Ni T.N. Trieu

PERSONAL INFORMATION

E-mail: nitrieu at asu.edu *Mobile:* +1 - 541 - 250 - 2918
Homepage: http://nitrieu.github.io *Github:* http://github.com/nitrieu

RESEARCH INTERESTS

My research interests are in the areas of cryptography and security, with a specific focus on secure computation and its applications such as contact tracing, online advertising, secure machine learning, and privacy-preserving bio-computing.

EDUCATION

Oregon State University, United States
Ph.D. in Computer Science — Mar 2020
- Thesis: Efficient Private Matching for Private Databases
- Advisor: Prof. Mike Rosulek

M.Sc. in Computer Science — June 2017
- Project: New Tools and Techniques for Practical Private Set Intersection

Saint-Petersburg State Polytechnic University, Saint-Petersburg, Russia
B.Sc., Computer Science — June 2013
- Thesis: Analysis of Efficient Parallel Algorithms for Graph Problems
- Advisor: Prof. Turalchuk K. A.

EMPLOYMENT HISTORY

Assistant Professor of Computer Science at Arizona State University, Tempe — Aug 2020 – Now

Postdoctoral researcher at UC Berkeley, United States — Mar 2020 to Aug 2020
with Dr. Dawn Song

Research Intern at Google, New York, United States — Summer 2019
with Dr. Mariana Raykova and Dr. Karn Seth

Research Intern at Visa Research, Palo Alto, United States — Summer 2018
with Dr. Payman Mohassel

Research Intern at Bell Labs, New Jersey, United States — Summer 2016, Summer 2017
with Dr. Vladimir Kolesnikov

Research Assistant at SUTD, Singapore — Sept 2014 – Aug 2015
with Dr. Yue Zhang

PUBLICATION

Articles in conferences (Note: Authorship is in **alphabetical** order.)

1. *MPCCache: Privacy-Preserving Multi-Party Cooperative Cache Sharing at the Edge*
   Duong Nguyen, Ni Trieu; In 25^{th} Financial Cryptography and Data Security **(FC)**, 2022.
2. *Simple, Fast Malicious Multiparty Private Set Intersection*;
   Ofri Nevo, Ni Trieu, Avishay Yanai; In 28^{th} ACM Conference on Computer and Communications Security **(CCS)**, 2021
3. *Compact and Malicious Private Set Intersection for Small Sets*;
   Mike Rosulek, Ni Trieu; In 28^{th} ACM Conference on Computer and Communications Security **(CCS)**, 2021
4. *Oblivious Key-Value Stores and Amplification for Private Set Intersection*
   Gayathri Garimella,Benny Pinkas, Mike Rosulek, Ni Trieu, Avishay Yanai; In 41^{st} International Cryptology Conference **(CRYPTO)**, 2021.
5. *Catalic: Delegated PSI Cardinality with Applications to Contact Tracing*
   Thai Duong, Duong Hieu Phan, Ni Trieu; In 26^{th} Annual International Conference on the Theory and Application of Cryptology and Information Security **(Asiacrypt)**, 2020.
6. *Practical Privacy-Preserving K-means Clustering*
   Payman Mohassel, Mike Rosulek, Ni Trieu; In 20th Privacy Enhancing Technologies Symposium **(PETS)** 2020.
7. *PSI from PaXoS: Fast, Malicious Private Set Intersection*
   Benny Pinkas, Mike Rosulek, Ni Trieu, Avishay Yanai; In 39^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques (**Eurocrypt**), 2020.

8. *Scalable Private Set Union from Symmetric-Key Techniques*
   Vladimir Kolesnikov, Mike Rosulek, Ni Trieu, Xiao Wang; In 25^{th} Annual International Conference on the Theory and Application of Cryptology and Information Security **(Asiacrypt)**, 2019.
9. *Minimalist Private Set Intersection via Sparse OT Extension*
   Benny Pinkas, Mike Rosulek, Ni Trieu, Avishay Yanai; In 39^{th} International Cryptology Conference **(CRYPTO)**, 2019.
10. *Attacks Only Get Better: How to Break FF3 on Large Domains*
    Viet Tung Hoang, David Miller, Ni Trieu; In 38^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques (**Eurocrypt**), 2019.
11. *The Curse of Small Domains: New Attacks on Format-Preserving Encryption*
    Viet Tung Hoang, Stefano Tessaro, Ni Trieu; In 38^{th} International Cryptology Conference **(CRYPTO)**, 2018.
12. *PIR-PSI: Private Contact Discovery at Scale*
    Daniel Demmler, Peter Rindal, Mike Rosulek, Ni Trieu; In 18th Privacy Enhancing Technologies Symposium **(PETS)** 2018.
13. *SWiM: Secure Wildcard Pattern Matching From OT Extension*
    Vladimir Kolesnikov, Mike Rosulek, Ni Trieu; In 22^{nd} International Conference on Financial Cryptography and Data Security **(FC)** 2018.
14. *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.
15. *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.
16. *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.

