

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, MPC-in-the-Head, and zero-knowledge proofs.

EXPERIENCE

- **COSIC (KU Leuven)** **Leuven, Belgium**
Visiting Researcher *Jun – Aug 2023*
Building and optimizing MPCitH-based Signatures
Supervisor: Nigel Smart
- **Research Institute IRIF** **Paris, France**
Research Intern *Mar – Aug 2021*
Batch equality tests and secure comparison from pseudorandom correlation generators
Supervisor: Geoffroy Couteau
- **Research Institute XLIM** **Limoges, France**
Summer Intern *Jun – Aug 2020*
PSI (Private Set Intersection) and its Applications
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

- **AlgoCRYPT Seminars** **Online**
J.P. Morgan *Mai 2024*
- **Conference** **Atlanta, USA**
PKC 2023 *May 2023*
- **Crypto Seminar** **Online**
Vietnam Institute for Advanced Study in Mathematics (VIASM) *May 2023*

- **Algorithm and Complexity Seminar**
IRIF
- **Crypto Student Seminar**
CWI
- **Workshop**
Journées C2 (Codage & Cryptographie)

Paris, France
Apr 2023

Online
Jul 2022

Hendaye, France
Apr 2022

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