Hao Chen | Resumé

14865 NE 36th St – Redmond, WA 98052 – USA
☎ +1 (206) 849-3515 • ✉ haoche@microsoft.com

Experience

Microsoft Research **Redmond**
Senior Researcher *2019.7 - Present*

Microsoft Research **Redmond**
Researcher *2018.1-2019.6*

Publications

2020

- **Hao Chen**, Ilaria Chillotti, Yihe Dong, Oxana Poburinnaya, Ilya Razenshteyn and M. Sadegh Riazi, *SANNS: Scaling Up Secure Nearest Neighbor Search*, USENIX 2020

2019

- **Hao Chen**, Wei Dai, Miran Kim and Yongsoo Song, *Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference*, ACM CCS 2019
- **Hao Chen**, Ilaria Chillotti, Ren Ling, *Onion Ring ORAM: Efficient Constant Bandwidth Oblivious RAM from (Leveled) TFHE*, ACM CCS 2019
- **Hao Chen**, Ilaria Chillotti, Yongsoo Song, *Multi-Key Homomophic Encryption from TFHE*, Asiacrypt 2019
- M. Sadegh Riazi, Mohammad Samragh, **Hao Chen**, Kim Laine, Kristin Lauter, Farinaz Koushanfar, *XONN: XNOR-based Oblivious Deep Neural Network Inference*, USENIX security 2019
- Roshan Dathathri, Olli Saarikivi, **Hao Chen**, Kim Laine, Kristin Lauter, Saeed Maleki, Madan Musuvathi, Todd Mytkowicz, *CHET: An Optimizing Compiler for Fully-Homomorphic Neural-Network Inferencing* , PLDI 2019
- **Hao Chen**, Ilaria Chillotti and Yongsoo Song, *Improved Bootstrapping for Approximate Homomorphic Encryption*, Eurocrypt 2019

2018

- **H. Chen**, Z. Huang, K. Laine and P.Rindal, *Labeled PSI from Fully Homomorphic Encryption with Malicious Security*, ACM Conference on Computer and Communications Security (CCS) 2018
- **H. Chen**, R. Gilad-Bachrach, K. Han, Z. Huang, A. Jalali, K. Lain and K. Lauter, *Logistic regression over encrypted data from fully homomorphic encryption* , BMC medical genomics (2018)
- **H. Chen** and Kyoohyung Han, *Homomorphic Lower Digits Removal and Improved FHE Bootstrapping*, Eurocrypt 2018
- S. Angel, **H. Chen**, K. Laine and S. Setty, *Concretely efficient PIR with compressed queries and probabilistic codes* , IEEE S&P Conference (Oakland) 2018

- **H. Chen**, K. Laine R. Player and Y. Xia, *High-Precision Arithmetic in Homomorphic Encryption*, CT-RSA 2018

2017

- **H. Chen**, K. Laine and P. Rindal, *Fast Private Set Intersection from Homomorphic Encryption*, ACM Conference on Computer and Communications Security (CCS) 2017
- **H. Chen**, K. Laine and R. Player, *Simple Encrypted Arithmetic Library-SEAL v2. 1.*, Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC) 2017
- Ç. Gizem S., **H. Chen**, K. Laine, K. Lauter, P. Rindal, and Y. Xia, *Private queries on encrypted genomic data*, BMC medical genomics 10, no. 2 (2017): 45.

2016

- **H. Chen**, K. Lauter and K. Stange, *Attacks on the Search-RLWE problem with small errors*, SIAM Journal on Applied Algebra and Geometry
- **H. Chen**, K. Lauter and K. Stange, *Security considerations for Galois non-dual RLWE families*, Selected Areas in Cryptography 2016
- **H. Chen**, *Computing the Mazur and Swinnerton-Dyer critical subgroup of elliptic curves*, Mathematics of Computation 85, no. 301 (2016): 2499-2514.

Software Projects

- Leading the development of an internal secure multiparty computation (MPC) library.
- Microsoft SEAL (a leading library for homomorphic encryption), `https://github.com/microsoft/SEAL`
- SealPIR (a leading library for private information retrieval), `https://github.com/microsoft/SealPIR`

Education

University of Washington — **Seattle**
Ph.D. Mathematics — *2011–2016*
Advisor: William Stein
Thesis: Computational Aspects of Modular Parametrizations of Elliptic Curves

Peking University — **Beijing**
B.Sc. Mathematics — *2007–2011*

Conference Talks

- [CCS18] Labeled PSI from Fully Homomorphic Encryption with Malicious Security, CCS 2018
- [CCS17] Fast Private Set Intersection from Homomorphic Encryption, The ACM Conference on Computer and Communications Security (CCS) 2017
- [SAC16] Security considerations for Galois (non-dual) RLWE families, Selected Areas in Cryptography, 2016

Invited Talks

- [UCSD18] Better PIR from homomorphic encryption and application to anonymous communication, University of California San Diego, 2018
- [CAS18] Security of homomorphic encryption, Chinese Academy of Sciences, 2018

- [HEStd18] Improved bootstrapping for BGV/BFV schemes under large plaintext modulus, 2nd Homomorphic Encryption Standardization Workshop at MIT, 2018
- [iDASH17] Training logistic regression model on encrypted data, iDASH secure genome analysis workshop, 2017
- [AG17] Security considerations for Galois RLWE families, SIAM conference on Applied Algebraic Geometry, 2017
- [PNNT16] Towards the computation of modular building blocks, Pacific Northwest Number theory, 2016
- [JMM16] Attacks on Search RLWE, AMS/MAA Joint Mathematics Meetings, 2016

Services

- Program Committee member for IACR Crypto 2020
- Program Committee member for ACM CCS 2020
- Program Committee member for ACM CCS 2019
- Reviewer for Journal of Mathematical Cryptology
- Reviewer for IEEE Transaction on Dependable and Secure Computing
- Program Committee member for Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC) 2018
- Subreviewer for Applied Cryptography and Network Security (ACNS) 2018
- Reviewer for DCC (Design, Code and Cryptography)
- Program Committee member for Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC) 2017

Patents

In review: 2

- Improved least significant digits removal in homomorphic encryption
- Logistic Regression on Homomorphically Encrypted Data

Approved: 9

- Compiler and Runtime for Homomorphic Evaluation of Tensor Programs
- Cuckoo hashing to accelerate batched private information retrieval
- Faster Private Set Intersection using Extension Fields
- Enabling constant plaintext space in bootstrapping in fully homomorphic encryption
- Private set intersection of arbitrarily large items from homomorphic encryption
- More Efficient Decryption for Certain Homomorphic Encryption Schemes
- Improved Relinearization in Homomorphic Encryption Using Variable Size Evaluation Keys
- String Matching on Encrypted Data
- Faster Operations in Homomorphic Encryption

Programming Skills

Fluent: C++, Python, Sage, Java, Matlab, LaTeX

Familiar: SQL, Mathematica