SEUNGHOON LEE

Postdoctoral Researcher | Department of Computer Science, Purdue University

305 N University St, West Lafayette, IN 47907, USA | https://lee2856.github.io | lee2856@purdue.edu

RESEARCH INTEREST

My research interests lie at the intersection of mathematics and cryptography. My past work has involved the application of combinatorial graph theory to analyze the (post-quantum) security of Memory-Hard Functions and Proofs of Sequential Work. I have also worked on analyzing the preprocessing security of cryptographic primitives in multiple idealized models, including short Schnorr signatures and Key Encapsulation Mechanisms. Recently, I have developed a deep interest in isogeny-based cryptography, drawing me toward its rich number-theoretic and algebraic foundations and its promising role in post-quantum cryptographic protocols.

EDUCATION

Aug. 2017 - May 2024 — **Ph.D. in Computer Science** — **Purdue University**
Dissertation: Applications of Combinatorial Graph Theory to the Classical and Post-Quantum Security Analysis of Memory-Hard Functions and Proofs of Sequential Work
Advisor: Jeremiah Blocki

Mar. 2013 - Dec. 2013 — **Doctoral Student in Mathematics** — **Seoul National University**
Left due to the mandatory military service

Sep. 2010 - Feb. 2013 — **M.S. in Mathematics** — **Seoul National University**
Thesis: Reinitializing Techniques in Level Set Method
Advisor: Myungjoo Kang

Mar. 2005 - Feb. 2010 — **B.S. in Mathematics** — **POSTECH (Pohang University of Science and Technology)**
Graduated *magna cum laude*, Recipient of the ***Presidential Science Scholarship***

PUBLICATIONS AND PREPRINTS

(Note: Authors are listed in alphabetical order by their last name.)

Preprints Under Review

1. **Differentially Private Compression and the Sensitivity of LZ77**
   Jeremiah Blocki, Seunghoon Lee, and Brayan Sebastián Yepes Garcia
   arXiv, 2025.
2. **Preprocessing Security in Multiple Idealized Models with Applications to Schnorr Signatures and PSEC-KEM**
   Jeremiah Blocki and Seunghoon Lee
   Cryptology ePrint Archive, 2025.
3. **A Tight Lower Bound on the TdScrypt Trapdoor Memory-Hard Function**
   Jeremiah Blocki and Seunghoon Lee
   Cryptology ePrint Archive, 2024.

Publications

4. **The Impact of Reversibility on Parallel Pebbling**
   Jeremiah Blocki, Blake Holman, and Seunghoon Lee
   *In Advances of Cryptology – **EUROCRYPT 2025** (To appear)*
5. **Differentially Private L_2-Heavy Hitters in the Sliding Window Model**
   Jeremiah Blocki, Seunghoon Lee, Tamalika Mukherjee, and Samson Zhou
   *In The Eleventh International Conference on Learning Representations **(ICLR 2023)***
6. **The Parallel Reversible Pebbling Game: Analyzing the Post-Quantum Security of iMHFs**
   Jeremiah Blocki, Blake Holman, and Seunghoon Lee
   *In Theory of Cryptography Conference **(TCC 2022)***
7. **On the Multi-User Security of Short Schnorr Signatures with Preprocessing**
   Jeremiah Blocki and Seunghoon Lee
   *In Advances of Cryptology – **EUROCRYPT 2022***

8. **On Explicit Constructions of Extremely Depth Robust Graphs**
   Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, and Jin Young Son
   In 39th International Symposium on Theoretical Aspects of Computer Science ***(STACS 2022)***
9. **On the Security of Proofs of Sequential Work in a Post-Quantum World**
   Jeremiah Blocki, Seunghoon Lee, and Samson Zhou
   In 2nd Conference on Information-Theoretic Cryptography ***(ITC 2021)***
10. **Approximating Cumulative Pebbling Cost is Unique Games Hard**
    Jeremiah Blocki, Seunghoon Lee, and Samson Zhou
    In 11th Innovations in Theoretical Computer Science Conference ***(ITCS 2020)***
11. **Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions**
    Jeremiah Blocki, Benjamin Harsha, Siteng Kang, Seunghoon Lee, Lu Xing, and Samson Zhou
    In Advances of Cryptology – ***CRYPTO 2019***

In Preparation

12. **Sparse Depth-Robust Graphs with Improved Lower Bounds**
    Jeremiah Blocki, Jong Chan Lee, Seunghoon Lee, Peiyuan Liu, and Ling Ren

Manuscript

13. **A Short Note on Improved Logic Circuits in a Hexagonal Minesweeper**
    Seunghoon Lee

WORK EXPERIENCE

Jul. 2024 –	**Postdoctoral Researcher**	**Purdue University**
Jan. 2022 – May 2024, Jan. 2019 – Aug. 2021	**Graduate Research Assistant**	**Purdue University**
Aug. 2021 – Dec. 2021, Aug. 2017 – Dec. 2018	**Graduate Teaching Assistant**	**Purdue University**
Dec. 2013 – Dec. 2016	**Senior Researcher (mandatory military service)**	**Security Management Institute**
Sep. 2010 – Dec. 2013	**Graduate Teaching Assistant**	**Seoul National University**

