



XIANGYU LIU

Post-Doctoral Research Associate

Department of Computer Science, Purdue University

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

xiangyu1994liu@gmail.com, liu3894@purdue.edu

EDUCATION

Ph.D. | Computer Science and Technology

Shanghai Jiao Tong University

Advisor: Prof. Shengli Liu

Apr. 2019 – Mar. 2023

Shanghai, China

Master of Engineering | Engineering (Software Engineering)

Sun Yat-sen University

Advisor: Prof. Fangguo Zhang

Sept. 2016 – June 2018

Guangzhou, China

Bachelor of Engineering | Information Security

Sun Yat-sen University

Sept. 2012 – June 2016

Guangzhou, China

WORK EXPERIENCE

Postdoctoral Researcher

Purdue University

Apr. 2023 – Present

West Lafayette, IN, U.S.

Software Engineer Intern

Figo Technology

Jan. 2017 – Feb. 2017

Guangzhou, China

RESEARCH INTERESTS

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

PUBLICATIONS

1. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Fine-grained Verifier NIZK and Its Applications. Public Key Cryptography 2023.
2. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. EKE Meets Tight Security in the Universally Composable Model. Public Key Cryptography 2023.
3. **Xiangyu Liu**, Shengli Liu, Shuai Han, Dawu Gu. Tightly CCA-Secure Inner Product Functional Encryption Scheme. Theoretical Computer Science: Vol.898, 2022.
4. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Identity-Based Signature Scheme. Journal of Cryptologic Research: Vol.8, No.1, 2021.
5. **Xiangyu Liu**, Shengli Liu, Dawu Gu, Jian Weng. Two-Pass Authenticated Key Exchange with Explicit Authentication and Tight Security. ASIACRYPT 2020 (top three conferences in cryptography).
6. **Xiangyu Liu**, Shengli Liu, Dawu Gu. Tightly Secure Chameleon Hash Functions in the Multi-User Setting and Their Applications. ACISP 2020.
7. **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.
8. CVICA: Coordinated Vehicle Infrastructure Cryptography Architecture with Fine-Grained Access Control. (Under Submission, corresponding author).
9. Blockchain Governance via Sharp Anonymous Multisignatures. (Under submission, co-first author).

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).

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 Dissertation: 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**)
- **Second Class Scholarship** for Postgraduates of Sun Yat-Sen University Sept. 2017

COMMUNITY INVOLVEMENT

- Wushu Club of Sun Yat-sen University Alumni Association May 2018 – Present
Program Committee Member Guangzhou, China
- Wushu Team of Shanghai Jiao Tong University Mar. 2021 – Mar. 2023
Caption Shanghai, China
- Siyuan Volunteer Association of Shanghai Jiao Tong University June 2019 – Aug. 2019
Caption of Summer Camp for Sancha Middle School Gansu, China
- Wushu Association of Sun Yat-sen University Apr. 2014 – May 2017
President Guangzhou, China

SKILLS

- Languages:** English (IELTS 6.5), 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)
- Music:** Flute