Clément Ducros

Postdoctoral researcher. My main interests lie in secure computing, Consensus and coding theory.

ducros.clement.dc@gmail.com https://clement-ducros.github.io/

EDUCATION

2021 – 2024 **Ph.D Thesis, Universé de Paris, IRIF**
Thesis title: *Linear Codes for Quantum-Resistant Secure Computation.*

2020 – 2021 **Parisian Master of Research in Computer Science (MPRI), Université de Paris**
Specialization in algorithmic and cryptography.

2018 – 2021 **Engineering school, Télécom Paris, Palaiseau**
Algebra, Cryptography, Algorithmic and Theoretical Computer Science.

2016 – 2018 **Preparatory class for entrance to Grandes Ecoles (MPSI,MP*), Lycée Janson de Sailly, Paris**
Maths, Physics and Computer Science.

WORK EXPERIENCE

Jenuary 2025 – . . . **Post-Doctoral Student, CISPA helmholtz center for information security**
with Julian Loss. *Theory of Consensus.*

October 2021 – October 2024 **PhD student, IRIF, Université de Paris**
under the supervision of Geoffroy Couteau and Alain Couvreur. *Linear Codes for Quantum-Resistant Secure Computation.*

March 2021 – Sept 2021 **Research intern in cryptography at IRIF, Université de Paris**
under the supervision of Geoffroy Couteau. *Multiparty Secure Computation via Coding Theory.*

July 2019 – August 2019 **Research intern in algorithmic at IRIF, Université de Paris**
under the supervision of Jean Krivine. *Modelling of concurrent processors using graphs and analysis of the induced structure.*

RESEARCH PUBLICATIONS

1. M. Bombar, D. Bui, G. Couteau, A. Couvreur, C. Ducros, and S. Servan-Schreiber, "FOLEAGE: F 4 OLE-Based Multi-Party Computation for Boolean Circuits," in *Advances in Cryptology – ASIACRYPT 2024*, ser. Lecture Notes in Computer Science, Chung, K.M. and Sazaki, Y., vol. 15489, Kolkata, India: Springer Nature Singapore, Dec. 2024, pp. 69–101. DOI: 10.1007/978-981-96-0938-3_3.

2. M. Bombar, G. Couteau, A. Couvreur, and C. Ducros, "*Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding*," in *CRYPTO 2023, Part IV*, ser. LNCS, Springer, Heidelberg, Aug. 2023, pp. 567–601. DOI: 10.1007/978-3-031-38551-3_18.

3. G. Couteau and C. Ducros, "*Pseudorandom Correlation Functions from Variable-Density LPN, Revisited*," in *PKC 2023, Part II*, A. Boldyreva and V. Kolesnikov, Eds., ser. LNCS, vol. 13941, Springer, Heidelberg, May 2023, pp. 221–250. DOI: 10.1007/978-3-031-31371-4_8.

TEACHING

2021 – 2024 Teaching assistant at Université de Paris Cité: Java, Python, Algorithmic, project managament (bachelor level - 64h/year).

SKILLS

Languages	French (native language), English (B2/C1), Korean (A2)
Coding	Java, Python, LaTeX