

CONTACT INFORMATION Room 707, Natural Science Building, Hanyang University, 222, Wangsimni-ro, Tel: +82 10-9559-6016

Homepage: <https://sunpillkim.com>  
 Linkedin: <https://www.linkedin.com/in/sunpillkim>  
 ✉ E-mail: [ksp0352@gmail.com](mailto:ksp0352@gmail.com)

RESEARCH BACKGROUND

- **AI Security:** Biometric Template Protection, Adversarial Attack.
- **Deep Learning:** Recognition System, Model Inversion, Knowledge Distillation.
- **Cryptography:** Private Set Operation, Zero-Knowledge Proofs, Homomorphic Encryption.

EDUCATION

**Hanyang University**, Seoul Mar 2020 - Aug 2025 (Expected)

- Ph.D. Department of Mathematics, GPA: **3.94/4** – via 52 credits.
- Advisor: Prof. [Jae Hong Seo](#).

**Hanyang University**, Seoul Mar 2015 - Feb 2020

- B.S. Department of Mathematics, GPA (Major): **3.53/4 (3.63/4)** – via 130 credits.
- Thesis: *Fuzzy Extractor for Face Recognition*.

PUBLICATIONS †: Equally contributed.

#### Conference

5. Seunghun Paik, Dongsu Kim, Chanwoo Hwang, **Sunpill Kim**, and Jae Hong Seo, Towards Certifiably Robust Face Recognition, *The 18th European Conference on Computer Vision (ECCV)*, 2024. (**A\*-tier** according to [CORE](#), acceptance rate: 27.9%)
4. Seunghun Paik, Dongsu Kim, Chanwoo Hwang, **Sunpill Kim**, and Jae Hong Seo, On the Certifiable Robustness of Face Recognition Systems, *Conference on Information Security and Cryptography Summer (CISC-S)*, 2024.
3. **Sunpill Kim**, Yong Kiam Tan, Bora Jeong, Soumik Mondal, Khin Mi Mi Aung, and Jae Hong Seo, Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems, *IEEE Symposium on Security and Privacy (S&P)*, 2024. (**A\*-tier** according to [CORE](#), acceptance rate: 17.8%)
2. Seunghun Paik, **Sunpill Kim**, and Jae Hong Seo, Security Analysis on Locality-Sensitive Hashing-based Biometric Template Protection Schemes, *34<sup>th</sup> British Machine Vision Conference (BMVC)*, 2023. (**A-tier** according to [CORE](#), **oral**, acceptance rate: 9%)
1. **Sunpill Kim**, Yunseong Jeong, Jinsu Kim, Jungkon Kim, Hyung Tae Lee, and Jae Hong Seo, IronMask: Modular Architecture for Protecting Deep Face Template, *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021. (**A\*-tier** according to [CORE](#), acceptance rate: 23.4%)

#### Journal

2. **Sunpill Kim**, Hoyong Shin, and Jae Hong Seo, Deep Face Template Protection in the Wild, *Pattern Recognition*, 162, 111336, 2025. (IF: 7.5)
1. Bora Jeong, **Sunpill Kim**, Seunghun Paik, and Jae Hong Seo, Analysis on Secure Triplet Loss, *IEEE Access*, 10, 124355-124362, 2022. (IF: 5.113)

#### Manuscripts

7. Hyunjung Son, Seunghun Paik, Yunki Kim, **Sunpill Kim**, Heewon Chung, and Jae Hong Seo, Doubly Efficient Fuzzy Private Set Intersection for High-dimensional Data with Cosine Similarity, (under Review)
6. **Sunpill Kim**, Seunghun Paik, Chanwoo Hwang, Minsu Kim, and Jae Hong Seo, Non-Adaptive Adversarial Face Generation in the Dark, (under review)
5. Seunghun Paik, Minsu Kim, **Sunpill Kim**, and Jae Hong Seo, On the Security-Accuracy Trade-off of Hash-based Face Template Protections, (under review)

4. Minsu Kim<sup>†</sup>, Seunghun Paik<sup>†</sup>, Seongae Baek, Sangyoon Shin, **Sunpill Kim**, and Jae Hong Seo, SilverMask: Face Template Protection with Fine-Grained Noise-Correction, (under review)
3. Seunghun Paik, Chanwoo Hwang, **Sunpill Kim**, and Jae Hong Seo, Locality-Sensitive Hashing-based Biometric Template Protection Schemes are fully Reversible!, (under review)
2. **Sunpill Kim**<sup>†</sup>, Seunghun Paik<sup>†</sup>, Chanwoo Hwang, Dongsu Kim, and Jae Hong Seo, IDFace: Efficient and Secure Identification for Face Images, (under review)
1. **Sunpill Kim**<sup>†</sup> and Yong Kiam Tan<sup>†</sup>, Formalization of the Schwartz-Zippel Lemma, *Archive of Formal Proofs*, April 2023.

