Meenatchi Sundaram Muthu Selva Annamalai

✉ *meenatchi.annamalai.22@ucl.ac.uk*
https://msundarmsa.github.io
https://github.com/msundarmsa

Education

2022— **PhD Cybersecurity**, *Cybersecurity CDT, University College London*, United Kingdom.

2021 **BEng Computing**, *Imperial College London*, United Kingdom.
First Class Honours

2015 **GCE A-Levels**, *National Junior College*, Singapore.
90 Rank Points (Straight As)

Honors and Awards

2021 **Winton Capital Applied Undergraduate Project Computing Prize**.
Awarded for an outstanding final year project in applied computing

2021 **Governors' Prize**.
Awarded to the final year student with the best overall performance in BEng Computing

2021 **Dean's List Year 3**.
Top 10% of year. Subjects taken: Number Theory, Network and Web Security, Type Systems, Distributed Algorithms, Computer Vision, Operations Research, Software Engineering Group Project, Final Year Project

2020 **Dean's List Year 2**.
Top 10% of year. Subjects taken: Algorithms II, Compilers, Computing Laboratory II, Models of Computation, Networks and Communications, Operating Systems, Probability and Statistics, Software Engineering and Design, Computing Group Project

2019 **Dean's List Year 1**.
Top 10% of year. Subjects taken: Computer Architecture, Databases I, Discrete Structures, Graphs and Algorithms, Hardware, Logic, Mathematical Methods, Programming, Reasoning about Programs, Computing Topics, Computing Group Project

2016 **National Science Scholarship (BS-PhD)**.
Awarded to students with a keen interest in Science and Research, and excellent academic standing to pursue an undergraduate followed by doctoral degree in overseas universities

Publications

Nearly Tight Black-Box Auditing of Differentially Private Machine Learning, *Under Review*.
Annamalai, M.S. M. S., De Cristofaro, E.

The Elusive Pursuit of Replicating PATE-GAN: Benchmarking, Auditing, Debugging, *Under Review*.
Ganev G., **Annamalai, M.S. M. S.**, De Cristofaro, E.

It's Our Loss: No Privacy Amplification for Hidden State DP-SGD With Non-Convex Loss, *In 17th ACM Workshop on Artificial Intelligence and Security (AISec 2024)*.
Annamalai, M.S. M. S.

"What do you want from theory alone?" Experimenting with Tight Auditing of Differentially Private Synthetic Data Generation, *In 33rd USENIX Security Symposium (USENIX Security 2024)*.
Annamalai, M.S. M. S., Ganev G., De Cristofaro, E.

A Linear Reconstruction Approach for Attribute Inference Attacks against Synthetic Data, *In 33rd USENIX Security Symposium (USENIX Security 2024)*.
Annamalai, M. S. M. S., Gadotti, A., Rocher, L.

Collaboration with Google Research

FP-Fed: Privacy-Preserving Federated Detection of Browser Fingerprinting, *In 31st Network and Distributed System Security Symposium (NDSS 2024)*.
Annamalai, M. S. M. S., Bilogrevic, I., De Cristofaro, E.

CoVnita, an end-to-end privacy-preserving framework for SARS-CoV-2 classification., *In Scientific Reports 13*.
Sim J. J., Zhou W., Chan F. M., **Annamalai, M. S. M. S.**, Deng X., Tan B. H. M. & Aung, K. M. M.

Communication-Efficient Secure Federated Statistical Tests from Multiparty Homomorphic Encryption., *In Applied Sciences 12*.
Annamalai, M. S. M. S., Jin, C., & Aung, K. M. M.

Pool Inference Attacks on Local Differential Privacy, *In 31st USENIX Security Symposium (USENIX Security 2022)*.
Gadotti, A., Houssiau, F., **Annamalai, M. S. M. S.**, & de Montjoye, Y. A.

The Observatory of Anonymity: An Interactive Tool to Understand Re-Identification Risks in 89 countries, *In Companion Proceedings of the Web Conference 2021 (pp. 687-689)*.
Rocher, L., **Muthu, M. S.**, & de Montjoye, Y. A.

Privacy Preserving Collective Learning with Homomorphic Encryption, *In IEEE Access*.
Paul, J., **Annamalai, M. S. M. S.**, Ming, W., Al Badawi, A., Veeravalli, B., & Aung, K. M. M.

Research Experiences

2022 **1 Year Research Attachment**, Institute for Infocomm Research.
Project 1: Collaborative polygenic risk score validation based on Multiparty Homomorphic Encryption and Secure Multiparty Computation
Project 2: Reconstruction attacks on synthetic data
Mentors: Khin Mi Mi Aung and Andrea Gadotti

2021 **Final Year Project**, Imperial College London.
Project: Studying the information leakage in differentially private mechanisms
Mentors: Andrea Gadotti and Yves-Alexandre de Montjoye

- Awarded Winton Capital Applied Undergraduate Project Computing Prize

2020 **Undergraduate Research Opportunities Programme**, Imperial College London.
Project: Privacy risk assessment tool for real-world data collections
Mentors: Luc Rocher and Yves-Alexandre de Montjoye

- Designed and created interactive website that demonstrates re-identification risk in 89 countries based on prior research done in the group. Ported over code from Julia to Typescript for deployment to website and further optimized routines using WebAssembly. https://cpg.doc.ic.ac.uk/observatory/
- Full code is available at https://github.com/computationalprivacy/observatory

2019 **8 Week Research Attachment**, Institute for Infocomm Research.
Project: Homomorphic Encryption for Transfer Learning with MIMIC-III Timeseries Data
Mentors: Jestine Paul and Khin Mi Mi Aung

- Explored the applicability of HE in a transfer learning setting for LSTMs

2014 **H3 Research, GCE A Levels**, Institute for High Performance Computing.
Project: Designing photonics components and circuits using photonic crystals
Mentors: Chu Hong Son

- Modelled and simulated photonic crystal structures in order to optimize them for biosensor applications

Presentations

2021 **The Observatory of Anonymity: An Interactive Tool to Understand Re-Identification Risks in 89 countries**.
Companion Proceedings of the Web Conference 2021. https://rocher.lc/observatory-www21.pdf

Teaching

Undergraduate Teaching Assistant

2021 **Discrete Structures, Logic, Reasoning about Programs and Graphs and Algorithms**, *Imperial College London*.
Conducted weekly tutorial sessions and graded homework

Personal Projects

2022 **STASYS**.
Created a cross-platform open source aim tracing application for air pistol/air rifle targets using OpenCV, React, Typescript and Rust. https://github.com/msundarmsa/stasys-tauri

2022 **Solli**.
Created a Wordle clone in Tamil using Vue and Javascript. https://github.com/msundarmsa/wordle-tamil-src

2013 **Encrichment Science and Training Programme**.
Developed mobile app to enhance classroom learning.

2011 **Special Programme in Enquiry and Research**.
Programmed a hygenic, non-touch interface for feedback systems deployed in unsanitary locations using Microsoft Kinect.

Computer skills

Languages: Python, Typescript/Javascript, Go, Rust, C/C++, Java, Haskell, Elixir

Experiences in: Software engineering and design, Secure multiparty computation (MP-SPDZ), Homomorphic encryption (Lattigo, Microsoft SEAL), Web, mobile and desktop applications, Multiprocess parallel programming, Machine Learning/Deep Learning, Numerical integration

Extra-curriculars

2019 **Major Event Officer of Imperial College Singapore Society**.
Produced a student-written and performed full-length musical

2014 **Vice President of IT & Innovation Club**.
Organized and taught programming courses and workshops for members, lead teams in competitions and managed club's administrative affairs