

# JIAYI KANG

✉ jiyi.kang2@outlook.com · ☎ (+32) 485-780491

## 🔍 RESEARCH INTERESTS

Homomorphic Encryption, Lattice-Based Zero-Knowledge Proofs

## 🎓 EDUCATION

**PhD Candidate in Cryptography** 2021 - Present

KU Leuven, Department of Electrical Engineering, COSIC research group

Supervised by Prof. Frederik Vercauteren, Prof. Nigel Smart and Dr. Ilia Iliashenko

**MSc in Mathematics (*With Great Distinction*)** 2019 - 2021

KU Leuven, Department of Mathematics

**Master of Physics (*First Class Honors*)** 2015 - 2017






The University of Manchester, Department of Physics and Astronomy

**BSc in Physics (*Honor Science Program*)** 2012 - 2016




Xi'an JiaoTong University, Department of Physics

Exchange to University of California, Berkeley in 2015 Spring

## ⚙️ PUBLICATIONS AND PREPRINTS

- Jacob Blindenbach, Jung Hee Cheon, Gamze Gürsoy, **Jiayi Kang**. On the overflow and  $p$ -adic theory applied to Homomorphic Encryption, accepted in *Cyber Security, Cryptology, and Machine Learning (CSCML)* 2024 
- Kelong Cong, **Jiayi Kang**, Georgio Nicolas, Jeongeun Park. Faster Private Decision Tree Evaluation for Batched Input from Homomorphic Encryption, in *Security and Cryptography for Networks (SCN)* 2024 
- Kelong Cong, Robin Geelen, **Jiayi Kang**, Jeongeun Park. Revisiting Oblivious Top- $k$  Selection with Applications to Secure  $k$ -NN Classification, accepted in *Selected Areas in Cryptography (SAC)* 2024 
- Robin Geelen, Ilia Iliashenko, **Jiayi Kang**, Frederik Vercauteren. On Polynomial Functions Modulo  $p^e$  and Faster Bootstrapping for Homomorphic Encryption, in *EUROCRYPT* 2023 
- Jacob Blindenbach<sup>1</sup>, **Jiayi Kang**<sup>1</sup>, Seungwan Hong<sup>1</sup>, Caline Karam, Thomas Lehner, and Gamze Gürsoy. Ultra-secure storage and analysis of genetic data for the advancement of precision medicine, *preprint* 

## 👤 TALKS AND SEMINARS

- Faster Private Decision Tree Evaluation for Batched Input from Homomorphic Encryption at *Security and Cryptography for Networks (SCN)*, Amalfi, Italy, 2024 
- Revisiting Oblivious Top- $k$  Selection with Applications to Secure  $k$ -NN Classification, invited seminar at University of Luxembourg, 2024 
- On Polynomial Functions Modulo  $p^e$  and Faster Bootstrapping for Homomorphic Encryption at *the 2nd Annual FHE.org Conference on Fully Homomorphic Encryption*, Tokyo, Japan, 2023 

## 👤 EXPERIENCE

**Intel Labs** Jul. - Sep. 2022

Privacy Technologies Graduate Research Intern

**Seoul National University** Jul.-Aug. 2023

Research visit in the group led by Prof. Jung Hee Cheon

**The Chinese University of Hong Kong** 2017-2019

Research assistant in the physics department

## 💖 TEACHING

- Guest Lecturer for the course *Privacy and Big Data* (2023 Fall, 2024 Fall)
- Guest Lecturer for the course *Privacy Technologies* (2024 Fall)
- Teaching Assistant for the course *Computer Algebra for Cryptography* (2023 Spring, 2024 Spring)

## ♡ MASTER THESIS CO-SUPERVISION

---

- Hua Xu (2024-Present), Horizontal scalability for privately accelerating ZK provers
- Sabrine Chentouf (2024-Present), Privacy-preserving federated learning
- Ibrahim Zaidan (2024-Present), Efficient polynomial evaluation on secret data
- Pritam Pak (2023-2024), From zero to HEro: zkSNARKs proof generation with Homomorphic Encryption
- Yingshuo Xi (2022-2023), An Investigation of Polynomial Activation Functions in Neural Networks
- Siva Kumar (2022), Secure Data Classification with Homomorphic Encryption

## ♡ COMMUNITY SERVICES

---

Reviewer for Designs, Codes and Cryptography (DCC) in 2024

Sub-reviewer for Eurocrypt 2024 and WAHC 2024

Sub-reviewer for Asiacrypt 2023 and CHES 2023