

Seunghoon LEE

Ph.D. Student, Graduate Research Assistant | Department of Computer Science, Purdue University

 [linkedin.com/in/seunghoon-lee-7673b1146](https://www.linkedin.com/in/seunghoon-lee-7673b1146)  www.cs.purdue.edu/homes/lee2856

 +1 765-413-6467  lee2856@purdue.edu  live :opt.s.lee

 LWSN 2161, 305 N University St., West Lafayette, IN 47907

RESEARCH INTEREST

My research interest lies in cryptography and relevant theoretical problems, especially in graph-theoretical aspects. In particular, I am drawn to analyzing the classical and post-quantum security of data-independent Memory-Hard Functions (iMHFs) and Proofs of Sequential Work. My recent work includes achieving better security bounds of Proofs of Sequential Work in the parallel quantum random oracle model and developing parallel reversible pebbling strategies to analyze the post-quantum security of iMHFs.

EDUCATION

- | | |
|----------------|--|
| 2017 - present | Ph.D. Student, Purdue University Department of Computer Science Advisor : Jeremiah Blocki |
| 2013 | Ph.D. Student, Seoul National University Department of Mathematical Sciences Left due to the mandatory military service |
| 2010 - 2012 | M.Sc., Seoul National University Department of Mathematical Sciences Thesis : <i>Reinitializing Techniques in Level Set Method</i> Advisor : Myungjoo Kang |
| 2005 - 2009 | 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 (Reverse Chronological Order)

1. Blocki, J., **Lee, S.**, Mukherjee, T., Zhou, S. Differentially Private L_2 -Heavy Hitters in the Sliding Window Model. **ICLR 2023.**
2. Blocki, J., Holman, B., **Lee, S.** The Parallel Reversible Pebbling Game : Analyzing the Post-Quantum Security of iMHFs. **TCC 2022.**
3. Blocki, J., **Lee, S.** On the Multi-User Security of Short Schnorr Signatures with Preprocessing. **EUROCRYPT 2022.**
4. Blocki, J., Cinkoske, M., **Lee, S.**, Son, J. On Explicit Constructions of Extremely Depth Robust Graphs. **STACS 2022.**
5. Blocki, J., **Lee, S.**, Zhou, S. On the Security of Proofs of Sequential Work in a Post-Quantum World. **ITC 2021.**
6. Blocki, J., **Lee, S.**, Zhou, S. (2019) Approximating Cumulative Pebbling Cost is Unique Games Hard. **ITCS 2020.**
7. Blocki, J., Harsha, B., Kang, S., **Lee, S.**, Xing, L., Zhou, S. (2019) Data-Independent Memory Hard Functions : New Attacks and Stronger Constructions. **CRYPTO 2019.**

Manuscript

1. **Lee, S.** A Short Note on Improved Logic Circuits in a Hexagonal Minesweeper.

WORK EXPERIENCE

- | | |
|---------------|--|
| December 2016 | Senior Researcher (mandatory military service), SECURITY MANAGEMENT INSTITUTE, Republic of Korea |
| December 2013 | <ul style="list-style-type: none">➢ 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.➢ Research Assistant for defense industry projects, including proposal and award policies and procedures guide in national defense. <div>National Defense Standard Data Analysis Defense Policies Mandatory Military Service</div> |

| | |
|------------|---|
| July 2013 | Research Assistant, SEOUL NATIONAL UNIVERSITY & NEXTIN SOLUTIONS, Republic of Korea |
| March 2013 | <ul style="list-style-type: none"> > 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. > Joint project by Seoul National University and Nextin Solutions. |
| | Numerical Analysis Finite Difference Method |

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

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 |

GRANTS & AWARDS

Academic Grants & Awards

| | | |
|----------------|---|---------------------------------------|
| 2019 - present | 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 |

LANGUAGES

Korean ●●●●●
English ●●●●○

TECHNICAL EXPERTISE

- > C/C++, JAVA, Python
- > Julia, MATLAB
- > \LaTeX

REFERENCES

Jeremiah Blocki

Assistant Professor, PURDUE UNIVERSITY

@ jblocki@purdue.edu
🌐 <https://www.cs.purdue.edu/homes/jblocki>

Myungjoo Kang

Professor, SEOUL NATIONAL UNIVERSITY

@ mkang@snu.ac.kr
🌐 <http://ncia.snu.ac.kr/xs/PROFESSOR>