Last Updated: October 12, 2024

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 also have 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

2017 - 2024 **Ph.D. in Computer Science** **Purdue University**
Thesis: 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

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

2005 - 2010 **B.S. in Mathematics** **POSTECH (Pohang University of Science and Technology)**
Recipient of the Presidential Science Scholarship

PUBLICATIONS AND PREPRINTS

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

1. **Reversible Pebbling: Parallel Quantum Circuits with Low Amortized Space-Time Complexity**
   Jeremiah Blocki, Blake Holman, and Seunghoon Lee
   *In Theory of Quantum Computation, Communication and Cryptography (**TQC 2024**)*

2. **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**)*

3. **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**)*

4. **On the Multi-User Security of Short Schnorr Signatures with Preprocessing**
   Jeremiah Blocki and Seunghoon Lee
   *In Advances of Cryptology – **EUROCRYPT 2022***

5. **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**)*

6. **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**)*

7. **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**)*

8. **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***

Under Submission

9. **The Impact of Reversibility on Parallel Pebbling**
   Jeremiah Blocki, Blake Holman, and Seunghoon Lee

10. **A Tight Lower Bound on the TdScrypt Trapdoor Memory-Hard Function**
    Jeremiah Blocki and Seunghoon Lee

In Preparation

11. **Preprocessing Security in Multiple Idealized Models with Applications to Schnorr Signatures and PSEC-KEM**
    Jeremiah Blocki and Seunghoon Lee

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

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

- **Research and Education Program (Sejong Science High School)**, Research Assistant (Spring 2013, Fall 2013)
- **300.204: Differential Equations**, Teaching Assistant (Spring 2013, 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, *Outstanding TA Award* (Spring 2011, Fall 2011, Spring 2012)

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**
Oct 2019	**On the Multi-User Security of Short Schnorr Signatures**	**Purdue Weekly Lab Meeting**

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, and ESA 2024.

GRANTS AND AWARDS

Academic Grants & Awards

2023 – 2024	**Bilsland Dissertation Fellowship**	**Purdue University**
2019 – 2023	**Graduate Research Assistantship**	**Purdue University**
2017 – 2018	**Graduate Teaching Assistantship**	**Purdue University**
2012	**Outstanding Teaching Assistant Award**	**Seoul National University**
2010 – 2013	**Brain Korea 21 Scholarship**	**National Research Foundation of Korea**
2005 – 2009	**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**

WORK EXPERIENCE

2024 –	**Postdoctoral Researcher**	**Purdue University**
2013 – 2016	**Senior Researcher (mandatory military service)**	**Security Management Institute**
2013 – 2013	**Research Assistant**	**Seoul National University & Nextin Solutions**

REFERENCES

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

Myungjoo Kang
Professor, Seoul National University
@ mkang@snu.ac.kr
🌐 https://www.ncia.snu.ac.kr/general-5-1