Haibin Zhang, Ph.D.

Contact Information

ITE 357, Department of CSEE
University of Maryland, Baltimore County

E-mail: hbzhang at umbc dot edu

Position

Assistant Professor, University of Maryland, Baltimore County 08/2017-Present

Education

Ph.D., Department of Computer Science, UC Davis 12/2014

M.S., Institute of Software, Chinese Academy of Sciences. 06/2019

B.S., School of Mathematics, Shandong University. 06/2016

Experience in Higher Education

- University of Connecticut 08/2016-08/2017

  Postdoctoral Research Associate Host: Prof. Marten van Dijk

  Worked on *NSF Frontier: the MACS project—A Modular Approach to Cloud Security*, a cross-institutional collaboration among BU, MIT, Northeastern, and UConn.

- University of North Carolina, Chapel Hill 01/2015-06/2016

  Postdoctoral Research Associate Host: Prof. Michael K. Reiter

  Worked on *NSF Frontier: Project Silver—Rethinking Security in the Era of Cloud Computing*, and also on cyber-physical system security, privacy-preserving techniques, information fusion, and multi-party computation.

- University of California, Davis 09/2009-12/2014

  Fellowship, Research/Teaching Assistant Advisor: Matt Franklin

  Worked in Theory Lab and Security Lab. During my PhD, my research involves the following topics: symmetric-key modes of operations, privacy-preserving techniques, public-key cryptography, foundations of computational hardness, elliptic curve cryptography, crash fault tolerant protocols (e.g., Paxos), Byzantine fault tolerant protocols, state machine replication, pub/sub systems, intrusion detection, and secure cloud storage and encrypted search.

- University of Stavanger, Norway 01/2014-03/2014

  Visiting Researcher Host: Prof. Hein Meling

  Designed and implemented crash/Byzantine fault tolerant distributed systems, funded by Leiv Eiriksson mobility programme award from Norwegian Research Council.

Experience in Other Than Higher Education

- Symantec Research Labs, Symantec Corporation 06/2013-08/2013

  Research Intern Host: W. Bogorad, S. Schneider, and S. Sundaram

  Participated in the design and implementation of Norton Zone, a fully featured and secure cloud storage. Zone started production in May 2013. At the peak time Zone had about 300,000 accounts.

Awards

- Feature Speaker at NASA Goddard Colloquium, 2019.
- IEEE SRDS 2014 best paper candidate award (runner-up award).
- NSF Student Travel Award for CRYPTO 2014.

- IFCA Student Travel Award for Financial Cryptography 2013.
- Graduate Student Travel Award, UC Davis, 2013.
- Graduate Program Fellowship, Graduate Group in Computer Science, 2013.
- Block Grant Fellowship, Office of Graduate Studies, UC Davis, 2009.

Research Support and Fellowships

External

- 2019-2022, $549,718. National Science Foundation. Partnership for Innovation - Research Partnership (PFI-RP) program.
  Haibin Zhang (co-PI). Yelena Yesha (PI), Sisi Duan (co-PI), Jeb Linton (IBM, co-PI)
  Building a Modular, Reliable, Scalable, and Secure Internet of Things Infrastructure
  IBM is not a direct recipient and does not receive funding.
- 2018-2019, $115,000. Maryland Technology Development Corporation.
  Maryland Innovation Initiative (MII) program.
  Haibin Zhang (PI).
  Building a Scalable and Intrusion-Tolerant Permissioned Blockchain
- 2018-2019, $50,000. Department of Homeland Security Science and Technology
  Haibin Zhang (co-PI). Sisi Duan (PI)
  Permissioned Blockchains for IoT, IoMT, and Storage
- 2018–2023, $4.9M . National Science Foundation. SFS program.
  Haibin Zhang (Investigator). Alan Sherman(PI), Richard Forno (Co-PI), Dhananjay Phatak (Investigator).
  UMBC CyberCorps Program Renewal and Building Research-Based SFS Relationships between Community Colleges and Four-Year Schools

Internal

- 2018, $6,000. Summer Research Faculty Fellowship (SURFF), UMBC
  PI: **Haibin Zhang**

Others (UMBC is not a direct recipient; the funding goes to UMBC via reimbursement and research collaboration agreement.)

