Jack W. Nero

Contact Information

jnero@nd.edu
(214) 422-0659
linkedin.com/in/jack-nero-b198752a2
github.com/jacknero2

Education

University of Notre Dame

Notre Dame, IN

B.S. in Computer Science (College of Engineering); Supplementary Major in Mathematics for Engineers

Expected May 2027

GPA: 3.52 / 4.00

Relevant Coursework

- **Computer Science:** Fundamentals of Computing, Data Structures, Logic Design, Systems Programming, Computer Architecture I, Operating System Principles, Theory of Computing, Programming Paradigms, Design & Analysis of Algorithms, Distributed Systems, Cryptography; Intro to Artificial Intelligence and Exotic Computing (in progress)
- **Mathematics:** Ordinary Differential Equations, Calculus (I, II, & III), Intro to Linear Algebra & Differential Equations, Introduction to Probability, Algebra, Real Analysis, Theory of Numbers, Complex Variables; Honors Algebra III and Honors Analysis I (in progress)

Research Experience

Data Security and Privacy Lab, University of Notre Dame

Aug 2024 – Present

Advisor: Prof. Taeho Jung

- DFPSI: Decoupled Fuzzy Private Set Intersection (submitted; 3rd author) – benchmarked quantized cosine similarity under BFV for biometric/financial data in collaboration with deep learning models; authored experimentation and evaluation; optimized latency and parameter choices.
- Scalable Private Membership Test over Distributed and Encrypted Data (3rd author) – built latency experiments for encrypted multi-server queries under FHE; tuned parameters for scale; applications to fraud detection and no-fly/watch-list screening.
- SLAP correction paper (2nd author) – corrected the security proof in SLAP, a secure multiparty protocol for private stream aggregation.

DREU (Distributed Research Experiences for Undergraduates) – Quantum Information Science, University of Maryland, Baltimore County

May – Present

Advisor: Prof. Lei Zhang

- Developing hybridized formal verification models for quantum algorithms with an application to post-quantum cryptography.

Teaching Experience

Math Tutor, Department of Mathematics, University of Notre Dame

Fall 2024

Technical Skills

Programming Languages: C++, Python, C, LaTeX
Libraries/Tools: SEAL, OpenFHE, PyTorch, ONNX, Git, Linux, Ovito, GROMACS
Languages: English (Native), Spanish (Intermediate)

Technical Projects

BFV Homomorphic Encryption Implementation (C++)

- Implemented core BFV components from scratch: polynomial modular arithmetic, encoding, and discrete noise sampling.

Publications

1. Paik, S., Koirala, N., Nero, J., Son, H., Kim, Y., Seo, J. H., & Jung, T. "Scalable Private Membership Test over Distributed and Encrypted Data." *21st ACM ASIA Conference on Computer and Communications Security (ACM AsiaCCS)*, 2026.
2. Paik, S., Koirala, N., Nero, J., Son, H., & Kim, Y. "DFPSI: Decoupled Fuzzy Private Set Intersection." Under review, 2026. *(title/venue evolving – see note)*
3. Takeshita, J., Nero, J., Karl, R., Gong, T., & Jung, T. "SLAP: Simpler, Improved Private Stream Aggregation from Ring Learning with Errors (Corrected Version)."

Awards

National Cryptographic Technology Contest – Excellence Award
September 2025
For "Scalable Private Membership Test over Distributed and Encrypted Data" (see Research Experience).