

VIET TUNG HOANG

Last update: February 7, 2018

Department of Computer Science
Florida State University
Tallahassee, FL 32306

Email: tvhoang@cs.fsu.edu
Phone: 850-644-2051
Website: <http://www.cs.fsu.edu/~tvhoang/>

CURRENT POSITION

Assistant Professor
Florida State University

8/2016 – Present

EDUCATION

University of California, Davis
Ph.D. in Computer Science
Dissertation: “Foundations of garbled circuits”
Advisor: Prof. Phillip Rogaway

Davis, CA, USA
2008 – 2013

National University of Singapore
First-class honor, B.S. in Computer Engineering

Singapore
2003 – 2007

RESEARCH INTERESTS

Cryptography, programming languages, privacy, and algorithms.

ACADEMIC HONORS

- Publication [7] is invited to Journal of Cryptology as one of the top-ranked papers at CRYPTO 2016.
- Publication [8] is selected for Best Paper Award at CCS 2015.
- Publication [11] is selected for Best Paper Honorable Mention at EUROCRYPT 2015 and invited to Journal of Cryptology.
- Publication [14] is invited to Journal of Cryptology as one of the top-ranked papers at CRYPTO 2013.
- UC Davis Summer Graduate Student Researcher Award, 2010.
- Teaching Assistant of the year, awarded by UC Davis Computer Science Club, 2009.
- NUS Outstanding Undergraduate Researcher Award, 2007.
- Defense Science & Technology Agency Prize for the best student in Undergraduate Research Opportunities Program, 2007.
- Singapore Scholarship, awarded by Singapore Ministry of Foreign Affairs, 2003.

PUBLICATIONS

- Summary: 13 papers in tier-1 crypto conferences (Crypto, Eurocrypt, Asiacrypt)
5 papers in tier-1 security conferences (CCS, S&P)
2 papers in other venues (PKC, STACS)
1. Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. “Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds”, to appear in *EUROCRYPT 2018*.
 2. Mihir Bellare and Viet Tung Hoang. “Identity-Based Format-Preserving Encryption”, *ACM Computer and Communications Security (CCS 2017)*, pp. 1515–1532, 2017.
 3. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. “Information-theoretic Indistinguishability via the Chi-Squared Method”, *Advances in Cryptology — CRYPTO 2017*, pp. 497–523, 2017.
 4. Viet Tung Hoang and Stefano Tessaro. “The Multi-User Security of Double Encryption”, *Advances in Cryptology — EUROCRYPT 2017*, pp. 381–411, 2017.
 5. Viet Tung Hoang, Jonathan Katz, Adam O’Neill, and Mohammad Zaheri. “Selective-Opening Security in the Presence of Randomness Failures”, *Advances in Cryptology — Asiacrypt 2016*, pp. 278–306, 2016.
 6. Mihir Bellare, Viet Tung Hoang, and Stefano Tessaro. “Message-recovery attacks on Feistel-based Format Preserving Encryption”, *ACM Computer and Communications Security (CCS 2016)*, pp. 444–455, 2016.
 7. Viet Tung Hoang and Stefano Tessaro. “Key-alternating Ciphers and Key-length Extension: Exact Bounds and Multi-user Security”, *Advances in Cryptology — CRYPTO 2016*, pp. 3–32, 2016. **Invited to Journal of Cryptology.**
 8. Viet Tung Hoang, Jonathan Katz, and Alex Malozemoff. “Automated analysis and synthesis of authenticated encryption schemes”, *ACM Computer and Communications Security (CCS 2015)*, pp. 84–95, 2015. **Best Paper Award.**
 9. Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway, and Damian Vizár. “Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance”, *Advances in Cryptology — CRYPTO 2015*, pp. 493–517, 2015.
 10. Mihir Bellare and Viet Tung Hoang. “Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model”, *Advances in Cryptology — EUROCRYPT 2015*, pp. 627–656, 2015.
 11. Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. “Robust authenticated-encryption: AEZ and the problem that it solves”, *Advances in Cryptology — EUROCRYPT 2015*, pp. 15–44, 2015. **Best Paper Honorable Mention; Invited to Journal of Cryptology.**
 12. Mihir Bellare and Viet Tung Hoang. “Adaptive witness encryption and asymmetric password-based cryptography”, *Public Key Cryptography — PKC 2015*, pp. 308–331, 2015.
 13. Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi. “Cryptography from compression functions: The UCE bridge to the ROM”, *Advances in Cryptology — CRYPTO 2014*, pp. 169–187, 2014.
 14. Mihir Bellare, Viet Tung Hoang, and Sriram Keelveedhi. “Instantiating random oracles via UCEs”. In *Advances in Cryptology — CRYPTO 2013*, pp. 398–415, 2013. **Invited to Journal of Cryptology.**
 15. Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway. “Efficient garbling from a fixed-key blockcipher”. In *IEEE Symposium of Security and Privacy 2013*, pp. 478–492, 2013.
 16. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. “Adaptive secure garbling with applications to one-time programs and secure outsourcing”. In *Advances in Cryptology — ASIACRYPT 2012*, pp. 134–153, 2012.
 17. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. “Foundations of garbled circuits”. In *ACM Computer and Communications Security (CCS 2012)*, pp. 784–796, 2012.

