

Chenkai Weng

+1-224-307-3331 | ckweng87@gmail.com | ckweng.github.io

RESEARCH INTERESTS

Applied cryptography with a focus on secure multi-party computation and zero-knowledge proofs. The design, analysis, and implementation of MPC (e.g., garbled circuits, oblivious transfer, homomorphic encryption, and secret sharing-based protocols) and ZKP protocols (VOLE-based ZK and non-interactive ZK). The building of secure systems by applying cryptography-based privacy-enhancing techniques to various fields, including the database, networking, formal verification, machine learning, health care, and decentralized systems.

EDUCATION

Northwestern University <i>PhD in Computer Science; Advisor: Xiao Wang</i>	Evanston, IL <i>Sept. 2019 – Present</i>
Xidian University <i>BSc in Information Security</i>	Xi'an, China <i>Sept. 2015 – June 2019</i>

EXPERIENCE

AI Research Summer Associate <i>JPMorgan Chase (mentor: Antigoni Polychroniadou)</i>	New York, NY <i>Jun. 2023 – Sept. 2023</i>
Research Intern <i>Chainlink Lab (mentor: Dahlia Malkhi)</i>	Remote <i>Oct. 2022 – May. 2023</i>
AI Research Summer Associate <i>JPMorgan Chase (mentor: Antigoni Polychroniadou)</i>	New York, NY <i>Jun. 2022 – Sept. 2022</i>
Research Intern <i>Microsoft Research (mentor: Melissa Chase)</i>	Remote <i>May. 2021 – Jul. 2021</i>
Security Engineering Intern <i>Alibaba Group (Mentor: Cheng Hong)</i>	Beijing, China <i>July 2018 – Jan. 2019</i>

GRANTS & AWARDS & FELLOWSHIPS

- Co-lead the development of an NSF grant (CNS Core: Medium: Privacy-Preserving and Censorship-Resistant Domain Name System)
- JPMorgan PhD Fellowship 2023.
- Northwestern Terminal Year Fellowship 2023-24.
- Runner-up for Best Paper Awards, ACM Conference on Computer and Communications Security (CCS) 2021.
- NUCS PhD Student Research Award, 2020-21.

PUBLICATIONS

* indicates alphabetical order

- 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
- *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
- 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. **Mystique: 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. **Quicksilver: 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
Best Paper Award runner-up
8. **Wolverine: 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

PREPRINTS

1. **Precio: Private Aggregate Measurement via Oblivious Shuffling**
F. Betül Durak, Chenkai Weng, Erik Anderson, Kim Laine, Melissa Chase
2. **Privacy-Preserving Regular Expression Matching using Nondeterministic Finite Automata**
Ning Luo, Chenkai Weng, Jaspal Singh, Gefei Tan, Ruzica Piskac, Mariana Raykova
3. **PDNS: A Fully Privacy-Preserving DNS**
Yunming Xiao, Chenkai Weng, Ruijie Yu, Peizhi Liu, Matteo Varvello, Aleksandar Kuzmanovic
4. **An Efficient ZK Compiler from SIMD Circuits to General Circuits**
Dung Bui, Haotian Chu, Geoffroy Couteau, Xiao Wang, Chenkai Weng, Kang Yang, Yu Yu

TEACHING

Co-lecturer

Northwestern University

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

Evanston, IL

Jan. 2023 – Mar. 2023

Teaching Assistant

Northwestern University

- Introduction to Cryptography

Evanston, IL

Sept. 2020 – Dec. 2020

INVITED TALKS

1. May. and Oct. 2023 - "SUPERPACK: Dishonest Majority MPC with Constant Online Communication", at NYU Crypto reading group, UPenn Security Seminar and CMU Cylab Crypto Seminar.
2. Apr. 2023 - "Efficient and Scalable Zero-Knowledge Proofs based on Vector Oblivious Linear Evaluation", at JPMorgan AlgoCRYPT Seminar.
3. Sept. 2022 - "Efficient Interactive Zero Knowledge Proof Based on VOLE", at Yale University CS talk.
4. Mar. 2021 - "Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs", Security and privacy seminar at Duke University.

SERVICE

Program committee member: AsiaCCS 2024.

External reviewer: CRYPTO 2021-23, ITC 2022, Asiacrypt 2022-23, IEEE S&P (Oakland) 2023, PKC 2023.

Journal reviewer: IEEE TDSC, IEEE TIFS, IEEE TCBB, ACM TOPS, IACR JoC.

SOFTWARE

EMP library: EMP-TOOL (Circuits for floating-point arithmetic, various fundamental cryptographic primitives), EMP-OT (Oblivious transfer based on VOLE), EMP-ZK (Interactive zero-knowledge proofs based on VOLE, including the circuit, polynomial and RAM models).

SUPERPACK: An actively-secure dishonest-majority MPC protocol based on packed Shamir secret sharing.