Jonathan Takeshita — 竹下ジョナサン賢

jtakeshi@odu.edu
https://sites.nd.edu/jonathan-takeshita/
https://www.linkedin.com/in/jonathan-t-33a73571/
(This CV last compiled on July 31, 2025)

EDUCATION

Postdoctoral Study
Tokyo Institute of Technology (Meguro, Tokyo) Aug. 2024 - Jan. 2025
Advised by Dr. Yang Cao

Doctor of Philosophy, Computer Science and Engineering
Master of Science, Computer Science and Engineering
University of Notre Dame (Notre Dame, IN) July 2018 - Jan. 2024
Dissertation: *Towards Improved Integration of Homomorphic Cryptography and Trusted Hardware*, advised by Dr. Taeho Jung

Bachelor of Science in Engineering (cum laude), Computer Science
University of Michigan (Ann Arbor, MI) Sept. 2015 - Dec. 2017
Minor in Mathematics

Bachelor of Arts (cum laude), Music and Combined Engineering (Physics)
Albion College (Albion, MI) Sept. 2012 - May 2017
Minor in Applied Mathematics
Thesis: *Classification of Consonance in Generalized Tonal Systems* (Mathematics)

HONORS AND AWARDS

The 35th Australasian Database Conference (Meguro, Tokyo)
Service Excellence Award (2024)

Meta Platforms, Inc. (Menlo Park, CA)
Meta PhD Research Fellowship Finalist, Security and Privacy (2022)

The University of Notre Dame (Notre Dame, IN)
CSE Outstanding Teaching Assistant Award (2021)
Jack and Mary Ann Remick Fellowship in Engineering (2018)

The University of Michigan - Ann Arbor (Ann Arbor, MI)
Dean's List (2016)
Order of the Engineer (2017)

Albion College (Albion, MI)
Bruce A. and Peggy Sale Kresge Science Fellowship (2015)
Dean's List (2014, 2015)
Kappa Mu Epsilon Mathematics Honor Society (2015)
Ruth Carter Roland Award (2015)
Harold Bristol Endowed Scholarship (2012)
Webster Scholarship (2012)

Boy Scouts of America Troop 54 (Novi, MI)
Eagle Scout Rank (2012)
Order of the Arrow - Brotherhood (2011, 2012)

JOURNAL PUBLICATIONS

Jonathan Takeshita, Nirajan Koirala, Colin McKechney, Taeho Jung. *HEProfiler: An In-Depth Profiler of Approximate Homomorphic Encryption Libraries.* Journal of Cryptographic Engineering 15, no. 2 (2025): 1-26.

Ryan Karl, Nirajan Koirala, Antonia Januszewicz, Jonathan Takeshita, Taeho Jung. *Cryptonite: A Framework for Flexible Time-Series Secure Aggregation with Non-interactive Fault Recovery.* SN Computer Science, (2025); impact factor of 4.34.

Nirajan Koirala, Jonathan Takeshita, Jeremy Stevens, Taeho Jung. *Summation-based Private Segmented Membership Test from Threshold-Fully Homomorphic Encryption.* Proceedings on Privacy Enhancing Technologies (2024), Volume 2024, Issue 4; impact factor of 3.4.

Jonathan Takeshita, Dayane Reis, Ting Gong, Michael Niemier, X. Sharon Hu, Taeho Jung. *Accelerating Finite-Field and Torus FHE via Compute-Enabled (S)RAM.* IEEE Transactions on Computers (TC) (2023); impact factor of 3.7. IEEE.

Jonathan Takeshita, Ryan Karl, Ting Gong, Taeho Jung. *SLAP: Simpler, Improved Private Stream Aggregation from Ring Learning With Errors.* Journal of Cryptology, Vol. 36 (2023); impact factor of 3.0. IACR.

Ryan Karl, Jonathan Takeshita, Hannah Burchfield, Taeho Jung. *Developing Non-Interactive MPC with Trusted Hardware for Enhanced Security.* International Journal of Information Security, 2022; impact factor of 3.2.

