Jonathan Takeshita
jtakeshi@nd.edu
https://sites.nd.edu/jonathan-takeshita/

EDUCATION

Doctor of Philosophy, Computer Science and Engineering
Master of Science, Computer Science and Engineering
University of Notre Dame (Notre Dame, IN) July 2018 - May 2023

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

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

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)

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

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

PUBLICATIONS

Jonathan Takeshita, Ryan Karl, Ting Gong, Taeho Jung. *SLAP: Simple Lattice-Based Private Stream Aggregation Protocol.* (Under revision at) Journal of Cryptology, 2022.

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).

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

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). IEEE.

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 Telecommuni-

cations Engineering Security and Privacy in Communication Networks, pp. 425–439, Oct. 2019.

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

WORK EXPERIENCE

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

- Led research and development for applying Trusted Execution Environments to privacy-preserving advertising analytics for the Statistics and Privacy Team.
- 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 Inc. (Sunnyvale, CA), Privacy Infrastructure Research

- Conducted research and development in homomorphic encryption. (Project work confidential.)
- 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 Student Researcher July 2018 - present
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.
- External research collaborations with Duality Technologies, Cryptolab Inc., Wireless Institute (Notre Dame), ASCENT Nanotechnology Center (Notre Dame).

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 Systems Corporation (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 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.

Kids on Campus Aide July 2013 - Aug. 2013, July 2014 - Aug. 2014
Schoolcraft College (Livonia, MI), Kids on Campus
- Aided teachers for the Schoolcraft College Kids On Campus program.
- Courses included Web Design and Creative Writing.

EXTRA-CURRICULAR ACTIVITIES

University of Notre Dame (Notre Dame, IN)
Vice President, Graduate Student Government (2020-2021)
Japan Club (2018-2022)

University of Michigan (Ann Arbor, MI)
Phi Mu Alpha Sinfonia Fraternity (elected Alumni Relations Officer)

Albion College (Albion, MI)
Phi Mu Alpha Sinfonia Fraternity (elected Music Director)

Boy Scouts of America Troop 54 (Novi, MI)
Elected to the positions of Senior Patrol Leader (1 term) and Patrol Leader (3 terms)