- 2018-2021, 5,856,000 NOK ($653,852). Research Council of Norway.
  PI: Hein Meling. co-PIs: Roman Vitenberg, Frank Eliassen, Fabiola Greve, Bettina Kemme, Kaiwen Zhang, Ken Birman, Robbert van Renesse, Keith Marzullo, Susan J. Winter, Sisi Duan, **Haibin Zhang**, Nalini Venkatasubramanian, Deborah Agarwal, and Sean Peisert. *CREDENCE: Collaboration Network for Excellent Education and Research in Dependable and Secure Distributed Systems*
  This is an international collaboration grant among top universities from US, Canada, and EU.

Advising

- PhD students (UMBC): Cyrus Bonyadi (NSF SFS scholarship, 2018 – present); James Clavin (co-advised with Sisi Duan, 2018 – present); Chao Liu (2018 – present); Shuai Xu (2018 – present); Russell Wu (2019 – present), Xin Wang (co-advised with Sisi Duan).
- Master students (UMBC): Siddhant Goenka (2017– 2018, Research Assistant); Jack Shan (co-advised with Sisi Duan, graduated August 2019); Sam Mendimasa (Fall 2019 – present)
- Undergraduate students (UMBC): Ezio Mei (2019 – present)

- Chenglu Jin (PhD at UConn, informally co-advised with Marten van Dijk; Topic: secure sensor aggregation)

- Reza Rahaeimehr (PhD at UConn, informally co-advised with Marten van Dijk; Topic: cloud computing and cloud security)

- Hoda Maleki (PhD at UConn, informally co-advised with Marten van Dijk; Topic: distributed systems)

- Nick Tobey (Undergraduate at UNC Chapel Hill, informally co-advised with Mike Reiter; Topic: OpenStack; now at Google)

Publications

[1] Chao Liu, Sisi Duan, and Haibin Zhang. EPIC: Efficient Asynchronous BFT with Adaptive Security. *The 50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2020).*

[2] Kyle Hogan, Hoda Maleki, Reza Rahaeimehr, Ran Canetti, Marten van Dijk, Jason Hennessey, Mayank Varia, and Haibin Zhang. On the Universally Composable Security of OpenStack. *IEEE SecDev 2019.*
Full paper available in eprint: http://eprint.iacr.org/2018/602

[3] Alan Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski. On the Origins and Variations of Blockchain Technologies. *IEEE Security and Privacy*, 2019.

[4] Siddhant Goenka, Sisi Duan, and Haibin Zhang. A Formal Treatment of Efficient Byzantine Routing Against Fully Byzantine Adversary. *The 17th IEEE International Symposium on Network Computing and Applications (NCA 2018).*

[5] Sisi Duan, Michael K. Reiter, and Haibin Zhang. BEAT: Asynchronous BFT Made Practical. *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS 2018).*

- Featured in the Morning Paper.

[6] Sisi Duan, Michael K. Reiter, and Haibin Zhang. Secure Causal Atomic Broadcast, Revisited. *47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2017).*

[7] Sherman S.M. Chow, Haibin Zhang, and Tao Zhang. Real Hidden Identity-Based Signatures. *The 21st International Conference on Financial Cryptography and Data Security 2017 (FC 2017).*

[8] Sisi Duan, Lucas Nicely, and Haibin Zhang. Byzantine Reliable Broadcast in Sparse Networks. *15th IEEE International Symposium on Network Computing and Applications (NCA 2016).*

[9] Walter Bogorad, Scott Schneider, and Haibin Zhang. Norton Zone: Symantec's Secure Cloud Storage System. *IEEE 35th International Symposium on Reliable Distributed Systems (SRDS 2016).*

- One of the three key inventors for Norton Zone (Zone is a production cloud storage system).