18. Viet Tung Hoang, Ben Morris, and Phillip Rogaway. “An enciphering scheme based on a card shuffle”. In *Advances in Cryptology — CRYPTO 2012*, pp. 1-13, 2012.
19. Viet Tung Hoang and Phillip Rogaway. “On generalized Feistel networks”. In *Advances in Cryptology — CRYPTO 2010*, pp. 613-630, 2010.
20. Viet Tung Hoang and Wing-Kin Sung. “Improved algorithms for maximum agreement and compatible supertrees”. *Algorithmica*, volume 59, number 2, pp. 195-214, 2011. (Journal version of [21])
21. Viet Tung Hoang and Wing-Kin Sung. “Fixed parameter polynomial time algorithms for maximum agreement and compatible supertrees”. In *Symposium of Theoretical Aspects of Computer Science (STACS 2008)*, pp. 361–372, 2008.

TALKS

1. **Identity-Based Format-Preserving Encryption.**
Conference talk at CCS 2017, Dallas, TX. October 2017.
2. **The Multi-User Security of Double Encryption.**
Conference talk at EUROCRYPT 2017, Paris, France. May 2017.
3. **Key-alternating Ciphers and Key-length Extension: Exact Bounds and Multi-user Security.**
Conference talk at CRYPTO 2016, Santa Barbara, CA, USA. August 2016.
4. **Rethinking cryptographic designs: The case of authenticated encryption.**
 - University of Georgia, Athens, GA, March 2016.
 - North Carolina State University, Raleigh, NC, February 2016.
 - UC Riverside, Riverside, CA, February 2016.
 - Florida State University, Tallahassee, FL, February 2016.
5. **Robust authenticated-encryption: AEZ and the problem that it solves.**
Conference talk at EUROCRYPT 2015, Sofia, Bulgaria. April 2015.
6. **Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model.**
Conference talk at EUROCRYPT 2015, Sofia, Bulgaria. April 2015.
7. **Adaptive witness encryption and asymmetric password-based cryptography.**
Conference talk at PKC 2015, Washington DC. March 2015.
8. **Practice-oriented cryptography: A definition-centric approach.**
 - George Mason University, Fairfax, MD. April 2015.
 - University of Waterloo, Waterloo, Canada. March 2015.
 - Simon Fraser University, Burnaby, Canada. March 2015.
 - Drexel University, Philadelphia, PA. February 2015.
9. **Cryptography from compression functions: The UCE bridge to the ROM.**
Conference talk at CRYPTO 2014, Santa Barbara, CA. August 2014.
10. **Efficient garbling from a fixed-key blockcipher.**
 - Workshop on Applied Multiparty Computation, Microsoft Research Redmond, Seattle, WA. February 2014.
 - Conference talk at IEEE Security & Privacy 2013, San Francisco, CA. May 2013.
11. **Adaptive secure garbling with applications to one-time programs and secure outsourcing.**
Conference talk at ASIACRYPT 2012, Beijing, China. December 2012.

12. **Foundations of garbled circuits.**
Conference talk at ACM CCS 2012, Raleigh, NC. October 2012.
13. **On generalized Feistel networks.**
Conference talk at CRYPTO 2010, Santa Barbara, CA, August 2010.

FUNDING

- “Data insurance in the cluster environment”. PI: Zhi Wang, co-PIs: Viet Tung Hoang, Paul Van Der Mark, and Xin Yuan. **\$590,317**, 2017–2020. NSF CICI 1738912.
- “Revising cryptographic proof techniques for exact security”. PI: Viet Tung Hoang. **\$20,000** for Summer 2017. First Year Assistant Professor Award, Florida State University.

SERVICE

- PC member for IWSEC 2016, ASIACRYPT 2016–2018, CCS 2016, and CRYPTO 2017 & 2018.
- Reviewer for ASIACRYPT 2009, 2013–2015, CRYPTO 2011–2016, TCC 2012, EUROCRYPT 2013, 2016–2018, ICALP 2014, ACM CCS 2014 & 2015, STOC 2015, PKC 2016, IEEE Transactions on Dependable and Secure Computing, Information and Computation, IET Information Security, Design, Codes and Cryptography.

EMPLOYMENT HISTORY

- **Assistant Professor**, Florida State University, 8/2016 – Present
- **Postdoctoral Scholar**, UC Santa Barbara, 2015 – 2016
Host: Prof. Stefano Tessaro
- **Postdoctoral Scholar**, University of Maryland & Georgetown University, 2014 – 2015
Hosts: Prof. Jonathan Katz and Prof. Adam O’Neill.
- **Postdoctoral Scholar**, UC San Diego, 2013 – 2014
Host: Prof. Mihir Bellare.
- **Research Assistant**, UC Davis, 2009 – 2013.
Advisor: Prof. Phillip Rogaway.
- **Research Specialist**, Genome Institute of Singapore, 2007 – 2008.
- **Student Researcher**, NUS, 2006 – 2007.
Advisor: Prof. Wing-Kin Sung.
- **Student Researcher**, NUS, 2005 – 2006.
Advisors: Prof. Akkihebbal Ananda and Prof. Mun-Choon Chan.

TEACHING EXPERIENCE

- **Instructor**. CIS5371: Cryptography, Spring 2018, graduate course at FSU.
- **Instructor**. CIS5930: Special Topics in Cryptography, Spring 2017, graduate course at FSU.
- **Instructor**. COP4531: Complexity and Analysis of Data Structures and Algorithms, Fall 2016 and Fall 2017, undergraduate course at FSU.
- **Teaching Assistant**. ECS189A: Special Topics in Computer Science—Crypto, Spring 2011, undergraduate course at UC Davis.
- **Teaching Assistant**. ECS120: Introduction to Theory of Computation, Spring 2009, undergraduate course at UC Davis.

- **Teaching Assistant.** ECS20: Discrete Mathematics for Computer Science, Fall 2008 & Winter 2009, undergraduate course at UC Davis.
- **Undergraduate Teaching Assistant.** CS1101C: Programming Methodology with C, Fall 2006, undergraduate course at NUS.