Dung Bui

bui@irif.fr https://dungbui15.github.io

EDUCATION

- **IRIF, University Paris Cité** — **Paris, France**
  PhD student in Secure Computation for Privacy-Preserving — *Oct 2021 – Current*
  Supervisor: Geoffroy Couteau

- **Université de Limoges** — **Limoges, France**
  Master degree in Mathematics, Cryptology, Coding and Application — *2019 – 2021*
  Highest Honours, Ranked 1st

RESEARCH INTERESTS

My research interests are in various aspects of both practical and theoretical cryptography, including secure multiparty computation, zero-knowledge proofs, and post-quantum cryptography.

EXPERIENCE

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

HONOURS/AWARDS

- **Fully-Funded DIM Math Innov Doctoral Grants** for doctoral degree, supported by grants from Ile-de-France Region (2021)
- **NSUCRYPTO Silver Medal** in the second round of the International Olympiad in Cryptography NsuCrypto (2021)
- **Fully-Funded Vingroup Scholarship** for Master's CRYPTIS Program in Mathematics, Cryptology, Coding and Applications (MCCA) (2019)
- **VIASM Scholarship** National Program for the Development of Mathematics, awarded by the Vietnam Institute for Advanced Study in Mathematics, Viet Nam (2017, 2018, 2019)
- **Bronze Medal** in Viet Nam National Mathematics Olympiad (VMO 2015)

PRESENTATION

- **Crypto Seminars** — **Tokyo, Japan**
  NTT Social Informatics Laboratories — *Jun 2024*

- **AlgoCRYPT Seminars** — **Virtual**
  J.P. Morgan — *Mai 2024*
- **Conference** — **Atlanta, USA**
  PKC 2023 — *May 2023*
- **Crypto Seminar** — **Virtual**
  Vietnam Institute for Advanced Study in Mathematics (VIASM) — *May 2023*
- **Algorithm and Complexity Seminar** — **Paris, France**
  IRIF — *Apr 2023*
- **Crypto Student Seminar** — **Virtual**
  CWI — *Jul 2022*
- **Workshop** — **Hendaye, France**
  Journées C2 (Codage & Cryptographie) — *Apr 2022*

PROFESSIONAL ACTIVITIES

- **External Reviewer:** TCC 2022, CSF 2022–2023, IEEE-TIFs 2023.

REFERENCES

Geoffroy Couteau
CNRS research scientist at IRIF, University Paris Cité
Tel: (+33)6 45 76 36 60
Email: couteau@irif.fr

Duong-Hieu Phan
Professor at Polytechnic Institute of Paris
Tel: (+33) 59 13 91 97
Email: hieu.phan@telecom-paris.fr