[10] Sisi Duan and Haibin Zhang. Practical State Machine Replication with Confidentiality. *IEEE 35th International Symposium on Reliable Distributed Systems (SRDS 2016).*

[11] Mingqiang Wang, Tao Zhan, and Haibin Zhang. Bit Security of the CDH Problems over Finite Fields. *Selected Areas in Cryptography 2015*, pages 441–461, 2015.
Full version available: eprint.iacr.org/2014/685

[12] Sisi Duan, Hein Meling, Sean Peisert, and Haibin Zhang. BChain: Byzantine Replication with High Throughput and Embedded Reconfiguration. *The 18th International Conference on Principles of Distributed Systems (OPODIS 2014)*, LNCS 8878, pages 91–106, 2014.

- Fully implemented in Iroha under Hyperledger framework. One of the five mature projects in Hyperledger.
- BChain detailed in Hyperledger whitepaper and Iroha document.
- More than 20 media outlets on BChain.
- Hyperledger is supported more than 250 companies and Hyperledger Iroha is independently supported by more than 40 Japanese companies.

[13] Sisi Duan, Karl Levitt, Hein Meling, Sean Peisert, and Haibin Zhang. ByzID: Byzantine Fault Tolerance from Intrusion Detection. *IEEE 33rd International Symposium on Reliable Distributed Systems (SRDS 2014)*, pages 253–264, 2014.

- **Runner-up for the best paper award**.

[14] Tiancheng Chang, Sisi Duan, Hein Meling, Sean Peisert, and Haibin Zhang. P2S: A Fault-Tolerant Publish/Subscribe Infrastructure. *The 8th ACM International Conference on Distributed Event-Based Systems (DEBS 2014)*, pages 189–197, ACM, 2014.

[15] Sherman Chow, Matthew Franklin, and Haibin Zhang. Practical Dual-Receiver Encryption: Soundness, Complete Non-Malleability, and Applications. *Topics in Cryptology — CT-RSA 2014*, LNCS 8366, pages 85–105, 2014. Full version: eprint.iacr.org/2013/858

[16] Matthew Franklin and Haibin Zhang. Unique Ring Signatures: A Practical Construction. *The 17th International Conference on Financial Cryptography and Data Security 2013 (FC 2013)*, LNCS 7859, pages 162–170, 2013.

- The underlying verifiable random function (VRF) has been used in practical and deployed Open-Source systems as the key component:
  - NSEC5 (NSEC5 is a proposal for providing authenticated denial of existence for DNSSEC, the de facto standard for security enhanced domain name system).
  - OmniLedger (A secure, scale-out, decentralized ledger).
  - CONIKS (An end-user key verification service).
  - Micropayments for decentralized currencies.
  - Mobius: Trustless tumbling for transaction privacy.

[17] Phillip Rogaway, Mark Wooding, and Haibin Zhang. The Security of Ciphertext Stealing. *IACR 19th International Workshop on Fast Software Encryption (FSE 2012)*, LNCS 7549, pages 180–195, 2012.

- Proved the security of NIST standard: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode. Addendum to NIST Special Publication 800-38A October, 2010.

[18] Matthew Franklin and Haibin Zhang. Unique Group Signatures. *The 17th European Symposium on Research in Computer Security (ESORICS 2012)*, LNCS 7459, pages 643–660, 2012. Full version: eprint.iacr.org/2012/204

[19] Haibin Zhang. Length-Doubling Ciphers and Tweakable Ciphers. *The 10th International Conference on Applied Cryptography and Network Security (ACNS 2012)*, LNCS 7341, pages 100–116, 2012.

[20] Phillip Rogaway and Haibin Zhang. Online Ciphers from Tweakable Blockciphers. *Topics in Cryptology — CT-RSA 2011*, LNCS 6558, pages 237–249, 2011.