## EXPERIENCE

### Work Experience

- **Ph.D. Student Researcher (ARAP Scholar)** Jan 2023 - Jan 2024  
A\*STAR Research Attachment Programme (ARAP): Computer-Aided Cryptography for Zero-Knowledge Proofs and Verifiable Computing  
Institute for Infocomm Research (I<sup>2</sup>R), A\*STAR, Singapore  
Advisor: Dr. Khin Mi Mi Aung and Dr. Yong Kiam Tan
- **Graduate Assistant Representative** Jul 2021 - Nov 2022
- **Teaching Assistant**
  - Fall 2021: Math Capstone PBL, Math Lab Internship 3
  - Fall 2020: Math Capstone PBL
  - Spring 2020: Number Theory
- **Research Intern** Jul 2018 - Feb 2020  
Development of Fuzzy Extractor Based on Real Numbers  
Cryptology & Algorithm Laboratory
  - Fuzzy Extractor (FE) is a cryptographic primitive that generates the same output for the input with a slight noise coming from the fuzziness of input. Typical Fuzzy data include biometric information such as a face, fingerprint, and iris. We develop FE based on real number and apply to ArcFace, which is a state-of-the-art face recognition algorithm.

### Others

- **Academic Seminar** Apr 2019 - Nov 2019  
“Security of Biometric Authentication”  
College of Natural Science, Hanyang University
  - We investigate the security of the face recognition system (FRS) in terms of cryptography. Using MXNet based DCGAN and improved NbNet, it succeeded in restoring the image from the template of ArcFace, proving that the current state-of-the-art FRS is unsafe.
- **Summer/Winter Schools**
  - Summer School on Cryptography 2018, 2019\*  
National Institute for Mathematical Sciences, Korean Mathematical Society\*
- **Coursera Certificate**
  - Getting Started with AWS Machine Learning (Amazon Web Services) Feb 2022
  - Convolutional Neural Networks (DeepLearning.AI) Jun 2019
  - Improving Deep Neural Networks (DeepLearning.AI) May 2019
  - Structuring Machine Learning Projects (DeepLearning.AI) May 2019
  - Neural Networks and Deep Learning (DeepLearning.AI) May 2019
  - Machine Learning (Stanford University) Mar 2019

## RESEARCH PROJECTS

### AI Security

- Secure Authentication System using Deep Learning-based Biometric Recognition System  
PI: **Sunpill Kim**, Total amount: ≈\$25,000  
Supported by National Research Foundation of Korea (NRF), Sep 2024 - Aug 2025.
- International Joint Research to Develop Next-generation Copyright Infringement Prevention Technology and Safe Content Distribution Technology  
Supported by Korea Creative Content Agency (KOCCA), Apr 2024 - Dec 2027.

- Development of Encrypted Face Template DB Search Technology  
Supported by CRYPTOLAB, July 2022 - June 2023.
- Research on Biometric Information Extraction Threats and Protection Methods in Deep Learning-based Face Recognition  
Supported by Korea Institute of Information Security & Cryptology (KIISC), Mar 2022 - Nov 2022.
- Development of Fuzzy Extractor Based on Real Numbers  
Supported by Samsung Electronics, Dec 2018 - Dec 2019.

#### Zero-Knowledge Proofs & Verifiable Computing

- Computer-Aided Cryptography for Zero-Knowledge Proofs and Verifiable Computing  
Supported by Agency for Science, Technology and Research (A\*STAR), Jan 2023 - Jan 2024.
- A Study on Cryptographic Primitives for SNARK  
Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP), Apr 2021 - Dec 2026.
- Research on Incrementally Verifiable Computation Design Technique and Application Method  
Supported by National Security Research Institute (NSR), Apr 2021 - Oct 2021.
- Research on Post-Quantum Non-Interactive Zero-Knowledge Proofs  
Supported by National Research Foundation of Korea (NRF), Mar 2020 - Feb 2025.
- Research on Post-Quantum Zero-Knowledge Proofs Design Technique and Application Method  
Supported by National Security Research Institute (NSR), Apr 2020 - Oct 2020.
- Research on Lattice-Based Zero-Knowledge Proofs Design Technique  
Supported by National Security Research Institute (NSR), May 2019 - Oct 2020.

#### Others

- Secure Multi-party Approximate Computation  
Supported by Samsung Science & Technology Foundation, Sep 2021 - Aug 2024.
- A Study of Functional Encryption and Its Core Techniques  
Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) & National Research Foundation of Korea (NRF), Aug 2018 - Jul 2021.
- Cryptographic Properties of Lattices  
Supported by National Research Foundation of Korea (NRF), Jul 2018 - Feb 2020.

#### TECHNICAL SKILLS

- *Programming Languages:* Python, Pytorch.
- *Technical Softwares:* MATLAB, L<sup>A</sup>T<sub>E</sub>X.

