Chenkai Weng

+1-224-307-3331 | ckweng@u.northwestern.edu | ckweng.github.io

Research Interests

My research interest lies in cryptography, with a focus on secure multi-party computation and zero-knowledge proofs. I have participated in projects related to VOLE-based interactive zero-knowledge proofs, the concrete security of garbled circuits protocol, efficient correlated oblivious transfer and private data aggregations.

Education

Northwestern University — Evanston, IL
PhD in Computer Science; Advisor: Xiao Wang — *Sept. 2019 – Present*

Xidian University — Xi'an, China
BSc in Information Security — *Sept. 2015 – June 2019*

Experience

Research Assistant — Evanston, IL
Northwestern University — *Sept. 2020 – Present*

- Scalable and Efficient interactive zero-knowledge protocols based on VOLE.
- Design of efficient VOLEs.
- Concrete security of the garbled circuit protocol.
- Design, implementation and evaluation of MPC/ZK applications.

AI Research Summer Associate — New York, NY
JPMorgan Chase — *Jun. 2023 – Sept. 2023*

- Research on MPC and ZK.

Research Intern — Remote
Chainlink Lab — *Oct. 2022 – May. 2023*

- Design and development of decentralized oracle system.

AI Research Summer Associate — New York, NY
JPMorgan Chase — *Jun. 2022 – Sept. 2022*

- Research on dishonest-majority maliciously-secure multi-party computation protocol.

Research Intern — Remote
Microsoft Research — *May. 2021 – Jul. 2021*

- Design and Develop secure multi-party computation and differential privacy applications for private aggregation.

Security Engineering Intern — Beijing, China
Alibaba Group — *July 2018 – Jan. 2019*

- Survey on secure multi-party computation techniques.
- Implementation of threshold encryption and digital signature schemes based on MPC.
- Implementation of private set intersection protocol and order-preserving encryption schemes.

Co-lecturer — Evanston, IL
Northwestern University — *Jan. 2023 – Mar. 2023*

- Advanced topics in cryptography: OT-extension, BGW, MPC-in-the-head, PSI.

Teaching Assistant — Evanston, IL
Northwestern University — *Sept. 2020 – Dec. 2020*

- Introduction to Cryptography

Publications

1. **ZKSQL: Verifiable and Efficient Query Evaluation with Zero-Knowledge Proofs**
   Xiling Li, Chenkai Weng, Yongxin Xu, Xiao Wang, Jennie Rogers
   Very Large Data Bases (VLDB), 2023

2. **SUPERPACK: Dishonest Majority MPC with Constant Online Communication**
   Daniel Escudero, Vipul Goyal, Antigoni Polychroniadou, Yifan Song, Chenkai Weng
   Annual International Conference on the Theory and Applications of Cryptology and Information Security (Eurocrypt), 2023

3. **AntMan: Interactive Zero-Knowledge Proofs with Sublinear Communication**
   Chenkai Weng, Kang Yang, Zhaomin Yang, Xiang Xie, and Xiao Wang
   ACM Conference on Computer and Communications Security (CCS), 2022

4. **More Efficient Secure Matrix Multiplication for Unbalanced Recommender Systems**
   Zhicong Huang, Cheng Hong, Wen-jie Lu, Chenkai Weng, Hunter Qu
   IEEE Transactions on Dependable and Secure Computing (TDSC)

5. **Constant-Overhead Zero-Knowledge for RAM Programs**
   Nicholas Franzese, Jonathan Katz, Steve Lu, Rafail Ostrovsky, Xiao Wang, Chenkai Weng
   ACM Conference on Computer and Communications Security (CCS), 2021

6. **Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning**
   Chenkai Weng, Kang Yang, Xiang Xie, Jonathan Katz, Xiao Wang
   USENIX Security Symposium, 2021

7. **Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field**
   Kang Yang, Pratik Sarkar, Chenkai Weng, Xiao Wang
   ACM Conference on Computer and Communications Security (CCS), 2021

8. **Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits**
   Chenkai Weng, Kang Yang, Jonathan Katz, Xiao Wang
   IEEE Symposium on Security and Privacy (Oakland), 2021

9. **Developing High Performance Secure Multi-Party Computation Protocols in Healthcare: A Case Study of Patient Risk Stratification**
   Xiao Dong, David Randolph, Chenkai Weng, Abel Kho, Jennie Rogers, Xiao Wang
   AMIA Informatics Summit, 2021

10. **Ferret: Fast Extension for coRRElated oT with small communication**
    Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, Xiao Wang
    ACM Conference on Computer and Communications Security (CCS), 2020

11. **Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting)**
    Chun Guo, Jonathan Katz, Xiao Wang, Chenkai Weng, Yu Yu
    International Cryptology Conference (CRYPTO), 2020

Talks

1. Nov. 2022 - ”AntMan: Interactive Zero-Knowledge Proofs with Sublinear Communication”, at ACM Conference on Computer and Communications Security (CCS), 2022.

2. Sept. 2022 - ”Efficient Interactive Zero Knowledge Proof Based on VOLE”, at Yale University CS talk.

3. Nov. 2021 - ”QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field”, ACM Conference on Computer and Communications Security (CCS), 2021.

4. Aug. 2021 - ”Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning”, USENIX Security Symposium, 2021.

5. May. 2021 - ”Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits”, IEEE Security & privacy (Oakland), 2021.
6. Mar. 2021 - ”Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs”, Security and privacy seminar at Duke Univeristy.
7. Nov. 2020 - ”Ferret: Fast Extension for coRRElated oT with small communication”, ACM Conference on Computer and Communications Security (CCS), 2020.
8. Aug. 2020 - ”Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting)”, International Cryptology Conference (CRYPTO), 2020.

Service

Conference: external reviewer for CRYPTO 21 22 23, ITC 22, Asiacrypt 22, IEEE S&P 23, PKC 23.

Journal: TDSC, TIFS, TOPS.

Awards

1. Runner-up for Best Paper Awards, CCS 2021.
2. PhD Student Research Award, Computer Science Department, Northwestern University, 2020-2021.

Software

EMP library

1. [EMP-TOOL] Float-point arithmetic based on Boolean circuits. Cryptographic building blocks.
2. [EMP-OT] Correlated-OT based on VOLE (The Ferret protocol).
3. [EMP-ZK] Interactive zero-knowledge proof protocols. For the circuit model, it supports boolean and arithmetic circuits, and their conversions. It also supports proving degree-2 polynomial satisfiabilies.