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; GPA: 3.44/4.3

RESEARCH PROJECTS

Private Set Union (PSU)

- Revisited the typical PSU protocols and compared the design frameworks behind them. Designed a more efficient and secure PSU protocol in the semi-honest setting based on symmetric-key operations. This work has been accepted by USENIX Security 2022.
- Observed that the existing PSU functionality cannot capture the security of different PSU protocols, and thus defined new different ideal functionalities to provide a systematic treatment for understanding the security of PSU protocols. Also, analyzed whether the typical PSU protocols can securely realize the new functionalities. This work is currently in submission.

Privacy Protection on Blockchain

- Proposed a privacy-preserving payment protocol on Blockchain with a smaller transaction size and less run time by designing a new linkable ring signature. This work has been accepted by IEEE TDSC in 2020.
- Proposed a new primitive called stateful Chameleon Hash with Revocable Subkey (sCHRS), and designed a redactable blockchain based on the new primitive, which is the first to support both supervision of improper content and self-management of personal data. This work has been accepted by AsiaCCS 2021.
- Designed a non-interactive Aggregate Cash System (NiACS) that can protect privacy and save storage. Defined an ideal functionality to abstract the security of NiACS, and proved that our scheme can UC-realize the ideal functionality in a hybrid model. This work has been accepted by AsiaCrypt 2022.

PUBLICATIONS

A Universally Composable Non-Interactive Aggregate Cash System
Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu
International Conference on the Theory and Application of Cryptology and Information Security (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 Symposium, 2022.

Redactable Blockchain Supporting Supervision and Self-Management
Yanxue Jia, Shi-Feng Sun, Yi Zhang, Zhiqiang Liu, Dawu Gu
ACM Asia Conference on Computer and Communications Security (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 Transactions on Dependable and Secure Computing (TDSC), 2020

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

HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted
Yanxue Jia, Varun Madathil, 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*

AWARDS

Distinguished Doctoral Dissertation Award of Chinese Association for Cryptologic Research (1 of 5 nationwide) *Dec, 2023*

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 (CET-6)

KEY COURSES

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