JIAYI KANG

Research Interests

Fully Homomorphic Encryption, Lattice-Based Protocols, 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

(authors ordered alphabetically except for publications marked with *)

Conferences

- Jacob Blindenbach, Jung Hee Cheon, Gamze Gürsoy, **Jiayi Kang**. On the overflow and p-adic theory applied to Homomorphic Encryption, 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

Journals

- **Jiayi Kang**, Leonard Schild. Pirouette: Query Efficient Single-Server PIR, to appear in *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2026
- Mariana Gama, Emad Heydari Beni, **Jiayi Kang**, Jannik Spiessens, Frederik Vercauteren. Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data, *Communications in Cryptology (CiC)* 2025
- * Jacob Blindenbach[1], **Jiayi Kang**[1], Seungwan Hong[1], Caline Karam, Thomas Lehner, and Gamze Gürsoy. Ultra-secure storage and analysis of genetic data for the advancement of precision medicine, in *Genome Biology* 2024

Preprints

- * Hua Xu[1], Mariana Gama, Emad Heydari Beni, **Jiayi Kang**. FRIttata: Distributed Proof Generation of FRI-based SNARKs, *eprint* 2025

Talks and Seminars

- Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data, invited seminar at IIE Chinese Academy of Sciences, Beijing, China, 2025
- Blind zkSNARKs for Private Proof Delegation and Verifiable Computation over Encrypted Data at *the 4th Annual FHE.org Conference on Fully Homomorphic Encryption*, Sofia, Bulgaria, 2025
- On the overflow and p-adic theory applied to Homomorphic Encryption at *Cyber Security, Cryptology, and Machine Learning (CSCML)*, virtual, 2024
- 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

Seoul National University Jul.-Aug. 2023

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

Intel Labs Jul. - Sep. 2022

Privacy Technologies Graduate Research Intern

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, 2025 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-supervison

- Fernando Javier Lopez Cerezo (2025-Present), Lattice-based anonymous credential
- Antoine Janssens (2025-Present), Private information retrieval using GBFV homomorphic encryption
- Hua Xu (2024-2025), Distributed Proof Generation of FRI-based SNARKs
- Sabrine Chentouf (2024-2025), Lattice-based zero-knowledge proofs for privacy-preserving federated learning
- Pritam Pal (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

- Program committee of the FHE.org conference 2026
- Program committee of ACM Web conference (WWW) 2026
- Reviewer for Designs, Codes and Cryptography (DCC) 2024

External reviewer

- PKC 2026
- Eurocrypt 2025, Asiacrypt 2025
- Eurocrypt 2024, WAHC 2024
- Asiacrypt 2023, CHES 2023