Ni T.N. Trieu

CONTACT INFORMATION

Oregon State University
1148 Kelly Engineering Center, 97331

Mobile: +1 - 541 - 250 - 2912[3]
E-mail: trieun at oregonstate.edu
Homepage: http://nitrieu.github.io/

EDUCATION

Oregon State University, Corvallis, Oregon, United States.

Ph.D. Candidate in Computer Science, September 2015 - Present

- Research Topic: *Secure Computation, Private Database System, and Secure Machine Learning, Attacks on Ciphers*
- Advisor: Prof. Mike Rosulek

M.Sc. in Computer Science, June 2017

- Title: New Tools and Techniques for Practical Private Set Intersection
- GPA: 3.93/4.0

Saint-Petersburg State Polytechnic University, Saint-Petersburg, Russia

B.Sc., Information Technology, September 2008 - June 2013.

- Thesis: Analysis of Efficient Parallel Algorithms in Graph Problems
- Advisor: Prof. Turalchuk K. A.
- GPA: 5.0/5.0 (**best student award** in the department)

PUBLICATION

Note: In all papers except [1,2] below, the **author names** are ordered **alphabetically**

8) *The Curse of Small Domains: New Attacks on Format-Preserving Encryption*
Viet Tung Hoang, Stefano Tessaro, Ni Trieu; In International Cryptology Conference **(CRYPTO)**, 2018.

7) *PIR-PSI: Private Contact Discovery at Scale*
Daniel Demmler, Peter Rindal, Mike Rosulek, Ni Trieu; 18th Privacy Enhancing Technologies Symposium **(PETS)** 2018.

6) *SWiM: Secure Wildcard Pattern Matching From OT Extension*
Vladimir Kolesnikov, Mike Rosulek, Ni Trieu; Financial Cryptography and Data Security **(FC)** 2018

5) *Practical Multi-party Private Set Intersection from Symmetric-Key Techniques*
Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, Ni Trieu; In 24^{rd} ACM Conference on Computer and Communications Security **(CCS)**, 2017.

4) *DUPLO: Unifying Cut-and-Choose for Garbled Circuits*
Vladimir Kolesnikov, Jesper Buus Nielsen, Mike Rosulek, Ni Trieu, Roberto Trifiletti; In 24^{rd} ACM Conference on Computer and Communications Security **(CCS**), 2017.

3) *Efficient Batched Oblivious PRF with Applications to Private Set Intersection*
Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, Ni Trieu; In 23^{rd} ACM Conference on Computer and Communications Security **(CCS)**, 2016.

2) *Models and Methods for the Urban Transit System Research*
Natalia Sadovnikova, Danila Parygin, Maria Kalinkina, Bulat Sanzhapov, Ni Trieu; Creativity in Intelligent, Technologies and Data Science, 2015

1) *Efficient Parallel Algorithm for The Minimum Spanning Tree*
Ni Trieu, Konstantin Turalchuk; 41^{th} International Scientific-practical Conference, SPbSPU, 2012

Research Experience

Research Intern Summer 2016, Summer 2017
Bell Labs, Nokia, United State
Research topics: Secure Computation, Private Set Operations, Private Database Queries

Research Assistant September 2014 to September 2015
Singapore University of Technology and Design (SUTD), Singapore
Research topics: Machine Learning, Financial Market Prediction.

Lecturer January 2014 to August 2014
Danang University of Science and Technology, Danang, Vietnam

Programming Experience

.NET Developer July 2013 to January 2014
FPT Software Company, Vietnam
RamquestOne Renovation project: reconstruct RamquestOne software to 3-tier architecture;

Sharepoint Software Engineer Intern October 2012
Reksoft Software Company, Russia
Social website: design and create a social website using Sharepoint.

Programming Project

Private Set Intersection & Pattern Matching
Implement protocols of publications [3,5,6]

DUPLO: Secure 2-party Computation
Implement a protocol (Frigate Extension) of publication [4] with Roberto Trifiletti

Honors and Awards

- Graduate Assistantship, OSU (2015-present).
- Scholarship from Vietnam Ministry of Education and Training to study in Russia, 2008-2013.
- Danang Talent Scholarship, 2004-2007.
- Top Graduation Award, Saint Petersburg State Polytechnic University, Russia (2013).
- Best student in Computer Science department, SPBSTU, 2013.
- Merit for Excellent Achievement in Study, Embassy of the Socialist Republic of Vietnam in Russia, 2012, 2013.
- Gold Medal in 30/4 Olympiad for Mathematics, Vietnam, 2006; and several prizes in mathematics and physics, city level,Vietnam, and SPbSTU, Russia.

Additional Information

- I have been an external reviewer for: PKC 2018, EUROCRYPT 2017, ASIACRYPT 2017, CCS 2016
- Give talks at CCS 2016, CCS 2017;
- Attend "MPC workshop" in Denmark ; " DIMACS Workshop on Cryptography and its Interactions" in Rutgers University, US; "Crypto conference 2016" in UCSB, US; "Huawei Seeds for the Future" in China.
- Teaching Assistant: CS 261 - Discrete Structures (Winter 2016)
- Language: English, Russian, Vietnamese.