Preprints

[21] Chenglu Jin, Marten van Dijk, Michael K. Reiter, Haibin Zhang. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. https://eprint.iacr.org/2018/1171

[22] Matthew Franklin and Haibin Zhang. A Framework for Unique Ring Signatures. Full version available: eprint.iacr.org/2012/577

Patents

[23] Haibin Zhang, Scott Schneider, Walter Bogorad, and Sharada Sundaram. SYSTEMS AND METHODS FOR SECURING DATA AT THIRD-PARTY STORAGE SERVICES, Patent No. 9258122, Symantec Corporation, USA, 2016.

[24] Haibin Zhang, Scott Schneider, Walter Bogorad, and Sharada Sundaram. SYSTEMS AND METHODS FOR MAINTAINING ENCRYPTED SEARCH INDEXES ON THIRD-PARTY STORAGE SYSTEMS, Patent No. 9679160, Symantec Corporation, USA, 2017.

[25] Scott Schneider, Walter Bogorad, Haibin Zhang, and Sharada Sundaram. SYSTEMS AND METHODS FOR SEARCHING SHARED ENCRYPTED FILES ON THIRD-PARTY STORAGE SYSTEMS, Patent No. 9342705, Symantec Corporation, USA, 2014.

[26] SYSTEMS AND METHODS FOR PERMISSIONED BLOCKCHAIN INFRASTRUCTURE WITH FINE-GRAINED ACCESS CONTROL AND CONFIDENTIALTIY PRESERVING PUBLISH/SUBSCRIBE MESSAGING. US Patent Application No. 16449227, 2019.

Other Publications

[27] Haibin Zhang. How secure is your data when it's stored in the cloud? *The Conversation*, Jan 2018.

- Republished in ScientificAmerican.
- An Italian version (Quanto sono al sicuro i dati immagazzinati nel cloud?) appears Galileonet.it
- UMBC news; UMBC CSEE news.

Teaching Experience

Instructor, CMSC 443/652, *Cryptography and Data Security*, Spring 2020.

Instructor, CMSC 491/691, *Blockchains*, Fall 2019.

Instructor, CMSC 443/652, *Cryptography and Data Security*, Spring 2019.

Instructor, CMSC 491/691, *Cybersecurity Research — INSuRE*, UMBC, Fall 2018.

Instructor, CMSC 626, *Principles of Computer Security*, UMBC, Fall 2017.

Professional Activities

Services

- Panel for Cyber Innovation Briefing (blockchain), 05/20/2018.
- NSF review panel, 2018.
- UMBC CSEE graduate committee, 2017 – present.
- UMBC CSEE graduate admission committee, 2017 – present.
- UMBC advising for CSEE undergraduates, 2017 – present.

Organizer

- UConn CSE/ECE security seminar with Prof. Marten van Dijk and Prof. Ben Fuller. Seminar webpage: scl.uconn.edu/seminar/index.php

Organizing/Steering Committee

- Blockchain Workshop: From Lab to App. November16, 2018, Washington DC.

Program Committee

- IEEE BigData SI of Federated Machine Learning 2019.
- IEEE DSC 2019.
- 2nd International Workshop on Distributed Ledger of Things, 2019.
- SCC 2019.
- 1st International Workshop on Distributed Ledger of Things (DLoT), 2018
- 36th International Symposium on Reliable Distributed Systems (SRDS 17)
- 2018 Cyber and Information Security Workshop workshop
- 12th Annual Cyber and Information Security Research Conference (CISRC 2017)
- 11th Annual Cyber and Information Security Research Conference (CISRC 2016)
- 10th Annual Cyber and Information Security Research Conference (CISRC 2015)
- 5th International Workshop on Security in Cloud Computing (SCC'17)
- 4th International Workshop on Security in Cloud Computing (SCC'16)
- 3rd International Workshop on Security in Cloud Computing (SCC'15)