Dayane Reis, Jonathan Takeshita, Taeho Jung, Michael Niemier, X. Sharon Hu. *Computing-in-Memory for Performance and Energy Efficient Homomorphic Encryption.* IEEE Transactions on VLSI Systems (TVLSI) (2020); impact factor or 2.8. IEEE.

Jonathan Takeshita. *Classification of Consonance in Generalized Tonal Systems*, The Pentagon, Vol. 76, No. 1, 2017. Kappa Mu Epsilon.

CONFERENCE AND WORKSHOP PUBLICATIONS

Notes: In computer science, conference publications are generally as valuable or more valuable than journal publications; this may differ from other fields. Due to double-blind submission requirements, one (1) publication(s) under review are omitted.

Antonia Januszewicz, Daniela Medrano Gutiérrez, Nirajan Koirala, Jiachen Zhao, Jonathan Takeshita, Jaewoo Lee, Taeho Jung. *PPSA: Polynomial Private Stream Aggregation for Time-Series Data Analysis.* 20th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2024).

Jonathan Takeshita, Zachary Carmichael, Ryan Karl, Taeho Jung. *TERSE: Tiny Encryptions and Really Speedy Execution for Post-Quantum Private Stream Aggregation.* 18th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2022).

Jonathan Takeshita, Ryan Karl, Al-Amin Mohammed, Aaron Striegel, Taeho Jung. *Provably Secure Contact Tracing with Conditional Private Set Intersection.* 17th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2021).

Ryan Karl, Jonathan Takeshita, Al-Amin Mohammed, Aaron Striegel, Taeho Jung. *Cryptonomial: A Framework for Private Time-Series Polynomial Calculations.* 17th

EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2021).

Ryan Karl, Jonathan Takeshita, Taeho Jung. *Cryptonite: A Framework for Flexible Time-Series Secure Aggregation with Non-interactive Fault Recovery.* 17th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2021).

Ryan Karl, Jonathan Takeshita, Al-Amin Mohammed, Aaron Striegel, Taeho Jung. *CryptoGram: Fast Private Calculations of Histograms over Multiple Users' Inputs.* IEEE 17th International Conference on Distributed Computing in Sensor Systems (DCOSS 2021).

Jonathan Takeshita, Dayane Reis, Ting Gong, Michael Niemier, X. Sharon Hu, Taeho Jung. *Algorithmic Acceleration of B/FV-like Somewhat Homomorphic Encryption for Compute-Enabled RAM.* The 27th International Conference on Selected Areas in Cryptography (SAC 2020).

Jonathan Takeshita, Ryan Karl, and Taeho Jung. *Secure Single-Server Nearly-Identical Image Deduplication.* 10th International Workshop on Security, Privacy, Trust, and Machine Learning for IoT (IoTSPT-ML 2020), The 29th International Conference on Computer Communications and Networks (ICCCN 2020). IEEE.

Ryan Karl, Jonathan Takeshita, and Taeho Jung. *WiP: Using Intel SGX to Improve Private Neural Network Training and Inference.* The 7th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS 2020). ACM.

Ryan Karl, Hannah Burchfield, Jonathan Takeshita, and Taeho Jung. *Non-Interactive MPC with Trusted Hardware Secure Against Residual Function Attacks*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Security and Privacy in Communication Networks, pp. 425–439, Oct. 2019.

TEACHING EXPERIENCE

Old Dominion University
Professor for Cryptography for Cybersecurity (1 semester)

University of Notre Dame
TA for Design/Analysis of Algorithms (1 semester), TA for Cryptography (2 semesters, won 2021 CSE TA award), guest lecturer for Design/Analysis of Algorithms

University of Michigan
IA for Data Structures and Algorithms (1 summer semester), IA for Programming for Scientists and Engineers (2 semesters)

Albion College
Peer Tutor for Calculus I, II, III (2 semesters), Differential Equations and Linear Algebra (1 semester), Introduction to Computer Science (1 semester), General Physics (1 semester), Peer Tutor and transcriber for Music Theory I-IV and Keyboard Skills (2 semesters)

WORK EXPERIENCE

Assistant Professor Jan. 2025 - present
Old Dominion University (Norfolk, VA),
Department of Computer Science and School of Cybersecurity

Visiting Scholar Summer 2025
Tokyo Institute of Technology (Meguro, Tokyo),
Department of Computer Science

Postdoctoral Researcher Aug. 2024 - Jan. 2025
Tokyo Institute of Technology (Meguro, Tokyo),
Department of Computer Science

- Led research projects on security and privacy.
- Presented novel and interdisciplinary research at various workshops.

