Sunpill Kim **Last update: Nov 5, 2021**

CONTACT INFORMATION

Room 736, Natural Science Building,
Hanyang University, 222, Wangsimni-ro,
Seongdong-gu, Seoul, 04763, Republic of Korea
Tel: +82 10-9559-6016

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

RESEARCH BACKGROUND

- **Cryptography**: Zero-Knowledge Proofs, Verifiable Computing.
- **Deep Learning**: Face Recognition, Deep Learning based Biometric.

EDUCATION

Hanyang University, Seoul — Mar 2020 - Present

- Ph.D. Department of Mathematics, GPA: **4/4** – via 33 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

Zero-Knowledge Proofs & Verifiable Computing

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

Deep Learning based Biometric

- **Development of Fuzzy Extractor Based on Real Numbers**
  Supported by Samsung Electronics, Research Associate, Dec 2018 - Dec 2019.

Others

- **Secure Multi-party Approximate Computation**
  Supported by Samsung Science & Technology Foundation, Researcher, 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), Researcher, Aug 2018 - Jul 2021.
- **Cryptographic Properties of Lattices**
  Supported by National Research Foundation of Korea (NRF), Research Associate, Jul 2018 - Feb 2020.

SELECTED PUBLICATIONS

1. **Sunpill Kim**, Yunseong Jeong, Jinsu Kim, Jungkon Kim, Hyung Tae Lee, and Jae Hong Seo, IronMask: Modular Architecture for Protecting Deep Face Template, In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 16125-16134, 2021. (acceptance rate 23.4%)

Experience

Work Experience

- **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 authentication system in terms of cryptography. Using MXNet based DCGAN and modified NbNet, it succeeded in restoring the image from the template of ArcFace, proving that the current face recognition system is unsafe.

- **Summer/Winter Schools**
  - Summer School on Cryptography 2018, 2019*
    National Institute for Mathematical Sciences, Korean Mathematical Society*

- **Coursera Certificate**
  - 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, Pytorch, MXNet.
- *Technical Softwares*: MATLAB, LaTeX.

Talks & Presentations

International

- IronMask: Modular Architecture for Protecting Deep Face Template
  1. 2021 KAIC Fall Meeting, Virtual, 5 Nov 2021
  2. CVPR 2021, Virtual, 25 June 2021

Honors & Awards

Awards

- ***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

- **Teaching Assistant Scholarship** Mar 2021 - Present
  Hanyang University
  $6000/year

- **HY-IN Scholarship** Mar 2020 - Present
  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)
- **Korea Student Aid Foundation's National Scholarship** Mar 2015 - Feb 2020
  Korea Student Aid Foundation
  $5000/year for 4 years

Services

External Reviewer

- ASIACRYPT 2021; ProvSec 2020