" — *Jul. 16, 2019*

10-th International Workshop on Coding and Cryptography — **St Petersburg – Russia**
"Identifying an Unknown Code by Partial Gaussian Elimination" — *Sept. 21, 2017*

Scientific Popularization

Café Scientifique, Pôle Judiciaire de la Gendarmerie Nationale (PJGN) — **Cergy – France**
"Post-Quantum Cryptography and Blind Code Recognition" — *Jan. 29, 2025*

CY Tech — **Cergy – France**
"Cybersécurité et IA pour la Santé" — *Nov. 28, 2024*
Co-organization and co-hosting of a public conference for the TalCyb project

Let's CY, CY Cergy-Paris Université — **Cergy – France**
"Les enjeux de la cryptographie post-quantique" — *Feb. 11, 2022*

Scientific Reviews

I am regularly invited to provide reviews within the cryptography community for prestigious events and journals such as Crypto, Eurocrypt, Asiacrypt, PQCrypto, WCC, DCC, and Journal of Cryptography. I also review for Information Theory events organized by IEEE, including IT and ISIT. Each year, I complete between 5 and 10 reviews.

Program Committee

Perugia – Italy **Program Committee Member**
International Workshop on Coding and Cryptography. *2024*

Teaching Activities

Yearly Summary

Teaching takes up a significant portion of my time. Here is a brief summary of my hourly volume over the last five years:

- **2025-2026:** 128 HETD (CM 33%, TD/TP 67%)
- **2024-2025:** 468,5 HETD (CM 36%, TD/TP 54%, other 10%)
- **2023-2024:** 456,5 HETD (CM 36%, TD/TP 50%, other 14%)
- **2022-2023:** 369 HETD (CM 34%, TD/TP 50%, other 16%)
- **2021-2022:** 316 HETD (CM 32%, TD/TP 59%, other 9%)

Responsibilities

Responsible of the Nework Security Master **CY Cergy-Paris Université**
Master "Informatique et Ingénierie des Systèmes Complexes (IISC)" *2022 – 2025*

- Administrative management of the program
- Promotion and communication of the program
- Regular update of the course catalog
- Student recruitment for the Master's program
- Approval of apprenticeship assignments
- Monitoring of apprentices in collaboration with their companies

Recruitment Committee Member **CY Cergy-Paris Université**
For two Associate Professor positions and one teaching position. *2023 – 2024*

Jury Member **CYU, ENSEA, Univ. Paris-Cité**
I am a member of the juries for several training programs *2021 – 2025*

- Master's degree in Computer Science at CY Univ. and ENSEA
- Professional master in Computer Science at CY Univ.
- Master's degree in Mathematics, Computer Sciences and applications to Cryptology at Univ. Paris-Cité
- DU Criminalistics Operations Coordinator (DU CoCrim) (only 2023)

Internship Supervision

Valérian Hatey (M2) **CY Cergy-Paris Université**
"Ternary decoding at large distance" *Apr. 2023 – Aug. 2023*

Thomas Remy (L3) **CY Cergy-Paris Université**
"Technological watch on Smart Cards" *June 2023 – Aug. 2023*

Julien Chaput (M2) — **Ministère des Armées**
"Non-binary LDPC codes" — *Apr. 2021 – Aug. 2021*

Émile Lalo (M2) — **Ministère des Armées**
"Polar codes in 5G" — *Apr. 2021 – Aug. 2021*

Monitoring End-Of-Year Projects

Here is a list of all the end-of-year projects that I mentored:

- "Operational Cybersecurity" – 5 M2 students – 2024-2025
- "Cybersecurity Awareness Escape Game" – 6 M1 students – 2024-2025
- "Authentication in a blockchain" – 3 M2 students – 2023-2024
- "Steganography, Steganalyse" – 5 M2 students – 2023-2024
- "Double spent attack on bitcoin-cli" – Dassine Mettouchi M1 – 2023-2024
- "Securing and monitoring a company network" – 3 M2 students – 2022-2023
- "Remote monitoring of a WiFi network" – 3 M2 students – 2022-2023
- "A Pokemon Go style game using a blockchain" – 5 M1 students – 2022-2023
- "Monitoring a company network with Splunk" – Yohan Chabot M1 – 2021-2022

