

Yunqing Sun

yunqing.sun@northwestern.edu

RESEARCH INTERESTS

My primary research interest is MPC protocols in practice, specifically *Private Set Intersection (PSI)*. I also have experience in *Network Security* during my master's.

EDUCATION

- **Northwestern University** Evanston, US
Ph.D. Candidate in Computer Science Sep 2021 - Present
- **Xidian University** Xi'an, China
M.E. in Cyber Security Sep 2018 - June 2021
B.E. in Information Security Sep 2014 - June 2018

PUBLICATION IN CRYPTO

1. Yunqing Sun, Jonathan Katz, Mariana Raykova, Phillip Schoppmann, Xiao Wang, **Large-Scale Private Set Intersection in the Client-Server Setting**, CCS'24.
2. Yunqing Sun, Hanlin Liu, Kang Yang, Yu Yu, Xiao Wang, Chenkai Weng, **Committed Vector Oblivious Linear Evaluation and Its Applications**, on submission.

PROJECT EXPERIENCES

- **Research on Large-Scale Private Set Intersection in Client-Server Setting** Oct. 2022 - Oct. 2023
We construct a fully malicious secure PSI protocol with reusable server encoding in password checkup/contact discovery setting with the server's set size up to millions and the client's set ranges from hundreds to thousands. We construct a new notion named Oblivious Verifiable Unpredictable Function (OVUF) to compute verifiable client encoding. We achieve comparable online computation with other semi-honest reusable server encoding schemes with communication overhead sacrificed.
- **Research on Committed-VOLE** Nov. 2023 - Jun. 2024
We construct a Vector Oblivious Linear Evaluation (VOLE) protocol on a committed input vector based on the structure of LPN commitment. We achieve a proof of LPN-based commitment opening from VOLE. C-VOLE has applications in improving the efficiency of generic multi-party MPC and VOLE-based commit-and-prove ZK or in improving the security of private set intersections in the client-server setting.

WORKING EXPERIENCE

- **Teaching Assistant** Northwestern University
CS 496 Advanced Cryptography Jan 2024 - Mar 2024
CS 307 Intro to Cryptography Sep 2023 - Dec 2023
CS 396 Intro to Cryptography Sep 2022 - Dec 2023
- **Summer Internship** Chinese Academy of Sciences
Institute of Information Engineering Jun 2016 - Aug 2016

SKILLS

- Proficient in C/C++/JAVA programming
- Proficient in Linux/Android system

For my experience in *Network Security*, here are the related *Publications* and *Patents*.

PUBLICATIONS IN NETWORK SECURITY

1. **Yunqing Sun**, Jin Cao, Maode Ma, Yinghui Zhang, Hui Li, Ben Niu, "EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing*, 2020, vol. 19, no. 1, pp. 370-387.
2. **Yunqing Sun**, Jin Cao, Xiongpeng Ren, Canhui Tang, Ben Niu, Yinghui Zhang, Hui Li, "An Anonymous and Secure Data Transmission Mechanism with Trajectory Tracking for D2D Relay Communication in 3GPP 5G networks," *IEEE Transactions on Intelligent Transportation Systems*, 2024.
3. **Yunqing Sun**, Jin Cao, Maode Ma, Hui Li, Ben Niu, Fenghua Li, "Privacy-Preserving Device Discovery and Authentication Scheme for D2D Communication in 3GPP 5G HetNet," *Proceedings of IEEE ICNC'19*, Honolulu, USA, Feb. 2019, pp. 425-431.
4. Jin Cao, Maode Ma, Hui Li, Ruhui Ma, **Yunqing Sun**, Pu Yu, Lihui Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys and Tutorials*, 2020, vol 22, no. 1, pp. 170-195.

5. Hao Xu, Lei Zhang, **Yunqing Sun**, Chih-Lin I, "BE-RAN: Blockchain-enabled Open RAN with Decentralized Identity Management and Privacy-Preserving Communication," arXiv e-prints, arXiv: 2101.10856. *2024 IEEE Globecom Workshops: Workshop on Mobile Network Enabled Synergies of Communication, Sensing and Computing Toward 6G*.
6. Hao Xu, **Yunqing Sun**, Zihao Li, Yao Sun, Xiaoshuai Zhang and Lei Zhang, "deController: A Web3 Native Cyberspace Infrastructure Perspective," *IEEE Communication Magazine*, vol. 61, no. 8, pp. 68-74, August 2023.
7. Hao Xu, **Yunqing Sun**, Xiaoshuai Zhang, Erwu Liu, Chih-Lin I, "When web 3.0 meets reality: A hyperdimensional fractal polytope p2p ecosystems," *IEEE Network*, 2024.

PATENTS IN NETWORK SECURITY

1. Yang Xu, Jin Cao, **Yunqing Sun**, Xumeng Bu, Hui Li, PCT/CN2020/086778, WO2021212495A1.
2. Yang Xu, Jin Cao, **Yunqing Sun**, Lihui Xiong, Hui Li, PCT/CN2020/086786, WO2021212497A1.
3. Yang Xu, Jin Cao, Lihui Xiong, **Yunqing Sun**, Hui Li, PCT/CN2020/110081, WO2022036600A1.
4. Jin Cao, **Yunqing Sun**, Hui Li, Yuanyuan Yang, Xiongpeng Ren, Unified Lightweight Traceable Security Data Transmission Method for D2D Auxiliary Communication, CN113423103B.
5. Jin Cao, **Yunqing Sun**, Hui Li, Ben Niu, An Anonymous Discovery Authentication and Key Negotiation method for Massive D2D Communication Devices, CN109768861B.
6. Jin Cao, Zhenyang Guo, **Yunqing Sun**, Pu Yu, NFC-Based Secure and Smart Hotel Access Control System and Method, CN109493493A.
7. Jin Cao, Yuxiang Gong, Pengchen Wei, Hui Li, Yulong Fu, **Yunqing Sun**, A Group Handover Authentication Method for Mobile Relays, CN106961682B.

HONORS AND AWARDS

- National Scholarship, Ministry of Education of P.R. China, 2020