Yifan Song

Cell Phone: +1 (412) 452-6378 Email: yifans2@andrew.cmu.edu

RESEARCH INTEREST

Cryptography

EDUCATION BACKGROUND

Carnegie Mellon University, School of Computer Science Pittsburgh, PA
PhD of Computer Science[1] May 2022

Tsinghua University, IIIS Beijing, China
Bachelor of Engineering, Computer Science July 2017
GPA: 90.49/100

PUBLICATIONS & MANUSCRIPTS

2021:

- Antigoni Polychroniadou, Yifan Song

Constant-Overhead Unconditionally Secure Multiparty Computation over Binary Fields
Eurocrypt 2021

- Vipul Goyal, Yifan Song, Akshayaram Srinivasan

Traceable Secret Sharing
Crypto 2021

- Vipul Goyal, Hanjun Li, Rafail Ostrovsky, Antigoni Polychroniadou, Yifan Song

ATLAS: Efficient and Scalable MPC in the Honest Majority Setting
Crypto 2021

- Vipul Goyal, Antigoni Polychroniadou, Yifan Song

Unconditional Communication-Efficient MPC via Hall's Marriage Theorem
Crypto 2021

- Vipul Goyal, Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno, Yifan Song

Extractable Witness Encryption on the Blockchain
Under Submission to TCC 2021

- Vipul Goyal, Elisaweta Masserova, Bryan Parno, Yifan Song

Asynchronous MPC based on Blockchains
Under Submission to TCC 2021

- Xiaoqi Duan, Vipul Goyal, Hanjun Li, Rafail Ostrovsky, Antigoni Polychroniadou, Yifan Song

ACCO: Algebraic Computation with Comparison

[1] PhD students in CSD are not provided a GPA.

Under Submission to CCS 2021, accepted talk in Crypto 2020 PPML

2020:

- Vipul Goyal, Yifan Song, Chenzhi Zhu

Guaranteed Output Delivery Comes Free in Honest-Majority MPC
Crypto 2020

- Vipul Goyal, Yifan Song

Malicious Security Comes Free in Honest-Majority MPC
Merged with the Crypto 2020 paper above

2019:

- Vipul Goyal, Yifan Song

Correlated-Source Extractors and Cryptography with Correlated-Random Tapes
Eurocrypt 2019

- Vipul Goyal, Yanyi Liu, Yifan Song

Communication-Efficient Unconditional MPC with Guaranteed Output Delivery
Crypto 2019

2017:

- Helene Haagh, Yue Ji, Chenxing Li, Claudio Orlandi, Yifan Song

Revealing Encryption for Partial Ordering
IMACC 2017

CONFERENCES & TALKS

Crypto 2020 August 17-21, 2020 Santa Barbara, CA, USA
Talk Title: Guaranteed Output Delivery Comes Free in Honest-Majority MPC.
[Video][PDF]

DC Area Crypto Day November 22, 2019 Washington, DC, USA
Talk Title: Communication-Efficient Unconditional MPC with Honest Majority.
[Home Page]

Crypto 2019 August 18-22, 2019 Santa Barbara, CA, USA
Talk Title: Communication-Efficient Unconditional MPC with Guaranteed Output Delivery.
[Video][PDF]

Eurocrypt 2019 May 19-23, 2019 Darmstadt, Germany
Talk Title: Correlated-Source Extractors and Cryptography with Correlated-Random Tapes.
[Video][PDF]

INTERNSHIP

JP Morgan, Chase New York, USA
Summer Associate in AI & Machine Learning Program June 2020 – August 2020

Project Title: Constant-Overhead Unconditionally Secure Multiparty Computation over Binary Fields

HONORS & ACHIEVEMENTS

Gold Medal (18 out of 300) in China Mathematical Olympiad (CMO 2013)
Cylab Presidential Fellowship (2019 - 2020)