Courses (Short Summary)

École Polytechnique — **Palaiseau – France**
Python programming (Bachelor 1) — *2025 – 2026*

EPITA — **Kremlin-Bicêtre – France**
Reverse Engineering and Graph Theory (Bachelor 2) — *2025 – 2026*

CY Cergy-Paris Université and CY Tech — **Cergy-Pontoise – France**
Applied Mathematics, Computer sciences and Cryptology — *2021 – 2025*
- Cryptography (M1, M2, Ing3)
- Smart Card (M2)
- Network security (M2, Ing3)
- Mathematics for computer sciences (L3)
- Formal language and Automata (L2)

ENSEA — **Cergy – France**
Information Theory (Ing2) and Advanced Cryptography (Ing3) — *2023 – 2025*

Université Paris Cité — **Paris – France**
Error-correcting codes (M2) — *2021 – 2025*

Université Paris Diderot — **Paris – France**
Mathematic Analysis (L1) — *2016 – 2019*

ENSTA ParisTech — **Palaiseau – France**
Discrete Mathematics and applications to Codes and Cryptography (Ing3) — *2016 – 2019*

Collège René Cassin — **Paray-Le-Monial – France**
Mathematics teacher — *Jan. 2013 – Jul. 2013*
Mathematics teacher in a middle school.

Courses (Details)

Course name	Brief description	Localization & Level	Type	Period	Volume
Python Programming	Variables and Data Types Conditional Statements Loops Collections Functions File Handling Object-Oriented Programming Bytecode	École Polytechnique Bachelor 1	CM 5% TP 95%	2025-2026	48HETD
Graph Theory	Basic definitions Representation of Graphs Special Types of Graphs Graph Operations Paths and Connectivity BFS,DFS Kosaraju-Sharir Bellman, Dijkstra Prim, Kruskal	EPITA Bachelor 2	CM 50% TP 50%	2025-2026	68HETD
Reverse Engineering	Motivation and Application Binary vs source code Executables and file formats CPU architecture ABI sysV and MS Assembly/Disassembly Static vs Dynamic Analysis Control Flow Graph Debugger Patching Obfuscation	EPITA Bachelor 2	CM 50% TP 50%	2025-2026	26HETD
Cryptography	Ancestral Ciphers Goal of cryptography Attacker model Side Channel Attack Stream Cipher (PRG, LFSR, A5/1) Block Cipher (DES, AES) Block Cipher Modes (ECB, CBC, CTR) Cryptographic Hash Function Message Authentication Code (MAC) Public Key Encryption (RSA) Digital signature (RSA, DSA) Key Establishment (Diffie-Hellmann) Introduction to post-quantum cryptography	CY Tech ING3	CM 50% TD/TP 50%	2024-2025 2023-2024	112HETD 105HETD
Cybersecurity	Ebios Risk Management Scapy, ARP spoofing, DNS spoofing Certificats (X509)	CY Tech ING3	TP	2024-2025 2023-2024	14HETD 14HETD
Error-Correcting Codes	Shannon digital transmission scheme Mapping, Scrambling, Interleaving... Quadrature Amplitude Modulation (QAM) Notions of Information Theory Linear codes over $\mathbb{F}_q$ Bounds on codes Shortening/Punctering Subfield-Subcodes/Trace-Codes List decoding of Reed-Solomon Codes Polar codes Low-Density Parity-Check (LDPC) codes Code-Based Crypto (McEliece, Niederreiter...) Attacks on GRS, $U\|U+V$ and LDPC codes Decoding random linear codes (ISD)	Univ. Paris-Cité M2	CM 50% TD/TP 50%	2024-2025 2023-2024 2022-2023 2021-2022	75HETD 75HETD 75HETD 75HETD

