Statement of Purpose

Jihwan Kim

Full Time Ph.D. in Columbia University/ 2024 Spring

I intend to apply for a Ph.D. program at Columbia University focusing on research in security systems and secure machine learning. My goal is to devise solutions that enhance the use of cryptographic algorithms, ensuring high-security levels, and bolster the robustness and security of machine learning.

Currently, I am a software engineer in the wallet R&D Group at Samsung Electronics, contributing to the 'Blockchain Keystore Project' and 'Digital Car Key Project' under the Mobile Experience Division. My role involves developing applications founded on various cryptographic algorithms, such as MPC and ZKP, ensuring optimal security. Recognizing my contributions and potential, Samsung has granted me financial support through their internal fellowship program for my entire doctoral journey.

I received my bachelor's degree in computer science and engineering from Sogang University in February 2015. During my undergraduate years, I was part of the Samsung Software Membership program, An initiative designed to identify and nurture IT talent at an early stage. Here, I undertook several projects including Android game and note-taking applications. These experiences solidified my passion for smartphone – related software research, leading me to join Samsung Electronics.

At Samsung Electronics, I was initially with the Samsung Health group, tasked with the porting of sensor drivers in the Android kernel and using HAL to deliver the sensor values

from the Android kernel to the Android framework. While implementing various protocols and interfaces, such as sysfs, i2c, ioctl, and so on. I delved deep into the operational principles of Android, mastering the platform architecture, which positioned me to contribute to diverse Android projects. Notably, as part of Samsung Health, I enhanced sensor drivers and algorithms for heart rate and SpO2 monitoring, innovations now utilized in the Galaxy Watch.

Shifting to the Blockchain R&D Group, I ventured into TrustZone development within the Blockchain Keystore project, sparking my interest in Blockchain research. I've played pivotal roles in the project, from developing signature algorithms for various cryptocurrencies to integrating ZKP algorithms. I managed private keys in TrustZone so that private keys can be stored safely in mobile environments. I developed an application that can hold keys and enable signatures to be made at the TrustZone level and support third-party coin wallets. To elaborate, I developed an algorithm for signatures used in Bitcoin, Ethereum, Klaytn, Stellar, and Tron in TrustZone. In addition, I developed the logic to manage the keys in wallets such as BIP32, BIP44 within TrustZone. Moreover, I developed the Blockchain Keystore app to support third-party DID apps, as well as third-party wallets. I implemented the private data used in the Hyperledger Indy in TrustZone, and also newly implemented the ZKP algorithm and applied it to the app. I implemented various encryption algorithms based on a limited memory and a low-level language in a secure OS environment. Moreover, currently I am trying to search for journals related to the application of Multi Party Computation technology to the Blockchain Keystore app and also trying to implement it in TrustZone. This project is currently used in the Samsung Blockchain Keystore app. The Samsung developer homepage also provides it as a SDK, thus everyone can easily use the APIs related to cryptocurrency.

Moreover, I've been actively participating in the Digital Car Key project, collaborating with multiple automobile manufacturers, in line with the standards set by the Car Connectivity

Consortium (CCC). My focus here is on software that manages private keys in TrustZone, facilitating encrypted communication with automobiles.

In the realm of security, I am particularly intrigued by vulnerabilities. I aim to explore groundbreaking algorithms and methodologies that bolster machine learning model resilience against adversarial assaults, while ensuring data privacy. The research endeavors of Professor Junfeng Yang, particularly in secure systems and the robustness of machine learning, align seamlessly with my ambitions. Under his guidance, I am confident in advancing my knowledge, especially relating to cryptographic algorithms and their vulnerabilities. I would like to enroll in a PhD program to research secure systems that operate efficiently and safely in mobile environments. More specifically, my aspiration is to design a platform that democratizes the use of cryptographic technologies in smartphones, particularly through TrustZone. I believe that Columbia University offers the perfect milieu to enhance security technology, ensuring its effective integration into various applications. Upon completing my Ph.D., my vision is to spearhead research in security systems tailored for mobile environments, offering cryptographic algorithms fortified by machine learning and TrustZone.

Jihwan Kim