DUC V. LE

(Last updated December 6, 2021.)

PERSONAL INFORMATION

PHONE: +1-330-999-0842
WEBSITE: https://levduc.github.io/
EMAIL: duc.leviet@inf.unibe.ch

RESEARCH EXPERIENCE

OCT 2021– PRESENT

University of Bern, Bern, Switzerland
Postdoctoral Researcher
Research Focus: Applied Cryptography, Privacy, and Distributed System
Supervisor: Christian Cachin

EDUCATION

AUG 2015–AUG 2021

Purdue University, West Lafayette, Indiana
Ph.D. in Computer Science
Research Focus: Applied Cryptography. Advisors: Aniket Kate & Mikhail Atallah
→ Key Courses: Algorithm Design and Analysis, Information Retrieval, Cryptography, Information Security, Network Security, Computer Network

AUG 2011– DEC 2014

University of Mount Union, Alliance, Ohio
B.S. in Mathematics & Computer Information Systems
→ Key Courses: Software Engineering, Algorithm and Data Structure, Database theory, Web Database Programming

PUBLICATIONS

JUNE 2021

SoK: Blockchain Privacy (Under Submission)
Zhipeng Wang, Michalis Christou, ***Duc V. Le****, Arthur Gervais*
→ conducted a comprehensive and systematic study of blockchain privacy literature
→ distilled a set of common privacy goals among blockchain privacy solutions.

SEP 2020

Autonomous Coin Mixer with Privacy Preserving Reward Distribution (AFT 2021)
Duc V. Le*, Arthur Gervais*
→ used zero-knowledge proof system (zkSnark) and decentralized finance (Defi) applications to design an autonomous mixer that allows blockchain users to obfuscate their transactions and receive financial incentives for performing the obfuscation
→ implemented the design in Javascript and Solidity, and deployed the mixer to Ethereum blockchain testnet

AUG 2020

High-Frequency Trading on Decentralized On-chain Exchanges (S&P 2021)
Liyi Zhou, Kaihua Quin, Christof Ferreira Torres, ***Duc V. Le****, Arthur Gervais*
→ introduced an augmented variant of front-running attack called sandwich attack against the largest decentralized exchange called Uniswap
→ investigated and proposed different ways to mitigate the attack

FEB 2020

DLSAG: Dual Linkable Ring Signature (FC 2020)
Pedro Moreno-Sanchez, Arthur Blue, ***Duc V. Le****, Sarang Noether, Brandon Goodell*
→ proposed a new linkable ring signature scheme that allows for the first time the capability of building payment channel in Monero and provided formal security proofs for the proposed scheme
→ implemented the prototype of the scheme in C++ and libsodium library

DEC 2019

T^3: Scaling oblivious accesses to Large-Scale Blockchain (PETS 2020, BITCOIN 2019)
Duc V. Le*, Lizzy Hurtado, Adil Ahmad, Mohsen Minaei, Byoungyoung Lee, Aniket Kate*
→ used privacy enhancing techniques (i.e., Oblivious RAM) and TEE (i.e., Intel SGX) to design and implement a system that provides privacy to a SPV client when he/she interacts with a bitcoin full client

JUL 2019 | Flexible Digital Signature (ESORICS 2019)
Duc V. Le, *Mahimna Kelkar, Aniket Kate*
→ designed a digital signature framework that offers partial security guarantees for partial verification
→ provided a concrete construction of the flexible scheme using hash-based signature scheme
→ implemented the flexible signature scheme and provided the security proof for the scheme

JUN 2018 | Efficient and Secure Perfect Hashing (Information Sciences 2021)
Javad Darivandpour, ***Duc V. Le****, Mikhail Atallah*
→ proposed the first perfect hashing scheme in a multi-parties setting where the input of each parties is private

WORK EXPERIENCE

MAY – AUG 2020 | Imperial College London, **Remote**
Internship under the supervision of Dr. Arthur Gervais
→ Designed and built an autonomous cryptocurrency mixer with privacy preserving reward distributation
→ worked on understanding how frontrunning attacks affect certain DeFi applications, and investigated different ways to mitigate frontrunning attacks

MAY – AUG 2019 | Security and Privacy Group, **TU Vienna**
Internship under the supervision of Dr. Pedro Moreno-Sanchez
→ designed a new linkable ring signature that enables off-chain scalability solutions in Monero

2015–2019 | Department of Computer Science, **Purdue University**
Graduate Teaching Assistant
→ Courses: Foundations in Computer Science (CS182), Analysis of Algorithm (CS381), Cryptography (CS555), Network Security (CS528)

MAY-AUG 2016 | Center for Career Opportunities, **Purdue University**
Back-end Web Developer
→ collaborated with co-workers to build a new version of CCO website using ASP.NET MVC
→ redesigned and maintained the relational database of CCO office

SERVICE

PROGRAM COMMITTEE | *IEEE Security and Privacy on the Blockchain, IEEE S&B 2021*
ACM Computer and Communications Security, CCS 2021 (Posters)

EXTERNAL REVIEWER | *European Security and Privacy, Euro SP 2021*
ACM Transactions on Privacy and Security, ACM TOPS 2021

HONORS

Purdue University:

Travel Grant: Scaling Bitcoin 2019, ESORICS 2019

Summer Research Grant 2017, 2019: Awarded to predoctoral students who maintain a satisfactory academic and research progress while serving full time teaching assistant

University of Mount Union:

The Ullman Mathematics Prize 2015: Awarded to a member of senior class who is judged to be the best student in mathematics

The Alumni Computer Science and Information Systems Senior Prize 2014: Awarded to outstanding students majoring in Computer Science or Information Systems

Nordson Scholarship Recipient 2014: Awarded to individuals whose are pursuing careers in manufacturing, STEM (science, technology, engineering, and mathematics), or business disciplines leading to a career in industry and corporate America

Faculty/Staff Junior Academic Prize 2013: Awarded to a member of junior class who exhibited extraordinary achievement in the overall academic program

The Wilbur & Burdekka Stuckey Carl Mathematics Prize 2012: Awarded to a member of the freshmen class who are ranked best in Mathematics