Jiwon Kim

Ph.D. candidate in Computer Science and Engineering
jiwonkp@umich.edu | https://jiwonkim-park.github.io

Fourth-year Ph.D. candidate in CSE at the University of Michigan, specializing in **applied cryptography**. My research focuses on building efficient privacy-preserving verification systems with **zero-knowledge proofs (ZKPs)**. I solve subtle challenges that arise when attempting to ensure privacy, integrity, and efficiency together and design cryptographic primitives that improve both security guarantees and practicality.

Education

University of Michigan ..... Ann Arbor, MI
Ph.D. in Computer Science and Engineering ..... Aug. 2023 – Present
Advisor: Paul Grubbs

Seoul National University (SNU) ..... Seoul, South Korea
B.S. in Computer Science and Engineering ..... Mar. 2014 – Feb. 2020
B.A. in History Education

Publications and Preprints

[1] **Centaur: A Flexible and Efficient Stateful Anonymous Moderation System**
Jiwon Kim, Abhiram Kothapalli, Paul Grubbs, Ian Miers, Riad Wahby
In submission

[2] **Haechi: Simple Commitment-based Keyless In-person Verifiable Elections**
Jiwon Kim, Michael Naehrig, Bharath Namboothiry, Olivier Pereira, Josh Benaloh
In submission

[3] **ALPACA: Anonymous Blocklisting with Constant-sized Updatable Proofs**
Jiwon Kim, Abhiram Kothapalli, Orestis Chardouvelis, Riad S. Wahby, Paul Grubbs
IEEE S&P 2025: IEEE Symposium on Security and Privacy

Professional Experience

Aug. 2023 – May. 2028 (Expected)

University of Michigan **Ann Arbor, MI**
Graduate Student Research Assistant

- Built two anonymous moderation systems with Rust that can moderate user behavior while preserving user privacy.
- Built ALPACA by designing an unlinkable variant of Incrementally Verifiable Computation (IVC) and using Spartan zkSNARK, achieving O(1) proofs and constant verifier time. [3]
- Built Centaur that provides optimal prover time across usage patterns using non-uniform IVC; achieved a 630× speedup on the median Wikipedia workload. [1]
- Formalized security games; proved security with non-trivial game hops and reductions.

Summers 2025 and 2026

Microsoft Research **Redmond, WA**
Research Intern, Cryptography Group
Mentor: Josh Benaloh (2025-2026) and Michael Naehrig (2025)

- Designed a new keyless verifiable election scheme and the underlying zero-knolwedge proof scheme; reduced the bulletin board size from 120GB in SOTA (Microsoft ElectionGuard) to 576MB for 1 million voters and 100 candidates. [2]
- Extended the scheme to provide post-quantum integrity using BDLOP commitments and (d)-ary bootstrapping for commitment aggregation.
- Designed a new verifiable ranked-choice voting, reducing communication complexity from $O(n^3)$ in SOTA to $O(n \log n)$.

May. 2021 – Jul. 2023	**Kakao Corp.**	**Seongnam, Korea**
	Software Engineer, Wallet Service Development Team	
	Kakao offers Kakaotalk, a Korea-based messenger app with 97% market share.	
	• Designed and implemented a new platform to securely issue, store, and present users' identity information, including a prototype of anonymous credential.	
Jan. 2020 – Apr. 2021	**Samsung SDS**	**Seoul, Korea**
	Researcher, Blockchain Research Lab	
	• Invented a cryptographic scheme for blockchain that shares actual files only with the owners and stores metadata to the distributed ledger [P3].	
	• Modeled a real-time private blockchain banking system and improved the TPS by 33% through a batch processor and a database connection resource scheduler [P1].	
Jun. 2019 – Dec. 2019	Student Researcher, Blockchain Research Lab	
	• Surveyed blockchain consensus algorithms and proposed an evaluation standard that helps determine appropriate consensus algorithms for specific purposes.	

Honors and Awards

May 2025	**Recognition for Exceptional Prelim Exams** Computer Science & Engineering, University of Michigan - Received "High Pass" by advisor and all examiners.
2023 – 2025	**Korean Government Scholarship Program** (USD $80K) Ministry of Education, Republic of Korea
Fall 2019	**Research Student Scholarship** (USD $4K) Samsung SDS
2017 – 2019	**Samsung Convergence Software Course** (USD $700) Samsung Electronics
2015 – 2017	**Merit-based Scholarship** (Total USD $9K) Seoul National University - Spring 2015, Fall 2016, Spring 2017

Invited Talks

	Haechi: Simple Commitment-based Keyless In-person Verifiable Elections
Jul. 2026	Microsoft Research, Cryptography Talk Series
	ALPACA: Anonymous Blocklisting with Constant-sized Updatable Proofs
Oct. 2025	UC Berkeley, Security Seminar
Sep. 2025	University of Maryland, Cryptography Seminar
	Proven Approaches to Privacy, Confidentiality, and Security in Distributed Ledger Technologies
Sep. 2020	Hyperledger Member Summit

Patents

[P1] S. Lee, Y. Heo, **Jiwon Kim**, J. Lee, "Method and Apparatus for Transaction in Blockchain Environment," Korea Patent 10-2022-0160299.

[P2] J. Lee, J. Kim, **Jiwon Kim**, S. Lee, K. Lee, "Distributed Data Management Method Based on Blockchain Network and Apparatus Therefor," Korea Patent 10-2020-0093717.

[P3] S. Bae, **Jiwon Kim**, S. Kang, H. Seo, "Off-chain Data Sharing System and Method Thereof," Korea Patent 10-2020-0059823.

Skills

Programming Languages
Rust, Go, Java, Kotlin, Python, C, C++

ZKP programming
ZoKrates, CirC compiler, bellman/bellpepper gadget

Database & DevOps
MySQL, MongoDB, Redis, Kubernetes, Docker, Jenkins

Research and interpersonal skills
Clear communication, teamwork, collaborative research, active listening, technical writing and speaking, conflict resolution