

Sunpill Kim

Curriculum Vitae

📍 Seoul, South Korea | 📩 ksp0352@gmail.com | 🌐 https://sunpillkim.com | 🎓 Google Scholar | 📞 (+82) 10-9559-6016

RESEARCH FOCUS

My research focuses on the security and vulnerability analysis of metric-learning-based recognition systems, including biometric and vision-language models. My work spans adversarial attacks, biometric template protection, and related detection tasks, with an emphasis on both theoretical foundations and practical deployment.

EDUCATION

Hanyang University, Seoul, South Korea

- Ph.D. in Mathematics (Applied Mathematics) Mar 2020 - Feb 2026
 - Thesis: Score-Based Non-Adaptive Attack Against Face Recognition Systems
 - Advisor: Jae Hong Seo
- B.S. in Mathematics Mar 2015 - Feb 2020

WORK EXPERIENCES

Institute for Infocomm Research (I²R), A*STAR, Singapore

- Ph.D. Student Researcher (ARAP Scholar), Cybersecurity Department Jan 2023 - Jan 2024
- Advisors: Dr. Khin Mi Mi Aung and Dr. Yong Kiam Tan

PUBLICATIONS

†: Equally contributed.

CONFERENCES

- [C8] “Non-Adaptive Adversarial Face Generation”
Sunpill Kim, Seunghun Paik, Chanwoo Hwang, Minsu Kim, Jae Hong Seo
NeurIPS 2025 (acceptance rate: 24.5%)
- [C7] “IDFace: Efficient and Secure Identification for Face Images”
Sunpill Kim†, Seunghun Paik†, Chanwoo Hwang, Dongsu Kim, Junbum Shin, Jae Hong Seo
ICCV 2025 (acceptance rate: 24.0%)
- [C6] “A Survey of Model Inversion Attacks on Image Domain”
Changjin Kim, Chanwoo Hwang, Sunpill Kim, Jae Hong Seo
IEEE ICTC 2025
- [C5] “Towards Certifiably Robust Face Recognition”
Seunghun Paik, Dongsu Kim, Chanwoo Hwang, Sunpill Kim, Jae Hong Seo
ECCV 2024
- [C4] “On the Certifiable Robustness of Face Recognition Systems”
Seunghun Paik, Dongsu Kim, Chanwoo Hwang, Sunpill Kim, Jae Hong Seo
CISC-S 2024 (South Korea)
- [C3] “Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems”
Sunpill Kim, Yong Kiam Tan, Bora Jeong, Soumik Mondal, Khin Mi Mi Aung, Jae Hong Seo
IEEE S&P 2024 (acceptance rate: 17.8%)
- [C2] “Security Analysis on Locality-Sensitive Hashing-based Biometric Template Protection Schemes”
Seunghun Paik, Sunpill Kim, Jae Hong Seo
BMVC 2023
- [C1] “IronMask: Modular Architecture for Protecting Deep Face Template”
Sunpill Kim, Yunseong Jeong, Jinsu Kim, Jungkon Kim, Hyung Tae Lee, Jae Hong Seo
CVPR 2021 (acceptance rate: 23.4%)

JOURNALS

- [J5] “Doubly Efficient Fuzzy Private Set Intersection for High-dimensional Data with Cosine Similarity”
Hyunjung Son, Seunghun Paik, Yunki Kim, Sunpill Kim, Jae Hong Seo
IEEE Access, to appear.
- [J4] “Towards Certifiably Robust Face Recognition: Analyses and Improvements”
Seunghun Paik, Dongsoo Kim, Chanwoo Hwang, Sunpill Kim, Jae Hong Seo
IEEE Transactions on Biometrics, Behavior, and Identity Science, to appear.
- [J3] “On the Reversibility of Locality-Sensitive Hashing-based Biometric Template Protections”
Seunghun Paik, Chanwoo Hwang, Sunpill Kim, Jae Hong Seo
IEEE Transactions on Dependable and Secure Computing, to appear.
- [J2] “Deep Face Template Protection in the Wild”
Sunpill Kim, Hoyong Shin, Jae Hong Seo
Pattern Recognition, 2025.
- [J1] “Analysis on Secure Triplet Loss”
Bora Jeong, Sunpill Kim, Seunghun Paik, Jae Hong Seo
IEEE Access, 2022.

OTHERS

- [O1] “Formalization of the Schwartz-Zippel Lemma”
Sunpill Kim[†] and Yong Kiam Tan[†]
Archive of Formal Proofs, 2023

HONORS & AWARDS

The 1st Graduate Presidential Science Scholarship, Korea Student Aid Foundation	2024 - 2026
– Sole recipient in Mathematics Ph.D. program; full living support (\$24K/year).	
Best Award, Best Research Paper Award 2024, The Research Institute for Natural Sciences, Hanyang University	2025
A*STAR Research Attachment (ARAP), Agency for Science, Technology and Research, Singapore	2023 - 2024
– Fully funded research attachment (~S\$47K).	
Excellence Award, National Cryptographic Technology Contest.	2023
The Samil Scholarship, The Samil Foundation.	2022 - 2023

RESEARCH PROJECT

Secure Authentication System using Deep Learning-based Biometric Recognition System, NRF (PI)	2024 - 2025
Computer-Aided Cryptography for Zero-Knowledge Proofs and Verifiable Computing, A*STAR (Participant)	2023 - 2024

PATENT

- [P4] Similarity-Private Set Intersection Protocol Using Cosine Similarity-based Similarity Measurement between High-dimensional Data
Jae Hong Seo, Hyeonjeong Son, Seunghun Paik, Yunki Kim, Sunpill Kim, Dongwoo Kim, Heewon Chung
KOR 10-2025-0200142
- [P3] Protocol System for Real-valued Error Correcting Code using Commutative Algebraic Structure over Hypersphere
Jae Hong Seo, Sunpill Kim, Sangyun Shin, Sungae Baik, Minsu Kim, Seunghun Paik
KOR 10-2025-0008685
- [P2] Server and method for identifying target user thereof
Sunpill Kim, Seunghun Paik, Chanwoo Hwang, Dongsu Kim, Jae Hong Seo, Junbum Shin, Jung Woo Kim
KOR 10-2024-0031957 and USPTO 18/598,233 (12,476,815)
- [P1] Protocol System for Real-valued Error Correcting Code over Hypersphere
Jae Hong Seo, Sunpill Kim, Sangyun Shin, Sungae Baik, Minsu Kim, Seunghun Paik
KOR 10-2023-0178374

PROFESSIONAL SERVICES

REVIEWER

Journals: IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing
Conferences: CVPR 2026, CVPR 2025, BMVC 2024, CVPR 2024, PKC 2023, ASIACRYPT 2021, ProvSec 2020

TEACHING EXPERIENCE

Hanyang University, Seoul, South Korea

- Part-time Lecturer, Mathematical Algorithms
- Teaching Assistant, Number Theory; Capstone PBL

Spring 2025

2020 - 2021

INVITED TALKS

Hanyang University, Department of Mathematics
“Non-Adaptive Adversarial Face Generation”

Oct 2025

Hanyang University, Department of Mathematics
“Are Deep-Learning Based Face Recognition Systems Secure?”

May 2025

Desilo Inc. (Industry Talk)
“Biometric Information Extraction Threats and Countermeasures in Deep Learning-based Face Recognition System”

Dec 2022

Korean Artificial Intelligence Association & LG AI Research
“IronMask: Modular Architecture for Protecting Deep Face Template”

Nov 2021