TEACHING EXPERIENCE

Purdue University

- **CS 58000-DEV: Algorithm Design, Analysis, and Implementation — Online Course Development**, Teaching Assistant (Fall 2021)
- **CS 51500: Numerical Linear Algebra**, Teaching Assistant (Fall 2018)
- **CS 25100: Data Structures and Algorithms**, Teaching Assistant (Fall 2017, Spring 2018)

Seoul National University

- **300.204: Differential Equations**, Teaching Assistant (Spring/Fall 2013)
- **033.002: Calculus 2**, Teaching Assistant (Fall 2010, Fall 2013)
- **033.001: Calculus 1**, Teaching Assistant (Spring 2013)
- **033.004: Honor Calculus and Practice 2**, Teaching Assistant (Fall 2012)
- **046.001: Mathematics in Civilization**, Teaching Assistant (Spring/Fall 2011, Spring 2012)
  Received ***Outstanding TA Award*** *(Spring 2012)*

MENTORING ACTIVITIES

Undergraduate Students

Spring/Fall 2024 — Brayan Sebastián Yepes Garcia — **Purdue University & Universidad Nacional de Colombia**
Topic: Differentially Private Compression and the Sensitivity of LZ77

TALKS AND POSTER PRESENTATIONS

Talks

Dec. 2023	Multi-User Security of Short Schnorr Signatures with Preprocessing	**Purdue Crypto Reading Group**
Nov. 2022	The Parallel Reversible Pebbling Game: Analyzing the Post-Quantum Security of iMHFs	**TCC 2022**
Mar. 2022	On Explicit Constructions of Extremely Depth Robust Graphs	**STACS 2022**
Jul. 2021	On the Security of Proofs of Sequential Work in a Post-Quantum World	**ITC 2021**
Jan. 2020	Approximating Cumulative Pebbling Cost is Unique Games Hard	**ITCS 2020**
Nov. 2019	Approximating Cumulative Pebbling Cost is Unique Games Hard	**Purdue Crypto Reading Group**

Posters

Mar. 2022	On the Multi-User Security of Short Schnorr Signatures with Preprocessing	**CERIAS Symposium 2022**
Jan. 2020	Approximating Cumulative Pebbling Cost is Unique Games Hard	**ITCS 2020**
Apr. 2019	On the Security of Short Schnorr Signatures	**Midwest Security Workshop 7**
Apr. 2019	On the Security of Short Schnorr Signatures	**CERIAS Symposium 2019**

PROFESSIONAL ACTIVITIES

External Reviewers

CCS 2019, NDSS 2020, CT-RSA 2020, ITC 2020, CRYPTO 2020, TCC 2020, CRYPTO 2021, ITCS 2022, FC 2022, ITC 2022, CRYPTO 2022, SYNASC 2022, IEEE S&P 2023, EUROCRYPT 2023, IEEE S&P 2024, EUROCRYPT 2024, ITC 2024, ESA 2024, QIP 2025, and IEEE S&P 2025.

Student Outreach

2013	Research and Education Program	**Sejong Science High School**

GRANTS AND AWARDS

Academic Grants & Awards

Aug. 2023 – May 2024	Bilsland Dissertation Fellowship	**Purdue University**
Spring 2012	Outstanding Teaching Assistant Award	**Seoul National University**
Sep. 2010 – Dec. 2013	Brain Korea 21 Scholarship	**National Research Foundation of Korea**
Mar. 2005 – Feb. 2010	Presidential Science Scholarship	**Korea Student Aid Foundation**

(Selected) Mathematical Olympiad Awards in High School

2004	Bronze Medal	**17th Korean Mathematical Olympiad 2nd Round, Korean Mathematical Society**
2003	Gold Medal	**15th Mathematical Olympiad, Gangwon-Do, Korean Mathematical Society**
2003	Gold Medal	**Mathematical Olympiad, Inha University**
2003	Gold Medal	**Mathematical Olympiad, Korea University**
2003	Gold Medal	**Mathematical Olympiad, Sungkyunkwan University**
2003	Bronze Medal	**Mathematical Olympiad, Chungnam University**
2003	Bronze Medal	**17th Korean Mathematical Olympiad, Korean Mathematical Society**

REFERENCES

Jeremiah Blocki
Associate Professor, Purdue University
@ jblocki@purdue.edu
https://www.cs.purdue.edu/homes/jblocki

Xavier Tricoche
Associate Professor, Purdue University
@ xmt@purdue.edu
https://www.cs.purdue.edu/homes/xmt/

Samson Zhou
Assistant Professor, Texas A&M University
@ samsonzhou@gmail.com
https://samsonzhou.github.io/