Chenkai Weng

+1-224-307-3331 | ckweng@u.northwestern.edu | carlweng.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 the security of garbled circuits protocol, efficient generation of correlated oblivious transfer, private data analysis in healthcare systems and scalable interactive zero-knowledge proofs.

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

- Design and Develop secure multi-party computation and differential privacy applications for online conversion measurement.

Research Assistant Evanston, IL
Northwestern University *Sept. 2020 – May. 2021*

- Interactive zero-knowledge protocols for arbitrary boolean/arithmetic circuits and polynomials.
- Correlated oblivious transfer based on vector oblivious linear evaluation.
- Concrete security of the garbled circuit protocol.
- Implementation and evaluation of MPC/ZK applications.

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

- Introduction to Cryptography

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.

Publications

1. **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

2. **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

3. **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

4. **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

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

Software

EMP library

1. [EMP-TOOL] Float-point circuits, utility functions
2. [EMP-OT] Correlated-OT based on VOLE (The Ferret protocol)
3. [EMP-ZK] Implementation of 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.