Software Engineer Sept. 2023 - July 2024
Cornami (Campbell, CA), FHE Team

- Gathered requirements and led the design and implementation of an internal benchmarking tool (details confidential).
- Conducted research and development on using Cornami's FractalCores compute fabric for accelerating private Large Language Models using homomorphic encryption.

Research Engineering Intern May 2022 - Sept. 2022
Meta (Menlo Park, CA), Statistics and Privacy

- Led research and development for applying Trusted Execution Environments to privacy-preserving advertising analytics.
- Conducted preliminary research, guided key design choices, and developed novel solutions for encountered theoretical and practical issues.
- Implemented a prototype that showed a 319x improvement in monetary cost and 60x improvement in speed, as compared to malicious MPC.

Software Engineering Intern May 2021 - Aug. 2021
Google (Sunnyvale, CA), Privacy Infrastructure Research

- Implemented the initial version of the Jaxite library (`https://github.com/google/jaxite`) for accelerating FHE on TPUs.
- Served as panelist for Tufts Coding 101 Intensive Career Panel.
- Authored article for internal engineering newsletter.
- Gave 4 presentations on internal work and external research.

Graduate Research Assistant July 2018 - Sept. 2023
University of Notre Dame (Notre Dame, IN), Department of Computer Science and Engineering

- Conducted research in areas including fully homomorphic encryption, quantum-secure aggregation, private contact tracing, secure multiparty computation, image deduplication, trusted hardware, and computing-in-memory.
- Mentored other graduate students, served as a guest lecturer, maintained lab computers, and wrote software and simulators for my projects and other projects.
- External research collaborations with Duality Technologies, Cryptolab Inc., Wireless Institute (Notre Dame), ASCENT Nanotechnology Center (Notre Dame).
- Published research as an IEEE Student Member.

Graduate Teaching Assistant Sept. 2018 - May 2019, Aug. - Nov. 2020
University of Notre Dame (Notre Dame, IN), Department of Computer Science and Engineering

- Held office hours, graded assignments, and evaluated examinations.
- Courses included CSE 40622 (Cryptography) and CSE 40113 (Design/Analysis of Algorithms).

Software Developer February 2018 - June 2018
Epic (Verona, WI)

- Certified in Chronicles Database Server Programming, Resolute Hospital Billing, and Single Billing Office Administrator.
- Also experienced in I18N Internationalization Programming and VB/HS Application Programming.

Instructional Aide January 2017 - December 2017
University of Michigan (Ann Arbor, MI), Department of Electrical Engineering and Computer Science

- Responsibilities included holding office hours, teaching discussion sections, writing exam questions, proctoring exams, and grading exams and projects.
- Courses included EECS 281 (Data Structures and Algorithms) and EECS 402 (Programming for Scientists and Engineers).

Student Researcher May 2016 - July 2016
Washington University in St. Louis (St. Louis, MO), Department of Computer Science and Engineering

- Research in low-power embedded software as part of an REU program.

Undergraduate Course Assistant August 2015
University of Michigan (Ann Arbor, MI), Department of Mathematics

- Assisted with a 2-week summer course exploring connections between mathematics and music theory.

Student Researcher May 2015 - July 2015
Albion College (Albion, MI), Department of Mathematics and Computer Science

- Conducted independent research in Applied Mathematics and Music Theory. Work resulted in an honors thesis and journal publication.

Peer Tutor September 2013 - May 2015
Albion College (Albion, MI), Quantitative Skills Center

- Held office hours and tutored individual students.
- Courses included Calculus I-III, Differential Equations and Linear Algebra, Introduction to Computer Science (Java), General Physics, Music Theory I-IV, Keyboard Skills.
- Transcribed textbooks with complex notation for visually-impaired students.

