Feng-Hao Liu

CONTACT

Department of Computer and Electrical Engineering and Computer Science
Florida Atlantic University
777 Glades Road, EE 529
Boca Raton, FL 33431
fenghao.liu@fau.edu
http://faculty.eng.fau.edu/fenghao

EDUCATION

Ph.D., Computer Science — Sep 2009 - May 2013
Brown University, Providence, RI.
Thesis: "*Error Tolerant Cryptography*"
Advisor: Anna Lysyanskaya

Sc.M., Computer Science — Sep 2007 - May 2009
Brown University, Providence, RI.

B.S., Electrical Engineering — Sep 2001- Jun 2005
National Taiwan University, Taipei, Taiwan.
Minor: Mathematics

RESEARCH INTERESTS

I am interested in information security and cryptography to tackle security challenges in various scenarios of cloud computing. I have studied and developed new techniques for different security tasks, such as: how to compute on encrypted data, how to verify computation in outsourced environments, and how to protect memory/computation under physical attacks.

APPOINTMENTS

Assistant Professor, *Florida Atlantic University* — May 2015 - Current

Postdoctoral Research Associate, *Maryland Cybersecurity Center at University of Maryland*
July 2013 - May 2015
- Hosted by Prof. Jonathan Katz, Prof. Elaine Shi and Prof. Dana Dachman-Soled

Research Assistant, *Dept. of Computer Science, Brown U., RI.* — Sep 2009 - May 2013
- Worked with Prof. Anna Lysyanskaya

Summer Intern, *Microsoft Research, Redmond, WA* — Jun 2012 - Aug 2012
- Worked with Dr. Melissa Chase and Dr. Nishanth Chandran in the Crypto Group
- Investigated different applications of re-encryption, relaxations of obfuscation, and lattice-based constructions

Research Assistant, *IIS, Academia Sinica, Taiwan.* — Dec 2006 - Jun 2007
- Worked with Prof. Bo-Yin Yang
- Implemented several multivariate cryptographic systems, in Java and C++

- Investigated a new stream cipher QUAD, and made generalizations and improvements

Second Lieutenant, *Chung Cheng Armed Forces Preparatory School, Taiwan.* Jul 2005 - Oct 2006

- Oversaw over 80 senior high school students, teaching both discipline and academic studies
- Advised as a math teaching assistant that increased average math scores and admission rates of all senior students by 15%, from 75% to 90%

HONORS

Selected as U.S. delegate to Heidelberg Laureate Forum via ORAU	Aug 2015
Best Student Paper Award of Theoretical Cryptography Conference (TCC) 2010	Feb 2010
Outstanding Mandatory Military Officer Award, Taiwan, ROC	Oct 2006
Bronze Medal, ranked 4 in Taiwan, Asian Pacific Mathematics Olympiad (APMO)	Nov 2001
2nd price, ranked 4 $\sim$ 10 in Taiwan, National Mathematics Contest, Taiwan	Jan 2001