Journal articles (Note: Authorship is in order of **contribution**)

1. *Epione: Lightweight Contact Tracing with Strong Privacy*
   Ni Trieu, Kareem Shehata, Prateek Saxena, Reza Shokri, Dawn Song. IEEE Bulletin of the Technical Committee on Data Engineering (TCDE), 2020.
2. *BeeTrace: A Unified Platform for Secure Contact Tracing that Breaks Data Silos*
   Xiaoyuan Liu, Ni Trieu, Evgenios M. Kornaropoulos, and Dawn Song. IEEE Bulletin of the Technical Committee on Data Engineering (TCDE), 2020.

Other writtings

1. *PrivShare: Symmetric Private Query Processing on Multiple Sources*
   Xiaoyuan Liu, Yujie Lu, Tynan Sigg, Ni Trieu, Dawn Song.
2. *Multiparty Private Set Intersection Cardinality and Its Applications*
   Ni Trieu, Avishay Yanai, Jiahui Gao

US Patent

1. *Two-Server Privacy-Preserving Clustering*
   Payman Mohassel, Ni Trieu; US Patent; Filed: November 2019.
2. *Private Information Retrieval with Default, and Applications to Private Set Intersection*
   Karn Seth, Tancrède Lepoint, Sarvar Patel, Ni Trieu, Mariana Raykova; Filed: April 2020.

Mentoring & Advising

1. Jiahui Gao, Arizona State University, PhD (2021 - present)
2. Manazir Ahsan, Arizona State University, PhD (2021 - present)
3. Son Nguyen, Arizona State University, PhD (2022 - present)
4. Chetan Surana, Arizona State University, MS (2020 - 2021), now @ Amazon.

Selected Talk

1. Secure Computation for Contact Tracing
   - Microsoft Research Cryptography Colloquium (Redmond, Washington), 2020.
2. Private Set Intersection and Its Applications
   - UC Berkeley, 2020.
   - Facebook AI Research (NYC), 2020.
   - JPMorgan&Chase AI Research (NYC), 2020.
   - Galois Inc (Portland, OR), 2020.
   - Arizona State University, 2020.
3. Private Join and Compute
   - Google (NYC), 2019.
4. Private Pattern Matching
   - Visa Research Seminar (Palo Alto, CA), 2018.
5. Scalable Private Set Union from Symmetric-Key Techniques
   - Asiacrypt (Kobe, Japan), 2019.
6. SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension
   - CRYPTO (Santa Barbara, CA), 2019.
7. Practical Private Database queries: Make Blind Seer System Real
   - Bell labs (New Providence, NJ), 2017.
8. Practical Multi-party Private Set Intersection from Symmetric-Key Techniques
   - ACM Conference on Computer and Communications Security (Dallas, TX), 2017.
9. DUPLO: Unifying Cut-and-Choose for Garbled Circuits
   - ACM Conference on Computer and Communications Security (Dallas, TX), 2017.
10. Efficient Batched Oblivious PRF with Applications to Private Set Intersection
    - ACM Conference on Computer and Communications Security (Vienna, Austria), 2016.

Professional Activities

Faculty Search Committee: Arizona State University 2021, 2022

Panel Reviewer: National Science Foundation (NSF) SaTC 2020

Conference Program Committee

- The Web Conference (WWW), 2021, 2022
- Privacy Enhancing Technologies Symposium (PETS), 2022, 2023
- the International Cryptology Conference (CRYPTO), 2021, 2022
- ACM Conference on Computer and Communications Security (CCS), 2021, 2022
- Australasian Conference on Information Security and Privacy (ACISP), 2021
- ACM Cloud Computing Security Workshop (CCSW), 2020
- International Conference on Cryptology in India (Indocrypt), 2020
- International Conference on Provable and Practical Security (ProvSec), 2020
- International Symposium on Cyber Security Cryptology & Machine Learning, (CSCML) 2020

Conference Reviewer/subreviewer: Eurocrypt 2022, IEEE TCAS 2021, TCC 2021, CRYPTO 2020, CCS 2020, Asiacrypt 2020, IJIS 2020, JCEN 2019, NeurIPs 2019, CCS 2019, PPML 2018 (NeurIPs workshop), IEEE Access, TCC 2018, Asiacrypt 2018, SCN 2018, PKC 2018, Eurocrypt 2017, Asiacrypt 2017, CCS 2016.