INVITED TALKS (not including conference paper presentations)

Old Dominion University and Map Communications April 30, 2025
“The Future of Voice Communications: AI Transformations Roundtable”

Old Dominion University, CS 800 (Research Methods) March 3, 2025
“Failure and Success in Graduate Study”

Australasian Database Conference 2024 (Tokyo site),
Encore Track Poster Presentation Dec. 18, 2024
“SLAP: Simpler, Improved Private Stream Aggregation from Ring Learning with Errors”

Kwansei Gakuin University (Osaka Umeda campus),
Workshop on Privacy-Enhancing Technologies and Law Nov. 23, 2024
“Privacy-Enhancing Technologies in American Law”

Tokyo Workshop on Trustworthy Foundation Models August 20, 2024
"Advances and Challenges in Applying Trusted Hardware for LLMs"

Old Dominion University, School of Cybersecurity March 14, 2024
"More Practical Cryptography for Computation on Private Data"

Trustworthy AI Lab for Education Summit Dec. 1, 2023
"Privacy-Enhancing Technologies for Educationally Focused AI"
`https://lucyinstitute.nd.edu/trustworthy-ai-lab-for-education-summit/`

Seagate Research Group June 6, 2023
"Privacy-Preserving Computation"

University of Notre Dame Book Club April 26, 2023
"A Brief Introduction to Japanese Society and Culture"

Albion College, Department of Mathematics and
Computer Science Colloquium Series Dec. 1, 2022
"Privacy-Preserving Computation"
`http://mathcs.albion.edu/Colloquium_List.php?year=2022`

PATENTS

63/240,128 (provisional): *Method of Contact Tracing With Enhanced Privacy Preservation*, filed Sept. 2, 2021

STUDENTS MENTORED

Doctoral student Bikash Thapa, Fall 2025 - present
- Served as Mr. Thapa's doctoral advisor.

Undergraduate student Aaron Killingbeck, Spring 2025 - present
- Mentored Mr. Killingbeck's research on trusted hardware.

Graduate student Alekhya Mengani, Spring 2025 - present
- Mentored Ms. Mengani's research on LLMs.
- Mentored Ms. Mengani's research on trusted hardware.

Doctoral student Nirajan Koirala, Summer 2021 - Fall 2024
- Mentored Mr. Koirala's research on profiling software libraries for homomorphic encryption.
- Mentored Mr. Koirala's research on privacy-preserving watchlist queries.

Doctoral student Tasha Januszewicz, Summer 2023 - present
- Mentored Ms. Januszewicz's research on Private Stream Aggregation.

Undergraduate student Ting Gong, Spring 2020 - Spring 2021
- Mentored Mr. Gong's research on finite-field algebra for homomorphic encryption.
- Now a Ph.D. student in mathematics at the University of Washington – Seattle.

Undergraduate student Justin Pajak, Summer 2021
- Mentored Mr. Pajak's research on integrating trusted hardware and homomorphic cryptography.
- Now a Software Development Engineer at Amazon.

Undergraduate student Colin McKechney, Summer 2021 - Fall 2021

- Mentored Mr. McKechney's research on integrating trusted hardware and homomorphic cryptography.
- Mentored Mr. McKechney's research on profiling software libraries for homomorphic encryption.
- Now a Security Software Engineer at Apple.

Undergraduate student Chris Boumalhab, Summer 2023

- Mentored Mr. Boumalhab's research on privacy-preserving watchlist queries.
- Now a Software Engineer at Balyasny Asset Management.

Undergraduate student Jeremy Stevens, Summer 2023

- Mentored Mr. Stevens' research on privacy-preserving watchlist queries.
- Now a Software Developer at Epic.

