Truong Son Nguyen

Tempe, AZ | snguye63@asu.edu | Google Scholar | LinkedIn | GitHub

Education

Arizona State University Tempe, AZ
Ph.D. in Computer Science (Advisor: Prof. Ni Trieu) *Jan 2022 – Expected Dec 2026*

- Focus: Secure Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and Secure AI Systems.

Tokyo Institute of Technology Tokyo, Japan
Bachelor of Engineering *Apr 2017 – Sep 2021*

Publications

1. **PULSE: Parallel Private Set Union for Large-Scale Entities**
ACM CCS 2025 (CORE: A)* – J. Gao, **S. Nguyen**, M. Blanton, N. Trieu
2. **Mario: Multi-round Multiple-aggregator Secure Aggregation with Robustness**
IEEE EuroS&P 2025 (CORE: A) – **T. S. Nguyen**, T. Lepoint, N. Trieu
3. **Achieving Data Reconstruction Hardness in Multiparty Minimax Training**
Privacy Enhancing Technologies (PETs) 2025 (CORE: A) – **T. S. Nguyen**, Y. Ren, G. Nie, N. Trieu
4. **AITIA: Efficient Secure Computation of Bivariate Causal Discovery**
ACM CCS 2024 (CORE: A)* – **T. S. Nguyen**, L. Wang, E. M. Kornaropoulos, N. Trieu
5. **Toward a Practical Multi-party Private Set Union**
PETS 2024 (CORE: A) – J. Gao, **T. S. Nguyen**, N. Trieu
6. **PrivateCalendar: Efficient and Secure Calendar Matching via Multiparty PSI over Small Universe**
Submitted to PETs 2026 (CORE: A) – **T. S. Nguyen**, MA M. Ahsan, J. Gao, N. Trieu
7. **Privacy preserving DNA Sequence Alignment**
in preparation for PETs 2026 (CORE: A) – **T. S. Nguyen**, S. Forrest, K. Buetow, J. Gao, K. Leybar, S. Hofmeyr, N. Trieu
8. **Privacy Preserving Retrieval Augmented Generation**
in preparation for NeurIPS 2026 (CORE: A)* – **T. S. Nguyen**, D. Brackley, N. Trieu, E. M. Kornaropoulos
9. **Security Analysis of Sparse Federated LoRA: Information Leakage and Defense via Lightweight Labeled Multiparty Private Set Union**
submitted to USENIX Security 2026 (CORE: A)* – **T. S. Nguyen**, N. Trieu

Research Projects

Privacy-Preserving Healthcare Analytics 2024 – Present

- Developing secure computation systems that enable medical institutions to analyze sensitive patient data without exposing raw records.
- Designed a privacy-preserving DNA sequence alignment framework allowing mutation detection while keeping genomic data encrypted.
- Reduced encrypted computation overhead through algorithm redesign and machine learning–assisted optimization, enabling practical runtime performance.

Secure Artificial Intelligence Systems 2022 – Present

- Building end-to-end privacy-preserving AI pipelines covering secure training, federated aggregation, and inference.
- Designed secure aggregation protocols enabling collaborative model training without revealing individual updates.
- Developed privacy-preserving large language model (LLM) systems that prevent user query leakage during retrieval and inference.

Experience

Arizona State University Tempe, AZ
Graduate Research Assistant *Jan 2022 – Present*

- Led development of **Mario**, a secure aggregation protocol enabling privacy-preserving federated learning in collaboration with Amazon AWS researchers; achieved **3.4x runtime improvement**.
- Co-developed **PULSE**, a distributed Private Set Union protocol processing millions of records with minimal communication overhead (ACM CCS 2025).
- Developed AITIA for privacy-preserving causal discovery; achieved **400x speedup** over prior secure computation approaches.
- Focused on translating cryptographic theory into deployable systems for healthcare and AI applications requiring regulatory-grade privacy guarantees.

VinBigData (VinGroup) Hanoi, Vietnam
AI Research Intern & Vision Researcher *Jun 2020 – Dec 2021*

- Optimized large-scale AI models for production deployment, emphasizing privacy-aware text and image analysis.
- Deployed face identification systems handling production-level traffic; integrated synthetic data pipelines.

Technical Expertise

Cryptography: Secure MPC, Fully Homomorphic Encryption (SEAL, TFHE.rs, DesiloFHE), PSI, Differential Privacy
Secure AI & ML: Federated Learning, Secure Aggregation, Knowledge Distillation, CrypTen, PyTorch
Systems Engineering: C++, Rust (Memory Safety), OpenMP, MPI, Pybind11
Deployment: Docker, Linux, Git, Distributed Systems Benchmarking