Sunpill Kim **Last update: September 14, 2023**

CONTACT INFORMATION

1 Fusionopolis Way, #10-36,
Connexis South Tower, Singapore, 138632
Tel: +82 10-9559-6016

Homepage: https://sunpillkim.com
Linkedin: https://www.linkedin.com/in/sunpillkim
✉ E-mail: ksp0352@gmail.com

RESEARCH BACKGROUND

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

EDUCATION

Hanyang University, Seoul Mar 2020 - Present

- 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.*

RESEARCH PROJECTS

Deep Learning based Biometric

- **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, Researcher, Sep 2021 - Dec 2022.
- **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.

Publications

†: Equally contributed.

Conference

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%)
2. Seunghun Paik, **Sunpill Kim**, and Jae Hong Seo, Security Analysis on Locality-Sensitive Hashing-based Biometric Template Protection Schemes, *34rd British Machine Vision Conference (BMVC)*, 2023. (**A-tier** according to CORE, **oral**, acceptance rate: TBD)

Journal

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 according to SCImago)

Manuscripts

1. **Sunpill Kim**† and Yong Kiam Tan†, Formalization of the Schwartz-Zippel Lemma, *Archive of Formal Proofs*, April 2023.
2. **Sunpill Kim**, Hoyong Shin, and Jae Hong Seo, Deep Face Template Protection in the Wild, (under review)
3. **Sunpill Kim**†, Seunghun Paik†, Chanwoo Hwang, Dongsu Kim, and Jae Hong Seo, IDFace: Efficient and Secure Identification for Face Images, (under review)
4. **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, (under review)
5. Minsu Kim†, Seunghun Paik†, Seongae Baek, Sangyoon Shin, **Sunpill Kim**, and Jae Hong Seo, SilverMask: Face Template Protection with Fine-Grained Noise-Correction, (under review)

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^2R), A*STAR, Singapore
- **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 algorithm 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

Technical Skills

- *Programming Languages*: Python, Numpy, Pytorch, MXNet.
- *Technical Softwares*: MATLAB, LaTeX.

Talks & Presentations

Conference

- **Deep Face Template Protection in the Wild** — **April, 2022**
  Korean Mathematical Society Spring Meeting, Virtual
- **IronMask: Modular Architecture for Protecting Deep Face Template** — **June, 2021**
  CVPR 2021, Virtual

Invited Talks

- **Desilo** — **December, 2022**
  "Biometric Information Extraction Threats and Countermeasures in Deep Learning-based Face Recognition System"
- **Korean Artificial Intelligence Association** — **November, 2021**
  Outstanding International Conference Paper Session
  "IronMask: Modular Architecture for Protecting Deep Face Template"

Patents

1. **Efficient and Secure Identification for Face Images** (10-2023-0030158)
   Hanyang Univ.: Sunpill Kim, Seunghun Paik, Chanwoo Hwang, Dongsu Kim and Jae Hong Seo
   CRYPTOLAB Inc.: Junbum Shin and JungWoo Kim

Honors & Awards

Awards

- ***Special Prize***, National Cryptographic Technology Contest. — Sep 2022
  National Intelligence Service, Republic of Korea
  "Deep Face Template Protection in the Wild"
  $500
- ***CUM LAUDE***, Graduate Honors. — Feb 2020
  Hanyang University
- ***Excellence Prize***, 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

- **A*STAR Research Attachment Programme (ARAP)** — Jan 2023 - Jan 2024
  Agency for Science, Technology and Research (A*STAR), Singapore
  S$43000
- **The Samil Scholarship** — Mar 2022 - Feb 2023
  The Samil Foundation
  $10000
- **Teaching Assistant Scholarship** — Mar 2021 - Feb 2023
  Hanyang University
  $6000/year

- **HY-IN Scholarship** Mar 2020 - Feb 2023
  Hanyang University
  Half Tuition for 2 years (≈$6000/year)
- **Hyung Namjin Scholarship** Mar 2019 - Feb 2020
  Hyung Namjin Scholarship Foundation
  $4000
- **Wooin Scholarship** Sep 2018 - Aug 2019
  Wooin Scholarship Foundation
  $4000
- **CSAT Scholarship** Mar 2015 - Feb 2020
  Hanyang University
  Half Tuition for 4 years (≈$4000/year)

Services

External Reviewer

- TIFS 2023, PKC 2023; ASIACRYPT 2021; ProvSec 2020