YANXUE JIA

jia168@purdue.edu
https://yanxue820.github.io/

RESEARCH INTERESTS

My research interests are applied cryptography and distributed systems. I advance cryptographic techniques for real-world applications and build privacy-enhancing systems. My current research projects focus on secure computations and blockchains.

PROFESSIONAL EXPERIENCE

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

EDUCATION

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
  *In ACM Conference on Computer and Communications Security (**CCS**), 2024. (Acceptance Rate:* 16.7%*)*
- **Scalable Private Set Union, with Stronger Security**
  Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Dawu Gu
  *In USENIX Security Symposium (**USENIX Security**), 2024. (Acceptance Rate:* 18.3%*)*
- **A Universally Composable Non-Interactive Aggregate Cash System**
  Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu
  *In Annual International Conference on the Theory and Application of Cryptology and Information Security (**Asiacrypt**), 2022. (Acceptance Rate:* 26.9%*)*
- **Shuffle-based Private Set Union: Faster and More Secure**
  Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu
  *In USENIX Security Symposium (**USENIX Security**), 2022. (Acceptance Rate:* 17.2%*)*
- **Redactable Blockchain Supporting Supervision and Self-Management**
  Yanxue Jia, Shi-Feng Sun, Yi Zhang, Zhiqiang Liu, Dawu Gu
  *In ACM Aisa Conference on Computer and Communications Security (**AsiaCCS**), 2021. (Acceptance Rate:* 18.9%*)*
- **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
  *In IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2020.*

PAPERS UNDER SUBMISSION

- **Proxying is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability**
  Zhongtang Luo, Yanxue Jia, Yaobin Shen, Aniket Kate
  *The Science of Blockchain Conference (**SBC**), 2024. (Acceptance Rate:* 14%*)*

- **Kerblam — Anonymous Messaging System Protecting Both Senders and Recipients**
  Yanxue Jia, Debajyoti Das, Wenhao Zhan, Aniket Kate
  In Submission
- **Cauchyproofs: Batch-Updatable Vector Commitment with Easy Aggregation and Application to Stateless Blockchains**
  Zhongtang Luo, Yanxue Jia, Alejandra Victoria Ospina Gracia, Aniket Kate
  In Submission

PROFESSIONAL SERVICE

Program Committee:	CCS (2025/2024), FC (2025);
Conference External Reviewer:	S&P (2025/2024/2023), CCS (2023/2021), EUROCRYPT (2020), ASIACRYPT (2024/2023/2021), ASIACCS (2020), FC (2024/2022), ACNS (2023/2022);
Journal Reviewer:	TIFS(2024), TOPS (2024), TDSC (2023);
Workshop Organizing Committee:	IMPACT (co-located with NDSS 2025);

AWARDS

Distinguished Doctoral Dissertation Award of Chinese Association for Cryptologic Research
(total 5 recipients nationwide) *Dec. 2023*

TALKS

HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted
CERIAS Security Seminar (Purdue University) *Nov. 2024*
Triangle Area Privacy and Security (TAPS) Day, Duke University *Oct. 2024*
ACM CCS 2024 *Oct. 2024*

Private Set Union: Challenges in Design and Security
University of Illinois Urbana-Champaign, Course CS591 Colloquium *Oct. 2024*

Scalable Private Set Union, with Stronger Security
USENIX Security 2024 *Aug. 2024*

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
ACM AsiaCCS 2021 *Jun. 2021*

TEACHING EXPERIENCE

Teaching Assistant *Sept. 2016 - Feb. 2017*
Shanghai Jiao Tong University

- Experiments of Programming in Python

SOFTWARE

- Implementation of "HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted"
  `https://github.com/yanxue820/HomeRun`
- Implementation of "Scalable Private Set Union, with Stronger Security"
  `https://github.com/yanxue820/SecurePSU`

REFEREES

- Aniket Kate (Purdue University, Associate Professor)
  Email: aniket@purdue.edu
- Xiao Wang (Northwestern University, Assistant Professor)
  Email: wangxiao@northwestern.edu
- Hong-Sheng Zhou (Virginia Commonwealth University, Associate Professor)
  Email: hszhou@vcu.edu