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, Phillipp Schoppmann, Xiao Wang, "**Large-Scale Private Set Intersection in the Client-Server Setting**", on submission.

Project Experiences

- **Research on Large-Scale Private Set Intersection in Client-server Setting** Oct 2022 - Oct. 2023
  This project constructs a fully malicious secure 2-party PSI protocol in unbalanced setting with server's set size up to billions and client's set size of hundreds. This scheme constructs a new notion named as Oblivious Verifiable Unpredictable Function (OVUF). By applying this functionality between server and each user, this project achieves communication overhead sublinear to the larger set and avoids heavy zero-knowledge proof operations.
- **Research on Committed-PSI in Client-server Setting** May 2022 - Ongoing
  This project mainly focuses on constructing a fully malicious secure PSI in multi-client and server setting with server's message resuing. We instantiated several committed functionalities securely. Up to now, this scheme is able to achieve communication overhead sublinear to the larger set, linear to the small set in each 2-party PSI.
- **Research on Efficient Multi-party Authenticated Shares over F_{p^r}** Jan 2022 - Ongoing
  This project aims to construct efficient and malicious secure multi-party MPC compiler over Boolean Circuits based on authenticated shares over F_{p^r}. We are still working on extending Ferret to multi-party authenticated shares.

Working Experience

- **Teaching Assistant** *Northwestern University*
  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/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. 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.
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. **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," *On Submission.*
6. 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. *On Submission.*

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