Xiangyu Liu

Postdoctoral Research Associate, CISPA
xiangyu1994liu@gmail.com, xiangyu.liu@cispa.de

Work Experience

Postdoctoral Researcher — June 2025 – Present
CISPA (Hosted by Doreen Riepel) — St Ingbert, Germany

Postdoctoral Researcher — Aug. 2024 – May 2025
Georgia Institute of Technology (Hosted by Vassilis Zikas) — Atlanta, GA, U.S.

Postdoctoral Researcher — Apr. 2023 – May 2025
Purdue University (Hosted by Vassilis Zikas) — West Lafayette, IN, U.S.

Software Engineer Intern — Jan. 2017 – Feb. 2017
Figo Technology — Guangzhou, China

Education

Ph.D. | *Computer Science and Technology* — Apr. 2019 – Mar. 2023
Shanghai Jiao Tong University (Advisor: Shengli Liu) — Shanghai, China
Thesis: Cryptographic Algorithms and Protocols with Tight Security

Master of Engineering | *Engineering (Software Engineering)* — Sept. 2016 – June 2018
Sun Yat-sen University (Advisor: Fangguo Zhang) — Guangzhou, China
Thesis: A Dynamic Searchable Encryption Scheme on Cloud Storage with Multi-level Access

Bachelor of Engineering | *Information Security* — Sept. 2012 – June 2016
Sun Yat-sen University — Guangzhou, China

Research Interests

Public Key Cryptography, **Blockchain**, Provable Security, Advanced Signatures, Tight Security, Universally Composable Framework, Key Exchange Protocols, Functional Encryption, etc.

Preprints / In Preparation

1. Wonseok Choi, Daniel Collins, **Xiangyu Liu**, Vassilis Zikas. A Unified Treatment of Anamorphic Encryption. Under submission.
2. Wonseok Choi, **Xiangyu Liu**, Lirong Xia, Vassilis Zikas. K-Linkable Ring Signatures and Their Applications in Voting. Under submission.

Publications

1. Wonseok Choi, **Xiangyu Liu**, Vassilis Zikas. Blockchain Governance via Sharp Anonymous Multisignatures. AFT 2025.
2. Michele Ciampi, **Xiangyu Liu**, Ioannis Tzannetos, Vassilis Zikas. Universal Adaptor Signatures from Blackbox Multi-Party Computation. CT-RSA 2025.
3. **Xiangyu Liu**, Ioannis Tzannetos, Vassilis Zikas. Adaptor Signatures: New Security Definition and A Generic Construction for NP Relations. ASIACRYPT 2024.

4. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Fine-Grained Verifier NIZK and Its Applications. PKC 2023.
5. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. EKE Meets Tight Security in the Universally Composable Model. PKC 2023.
6. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Tightly CCA-Secure Inner Product Functional Encryption Scheme. Theoretical Computer Science: Vol.898, 2022.
7. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Identity-Based Signature Scheme. Journal of Cryptologic Research: Vol.8, No.1, 2021.
8. **Xiangyu Liu**, Shengli Liu, Dawu Gu, Jian Weng. Two-Pass Authenticated Key Exchange with Explicit Authentication and Tight Security. ASIACRYPT 2020.
9. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Chameleon Hash Functions in the Multi-User Setting and Their Applications. ACISP 2020.
10. **Xiangyu Liu**, Huige Li, Fangguo Zhang. A Dynamic Searchable Encryption Scheme on Cloud Storage with Multi-level Access. Journal of Cryptologic Research: Vol.6, No.1, 2019.

Patents

1. **Xiangyu Liu**, Fangguo Zhang. A New Data Storage System Based on Access Trees. Feb. 2021
   ZL 201810051389.0 (**Authorized**).
2. **Xiangyu Liu**, Fangguo Zhang. A Computation Method Based on Shared Secrets. Sept. 2021
   ZL 201810057559.6 (**Authorized**).
3. **Xiangyu Liu**, Fangguo Zhang, Haibo Tian, Huige Li. A Storage Method for Digital Documents with Multi-level Access. Sept. 2017
   CN 107222483A (Public).

Academic Service

- Program Committee: Africacrypt 2025, FC 2025, PKC 2025.
- External Reviewer: ASIACRYPT 2024, ISC 2024, CRYPTO 2024, EUROCRYPT 2023, ASIACRYPT 2022, EUROCRYPT 2022, PKC 2022, APKC 2022, ICDCS 2022, APKC 2021, Inscrypt 2021, ProvSec 2021, ACISP 2020, ProvSec 2020.

Invited Talks

1. ChinaCrypt 2023, Chinese Association for Cryptologic Research. Dec. 2023
2. YSec Academic Forum, Shanghai Computer Society. Mar. 2021

Honors And Awards

- **2023 Outstanding Doctoral Dissertation Award of CACR** Nov. 2023
  Title of Doctoral Thesis: Cryptographic Algorithms and Protocols with Tight Security
- **Outstanding Graduate of the Class of 2023**, Shanghai Jiao Tong University June 2023
- **Three Good Student** of Shanghai Jiao Tong University Nov. 2020
- **First Prize of the 3rd National Cryptographic Technology Competition** Nov. 2017
  Project Title: Encryption Algorithms for Individuals with Multi-level Access (**as the leader**)

Community Involvement

- Wushu Club of Sun Yat-sen University Alumni Association May 2018 – Mar. 2023
  Program Committee Member Guangzhou, China

- Wushu Team of Shanghai Jiao Tong University — Mar. 2021 – Mar. 2023
  Caption — Shanghai, China
- Wushu Association of Sun Yat-sen University — Apr. 2014 – May 2017
  President — Guangzhou, China

Skills

Languages:	English, Mandarin (Rate A, Level 2)
Programming:	C++, Java, HTML, Python
Document Creation:	LaTex, Microsoft Office Suite
Design:	Photoshop, Adobe Premiere, AE
Sport:	Martial Arts and Wushu (Level 4, the Duan Wei of Chinese Wushu), Badminton, Gymnastics, Running, Hiking, and any kinds of sports in general
Music:	Flute