DUNG BUI

IRIF, University Paris Cité
(+64) 85 70 27 94
bui@irir.fr
Personal Webpage
Google Scholar DBLP Linkedin

EDUCATION

- **IRIF, University Paris Cité** — **Paris, France**
  PhD student in Secure Computation for Privacy-Preserving — *Oct 2021 – Mar 2025*
  Supervisor: Geoffroy Couteau
- **Université de Limoges** — **Limoges, France**
  Master degree in Mathematics, Cryptology, Coding and Application — *2019 – 2021*
  Highest Honours, Ranked 1st
- **Ha Noi National University of Education** — **Ha Noi, Viet Nam**
  Pure Mathematics — *2015 – 2019*
  Highest Honours, top 5%

RESEARCH INTERESTS

My research interests are in various aspects of both practical and theoretical cryptography, including Secure Multiparty Computation (MPC), Zero-Knowledge Proofs (ZKP), and Post-Quantum Cryptography (PQC).

RESEARCH EXPERIENCE

- **NTT Social Informatics Laboratories** — **Tokyo, Japan**
  Visiting Researcher, Supervisor: Masayuki Abe — *Jun – Aug 2024*
  Multi-round Zero-Knowledge Proofs and Applications to Advanced Post-quantum Signatures based on Multiparty Computation (MPC)
- **COSIC (KU Leuven)** — **Leuven, Belgium**
  Visiting Researcher, Supervisor: Nigel Smart — *Jul – Aug 2023*
  Efficient Post-quantum Signatures from Multiparty Computation (MPC)
- **Research Institute IRIF** — **Paris, France**
  Research Intern, Supervisor: Geoffroy Couteau — *Mar – Aug 2021*
  Efficient Multiparty Computation (MPC) Protocols from Pseudorandom Correlation Generators
- **Research Institute XLIM** — **Limoges, France**
  Summer Intern, Supervisor: Duong Hieu Phan — *Jun – Aug 2020*
  Private Set Intersection and its Application to Covid 19

PUBLICATION

In Conference Proceedings:

[Bui25] Dung Bui. “Efficient Multi-instance Vector Commitment and Application to Post-quantum Signatures”. In: *Information Security and Privacy – ACISP 2025*. Springer Nature Singapore, 2025. URL: https://eprint.iacr.org/2024/254.

[BCS25] Dung Bui, Kelong Cong, and Cyprien Delpech de Saint Guilhem. *Faster VOLEitH Signatures from All-but-One Vector Commitment and Half-Tree*. ePrint Archive. Available at https://eprint.iacr.org/2024/255. 2025.

[BBC+24] Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, and Sacha Servan-Schreiber. “FOLEAGE: $\mathbb{F}_4$OLE-Based Multi-party Computation for Boolean Circuits”. In: *Advances in Cryptology – ASIACRYPT 2024*. Springer Nature Singapore, 2024, pp. 69–101. DOI: 10.1007/978-981-96-0938-3.

[BCC+24] Dung Bui, Eliana Carozza, Geoffroy Couteau, Dahmun Goudarzi, and Antoine Joux. “Faster Signatures from MPC-in-the-Head”. In: *Advances in Cryptology – ASIACRYPT 2024*. Springer Nature Singapore, 2024, pp. 396–428. DOI: 10.1007/978-981-96-0875-1_13.

[BCM+24] Dung Bui, Geoffroy Couteau, Pierre Meyer, Alain Passelègue, and Mahshid Riahinia. “Fast Public-Key Silent OT and More from Constrained Naor-Reingold”. In: *Advances in Cryptology – EUROCRYPT 2024*. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 88–118. DOI: 10.1007/978-3-031-58751-1_4.

[BC23] Dung Bui and Geoffroy Couteau. “Improved Private Set Intersection with Small Entries”. In: *Public-Key Cryptography – PKC 2023*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Berlin, Heidelberg: Springer-Verlag, 2023, pp. 190–220. DOI: 10.1007/978-3-031-31371-4_7.

Journal Articles:

[BCC+24] Dung Bui, Haotian Chu, Geoffroy Couteau, Xiao Wang, Chenkai Weng, Kang Yang, and Yu Yu. “An Efficient ZK Compiler from SIMD Circuits to General Circuits”. In: *Journal of Cryptology* 38.1 (Dec. 2024), p. 10. ISSN: 1432-1378. DOI: `10.1007/s00145-024-09531-4`.

