



XIANGYU LIU

Postdoctoral Research Associate

CS Department, Purdue University & Georgia Institute of Technology

(U.S.) +1 765 637 8088, (China) +86 138 2440 3866

xiangyu1994liu@gmail.com, liu3894@purdue.edu, xliu3028@gatech.edu

WORK EXPERIENCE

Postdoctoral Researcher

Georgia Institute of Technology (Hosted by Vassilis Zikas)

Aug. 2024 – Present

Atlanta, GA, U.S.

Postdoctoral Researcher

Purdue University (Hosted by Vassilis Zikas)

Apr. 2023 – Present

West Lafayette, IN, U.S.

Software Engineer Intern

Figo Technology

Jan. 2017 – Feb. 2017

Guangzhou, China

EDUCATION

Ph.D. | *Computer Science and Technology*

Shanghai Jiao Tong University (Advisor: Shengli Liu)

Thesis: Cryptographic Algorithms and Protocols with Tight Security

Apr. 2019 – Mar. 2023

Shanghai, China

Master of Engineering | *Engineering (Software Engineering)*

Sun Yat-sen University (Advisor: Fangguo Zhang)

Thesis: A Dynamic Searchable Encryption Scheme on Cloud Storage with Multi-level Access

Sept. 2016 – June 2018

Guangzhou, China

Bachelor of Engineering | *Information Security*

Sun Yat-sen University

Sept. 2012 – June 2016

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, **Xiangyu Liu**, Vassilis Zikas. Blockchain Governance via Sharp Anonymous Multisignatures. Preprint.
2. **Xiangyu Liu**, Shiqi Ou. CVICA: Coordinated Vehicle Infrastructure Cryptography Architecture with Fine-Grained Access Control. Under submission.

PUBLICATIONS

1. Michele Ciampi, **Xiangyu Liu**, Ioannis Tzannetos, Vassilis Zikas. Universal Adaptor Signatures from Blackbox Multi-Party Computation. CT-RSA 2025 (to appear).
2. **Xiangyu Liu**, Ioannis Tzannetos, Vassilis Zikas. Adaptor Signatures: New Security Definition and A Generic Construction for NP Relations. ASIACRYPT 2024.
3. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Fine-Grained Verifier NIZK and Its Applications. PKC 2023.
4. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. EKE Meets Tight Security in the Universally Composable Model. PKC 2023.

5. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Tightly CCA-Secure Inner Product Functional Encryption Scheme. Theoretical Computer Science: Vol.898, 2022.
6. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Identity-Based Signature Scheme. Journal of Cryptologic Research: Vol.8, No.1, 2021.
7. **Xiangyu Liu**, Shengli Liu, Dawu Gu, Jian Weng. Two-Pass Authenticated Key Exchange with Explicit Authentication and Tight Security. ASIACRYPT 2020.
8. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Chameleon Hash Functions in the Multi-User Setting and Their Applications. ACISP 2020.
9. **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. ZL 201810051389.0 (Authorized). | Feb. 2021 |
| 2. Xiangyu Liu , Fangguo Zhang. A Computation Method Based on Shared Secrets. ZL 201810057559.6 (Authorized). | Sept. 2021 |
| 3. Xiangyu Liu , Fangguo Zhang, Haibo Tian, Huige Li. A Storage Method for Digital Documents with Multi-level Access. CN 107222483A (Public). | Sept. 2017 |

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 Title of Doctoral Thesis: Cryptographic Algorithms and Protocols with Tight Security | Nov. 2023 |
| • 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 Project Title: Encryption Algorithms for Individuals with Multi-level Access (as the leader) | Nov. 2017 |

COMMUNITY INVOLVEMENT

- | | |
|---|--|
| • Wushu Club of Sun Yat-sen University Alumni Association Program Committee Member | May 2018 – Mar. 2023 Guangzhou, China |
| • Wushu Team of Shanghai Jiao Tong University Caption | Mar. 2021 – Mar. 2023 Shanghai, China |
| • Wushu Association of Sun Yat-sen University President | Apr. 2014 – May 2017 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 |