Seoyeon Hwang

Contact: seoyh1@uci.edu **Address**: Irvine, CA, USA

Research Interests

Applied Cryptography, Security, Privacy, Formal Verification, and Applied Mathematics

Education

University of California, Irvine (UCI) **Irvine, CA, USA**
Ph.D. Candidate in Computer Science (Advisor: Prof. Gene Tsudik) September 2018 – Present
GPA: 3.972/4.00

Ewha Womans University (Ewha) **Seoul, South Korea**
M.S. in Mathematics (Advisor: Prof. Hyang-Sook, Lee) March 2014 – February 2016
GPA: 4.19/4.30 (4.41/4.50)
Thesis: Cryptanalysis of Feistel Block Ciphers, SIMON and SEED using Low Data Attack

Ewha Womans University (Ewha) **Seoul, South Korea**
B.S. in Mathematics & Information Security, Minor in Computational Science March 2010 – February 2014
GPA: 3.99/4.30 (4.24/4.50) (Magna Cum Laude), 4.195/4.30 for last 4 semesters
Thesis: Low Exponent RSA Attack using LLL algorithm

Work Experiences

Amazon.com – Cryptography Team **(Remote) Seattle, WA, USA**
Applied Scientist Intern June 2021 – September 2021
I joined research in Cryptographic computing, especially in available operations atop the Private Set Intersection (PSI), encrypted database management system, and key establishment problem.

Amazon.com – Cryptography Team **(Remote) Seattle, WA, USA**
Applied Scientist Intern June 2020 – September 2020
I joined research in Cryptographic computing, especially in Two Party Computation (2PC) and circuit-based PSI, including open-sourced libraries in 2PC and prototyping the performance.

Stanford Research Institute International (SRI) **Menlo Park, CA, USA**
Security Intern June 2019 – September 2019
I worked on Cryptography, especially in Secret Sharing and Multi-Party Computation (MPC), mainly working on protocol design and security proofs. Continuing the project afterwards, our work is published in the conference, Security and Cryptography for Networks (SCN)' 2020.

Telecommunications Technology Association (TTA) **Gyeonggi-do, South Korea**
Junior Engineering Staff June 2016 – July 2017
Working in Information Security Evaluation team, I mainly evaluated and certified the safety of IT products according to the Common Criteria. Also, I joined to improve cryptographic functional requirements on the national Protection Profile, and various research such as AI security.

Penta Security Systems Inc. **Seoul, South Korea**
Intern July 2013 – August 2013
I mainly trained software engineers on the basics of cryptography, surveyed on Bring Your Own Device security, and redeemed a networking protocol to apply for a patent.

Other Research Experiences (Current / Past Projects)

(Ongoing) Proof of Participation in Secure Federated Learning **2023 - Present**
For individuals' right on their personal data by privacy laws such as GDPR/CCPA, we research on how to prove the participation in secure federated learning without revealing their local data.

(Ongoing) Private List Intersection and Its Variants **2023 - Present**
We investigate how PSI can be modified for lists and come up with more realistic PLI variants with applications

(Under Submission) Publicly Verifiable Watermarking **2022 - 2023**
For better ownership verification in digital assets, we suggest a framework using secret sharing and trusted execution environment that allows any watermarking techniques to be publicly verifiable unlimited amount of times without owner's involvement.

(Under Submission) Input Verification of Private Set Intersection and Its Variants **2020 - 2023**
Considering malicious inputs in PSI as non-sets (with duplicates), we propose protocols to prove "set"ness without revealing any other information about the input elements using generalized two billiard balls problem and zero-knowledge proof (ZKP). We also show ways of applying these techniques to PSI variants.

Security by Formally Verified Design for Middle-end IoT Devices (Published in ICCAD'23) **2020 - 2023**
We design a remote attestation architecture over a formally verified microkernel, seL4, to deploy on middle-end IoT devices and formally verify the security on runtime attestation using F*.

Security by Formally Verified Design for Low-end IoT Devices (Published in S&P'22) **2021 - 2022**
To guarantee data privacy on low-end IoT devices from when it is first available, we formally defined "Privacy-from-Birth" and designed a provable secure and formally verified architecture, VERSA. Our implementation is formally verified (using Verilog HDL, SPOT LTL proof assistant, and cryptographic reduction), and S/W component uses HACL*.

Secure Computation for Genomic Security & Privacy (Published in TOPS'22) **2019 - 2021**
To reveal minimal amount of genomic data to a testing facility, while guaranteeing the authenticity and integrity, we proposed protocols for genomic range queries using Zero-Knowledge Range Proofs and then extended the idea to private matching tests using homomorphic encryption. This is extended from the previous work published in WPES'19.