Preprints:

[ABB+24] Masayuki Abe, David Balbás, Dung Bui, Miyako Ohkubo, Zehua Shang, and Mehdi Tibouchi. *Critical Round in Multi-Round Proofs: Compositions and Transformation to Trapdoor Commitments*. ePrint Archive. Available at `https://eprint.iacr.org/2024/252`. 2024.

[BCM24] Dung Bui, Geoffroy Couteau, and Nikolas Melissaris. *Structured-Seed Local Pseudorandom Generators and their Applications*. ePrint Archive. Available at `https://eprint.iacr.org/2024/253`. 2024.

FELLOWSHIPS & AWARDS

- **Fully-Funded Doctoral Grants, DIM Math Innov (2021)**
  Awarded by the Ile-de-France Region for doctoral studies, with a selection of up to 9 PhD fellowships in mathematics and computer science.
- **Silver Medal, NSUCRYPTO (2021)**
  Awarded in the second round of International Olympiad in Cryptography Non-Stop University CRYPTO.
- **Fully-Funded Scholarship For Master’s CRYPTIS Program (2019)**
  Awarded by Vingroup Scholarship Program for Master’s CRYPTIS Program in Mathematics, Cryptology, Coding and Applications (MCCA) at the University of Limoges.
- **VIASM Scholarship, National Program for the Development of Mathematics (2017, 2018, 2019)**
  Awarded by the Vietnam Institute for Advanced Study in Mathematics, Viet Nam (VIASM) for encouraging young students to learn mathematics.
- **Bronze Medal, Viet Nam National Mathematical Olympiad (VMO 2015)**.
  Awarded in the most prestigious high school mathematics competition in Vietnam, part of the selection process for the International Mathematical Olympiad (IMO).

PRESENTATION

Conference, workshops:

Dec 2024 **Faster Signatures from MPC-in-the-Head**, *Conference Asiacrypt 2024*, Kolkata, India

May 2023 **Improved Private Set Intersection with Small Entries**, *Conference PKC 2023*, Atlanta, USA

Apr 2022 **Private Set Intersection from Correlated Randomness**, *Workshop Journées C2 (Codage & Cryptographie)* , Hendaye, France

Seminars:

FOLEAGE: $\mathbf{F}_4$OLE-Based Multi-party Computation for Boolean Circuits

Mar 2025 ALMASTY seminar, Sorbonne Université, Paris, France.

Optimized MPC-in-the-Head based signatures from Puncturable PRF

Apr 2025 Vietnam Institute for Advanced Study in Mathematics (VIASM), Ha Noi, VietNam (Virtual).

Dec 2024 Crypto Student Seminar CWI, Amsterdam, Netherlands.

Nov 2024 Crypto Day, Telecom Paris, Institut Polytechnique de Paris, Paris, France.

Efficient MPC from Correlated Randomness

Jun 2024 Crypto Seminars, NTT Social Informatics Laboratories, Tokyo, Japan.

Fast Public-Key Silent OT and More from Constrained Naor-Reingold

May 2024 AlgoCRYPT Seminars, J.P. Morgan, New York, USA (Virtual).

May 2024 IRIF, Algorithm and Complexity Seminars, Paris, France.

Efficient PSI from Pseudorandom Correlation Generators

July 2023 Crypto Seminar, COSIC (KU Leuven), Leuven, Belgium.

May 2023 Vietnam Institute for Advanced Study in Mathematics (VIASM), Ha Noi, VietNam (Virtual).

Apr 2023 IRIF, Algorithm and Complexity Seminar, Paris, France.

Jul 2022 Crypto Student Seminar CWI, Amsterdam, Netherlands (Virtual).

PROFESSIONAL ACTIVITIES

- **External Reviewer:** TCC 2022, CSF 2022–2023, IEEE-TIFs 2023, EUROCRYPT 2025, ACNS 2025, CRYPTO 2025 (x3), PRICRYPT 2025, CCS 2025.
- **Program Committee:** APKC 2025, LATINCRYPT 2025.