Publications

- *"Computation Over Encrypted Data."* Invited Book Chapter of Cloud Computing Security: Foundations and Challenges, CRC Press. In Progress.
- Daniel Apon, Xiong Fan, and Feng-Hao Liu. *"Bi-Deniable Inner Product Encryption from LWE."* Manuscript.
- Dana Dachman-Soled, S. Dov Gordon, Feng-Hao Liu, Adam O'Neill, and Hong-Sheng Zhou. *" Leakage-Resilient Public-Key Encryption from Obfuscation."* To appear in PKC 2016.
- S. Dov Gordon, Feng-Hao Liu, and Elaine Shi. *" Constant-Round MPC with Fairness and Guarantee of Output Delivery"* In Crypto 2015, volumn 9216 of Lecture Notes in Computer Science, pages 63 - 82. Springer, 2015.
- Dana Dachman-Soled, Feng-Hao Liu, and Hong-Sheng Zhou. *" Leakage-Resilient Circuits Revisited – Optimal Number of Computing Components without Leak-free Hardware."* In Eurocrypt 2015, volume 9057 of Lecture Notes in Computer Science, pages 131-158. Springer, 2015.
- Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. *" Locally Decodable and Updatable Non-Malleable Codes and Their Applications."* In TCC 2015, volume 9014 of Lecture Notes in Computer Science, pages 427-450. Springer, 2015.
- S. Dov Gordon, Jonathan Katz, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. *"Multi-client Verifiable Computation with Stronger Security Guarantees."* In TCC 2015, volume 9015 of Lecture Notes in Computer Science, pages 144-168. Springer, 2015.
- Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. *"Multi-input Functional Encryption."* In Eurocrypt 2014, volume 8441 of Lecture Notes in Computer Science, pages 578-602. Springer, 2014.
- Nishanth Chandran, Melissa Chase, Feng-Hao Liu, Ryo Nishimaki and Keita Xagawa. *"Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from Lattices."* In Public-Key Cryptography (PKC) 2014, volume 8383 of Lecture Notes in Computer Science, pages 95-112. Springer, 2014.

- Alexandra Berkoff and Feng-Hao Liu. *"Leakage Resilient Fully Homomorphic Encryption"* In Theoretical Cryptography Conference (TCC) 2014, volume 8349 of Lecture Notes in Computer Science, pages 515-539. Springer, 2014.
- Kai-Min Chung, Daniel Dadush, Feng-Hao Liu and Chris Peikert. *"On the Lattice Smoothing Parameter Problem."* In Computational Complexity Conference (CCC) 2013.
- Feng-Hao Liu and Anna Lysyanskaya. *"Tamper and Leakage Resilience in the Split-State Model."* In Advances in Cryptology – CRYPTO 2012, volume 7417 of Lecture Notes in Computer Science, pages 517-532. Springer, 2012.
- Yun-Ju Huang, Feng-Hao Liu and Bo-Yin Yang. *"Public-Key Cryptography from New Multivariate Quadratic Assumptions."* In Public Key Cryptography – PKC 2012, volume 7293 of Lecture Notes in Computer Science, pages 190-205. Springer, 2012.
- Kai-Min Chung, Yael Tauman Kalai, Feng-Hao Liu and Ran Raz. *"Memory Delegation."* In Advances in Cryptology – CRYPTO 2011, volume 6841 of Lecture Notes in Computer Science, pages 151-168. Springer, 2011.
- Ching-Yua Yu, Kai-Min Chung, Sherman Chow and Feng-Hao Liu. *"Efficient Secure Two-Party Exponentiation."* In Topics in Cryptology – CT-RSA 2011 – The Cryptographers' Track at the RSA Conference 2011, volume 6558 of Lecture Notes in Computer Science, pages 17-32. Springer, 2011.
- Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu and Bo-Yin Yang. *"Efficient String-Commitment from Weak Bit-Commitment."* In Advances in Cryptology - ASIACRYPT 2010, volume 6477 of Lecture Notes in Computer Science, pages 268-282. Springer, 2010.
- Feng-Hao Liu, Anna Lysyanskaya. *"Algorithmic Tamper-Proof Security Under Probing Attacks."* In Security and Cryptography for Networks (SCN) 2010, volume 6280 of Lecture Notes in Computer Science, pages 106-120. Springer, 2010.
- Kai-Min Chung and Feng-Hao Liu. *"Tight Parallel Repetition Theorems for Public-coin Arguments."* In Theoretical Cryptography Conference (TCC) 2010, volume 5978 of Lecture Notes in Computer Science, pages 19-36. Springer, 2010. **(Best Student Paper Award)**
- Feng-Hao Liu, Chi-Jen Lu and Bo-Yin Yang. *"Secure PRNGs from Specialized Polynomial Maps over Any F_q."* In Post-Quantum Cryptography (PQCrypto) 2008, volume 5299 of Lecture Notes in Computer Science, pages 181-202. Springer, 2008 .

