VIET TUNG HOANG

Last update: August 14, 2022

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

Associate Professor — 8/2022 – Present
Florida State University

EDUCATION

University of California, Davis — Davis, CA, USA
Ph.D. in Computer Science — 2008 – 2013
Dissertation: "Foundations of garbled circuits"
Advisor: Prof. Phillip Rogaway

National University of Singapore — Singapore
First-class honor, B.S. in Computer Engineering — 2003 – 2007

RESEARCH INTERESTS

Cryptography and algorithms.

ACADEMIC HONORS

- Publication [1] is selected for the Distinguished Paper Award at Usenix Security 2022.
- NSF CAREER Award, 2021.
- Google's gift (under their Patch Rewards Program) for publication [4], 2021.
- Faculty Research Award, given by Department of Computer Science at FSU, 2019.
- Publication [16] is invited to the Journal of Cryptology as one of the top-ranked papers at CRYPTO 2016.
- Publication [17] is selected for the Best Paper Award at CCS 2015.
- Publication [20] is selected for the Best Paper Honorable Mention at EUROCRYPT 2015 and invited to the Journal of Cryptology.
- Publication [23] is invited to the 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.
- NUS Defense Science & Technology Agency Prize for the best student in the Undergraduate Research Opportunities Program, 2007.
- Singapore Scholarship, awarded by Singapore Ministry of Foreign Affairs, 2003.

PUBLICATIONS

- Summary: 17 papers in tier-1 crypto conferences (Crypto, Eurocrypt, Asiacrypt)
  8 papers in tier-1 security conferences (CCS, S&P, Usenix Security)
  4 papers in other venues (PKC, STACS, Cluster, IPDPS)

1. Viet Tung Hoang, Cong Wu, and Xin Yuan."Faster Yet Safer: Logging System Via Fixed-Key Blockcipher", *USENIX Security 2022*, pp. 2389–2406, 2022. **Distinguished Paper Award.**
2. Mihir Bellare and Viet Tung Hoang. "Efficient Schemes for Committing Authenticated Encryption", *EUROCRYPT 2022*, pp. 845–875, 2022.
3. Mehran Sadeghi Lahijani, Abu Naser, Cong Wu, Mohsen Gavahi, Viet Tung Hoang, Zhi Wang, and Xin Yuan. "Efficient Algorithms for Encrypted All-gather Operation", *IEEE International Parallel and Distributed Processing Symposium* (IPDPS 2021), pp. 372–381, 2021.
4. Viet Tung Hoang and Yaobin Shen. "Security of Streaming Encryption in Google's Tink Library", *ACM Computer and Communications Security (CCS 2020)*, pp. 243–262.
5. Viet Tung Hoang and Yaobin Shen. "Security Analysis of NIST CTR-DRBG", *Advances in Cryptology — CRYPTO 2020*, pp. 218–247, 2020.
6. Abu Naser, Mohsen Gavahi, Cong Wu, Viet Tung Hoang, Zhi Wang, and Xin Yuan. "An Empirical Study of Cryptographic Libraries for MPI Communications", *IEEE Cluster 2019*, pp 1–11, 2019.
7. Viet Tung Hoang, David Miller, and Ni Trieu. "Attacks Only Get Better: How to Break FF3 on Large Domains", *Advances in Cryptology — EUROCRYPT 2019*, pp 85–116, 2019.
8. Viet Tung Hoang, Stefano Tessaro, and Aishwarya Thiruvengadam. "The Multi-user Security of GCM, Revisited: Tight Bounds for Nonce Randomization", *ACM Computer and Communications Security (CCS 2018)*, pp. 1429–1440, 2018.
9. Viet Tung Hoang, Stefano Tessaro, and Ni Trieu. "The Curse of Small Domains: New Attacks on Format-Preserving Encryption", *Advances in Cryptology — CRYPTO 2018*, pp. 221–251, 2018.
10. Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. "Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds", *Advances in Cryptology — EUROCRYPT 2018*, pp. 468–499, 2018.
11. Mihir Bellare and Viet Tung Hoang. "Identity-Based Format-Preserving Encryption", *ACM Computer and Communications Security (CCS 2017)*, pp. 1515–1532, 2017.
12. 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.
13. Viet Tung Hoang and Stefano Tessaro. "The Multi-User Security of Double Encryption", *Advances in Cryptology — EUROCRYPT 2017*, pp. 381–411, 2017.
14. 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.
15. 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.
16. 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.**
17. 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.**

18. 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.

19. 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.

20. 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.**

21. Mihir Bellare and Viet Tung Hoang. "Adaptive witness encryption and asymmetric password-based cryptography", *Public Key Cryptography — PKC 2015*, pp. 308–331, 2015.

22. 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.

23. 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.**

24. 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.

25. 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.

26. Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. "Foundations of garbled circuits". In *ACM Computer and Communications Security (CCS 2012)*, pp. 784–796, 2012.

27. 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.