Protocol Design for Proactive MPC against Mobile Adversary Model (Published in SCN'20) **2019 - 2020**
We designed proactive MPC protocols for dynamic general adversary structures and dynamic groups, considering the mobile adversary settings. We made two MPC schemes, one based on additive secret sharing and the other based on monotone span programs, to be proactively secure by adding three protocols. We also showed share conversion between the two MPC schemes.

National Security Research Institute (NSR) Cryptographic Skill Training Course **2015 - 2016**
I was selected as one of the 8 outstanding graduates across the country organized by NSR for 6 months training course. Our team conducted a research of designing new block ciphers. We studied various block ciphers and attacks on them. Then we designed new block ciphers and analyzed them using linear and differential cryptanalysis.

Undergraduate Internships at *Cryptography Lab / ** Institute of Mathematical Science (IMS), in Ewha

- Programming PKEs with Sage (*) **2013 Summer**
I implemented some Public-Key Encryption algorithms including Diffie-Hellman Key exchange, RSA, ElGamal, and Elliptic Curve Cryptosystem, using a programming language, Sage.
- Hacking Skills on Linux (*) **2012 Winter**
I studied the basic language of Linux and practiced foundational hacking skills including buffer overflow and format string.
- Coding Theory (**) **2012 Summer**
I participated in studying Coding Theory. I mainly surveyed some bounds for codes, perfect code, and Hamming code.
- MATLAB study, Computational Science Project (**) **2011 Winter**
I studied MATLAB and modeled and implemented a problem in Computational Science (computing sundials with real time and analemma graphs).

Publications (Author List in Alphabetical Order)

PARseL: Towards a Verified Root-of-Trust over seL4
To be appeared in IEEE/ACM International Conference on Computer-Aided Design, 2023 (**ICCAD'23**)
Authors: Ivan De Oliveira Nunes, **Seoyeon Hwang**, Sashidhar Jakkamsetti, Norrathep Rattanavipanon, and Gene Tsudik

Balancing Security and Privacy in Genomic Range Queries
Published in ACM Transactions on Privacy and Security, 2023 (**TOPS'23**)
Authors: **Seoyeon Hwang**, Ercan Ozturk, and Gene Tsudik

Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA
Published in IEEE Security and Privacy (**S&P'22**)
Authors: Ivan De Oliveira Nunes, **Seoyeon Hwang**, Sashidhar Jakkamsetti, Gene Tsudik

Communication-Efficient (Proactive) Secure Computation for Dynamic General Adversary Structures and Dynamic Groups
Published in Security and Cryptography for Networks, 2020 (**SCN'20**)
Authors: Karim Eldefrawy, **Seoyeon Hwang**, Rafail Ostrovsky, and Moti Yung

Language

Spoken: Korean(native), English(fluent), Japanese(beginner)
Programming: C/C++, Python, GoLang, JAVA, Sage, MATLAB

Organization

Women In CyberSecurity (WiCyS) Student Chapter at UCI **UCI**
Secretary → Co-president → (current) Marketing Chair February 2021 – Present
WiCyS Student Chapter at UCI is a Student Chapter from the national WiCyS which is organized with the following purposes: 1. To decrease the gender disparity in cybersecurity; 2. To provide education, mentorship, and networking support to students through the WiCyS community; and 3. To promote and recruit women in cybersecurity workforce through UCI.

Information Security Group, E-COPS **Ewha**
Founding member January 2013 – February 2014
E-COPS is a security and cryptography research group consisting of CS and Math students. I mainly studied system security, network security, and cryptography, shared updated security issues, and participated in the national security contest as a team.

Mathematics Research Group, Mathclub **Ewha**
Founding member March 2012 – February 2014
Mathclub is a math research group to study extracurricular mathematics for fun. I mainly studied general topology, knot theory, combinatorics, graph theory, and game theory.

Honors and Awards

Dean's Award **UCI**
1 Academic Year, 2018

Research Assistant (RA) Scholarship **Ewha**
Financial Aid for Full Tuition Fee 1 Year, 2015

Full Scholarship for Outstanding Student in Ewha **Ewha**
Financial Aid for Full Tuition Fee 1 Year, 2014

Dean's List (1st Semester in 2010 and All Semesters in 2011–2013) **Ewha**
Scholarship for Partial Tuition Fee 2010 – 2013