

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: <a href="https://sunpillkim.com">https://sunpillkim.com</a> Linkedin: <a href="https://www.linkedin.com/in/sunpillkim">https://www.linkedin.com/in/sunpillkim</a> ✉ E-mail: <a href="mailto:ksp0352@gmail.com">ksp0352@gmail.com</a>
RESEARCH BACKGROUND	<ul style="list-style-type: none"> <li>• <b>Cryptography:</b> Zero-Knowledge Proofs, Verifiable Computing.</li> <li>• <b>Deep Learning:</b> Face Recognition, Deep Learning based Biometric.</li> </ul>	
EDUCATION	<b>Hanyang University</b> , Seoul <ul style="list-style-type: none"> <li>• Ph.D. <b>Department of Mathematics</b>, GPA: <b>4/4</b> – via 33 credits.</li> <li>• Advisor: Prof. <b>Jae Hong Seo</b>.</li> </ul> <b>Hanyang University</b> , Seoul.	Mar 2020 - Present  Mar 2015 - Feb 2020
RESEARCH PROJECTS	<b>Zero-Knowledge Proofs &amp; Verifiable Computing</b> <ul style="list-style-type: none"> <li>• <b>A Study on Cryptographic Primitives for SNARK</b> Supported by Institute of Information &amp; Communications Technology Planning &amp; Evaluation (IITP), Research Associate, Apr 2021 - Dec 2026.</li> <li>• <b>Research on Incrementally Verifiable Computation Design Technique and Application Method</b> Supported by National Security Research Institute (NSR), Researcher, Apr 2021 - Oct 2021.</li> <li>• <b>Research on Post-Quantum Non-Interactive Zero-Knowledge Proofs</b> Supported by National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Feb 2025.</li> <li>• <b>Research on Post-Quantum Zero-Knowledge Proofs Design Technique and Application Method</b> Supported by National Security Research Institute (NSR), Researcher, Apr 2020 - Oct 2020.</li> <li>• <b>Research on Lattice-Based Zero-Knowledge Proofs Design Technique</b> Supported by National Security Research Institute (NSR), Researcher Associate, May 2019 - Oct 2020.</li> </ul> <b>Deep Learning based Biometric</b> <ul style="list-style-type: none"> <li>• <b>Development of Fuzzy Extractor Based on Real Numbers</b> Supported by Samsung Electronics, Research Associate, Dec 2018 - Dec 2019.</li> </ul> <b>Others</b> <ul style="list-style-type: none"> <li>• <b>Secure Multi-party Approximate Computation</b> Supported by Samsung Science &amp; Technology Foundation, Researcher, Sep 2021 - Aug 2024.</li> <li>• <b>A Study of Functional Encryption and Its Core Techniques</b> Supported by Institute of Information &amp; Communications Technology Planning &amp; Evaluation (IITP) &amp; National Research Foundation of Korea (NRF), Researcher, Aug 2018 - Jul 2021.</li> <li>• <b>Cryptographic Properties of Lattices</b> Supported by National Research Foundation of Korea (NRF), Research Associate, Jul 2017 - Feb 2020.</li> </ul>	
SELECTED PUBLICATIONS	<ol style="list-style-type: none"> <li>1. <b>Sunpill Kim</b>, Yunseong Jeong, Jinsu Kim, Jungkon Kim, Hyung Tae Lee, and Jae Hong Seo, IronMask: Modular Architecture for Protecting Deep Face Template, In <i>Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)</i>, pages 16125-16134, 2021. (acceptance rate 23.4%)</li> </ol>	

## 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, L<sup>A</sup>T<sub>E</sub>X.

## TALKS & PRESENTATIONS

### International

- IronMask: Modular Architecture for Protecting Deep Face Template  
CVPR 2021, Virtual

## 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 ( $\approx$ \$6000/year)

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