Duc Viet Le

1200 Happy Hollow Apt 202, West Lafayette, IN, 47906

Email: le52@purdue.edu
Phone: 330-999-0842

Education

- **Purdue University** — West Lafayette, IN
  Ph.D. Computer Science; — *December 2021 (Expected)*
  - Key Courses: Algorithm design and analysis, Information Retrieval, Cryptography, Information Security, Data Communication and Computer Networks
  - Teaching Assistant: *Foundations in Computer Science* (CS182), *Introduction to the Analysis of Algorithms* (CS381), *Cryptography* (CS555), *Network Security* (CS528)
- **University of Mount Union** — Alliance, OH
  Bachelor of Science, Mathematics & Computer Information Systems; — *August 2011 - Dec. 2014*
  - Key Courses: Software Engineering, Web Database Programming, Programming Parallel System, Database Theory, Algorithms and Data Structures

Research Projects

- **Flexible Digital Signature Scheme (ePrint)** — Purdue University
  Research Project with Prof. Aniket Kate & Prof. Mikhail Atallah — *September 2016 - Present*
  - Used standard hash-based signature schemes to design a digital signature scheme that can offer partial security guarantees for partial/incomplete verification
  - Provided concrete constructions and security proofs of the proposed schemes
  - Implemented the flexible signature scheme in JAVA, and measured the performance of the scheme
- **Private Information Retrieval for Bitcoin Mobile Client** — Purdue University
  Research Project with Prof. Aniket Kate & Prof. Byoungyoung Lee — *September 2017 - Present*
  - Used privacy enhancing techniques (i.e. Oblivious RAM) and trusted execution environments (i.e. Intel SGX) to design a system that provides oblivious search to a Bitcoin Simplified Payment Verification client when it interacts with bitcoin full client.
  - Implemented the proposed system using C++ and Intel SGX.
- **Efficient and Secure Perfect Hashing** — Purdue University
  Research Project with Prof. Mikhail Atallah — *June 2018 - Present*
  - Proposed the first perfect hashing scheme in a multiparty setting where the input set of each parties is private
  - Used standard techniques like secret sharing and private set intersection to design the scheme

Experience

- **Back-end Web Developer** — Center for Career Opportunities, Purdue University
  Summer Job — *Summer 2016*
  - Collaborated with co-workers to build a new version of CCO website using ASP.NET MVC
  - Re-designed the database schema and used Microsoft SQL server to maintain CCO office SQL database
- **Knight's Tour Project** — University of Mount Union
  Project — *Spring 2014*
  - Developed a naive polynomial-time parallelizable algorithm for knight's tour puzzle
  - Implemented and parallelized the algorithm using CUDA programming language to test on NVIDIA graphics card

Skills

Machine Languages: C#, Java, C (basic), C++ (basic), CUDA (basic), Python, ASP.NET MVC, SQL, Julia, LaTeX

Softwares: Git (github), MS Office Suite, MS Visual Studio, IntelliJ

Honors

Summer Research Grant 2017 Awarded to predoctoral students who maintain a good academic and research progress while serving as a full time teaching assistant

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 Computer Information Systems