INVITED RESEARCH LECTURES

Constant-Round MPC with Fairness and Guarantee of Output Delivery.

- *Florida Atlantic University (CCIS Seminar)* *Sep 2015*
- *Crypto, Santa Barbara, USA* *Aug 2015*

Computation in the Presence of Leakage.

- *United States Naval Academy* *Dec 2014*
- *Virginia Commonwealth University* *Nov 2014*

Locally Decodable and Updatable Non-Malleable Codes and Their Applications.

- *University of Athens, Greece* *July 2014*

Multi-input Functional Encryption.

- *Eurocrypt, Denmark* *May 2014*

Public-Key Cryptography from New Multivariate Quadratic Assumptions.

- *Microsoft Research - Redmond* *Jun 2012*
- *Public Key Cryptography, Darmstadt, Germany* *May 2012*

Delegation in the Cloud.
- *Brown Industrial Partners Program Symposium* *Feb 2012*

Tamper and Leakage Resilience in the Split-State Model.
- *Crypto, Santa Barbara, USA* *Aug 2012*
- *NYU Theory Seminar* *Nov 2011*
- *IBM TJ Watson Crypto Seminar* *Nov 2011*

Efficient String-Commitment from Weak Bit-Commitment.
- *Asiacrypt, Singapore* *Dec 2010*

Algorithmic Tamper-Proof Security Under Probing Attacks.
- *Security and Cryptography for Networks (SCN), Italy* *Sep 2010*

Fully Homomorphic Encryption Using Ideal Lattices.
- *Seminar in Academia Sinica, Taiwan* *July 2009*

TEACHING EXPERIENCE

Guest Lecturer, *Dept. of Computer Science, University of Maryland, MD.*
- Taught guest lectures at *CMSC 414: Computer and Network Security*
- Taught guest lectures at *ENEE459E/CMSC498R: Introduction to Cryptology*
- Taught guest lectures at *ENEE759O/CMSC858T: Cryptography Against Physical Attacks*

Guest Lecturer, *Dept. of Computer Science, Brown U., RI.*
- Taught guest lectures at *CS 0510 Models of Computation* about a survey of advanced topics
- Taught guest lectures at *CS 2590 Advanced Cryptography* about latticed-based cryptographic constructions

Teaching Assistant, *Dept. of Computer Science, Brown U., RI.* Sep 2010 - Dec 2010
- Worked for Prof. John Savage for *CS 0510 Models of Computation*

Teaching Assistant, *Dept. of Computer Science, Brown U., RI.* Sep 2008 - Dec 2008
- Worked for Prof. Eli Upfal for *CS 1550 Probabilistic Methods in Computer Science*

Tutor, *Resource Center, Brown U., RI.* Sep 2007 - Current
- Assisted undergraduate level calculus, statics
- (Voluntarily) assisted graduate level algorithm, randomized algorithm, mathematics in economics

OTHER SELECTED ACTIVITIES

Program Committee Member
- AsiaPKC 2016, PKC 2016, International Workshop on Security in Cloud Computing (Asiaccs-SCC 2014), Information Security Conference (ISC 2014)

Volunteer at Brown Ballroom Competitions, *Brown Ballroom Dance Team* Nov 2011 & 2012
- Processed registration data for the scrutineering system

Moderator at Strait Talk Symposium,*Watson Institute, Brown U., RI.* Oct 2012

- Moderated a discussion panel in the symposium about the topic: "Cyber-security and US-China-Taiwan Relations"

Theory Lunch Organizer, *Dept. of Computer Science, Brown U., RI.* Sep 2009 - Dec 2009

- Voluntarily organized a weekly event theory lunch for the theory group

External Reviewer

- CRYPTO 2009, CHES 2009, TCC 2011, EUROCRYPT 2013, CRYPTO 2013, STOC 2013, TCC 2014, PKC 2014, STOC 2014, ICALP 2014, CRYPTO 2014, EUROCRYPT 2015, TCC 2015, PKC 2015.