28. Viet Tung Hoang and Phillip Rogaway. "On generalized Feistel networks". In *Advances in Cryptology — CRYPTO 2010*, pp. 613-630, 2010.

29. 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 [30])

30. 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. **Faster Yet Safer: Logging System Via Fixed-Key Blockcipher.**
   Conference talk at Usenix Security 2022, Boston, MA. August 2022.

2. **Efficient Schemes for Committing Authenticated Encryption.**
   Conference talk at EURORYPT 2022. Virtual. May 2022.

3. **Security of Streaming Encryption in Google's Tink Library.**
   Conference talk at CCS 2020, Virtual. November 2020.

4. **Security Analysis of NIST CTR-DRBG.**
   Conference talk at CRYPTO 2020, Virtual. August 2020.

5. **Attacks Only Get Better: How to Break FF3 on Large Domains.**
   Conference talk at EUROCRYPT 2019, Darmstadt, Germany. May 2019.

6. **The Curse of Small Domains: New Attacks on Format-Preserving Encryption.**
   Conference talk at CRYPTO 2018, Santa Barbara, CA. August 2018.

7. **Identity-Based Format-Preserving Encryption.**
   Conference talk at CCS 2017, Dallas, TX. October 2017.
8. **The Multi-User Security of Double Encryption.**
   Conference talk at EUROCRYPT 2017, Paris, France. May 2017.
9. **Key-alternating Ciphers and Key-length Extension: Exact Bounds and Multi-user Security.**
   Conference talk at CRYPTO 2016, Santa Barbara, CA. August 2016.
10. **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.
11. **Robust authenticated-encryption: AEZ and the problem that it solves**.
    Conference talk at EUROCRYPT 2015, Sofia, Bulgaria. April 2015.
12. **Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model**.
    Conference talk at EUROCRYPT 2015, Sofia, Bulgaria. April 2015.
13. **Adaptive witness encryption and asymmetric password-based cryptography**.
    Conference talk at PKC 2015, Washington DC. March 2015.
14. **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.
15. **Cryptography from compression functions: The UCE bridge to the ROM**.
    Conference talk at CRYPTO 2014, Santa Barbara, CA. August 2014.
16. **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 Fracisco, CA. May 2013.
17. **Adaptive secure garbling with applications to one-time programs and secure outsourcing**.
    Conference talk at ASIACRYPT 2012, Beijing, China. December 2012.
18. **Foundations of garbled circuits**.
    Conference talk at ACM CCS 2012, Raleigh, NC. October 2012.
19. **On generalized Feistel networks**.
    Conference talk at CRYPTO 2010, Santa Barbara, CA, August 2010.

FUNDING

- "New Analytic Frontiers for Symmetric Cryptography", PI: Viet Tung Hoang. **$563,971**, 2021–2026. NSF CNS 2046540 (CAREER).
- Google's gift (Patch Rewards Program), **$10,000**, 2021.
- "Towards Stronger and Verified Security for Real-World Cryptography". PI: Viet Tung Hoang. **$174,469**, 2018–2022. NSF CRII 1755539.
- "Data insurance in the cluster environment". PI: Zhi Wang, co-PIs: Viet Tung Hoang, Paul Van Der Mark, and Xin Yuan. **$590,317**, 2017–2021. 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, 2017, 2018, 2022), CCS 2016, CRYPTO (2017, 2018, 2021, 2022), EUROCRYPT 2023, and INDOCRYPT 2018.
- Reviewer for Journal of Cryptology, IEEE Transactions on Dependable and Secure Computing, Information and Computation, IET Information Security, Design, Codes and Cryptography.
- Reviewer and panelist for the National Science Foundation (NSF).
- External reviewer for the Austrian Science Fund (FWF).

INDUSTRIAL RELATIONS

- Consultant for Google and Comforte AG.

EMPLOYMENT HISTORY

- **Associate Professor**, Florida State University, 8/2022 – Present
- **Assistant Professor**, Florida State University, 8/2016 – 7/2022
- **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.** CIS4930: Special Topics in Computer Science—Problem Solving, Spring 2022 & Fall 2022, undergraduate course at FSU.
- **Instructor.** CIS4930: Special Topics in Computer Science—Introduction to Cryptography, Spring 2021, undergraduate course at FSU.
- **Instructor.** COT5507: Analytic Methods in Computer Science, Fall 2018 and Spring 2020, graduate course at FSU.
- **Instructor.** CIS5371: Cryptography, various years, graduate course at FSU.
- **Instructor.** CIS5930: Special Topics in Computer Science—Cryptography, Spring 2017, graduate course at FSU.
- **Instructor.** COP4531: Complexity and Analysis of Data Structures and Algorithms, various years, undergraduate course at FSU.
- **Teaching Assistant.** ECS189A: Special Topics in Computer Science—Cryptography, 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.

ADVISING

- Cong Wu (Ph.D. student, 2018 – current)
- Yaobin Shen (visiting Ph.D. student from Shanghai Jiaotong University, 2019–2020) → Postdoc at Catholic University of Louvain.