Journal Reviewer

- *IEEE/ACM Transactions on Networking*
- *ACM Transactions on Privacy and Security (formerly ACM TISSEC)*
- *Designs, Codes and Cryptography*
- *IEEE Transactions on Vehicular Technology*
- *IEEE Transactions on Computers*
- *Information and Computation*
- *Frontiers of Computer Science*

Conference Reviewer

- EUROCRYPT 2010, ASIACRYPT 2012, ICICS 2012, CANS 2012, CSIIRW 2012, Financial Crypto 2013, ACNS 2013, ICDCS 2014, ESORICS 2014, Theory of Cryptography Conference (TCC) 2015, PETS 2015, SODA 2016, S&P 2016, WAHC 2017, NCA 2017, CCS 2018.

Talks

- BEAT: Asynchronous BFT Made Practical. *Invited Talk*, IEEE DLoT, CNS, Washington, DC, 2019.

- Intrusion-Tolerant Permissioned Blockchains. *Invited Talk as Featured Speaker*, NASA Goddard IS & T Colloquium, 2019.

- How to Select a Blockchain and BEAT: Asynchronous Blockchain Made Practical, AAAS Headquarters, 2018.

- Blockchains for Finance. NSF CARTA IAB meeting, 2018.

- Building a Cross-Site Cloud Storage for CHMPR Partners. NSF CHMPR IAB meeting, 2017.

- BFT — From the Saddest Moment to the Era of Blockchains. *Invited Talks*, Various occasions (UMBC CDL, USNA), 2017.

- Secure Causal Atomic Broadcast, Revisited. *DSN 2017*, Denver, June 2017.

- Secure Causal Atomic Broadcast, Revisited. *Invited Talk*, NorthEastern University, May 2017.

- Building “Incorruptible” Systems (in Cloud Environments). Various occasions (e.g., UMBC, UConn, FIU, NMSU), 2017.

- Better Swift and Keystone. *Massachusetts Open Cloud (MOC) Invited Talk*, Boston, MA, 2016.

- High-Throughput BFT Protocols. MIT Star Conference Room, Cambridge, MA, 2016.

- Privacy-Preserving and Fault-Tolerant Data Storage. UConn CSE/ECE Security Seminar, Storrs, CT, 2016.

- Privacy-Preserving Data Storage and Information Retrieval. *Invited Talk*, ORNL, Oak Ridge, TN, 2016.

- BChain: Byzantine Replication with High Throughput and Embedded Reconfiguration. *OPODIS 2014*, Cortina d’Ampezzo, Italy, 2014.

- Bits Security of the CDH Problems over Finite Fields. *Crypto 2014 rump session*, UCSB, 2014.

- Internet Voting and Internet Polling. *Invited Talk*, University of Stavanger, Norway, 2014.

- Practical Encrypted Search. Symantec Research Labs, Mountain View, US, 2013.

- Exploiting Uniqueness in Various Signature Schemes. *Invited Talk*, Key Lab of Cryptologic Technology and Information Security, Shandong University, China, 2013.

- Making Practical Byzantine Fault-Tolerance Practical. *Invited Talk*, Symantec Research Labs, Mountain View, US, 2013.

- Byzantine Fault-Tolerance Made Faster. *FC 2013 rump session*, Okinawa, Japan.

- Unique Ring Signatures. *FC 2013*, Okinawa, Japan, 2013.

- Bridging Efficient Cryptography and Reliable Distributed Computing. *Invited Talk*, *Security Lab Seminar*, UC Davis, 03/05/13.

- Unique Group Signatures. *ESORICS 2012*, Pisa, Italy, 2012.

- Length-Doubling Ciphers and Tweakable Ciphers. *ACNS 2012*, Singapore, 2012.

- Online Ciphers from Tweakable Blockciphers. *CT-RSA 2011*, San Francisco, 2011.