DUC V. LE

(Last updated November 19, 2020.)

BASIC INFO

PHONE: +1-330-999-0842
WEBSITE: https://levduc.keybase.pub/
EMAIL: le52@purdue.edu

INSTITUTIONS

AUG 2015–PRESENT

Purdue University, West Lafayette, Indiana
M.S and Ph.D in Computer Science (Degree expected 2021)
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

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

RESEARCH

SEPTEMBER 2020

AMR: Autonomous Coin Mixer with Privacy Preserving Reward Distribution (Under submission)
Work with Prof. Arthur Gervais
→ used zero-knowledge proof system (zkSnark) to design an autonomous mixer that allows users on smart-contract-based blockchains to mix their transactions.
→ implemented the mixer contract and deployed to Ethereum blockchain.

AUGUST 2020

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

FEB 2020

DLSAG: Dual Linkable Ring Signature (FC 2020)
Work with Arthur Blue, Sarang Noether, Brandon Goodell, Prof. Aniket Kate, Prof. Pedro Moreno-Sanchez
→ 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 proof for the scheme
→ implemented a prototype of the proposed scheme

DEC 2019

T^3: Scaling oblivious accesses to Large-Scale Blockchain (PETS 2020)
Work with Lizzy Hurtado, Adil Ahmad, Mohsen Minaei, Prof. Byoungyoung Lee, Prof. 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
→ presented at Scaling Bitcoin 2019 and PETS 2020

JUL 2019

Flexible Digital Signature (ESORICS 2019)
Work with Mahimna Kelkar, Prof. Aniket Kate
→ designed a digital signature scheme 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– AUG 2020

Efficient and Secure Perfect Hashing
*Work with Javad Darivandpour, **Duc V. Le**, Prof. Mikhail Atallah*
→ proposed a perfect hashing scheme in a multi-party setting in which participants' inputs are private

Work Experience

May – Aug 2020	Liquidity Network, **Zurich, Switzerland** *Internship under the supervision of Dr. Arthur Gervais* → designed and built autonomous cryptocurrency tumbler with privacy preserving reward distributation. Used standard technique like zkSnark to design the tumbler → worked on understanding how frontrunning attacks affect certain DeFi applications, and investigated different way to mitigate frontrunning attacks
May – Aug 2019	Security and Privacy Group, **TU Vienna** *Internship under the supervision of Dr. Pedro Moreno-Sanchez* → worked on designing a new linkable ring signature that enables off-chain scalability solutions in Monero such as payment channels, conditional payments
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) → held weekly office hour to for students → created and wrote solutions for assigned homeworks and labs
May 2016-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

Languages

Machine	Java, C#, C, C++ (Basic), Julia, LaTeX, ASP.NET MVC, Javascript (Basic)
Human	Vietnamese (Native), English (Fluent)

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