Seunghoon **Lee**

Postdoctoral Researcher | Department of Computer Science, Purdue University

305 N University St., West Lafayette, IN 47907
https ://lee2856.github.io @ lee2856@purdue.edu
linkedin.com/in/seunghoon-lee-7673b1146

Research Interest

My research interest lies in cryptography and relevant theoretical problems. In particular, I have been fascinated by exploring the intersection of graph theory and cryptography, focusing on the classical and post-quantum security analysis of Memory-Hard Functions and Proofs of Sequential Work. In particular, I have worked on analyzing the (amortized) space-time cost of a quantum circuit that evaluates a data-independent Memory-Hard Function via the parallel reversible pebbling game, which is a useful metric for understanding the memory hardness of a data-independent Memory-Hard Function against quantum pre-image attacks. I have further studied the impact of the reversibility constraints on the parallel pebbling game. I am also drawn to analyzing the preprocessing security of cryptographic primitives in multiple idealized models, including short Schnorr signatures and Key Encapsulation Mechanisms.

Current Position

May 2024 – **Postdoctoral Researcher, Purdue University**
Department of Computer Science
Host : Jeremiah Blocki

Education

August 2017 – May 2024 **Ph.D., Purdue University**
Department of Computer Science
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

March 2013 – December 2013 **Ph.D. Student, Seoul National University**
Department of Mathematical Sciences
Left due to the mandatory military service

September 2010 – February 2013 **M.Sc., Seoul National University**
Department of Mathematical Sciences
Thesis : *Reinitializing Techniques in Level Set Method*
Advisor : Myungjoo Kang

March 2005 – February 2010 **B.Sc., POSTECH (Pohang University of Science and Technology)**
Department of Mathematics
Graduated magna cum laude, Recipient of the Presidential Science Scholarship

Publications and Preprints

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

1. Jeremiah Blocki, Seunghoon Lee, Tamalika Mukherjee, and Samson Zhou, *Differentially Private L_2-Heavy Hitters in the Sliding Window Model*. In The Eleventh International Conference on Learning Representations (**ICLR 2023**).
2. Jeremiah Blocki, Blake Holman, and Seunghoon Lee, *The Parallel Reversible Pebbling Game : Analyzing the Post-Quantum Security of iMHFs.* In Theory of Cryptography Conference (**TCC 2022**), Part I, volume 13747 of LNCS, pp. 52-79. Springer, Heidelberg, November 2022.
3. Jeremiah Blocki and Seunghoon Lee, *On the Multi-User Security of Short Schnorr Signatures with Preprocessing.* In Advances of Cryptology – **EUROCRYPT 2022**, Part II, volume 13276 of Lecture Notes in Computer Science, pp. 614-643. Springer, Heidelberg. May/June 2022.
4. Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, and Jin Young Son, *On Explicit Constructions of Extremely Depth Robust Graphs.* In 39th International Symposium on Theoretical Aspects of Computer Science (**STACS 2022**). Leibniz International Proceedings in Informatics (LIPIcs), Volume 219, pp. 14 :1-14 :11, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2022).
5. Jeremiah Blocki, Seunghoon Lee, and Samson Zhou, *On the Security of Proofs of Sequential Work in a Post-Quantum World.* In 2nd Conference on Information-Theoretic Cryptography (**ITC 2021**). Leibniz International Proceedings in Informatics (LIPIcs), Volume 199, pp. 22 :1-22 :27, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2021).

6. Jeremiah Blocki, Seunghoon Lee, and Samson Zhou, *Approximating Cumulative Pebbling Cost is Unique Games Hard.* In 11th Innovations in Theoretical Computer Science Conference (**ITCS 2020**). Leibniz International Proceedings in Informatics (LIPIcs), Volume 151, pp. 13 :1-13 :27, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2020).
7. Jeremiah Blocki, Benjamin Harsha, Siteng Kang, Seunghoon Lee, Lu Xing, and Samson Zhou, *Data-Independent Memory Hard Functions : New Attacks and Stronger Constructions.* In Advances of Cryptology – **CRYPTO 2019** – 39th Annual International Cryptology Conference, Proceedings, Part II, pp. 573-607. 2019.

Under Submission

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

In Preparation

9. Jeremiah Blocki and Seunghoon Lee, *Preprocessing Security in Multiple Idealized Models with Applications to Schnorr Signatures and PSEC-KEM*
10. Jeremiah Blocki, Jong Chan Lee, Seunghoon Lee, Peiyuan Liu, and Ling Ren, *Sparse Depth-Robust Graphs with Improved Lower Bounds*

Manuscript

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

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

November 2022	**The Parallel Reversible Pebbling Game : Analyzing the Post-Quantum Security of iMHFs**	TCC 2022
March 2022	**On Explicit Constructions of Extremely Depth Robust Graphs**	STACS 2022
July 2021	**On the Security of Proofs of Sequential Work in a Post-Quantum World**	ITC 2021
January 2020	**Approximating Cumulative Pebbling Cost is Unique Games Hard**	ITCS 2020
November 2019	**Approximating Cumulative Pebbling Cost is Unique Games Hard**	Purdue Crypto Reading Group
October 2019	**On the Multi-User Security of Short Schnorr Signatures**	Purdue Weekly Lab Meeting
June 2019	**Approximating Cumulative Pebbling Cost is Unique Games Hard**	Purdue Weekly Lab Meeting

Posters

March 2022	**On the Multi-User Security of Short Schnorr Signatures with Preprocessing**	CERIAS Symposium 2022
January 2020	**Approximating Cumulative Pebbling Cost is Unique Games Hard**	ITCS 2020
April 2019	**On the Security of Short Schnorr Signatures**	Midwest Security Workshop 7
April 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, and ITC 2024.

Grants & 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**, Mathematics in Civilization	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

Extracurricular Awards

2013	**Silver Medal**, Dormitory Table Tennis Competition - Men's Double	Seoul National University
2013	**Silver Medal**, Table Tennis Competition (Dept. of Math) - Men's Single	Seoul National University
2009	**Gold Prize**, Video Contents Contest in Educational Development Center	POSTECH

Work Experience

December 2016 – December 2013 — **Senior Researcher (mandatory military service), Security Management Institute, Republic of Korea**

- Worked as Research Assistant to improve an algorithm about distinguishing technical data in relation to the National Defense Standard (NDS.)
- Participated 17 research projects on national defense policies.
- Used data analysis to assess TRL impact on development schedule and cost in the aerospace project.

National Defense Standard | Data Analysis | Defense Policies | Mandatory Military Service

July 2013 – March 2013 — **Research Assistant, Seoul National University & Nextin Solutions, Republic of Korea**

- Assisted a project which aimed to improve an yield-rate of OLEDs by detecting possible types of false defects such as short fail, open fail, and line fail, etc.
- Detected defects by analyzing the voltage of storage caps in the inner circuits of OLED panels.
- Used ℓ_1-norm, Gaussian fitting, or finding Wavelet coefficient to accurately categorize the defections.

Numerical Analysis | Finite Difference Method

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