

# Minkyung Park

## Security Researcher

✉ [tnstnii23@gmail.com](mailto:tnstnii23@gmail.com)

in [linkedin.com/in/mk-alsroad](https://www.linkedin.com/in/mk-alsroad)  
🌐 [alsroad.github.io](https://alsroad.github.io)

I am a security and privacy researcher. My research focus is in system and network security, e.g., designing privacy-preserving system architectures or analyzing network protocol security of secure protocols.

### SKILLS

<b>Quantitative Research</b>	Dynamic Information Flow Control (taint tracking and secure multi execution) Trusted Execution Environment (Intel SGX, Arm TrustZone, side/covert-channel attacks) Authentication and authorization (PKI, SSL/TLS, DNS security, SMTP, etc.) User privacy (tracking/fingerprinting and privacy-preserving advertising) Software vulnerability (fuzz testing) Network (Layer 2-4 protocols, data center networking)
<b>Programmings and tools</b>	C/C++ (Proficient), Assembly (Intel x64), Java, Python, Linux Operating System, CMake, Make, Git, SCons

### PROFESSIONAL EXPERIENCE

<b>Postdoctoral Researcher</b> , <i>Network Convergence and Security Laboratory, Seoul National University</i>	September 2022 — Present
<b>Assistant Researcher</b> , <i>Network Convergence and Security Laboratory, Seoul National University</i>	March 2014 — August 2022

### EDUCATION

<b>Ph.D. in Computer Science and Engineering</b> , <i>Seoul National University</i>	March 2014 — August 2022
<b>B.S. in Computer Science and Engineering</b> , <i>Korea Aerospace University</i>	March 2010 — February 2014

### SELECTED PAPERS

#### Ph.D Thesis: Information Flow Control for Privacy-preserving Advertising.

- Keywords: Privacy-preserving Advertising, Information Flow Control, Intel SGX, Side/covert-channel Attack, Native Client (SFI)
- Advisor: Prof. Taekyoung “Ted” Kwon (✉ [tkkwon@snu.ac.kr](mailto:tkkwon@snu.ac.kr))

#### An SGX-Based Key Management Framework for Data Centric Networking

- M. Park, J. Kim, Y. Kim, E. Cho, S. Park, S. Sohn, M. Kang, T. T. Kwon
- IEEE Access (SCI-E) 2020
- Keywords: Intel SGX, Public Key Infrastructure, Information Centric Networking

#### MaxPass: Credit-based multipath transmission for load balancing in data centers

- M. Park, S. Sohn, K. Kwon, T. T. Kwon
- IEEE Journal of Communications and Networks (JCN) (SCI-E) 2019
- Keywords: Data Center Networking, Transport Layer Protocol

### SELECTED PROJECTS

#### Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy

- Role: Implemented OP-TEE applications that handles private data (homomorphically encrypted)
- Keywords: Arm TrustZone (OP-TEE), Data Privacy, FHE, Cloud Machine Learning
- Funded by Ministry of SMEs and Startups

June 2022 — Present

#### Research on Grey-box Fuzzing Techniques for TLS Protocol

- Role (project manager): Designed a new grey-box fuzzer for the TLS protocol and implemented and tested it with 10+ test programs including OpenSSL, WolfSSL, mbedTLS, lighttpd, etc.
- Keywords: TLS, Fuzzing, Differential analysis
- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC)

March 2022 — November 2022

#### Research on Traceability for Data Stability on Cloud-edge Lifecycle

- Role (project manager): Designed and implemented an Information Flow Control framework that tracks data leakage on a remote server.
- Keywords: Information Flow Control, Intel SGX
- Funded by Institute for Information and Communications Technology Promotion (IITP)

April 2020 — December 2021

#### Research on GPU Acceleration for Fully Homomorphic Encryption (FHE)

- Role (project manager): Designed the GPU-accelerated FHE library (compatible with BGV) and implemented a scheduler that schedule HE evaluation operations to minimize the GPU synchronization overhead.
- Keywords: GPU, CUDA, FHE, BGV, HELib
- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC)

February 2020 — November 2020

## MISC ACTIVITIES

---

### Technical Advisor (volunteer work), Global IT Challenge

- I made up MS Excel and PowerPoint questions in the IT competition for disabled children. Mar 2016 -- Feb 2017

### Researcher, Samsung Software Membership

- Samsung Software Membership is an IT training program supported by Samsung Electronics. Jan 2012 -- Dec 2013

## COMPLETE LIST OF PAPERS

---

### TwinPeaks: An Approach for Certificateless Public Key Distribution for the Internet and Internet of Things

- Eunsang Cho, Jeongnyeo Kim, **Minkyung Park**, Hyeonmin Lee, Chorom Hamm, Soobin Park, Sungmin Sohn, Minhyeok Kang, Ted “Taekyoung” Kwon
- Elsevier Computer Networks (SCI-E) 2020

