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*** — Apr. 2019 – Mar. 2023
Shanghai Jiao Tong University — Shanghai, China
Advisor: Prof. Shengli Liu

Master of Engineering | ***Engineering (Software Engineering)*** — Sept. 2016 – June 2018
Sun Yat-sen University — Guangzhou, China
Advisor: Prof. Fangguo Zhang

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

Work Experience

Postdoctoral Researcher — Apr. 2023 – Present
Purdue University — West Lafayette, IN, U.S.

Research Interests

Public Key Cryptography, 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, IEEE Internet of Things Journal, corresponding 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).

PROJECT EXPERIENCES

1. Design and Proof of Public Key Cryptography Algorithm in Complex Network Environment.
   National Natural Science Foundation of China. Jan. 2020 – Dec. 2024
2. Cryptographic Technology for Blockchain Distributed Scenarios.
   National Key Research and Development Plan. Nov. 2022 – Oct. 2025
3. Research on New Techniques in Public Key Cryptosystem.
   National Natural Science Foundation of China. Jan. 2017 – Dec. 2020
4. Research on Leakage-Resistant Public Key Encryption.
   Guangdong Major Project of Basic and Applied Basic Research. Jan. 2020 – Dec. 2024

INVITED TALKS

1. YSec Academic Forum, Shanghai Computer Society. Mar. 2021

HONORS AND AWARDS

- **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 Team of Shanghai Jiao Tong University Mar. 2021 – Present
  Caption Shanghai, China
- Wushu Club of Sun Yat-sen University Alumni Association May 2018 – Present
  Program Committee Member Guangzhou, 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