Course name	Brief description	Localization & Level	Type	Period	Volume
Advanced Cryptography	Digital signature (RSA, DSA) Diffie-Hellmann Man-in-the-middle (ARP spoofing, scapy) Certificats (X509) Blockchain (bitcoin-cli) Introduction to post-quantum cryptography	CY Univ. M2	CM 50% TD/TP 50%	2024-2025 2023-2024 2022-2023 2021-2022	42HETD 42HETD 42HETD 42HETD
Smart Card	History of the smart card Smart/Hardwired-Logic/Memory Cards TPDU, APDU Authentication protocols	CY Univ. M2	TP	2024-2025 2023-2024 2022-2023 2021-2022	16,5HETD 16,5HETD 16,5HETD 16,5HETD
Cryptography	Ancestral Ciphers Goal of cryptography Attacker model Side Channel Attack Stream Cipher (PRG, LFSR, A5/1) Block Cipher (DES, AES) Block Cipher Modes (ECB, CBC, CTR) Cryptographic Hash Function Public Key Encryption (RSA) Digital signature (RSA)	ENSEA ING3	CM	2023-2024 2022-2023	24HETD 24HETD
Network Security	Ebios Risk Management Firewall, Tunneling (Pfsense, IPsec...) Kali Linux, Wireshark Scapy, ARP spoofing, DNS spoofing Certificats (X509) Authentication (RADIUS) Dynamic VLAN Supervision (Syslog, Prometheus, Nagios)	CY Univ. M2	CM 30% TP 70%	2022-2023 2021-2022	35HETD 35HETD
Information Theory	Information content Entropy of a discrete memoryless source Variable length codes Huffman codes Lempel-Ziv compression Markov source Mutual Information Channel Capacity Error correcting codes binary linear codes	ENSEA ING2	CM 50% TD 50%	2024-2025	44HETD
Cryptography	Ancestral Ciphers Goal of cryptography Attacker model Side Channel Attack Shannon secrecy, Perfect secrecy Computational security (Complexity theory) Stream Cipher (PRG, LFSR, A5/1) Block Cipher (DES, AES) Block Cipher Modes (ECB, CBC, CTR) Cryptographic Hash Function Message Authentication Code (MAC) Public Key Encryption (RSA)	CY Univ. M1	CM 50% TD/TP 50%	2024-2025 2023-2024 2022-2023 2021-2022	60HETD 60HETD 60HETD 60HETD
Probability Statistic	Event, Probability... Dependencies, Conditional probability Probability tree Discrete Random Variable Uniform, Bernoulli, Binomial distributions Geometric, Poisson distributions Continuous Random Variable Uniform, Normal, Exponential distributions Pair of Random Variables	CY Univ. L3	TD	2024-2025 2023-2024 2022-2023 2021-2022	27,5HETD 27,5HETD 27,5HETD 27,5HETD

Course name	Brief description	Localization & Level	Type	Period	Volume
Languages and Automata	Languages Automata Synchronization, Determinization, Minimization Regular Language Context-free Language Pushdown automaton Turing Machine	CY Univ. L2	TD	2024-2025 2023-2024 2022-2023 2021-2022	30HETD 30HETD 30HETD 30HETD
Discrete Mathematics for Error-Correcting Codes and Cryptography	Algebraic structures Construction and implementation of Finite Fields Applications to Error Correcting Codes: BCH codes, Reed-Solomon codes... Applications to Cryptography: Primality tests, Discrete Logarithm problem, Linear Feedback Shift Register (LFSR), Blum-Blum-Shub generator, Blum-Goldvasser cryptosystem	ENSTA ING3	TD TP	2018-2019 2017-2018 2016-2017	16HETD 16HETD 16HETD
Mathematical analysis	Limits, continuity and derivatives of real functions Riemann integration Linear differential equations	Univ. Paris Diderot L1	CM TD	2018-2019 2017-2018 2016-2017	70HETD 70HETD 70HETD
Secondary school mathematics teacher		Collège René-Cassin Paray-le-Monial $3^{\text{ème}}, 4^{\text{ème}}, 5^{\text{ème}}, 6^{\text{ème}}$		2013	20h/week