### An SGX-Based Key Management Framework for Data Centric Networking

- **Minkyung Park**, Jeongnyeo Kim, Youngho Kim, Eunsang Cho, Soobin Park, Sungmin Sohn, Minhyeok Kang, Ted “Taekyoung” Kwon
- IEEE Access (SCI-E) 2020

### D2TLS: Delegation-based DTLS for Cloud-based IoT Services

- Eunsang Cho, **Minkyung Park**, Hyunwoo Lee, Junhyeok Choi, and Ted “Taekyoung” Kwon
- ACM/IEEE Fourth International Conference on Internet-of-Things Design and Implementation (IEEE IoTDI) Montreal, Canada 2019

### MaxPass: Credit-based multipath transmission for load balancing in data centers

- **Minkyung Park**, Sungmin Sohn, Kwangwook Kwon, Ted “Taekyoung” Kwon
- IEEE Journal of Communications and Networks (JCN) (SCI-E) 2019

### User-Centric Identity Management System Using Smart Contact

- Minhyeok Kang, **Minkyung Park**, and Ted “Taekyoung” Kwon
- Korean Institutes of Communications and Information Sciences Conference (KICS Conference) Jungsun, Korea 2018

### An Automatic Attendance Checking System using Smartphones: An Infrastructureless Approach

- Selin Chun, Myungchul Kwak, **Minkyung Park**, and Ted “Taekyoung” Kwon
- International Conference on Indoor Positioning and Indoor Navigation (IPIN) Sapporo, Japan 2017

### Pay-Per-Use in User-Provided Networks: A Bitcoin-based Approach (poster)

- **Minkyung Park**, Soobin Park, Eunsang Cho and Ted “Taekyoung” Kwon
- International Conference on emerging Networking EXperiments and Technologies (ACM Conext) Incheon, Korea 2017

### TwinPeaks: A New Approach for Certificateless Public Key Distribution

- Eunsang Cho, **Minkyung Park**, Ted “Taekyoung” Kwon
- IEEE Conference on Communications and Network Security (IEEE CNS) Philadelphia, USA 2016

### Privacy-preserving Authorizaion Scheme for the Internet of Things (poster)

- **Minkyung Park**, Eunsang Cho and Ted “Taekyoung” Kwon
- The 11th International Conference on Future Internet Technologies (CFI) Nanjing, China 2016

### Multi Server Password Authenticated Key Exchange Using Attribute-based Encryption

- **Minkyung Park**, Eunsang Cho and Ted “Taekyoung” Kwon
- The Journal of Korean Institute of Communications and Information Sciences (JKICS) 2015

### Multi Server Password Authenticated Key Exchange Using Attribute-based Encryption

- **Minkyung Park**, Eunsang Cho and Ted “Taekyoung” Kwon
- Korean Institutes of Communications and Information Sciences Conference (KICS Conference) Jungsun, Korea 2015

## COMPLETE LIST OF PROJECTS

---

### Development of Homomorphic Encryption and Trusted Execution Environment for Data Privacy

- Funded by Ministry of SMEs and Startups June 2022 — Present

### Research on Grey-box Fuzzing Techniques for TLS Protocol

- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC) March 2022 — November 2022

### Research on Traceability for Data Stability on Cloud-edge Lifecycle

- Funded by Institute for Information and Communications Technology Promotion (IITP) April 2020 — December 2021

**Research on GPU Acceleration for Fully Homomorphic Encryption (FHE)**

- Funded by KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY (KIISC)

February 2020 — November 2020

**Developing high-performance programming environments and computing systems**

- Funded by National Research Foundation of Korea (NRF)

November 2016 — June 2021

**Research on Security Scheme for Interconnection of Heterogeneous Networks**

- Funded by Electronics and Telecommunications Research Institute (ETRI)

June 2019 — November 2019

**Research on Decentralized Internet Architecture**

- Funded by Electronics and Telecommunications Research Institute (ETRI)

March 2019 — November 2019

**Research on Security for Data-centric Platform**

- Funded by Electronics and Telecommunications Research Institute (ETRI)

November 2017 — March 2018

**Research on Trust and Security Scheme for Interconnection of Heterogeneous Networks**

- Funded by Electronics and Telecommunications Research Institute (ETRI)

September 2018 — November 2018

**Smartcampus: A Research on Localization Scheme based on Multiple Sensors**

- Funded by Samsung Electronics

May 2016 — December 2019

**Mashup API Design Consultation for the Advancement of IoT Platform**

- Funded by JC square

January 2016 — March 2016

**Development of Network Security Acceleration for Next-generation Low-power SoC**

- Funded by Samsung Electronics

July 2015 — December 2015

**Study on IP-based IoT Security Architecture**

- Funded by SK Telecom

October 2014 — December 2014

**Content Delivery Framework Using Spatial and Temporal Dynamics in Mobile networks**

- Funded by National Research Foundation of Korea (NRF)

March 2014 — April 2016