Curriculum Vitae

CLÉMENT DUCROS

Postdoctoral Researcher at CISPA, Helmoltz Center for Information Security, Saarbrücken, Germany.

Nationality: French.

Research Interests: Secure Multiparty Computation, Coding Theory, Pseudorandom Correlation Generators, Pseudorandom Functions, Consensus.

clement.ducros@cispa.de Fürstenstraße 5-7 Saarbrücken, 66111, Allemagne.
https://clement-ducros.github.io/ +336 20 49 38 84.

EDUCATION

2021–2024 ● **Ph.D Thesis, University Paris-Cité, IRIF**
Multiparty Computation from the Hardness of Coding Theory, Under the supervision of Geoffroy Couteau and Alain Couvreur. Thesis Defended on the 12/11/2024, Speciality: Computer Science
Examiners:
- Nico Döttling (President of the jury, Professor, Helmholtz Center for Information Security (CISPA)).
- Nicolas Sendrier (Reviewer, Research Director, INRIA Paris).
- Emmanuela Orsini (Reviewer, Tenure-Track Assistant Professor, Bocconi University).
- Yixin Shen (Examiner, Research Scientist, INRIA Rennes).
- Philippe Gaborit (Examiner, Professor, CNRS, University of Limoges).
- Lisa Kohl (Examiner, Researcher, CWI, Amsterdam, The Netherlands).

.

2020–2021 ● **Parisian Master of Research in Computer Sciency (MPRI), University Paris-Cité**
Specialization in algorithmic and cryptography.

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

WORK EXPERIENCE

January 2025 – . . . ● **Post-Doctoral Researcher, CISPA Helmoltz Center for Information Security**
with Julian Loss. Theory of Consensus

October 2021– November 2024 ● **PhD student, IRIF, University Paris-Cité**
under the supervision of Geoffroy Couteau and Alain Couvreur. Multiparty Computation from the Hardness of Coding Theory.

July 2019– August 2019 ● **Research Intern, IRIF, University Paris-Cité**
under the supervision of Jean Krivine. Modelling of concurrent processors using graphs and analysis of the induced structure.

RESEARCH PUBLICATIONS

Conference Paper.

- M. Bombar, D. Bui, G. Couteau, Alain Couvreur, C. Ducros and S. Servan-Schreiber, *FOLEAGE: F_4 OLE-Based Multi-Party Computation for Boolean Circuits*, ASIACRYPT 2024, Kolkata, India.

  New method to transform OLE over the field F_4 into OLE over field F_2, and optimizations of previous PCG based and the QA-SD assumption to target the F_4 field.

- M. Bombar, G. Couteau, A. Couvreur and C. Ducros, *Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding*, CRYPTO 2023, Santa Barbara, USA (Speaker).

  We introduce a new PCG for OLE over any field $F_q, q > 2$, based on a new variant of the Syndrom Decoding assumption, named the Quasi-Abelian Syndrom Decoding.

- G. Couteau and C. Ducros, *Pseudorandom Correlation Functions from Variable-Density LPN, Revisited*, PKC 2023, Atlanta (Speaker).

  We improve over the construction given by Boyle et. al., which introduced the VDLPN assumption and the PCF. We correct a mistake in the original proof and improve drastrically the efficiency.

Pre-print

- M. Ball, C. Ducros, S. Erabelli, L. Kohl, N. Resch, *Strong Pseudorandom Functions in ACo[2] in the Bounded-Query Setting*.

  We analyze PRFs constructions in a new setting where the adversary is only limited to a bounded number of query. We introduce a new candidate strong PRF in the low complexity class ACo[2], if the advesrsary is limited to a fixed quasipolynomial amount of query.

- C. Ducros, J. Loss, M. Rambaud, *Strong Efficiency Lower Bounds for Byzantine Agreement*.

  We prove two lower bounds on the comunication complexity of randomized BA protocols that hold against even a standard adaptive adversary, for some settings unexplored by the literature.

TEACHING

2021–2024 ● **Teaching assistant at University Paris- Cité.**
Introduction to computer science(Java) (bachelor level - 64h)

2021–2024 ● **Teaching assistant at University Paris- Cité.**
Algorithmics, Introduction to computer science(Java, Python) (bachelor level - 64h)

2021–2024 ● **Teaching assistant at University Paris- Cité.**
Introduction to Computer Science (Java, Python), Project managament (bachelor level - 64h)

SERVICE TO THE SCIENTIFIC COMMUNITY

2022–present ● **Reviewer for major cryptographic conferences**
CRYPTO(2023,2025), EUROCRYPTO(2024), ASIACRYPT(2025)

2022 ● **assisted in organizing conference**
49th ICALP (Paris 2022)

SEMINARS AND INVITED TALKS

- 29/04/2025 — **ECO Team Seminar, Montpellier.**
- 12/09/2024 — **Group Seminar at CWI, Amsterdam, Netherlands.**
- 16/05/2024 — **Non-permanent Researchers Seminar, IRIF, Université Paris-Cité.**
- 01/05/2024 — **Cybersecurity Section Seminar, DTU, Copenhagen, Denmark.**
- 24/01/2024 — **PEPR-SecureCompute, ENS ULM, Paris.**
- 19/01/2024 — **IRMAR Seminar, University of Rennes.**
- 08/12/2023 — **ALMASTY Seminar, LIP6, Paris.**
- 23/08/2023 — **CRYPTO 2023, Santa Barbara, USA.**
- 10/05/2023 — **PKC 2023, Atlanta, USA.**
- 15/04/2022 — **C2 Days 2022, Hendaye.**
- 15/04/2022 — **C2 Days 2022, Hendaye.**
- 05/05/2022 — **GRACE Team Seminar, INRIA Saclay.**

SKILLS

- Languages — **French (native), English (C1), Korean (A2)**
- Coding — **Java, Python, SageMath**