Haibin Zhang, Ph.D.

Contact Information

Department of ECE
University of Connecticut
Storrs, CT 06269

Mobile: +1-919-699-0832
E-mail: ucdhbzhang@gmail.com
WWW: scl.uconn.edu/people/haibin/info.php
and cs.unc.edu/~haibin/

Current Position

Postdoctoral Fellow, University of Connecticut 08/2016-Present

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

Research Interests

Cryptography, Security, and Privacy; Systems and Distributed Systems

Education

Ph.D., Department of Computer Science, UC Davis 09/2009-10/2014

- Advisor: Prof. Matthew Franklin
- Dissertation: Building Efficient, Secure, and Reliable Distributed Systems.

M.S., Institute of Software, Chinese Academy of Sciences 09/2006-06/2009

- Advisor: Prof. Chuankun Wu

B.S., School of Mathematics, Shandong University 09/2002-06/2006

- Advisor: Prof. Xiaoyun Wang

Research and Work Experience

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

  Postdoctoral Research Associate Host: Prof. Michael 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

  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. See publications [4, 5].

- 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. See publications [4, 17, 18, 19].

PUBLICATIONS All my publications use an alphabetical order.

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

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

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

[4] 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)*.

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

[6] 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

[7] 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.

[8] 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**.

[9] 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.

[10] 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

[11] 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.

[12] 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. **Impact**: 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.

[13] 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

[14] 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.

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

PREPRINTS

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

PATENTS

[17] 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, 2014.

[18] Haibin Zhang, Scott Schneider, Walter Bogorad, and Sharada Sundaram. SYSTEMS AND METHODS FOR MAINTAINING ENCRYPTED SEARCH INDEXES ON THIRD-PARTY STORAGE SYSTEMS, Application No. 14199240, Symantec Corporation, USA, 2014.

[19] 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.

AWARDS

- IEEE SRDS 2014 best paper candidate award (runner-up award).
- Co-awardee for Leiv Eiriksson mobility programme award, Norwegian Research Council, 2014.
- 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.
- Outstanding Student Award, Shandong University, 2005.
- All-round Pace-setter, School of Mathematics, Shandong University, 2005.
- University Excellent League Member, Shandong University, 2005.
- University Excellent Student Scholarship, Shandong University, 2003-2005.
- University Outstanding Student Leader, Shandong University, 2004.
- University Excellent Youth Volunteer, Shandong University, 2004.
- Award of Scholarship for National Key Training Program of Mathematics, 2003-2004.
- University Excellent Individual in Program for Student Quality Development, Shandong University, 2003.

TEACHING EXPERIENCE

Teaching Assistant, ECS 20, *Discrete Math for Computer Science*, UC Davis, Winter 2010. Instructor: Nelson Max

Teaching Assistant, ECS 120, *Theory of Computation*, UC Davis, Fall 2012. Instructor: Phillip Rogaway

Teaching Assistant, ECS 132, *Probability and Statistical Modeling for Computer Science*, UC Davis, Winter 2014. Instructor: Dipak Ghosal

Guest Lecturer, ECS 15, *Introduction to Computers*, UC Davis, 16/04, 18/04, and 20/04, Spring 2012. Instructor: Matthew Franklin

Professional Activities

Organizer

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

Program Committee

- 36th International Symposium on Reliable Distributed Systems (SRDS 17)
- 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

- *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*

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.

Advising

- 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)

Talks

- 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.