COURSEWORK AND SKILLS

Computer Science: Cryptography, Computer Security, Operating Systems, Cloud Computing, Computer Architecture/Organization, Advanced Algorithms, Hardware for Deep Learning, Exotic Computing, Foundations of Computer Science, Data Structures and Algorithms, Accessible Software System Development

Mathematics: Abstract Algebra, Real Analysis, Axiomatic Geometry, Combinatorics and Graph Theory, Discrete Mathematics, Linear Algebra, Calculus I-III, Differential Equations

Languages and Tools: C++, C, Python, Intel SGX, Java, MUMPS, Git, Linux, GDB, LaTeX, HTCondor, OpenMP, Docker, Singularity, OpenFHE, Microsoft SEAL, HEaaN, HElib

Other: Cyber Law, Statistics, Technical Writing, Analytical Physics, Mathematical Methods in Physics, Electronics, Microeconomics, Entrepreneurship, Inorganic Chemistry, Intermediate Japanese, Music Theory, Music History, Classical Piano

SERVICE

- Host for the ODU Computer Science Open House, 2025
- ODU Computer Science Systems Committee Member, 2025–present (3 candidacy exams)
- Artifact Reviewer for the 32^{nd} ACM Conference on Computer and Communications Security (2025)
- Reviewer for IEEE Transactions on Dependable and Secure Computing, 2025 (2 papers reviewed)
- Local Chair and Session Chair for the Australasian Database Conference, 2024
- Reviewer for Discover Computing, 2024 (1 paper reviewed)
- Reviewer for Quantum Information Processing, 2024 (1 paper reviewed)
- Reviewer for IEEE Transactions on Dependable and Secure Computing, 2024 (3 papers reviewed)
- Reviewer for the Journal of Supercomputing, 2024 (1 paper reviewed)
- Reviewer for Signal, Image, and Video Processing, 2024 (1 paper reviewed)
- Reviewer for the International Journal of Information Security, 2024 (3 papers reviewed)

- Reviewer for Securecomm, 2023 (5 papers reviewed)
- Reviewer for the 2nd Annual `FHE.org` Conference on Fully Homomorphic Encryption, 2023 (5 papers reviewed)
- Vice President, Notre Dame Graduate Student Government, 2020-2021
- Reviewer for IEEE Transactions on Dependable and Secure Computing, 2019 (1 paper reviewed)

DEVELOPMENT EXPERIENCE

Benchmarking FHE

- Performed comprehensive experimental evaluations of leading FHE software libraries.
- Wrote a custom scheduling script to integrate our testing framework's unique needs with University computing resources.
- **C++, OpenFHE, OpenMP, HEaaN, Microsoft SEAL, HElib, Linux, git, make, CMake, Bash, Univa Grid Engine**

Set Membership Test

- Implemented multi-party private set membership querying using homomorphic encryption.
- **C++, OpenFHE, OpenMP**

Advertising Attribution

- Implemented privacy-preserving advertising click attribution utilizing trusted hardware.
- **C++, C, Intel SGX, Microsoft Azure, Linux, Rust**

Hybridized Private Analytics

- Implemented a method for privacy-preserving machine learning using trusted hardware and homomorphic encryption.
- **C++, Intel SGX, Graphene, PALISADE, Linux**

Jaxite FHE library

- Initial design and implementation of Google's Jaxite library for implementing fully homomorphic encryption on Tensor Processing Units.
- **Python, Jax, Cider, Piper**

Contact Tracing System

- Implemented privacy-preserving contact tracing using trusted hardware and homomorphic encryption.
- **C++, Intel SGX, PALISADE, Microsoft SEAL, Linux, HTCondor**

Private Stream Aggregation

- Implemented efficient polynomial arithmetic, random number generation, and Private Stream Aggregation core functionality.
- **C++, C, Intel Software Guard eXtensions, GMP, Linux, Android, git**

CryptoGram/Cryptonomial/Cryptonite SGX development

- Implemented various cryptographic protocols for secure data aggregation and processing using Intel SGX.
- **C++, C, Intel Software Guard eXtensions, GMP, Linux, git**

Single-Server Nearly-Identical Image Deduplication

- Implemented AI-based image recognition, specialized database backend, and password-authenticated key exchange.
- **Python, C++, Tensorflow, pickle, GMP, ImageMagick, Linux, Univa Grid Engine, git**

Non-Interactive Multiparty Computation via Trusted Hardware

- Implemented a garbled circuit module, client and server programs, and communication overhead simulator.
- **C, C++, Trusted Platform Module, Linux, Windows**