

DUNG BUI

Born on 15/11/1997, Vietnamese

 Sorbonne Université, CNRS, LIP6

 (+33) 01 44 27 94

 dung.bui@lip6.fr

 <https://dungbui15.github.io>

 Google Scholar  DBLP  LinkedIn

CURRENT POSITION

Sorbonne Université, CNRS, LIP6

Postdoctoral Researcher

Hosted by: Eleni Diamanti, Alex B.Grilo, Ludovic Perret

Paris, France

Jun 2025 – Current

EDUCATION

Université Paris Cité, CNRS, IRIF

PhD, Computer Science

Thesis: Efficient Secure Computation from Correlated Pseudorandomness

Supervisor: Geoffroy Couteau

Paris, France

Oct 2021 – Mar 2025

Université de Limoges

Master degree in Mathematics, Cryptology, Coding and Application

Highest Honours, Ranked 1st

Limoges, France

2019 – 2021

École Normale Supérieure de Hanoï

Pure Mathematics

Highest Honours, top 5%

Ha Noi, Viet Nam

2015 – 2019

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

Visiting Researcher

Supervisor: Masayuki Abe

Multi-round Zero-Knowledge Proofs and Applications to Advanced Post-quantum Signatures based on Multiparty Computation (MPC)

Tokyo, Japan

Jun – Aug 2024

COSIC, KU Leuven

Visiting Researcher

Supervisor: Nigel Smart

Efficient Post-quantum Signatures from Multiparty Computation (MPC)

Leuven, Belgium

Jul – Aug 2023

Research Institute IRIF, Université Paris Cité

Research Intern

Supervisor: Geoffroy Couteau

Efficient Multiparty Computation (MPC) Protocols from Pseudorandom Correlation Generators

Paris, France

Mar – Aug 2021

Research Institute XLIM, Université de Limoges

Summer Intern

Supervisor: Duong Hieu Phan

Private Set Intersection and its Application

Limoges, France

Jun – Aug 2020

SHORT-TERM VISIT

- **NTT Social Informatics Laboratories** Tokyo, Japan
Nov 2025
Hosted by: Masayuki Abe
- **Centrum Wiskunde & Informatica (CWI)** Amsterdam, Netherlands
Dec 2024
Hosted by: Lisa Kohl

FELLOWSHIPS & AWARDS

- **Best Paper Award at 24th International Conference on Cryptology and Network Security (CANS 2025)**
Paper: Efficient Fuzzy Labeled PSI from Vector Ring-OLE.
- **Fully-Funded Doctoral Grants, DIM Math Innov – FSMP (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 Université de 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:

- Nov 2025 **Efficient Fuzzy Labeled PSI from Vector Ring-OLE**
Conference CANS 2025, Osaka, Japan
- Jul 2025 **Improved All-but-One Vector Commitment with Applications to Post-Quantum Signatures**
Conference ACISP 2025, Wollongong, Australia
- 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:

- Critical Round in Multi-round Zero-Knowledge Proofs**
Jan 2026 INRIA – C2 (Codage & Cryptographie) seminar, Paris, France.
- FOLEAGE: F_4 OLE-Based Multi-party Computation for Boolean Circuits**
Sep 2025 Crypto Café, Florida Atlantic University, Florida, USA (Virtual).
- Mar 2025 ALMASTY seminar, Université Sorbonne, Paris, France.
Optimized MPC-in-the-Head based signatures from Puncturable PRF
Nov 2025 Crypto Seminars, NTT Social Informatics Laboratories, Tokyo, Japan.
- 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, ASIACRYPT 2025, EUROCRYPT 2026 (x2), PKC 2026.
- **Program Committee:** APKC 2025, LATINCRYPT 2025, APKC 2026, CCS 2026.

PUBLICATION

In Conference Proceedings:

- [ABB+26] Masayuki Abe, David Balbás, Dung Bui, Miyako Ohkubo, Zehua Shang, Akira Takahashi, and Mehdi Tibouchi. “Critical Rounds in Multi-Round Proofs: Proof of Partial Knowledge and Trapdoor Commitments”. In: *Advances in Cryptology – EUROCRYPT 2026*. 2026.
- [BGM+26] Dung Bui, Gayathri Garimella, Peihan Miao, and Phuoc Van Long Pham. “New Framework for Structure-Aware PSI From Distributed Function Secret Sharing”. In: *Advances in Cryptology – ASIACRYPT 2025*. 2026.
- [ABC+25] Benny Applebaum, Dung Bui, Geoffroy Couteau, and Nikolas Melissaris. “Structured-Seed Local Pseudorandom Generators and Their Applications”. In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2025)*. 2025.
- [Bui25] Dung Bui. “Efficient Multi-instance Vector Commitment and Application to Post-quantum Signatures”. In: *Information Security and Privacy – ACISP 2025*. 2025.
- [BC25] Dung Bui and Kelong Cong. “Efficient Fuzzy Labeled PSI from Vector Ring-OLE”. In: *Cryptology and Network Security - 24th International Conference, CANS 2025*. 2025.
- [BCS25] Dung Bui, Kelong Cong, and Cyprien Delpech de Saint Guilhem. “Faster VOLEitH Signatures from All-But-One Vector Commitment and Half-Tree”. In: *Information Security and Privacy – ACISP 2025*. 2025.
- [BBC+24] Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, and Sacha Servan-Schreiber. “FOLEAGE: F_4 OLE-Based Multi-party Computation for Boolean Circuits”. In: *Advances in Cryptology – ASIACRYPT 2024*. 2024.
- [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*. 2024.
- [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*. 2024.
- [BC23] Dung Bui and Geoffroy Couteau. “Improved Private Set Intersection with Small Entries”. In: *Public-Key Cryptography – PKC 2023*. 2023.

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* (2024).

■ OUTREACH ACTIVITIES

- **Co-organizer of an educational board game on quantum mechanics (QATS):** Led activities during "Quantum Day (Lumière sur la quantique)" organized by DIM QuanTiP, PCQT, Quantum Saclay, Atouts Sciences, QICS, and la SFP ([link](#)).
- **Organizer of the IRIF Crypto Seminar.**
- **Founder and author of the Vcryptis Blog:** Shared experiences and practical advice on student life and academic survival at the University of Limoges (vcryptis.tech.blog).
- **Featured in a Vietnamese national magazine:** Interview on career paths and motivation in cryptography (*Tuổi Trẻ*, [link](#)).

■ SKILLS

- **Programming Languages:** Python, C/C++, L^AT_EX, R, Maple
- **Languages:** Vietnamese (native), English (Professional proficiency), French (B2).