#### TALKS & PRE-SENTATIONS

##### Conference

- Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems  
Korean Mathematical Society Spring Meeting, Daejeon April, 2024  
45th IEEE Symposium on Security and Privacy, San Francisco May, 2024
- Deep Face Template Protection in the Wild  
Korean Mathematical Society Spring Meeting, Virtual April, 2022
- IronMask: Modular Architecture for Protecting Deep Face Template  
CVPR 2021, Virtual June, 2021

#### Invited Talks

- Hanyang University May, 2024  
Mathematics Colloquium (Department of Mathematics)  
“Is Deep-Learning Based Face Recognition System Secure?”
- Desilo December, 2022  
“Biometric Information Extraction Threats and Countermeasures in Deep Learning-based Face Recognition System”
- Korean Artificial Intelligence Association & LG AI Research November, 2021  
Outstanding International Conference Paper Session  
“IronMask: Modular Architecture for Protecting Deep Face Template”

## PATENTS

1. Server and method for identifying target user thereof (submitted to USPTO, provisional patent application no.: 18/598,233)  
Hanyang Univ.: Sunpill Kim, Seunghun Paik, Chanwoo Hwang, Dongsu Kim and Jae Hong Seo  
CRYPTOLAB Inc.: Junbum Shin and JungWoo Kim
2. Protocol System for Real-valued Error Correcting Code over Hypersphere (submitted to Korean Patent Office, 10-2023-0178374)  
Hanyang Univ.: Jae Hong Seo, Sunpill Kim, Sangyun Shin, Sungae Baik, and Seunghun Paik

## HONORS & AWARDS

### Awards

- *Encouragement Award*, 18<sup>th</sup> National Cryptographic Technology Contest. Oct 2024  
National Intelligence Service, Republic of Korea  
“On the Security-Accuracy Trade-off of Hash-based Face Template Protections”  
\$1500
- *Outstanding Paper Award*, CISC-S’2024 Jun 2024  
National Security Research Institute, Republic of Korea  
“On the Certifiable Robustness of Face Recognition Systems”
- *Excellence Award*, 17<sup>th</sup> National Cryptographic Technology Contest. Oct 2023  
National Intelligence Service, Republic of Korea  
“IDFace: Efficient and Secure Identification for Face Images”  
\$2000
- *Encouragement Award*, 17<sup>th</sup> National Cryptographic Technology Contest. Oct 2023  
National Intelligence Service, Republic of Korea  
“Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems”  
\$1500
- *Special Award*, 16<sup>th</sup> National Cryptographic Technology Contest. Oct 2022  
National Intelligence Service, Republic of Korea  
“Deep Face Template Protection in the Wild”  
\$500
- *CUM LAUDE*, Graduate Honors. Feb 2020  
Hanyang University
- *Excellence Award*, Academic Seminar. Nov 2019  
College of Natural Science, Hanyang University  
“Security of Biometric Authentication”  
\$300
- *Dean’s list* 2018 (Spring, Fall), 2019 (Spring)  
Hanyang University

### Scholarships

- **The 1st Graduate Presidential Science Scholarship** Mar 2024 - Present  
(Ph.D. student in the Department of Mathematics, 2 finalists selected)  
Korea Student Aid Foundation  
≈\$24000/year
- **A\*STAR Research Attachment Programme (ARAP)** Jan 2023 - Jan 2024  
Agency for Science, Technology and Research (A\*STAR), Singapore  
S\$47000
- The Samil Scholarship Mar 2022 - Feb 2023  
The Samil Foundation
- Teaching Assistant Scholarship Mar 2021 - Feb 2023  
Hanyang University
- HY-IN Scholarship Mar 2020 - Feb 2023  
Hanyang University  
Half Tuition for 3 years (≈\$6000/year)

- Hyung Namjin Scholarship  
Hyung Namjin Scholarship Foundation  
Mar 2019 - Feb 2020
- Woon Scholarship  
Woon Scholarship Foundation  
Sep 2018 - Aug 2019
- CSAT Scholarship  
Hanyang University  
Half Tuition for 4 years ( $\approx$ \$4000/year)  
Mar 2015 - Feb 2020

#### SERVICES

##### **Reviewer / External Reviewer**

- IEEE Transactions on Information Forensics and Security (TIFS)
- CVPR 2025; BMVC 2024, CVPR 2024; PKC 2023; ASIACRYPT 2021; ProvSec 2020

#### REFERENCE

##### **Academia**

- Prof. Jae Hong Seo  
Professor, Department of Mathematics, Hanyang University, Seoul, Korea  
✉ E-mail: [jaehongseo@hanyang.ac.kr](mailto:jaehongseo@hanyang.ac.kr)
- Dr. Khin Mi Mi Aung  
Senior Principal Scientist, Cybersecurity Department, Institute for Infocomm Research (I2R), A\*STAR, Singapore  
✉ E-mail: [mi\\_mi\\_aung@i2r.a-star.edu.sg](mailto:mi_mi_aung@i2r.a-star.edu.sg)

##### **Industry**

- Dr. Heewon Chung  
Cryptography Researcher, Research Team, Desilo Inc., Seoul, Korea  
✉ E-mail: [heewon.chung@desilo.ai](mailto:heewon.chung@desilo.ai)