YANXUE JIA

jia168@purdue.edu
305 N. University Street, West Lafayette, IN 47907, USA

RESEARCH INTERESTS

Applied Cryptography, Secure Computation, Blockchain and Cryptocurrency

EDUCATION

Purdue University *Jan. 2023 - now*
Postdoctoral researcher; Advisor: Prof. Aniket Kate

Shanghai Jiao Tong University *Sept. 2018 - Dec. 2022*
Ph.D. in Computer Science; Advisor: Prof. Dawu Gu

Shanghai Jiao Tong University *Sept. 2016 - Jul. 2018*
M.E. in Information and Communication Engineering; Advisor: Prof. Lei Fan

Shanghai Jiao Tong University *Sept. 2012 - Jul. 2016*
B.E. in Information Security

PUBLICATIONS

HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted
Yanxue Jia, Varun Madathil, Aniket Kate
CCS 2024

Scalable Private Set Union, with Stronger Security
Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Dawu Gu
USENIX Security 2024

A Universally Composable Non-Interactive Aggregate Cash System
Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu
AsiaCrypt 2022

Shuffle-based Private Set Union: Faster and More Secure
Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu
USENIX Security 2022

Redactable Blockchain Supporting Supervision and Self-Management
Yanxue Jia, Shi-Feng Sun, Yi Zhang, Zhiqiang Liu, Dawu Gu
AsiaCCS 2021.

PBT: A New Privacy-Preserving Payment Protocol for Blockchain Transaction
Yanxue Jia, Shi-Feng Sun, Yuncong Zhang, Qingzhao Zhang, Ning Ding, Zhiqiang Liu, Joseph Liu, Dawu Gu
IEEE TDSC 2020

Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability
Zhongtang Luo, Yanxue Jia, Yaobin Shen, Aniket Kate
In Submission

TALKS

A Universally Composable Non-Interactive Aggregate Cash System
AsiaCrypt 2022 *Dec. 2022*

Shuffle-based Private Set Union: Faster and More Secure
USENIX Security 2022 *Aug. 2022*
The 23rd annual CERIAS Information Security Symposium (Purdue University) *Mar. 2023*

Redactable Blockchain Supporting Supervision and Self-Management
AsiaCCS 2021 *Jun. 2021*

TEACHING EXPERIENCE

Teaching Assistant *Sept. 2016 - Feb. 2017*

Shanghai Jiao Tong University

- Experiments of Programming in Python

SKILLS

Programming Languages: C++/Python/Java/Go

Language: English, Mandarin (native language)

KEY COURSES

Introduction to Secure Distributed Computation, Modern Cryptographic Algorithm, On the Principle of Provable Security, Blockchain Technologies, Mathematic Fundamentals of Information Security