KARTIK NAYAK

kartik@cs.duke.edu http://www.users.cs.duke.edu/~kartik/ +1 (301) 547 9741

(Last updated: May 17, 2020)

EDUCATION

University of Maryland — College Park, Maryland
Ph.D., Computer Science — August, 2018
Advisors: Jonathan Katz, Elaine Shi
Thesis Title: Efficient Data Oblivious Computation

University of Maryland — College Park, Maryland
M.S., Computer Science — December, 2016
GPA: 3.94 out of 4

Veermata Jijabai Technological Institute — Mumbai, India
B.Tech, Computer Science — May, 2011
GPA: 9.8 out of 10

PROFESSIONAL POSITIONS

Duke University, Assistant Professor — Durham, NC | July 2019 - Present
VMware Research, Postdoctoral Researcher — Palo Alto, CA | July 2018 - August 2019
Microsoft Research, Research Intern — Cambridge, UK | June 2017 - August 2017
VMware Research, Research Intern — Palo Alto, CA | June 2016 - August 2016
Microsoft Research, Research Intern — Bangalore, India | June 2015 - August 2015
Technicolor Research, Research Intern — Los Altos, CA | May 2014 - August 2014
Google, Software Engineer — Bangalore, India | July 2011 - May 2013

PUBLICATIONS

Peer-Reviewed Conferences

1. **On the Optimality of Optimistic Responsiveness**[*]
   Published in ACM Computer and Communication Security (CCS) 2020
   Ittai Abraham, *Kartik Nayak*, Ling Ren, Nibesh Shrestha

2. **Optimal Good-case Latency for Byzantine Broadcast and State Machine Replication**[*]
   Brief Announcement, International Symposium on Distributed Computing (DISC) 2020
   Ittai Abraham, *Kartik Nayak*, Ling Ren, and Zhuolun Xiang

3. **Improved Extension Protocols for Byzantine Broadcast and Agreement**[*]
   Accepted in International Symposium on Distributed Computing (DISC) 2020
   Kartik Nayak, Ling Ren, Elaine Shi, Nitin H. Vaidya, and Zhuolun Xiang

4. **OptORAMa: Optimal Oblivious RAM**[*]
   Published in Eurocrypt 2020
   Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, *Kartik Nayak*, Enoch Peserico, and Elaine Shi

5. **Sync HotStuff: Simple and Practical State Machine Replication**[*]
   Published in IEEE Security and Privacy (S&P) 2020
   Ittai Abraham, Dahlia Malkhi, *Kartik Nayak*, Ling Ren, and Maofan Yin

[*]Authors listed in alphabetical order.

6. **Bucket Sort: A Simple Oblivious Sort***
   Published in Symposium on Simplicity in Algorithms (SOSA) 2020
   Gilad Asharov, T-H. Hubert Chan, *Kartik Nayak*, Rafael Pass, Ling Ren, and Elaine Shi

7. **Flexible Byzantine Fault Tolerance***
   Published in ACM Computer and Communication Security (CCS) 2019
   Dahlia Malkhi, *Kartik Nayak*, and Ling Ren

8. **Communication Complexity of Byzantine Agreement, Revisited***
   Published in Principles of Distributed Computing (PODC) 2019
   Ittai Abraham, T-H. Hubert Chan, Danny Dolev, *Kartik Nayak*, Rafael Pass, Ling Ren, and Elaine Shi

9. **Locality-Preserving Oblivious RAM***
   Published in Eurocrypt 2019
   Gilad Asharov, T-H. Hubert Chan, *Kartik Nayak*, Rafael Pass, Ling Ren, and Elaine Shi

10. **Synchronous Byzantine Agreement with Expected $O(1)$ Rounds, Expected $O(n^2)$ Communication, and Optimal Resilience***
    Published in Financial Cryptography and Data Security (FC) 2019
    Ittai Abraham, Srinivas Devadas, Danny Dolev, *Kartik Nayak*, and Ling Ren

11. **More is Less: Perfectly Secure Oblivious Algorithms in the Multi-Server Setting***
    Published in Asiacrypt 2018
    T-H. Hubert Chan, Jonathan Katz, *Kartik Nayak*, Antigoni Polychroniadou, and Elaine Shi

12. **Perfectly Secure Oblivious Parallel RAM***
    Published in Theory of Cryptography Conference (TCC) 2018
    T-H. Hubert Chan, *Kartik Nayak*, and Elaine Shi

13. **Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus***
    Published in Conference on Principles of Distributed Systems (OPODIS) 2017
    Ittai Abraham, Dahlia Malkhi, *Kartik Nayak*, Ling Ren, and Alexander Spiegelman

14. **Asymptotically Tight Bounds for Composing ORAM with PIR***
    Published in Conference on Practice and Theory of Public Key Cryptography (PKC) 2017
    Ittai Abraham, Christopher W. Fletcher, *Kartik Nayak*, Benny Pinkas, and Ling Ren

15. **HOP: Hardware makes Obfuscation Practical**
    Published in Network and Distributed System Security (NDSS) 2017
    Kartik Nayak, Christopher W. Fletcher, Ling Ren, Nishanth Chandran, Satya Lokam, Elaine Shi, and Vipul Goyal

16. **Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack**
    Published in IEEE European Symposium on Security and Privacy (Euro S&P) 2016
    Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi

17. **Helping Johny Encrypt: Toward Semantic Interfaces for Cryptographic Frameworks**
    Published in ACM Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software (Onward!) 2016
    Soumya Indela, Mukul Kulkarni, *Kartik Nayak* and Tudor Dumitras

18. **GraphSC: Parallel Secure Computation Made Easy**
    Published in IEEE Symposium on Security and Privacy (S&P) 2015
    Kartik Nayak, Xiao Shaun Wang, Stratis Ioannidis, Udi Weinsberg, Nina Taft, and Elaine Shi

19. **ObliVM: A Programming Framework for Secure Computation**
    Published in IEEE Symposium on Security and Privacy (S&P) 2015

Chang Liu, Xiao Shaun Wang, *Kartik Nayak*, Yan Huang, and Elaine Shi

20. **Oblivious Data Structures**
    Published in ACM Conference on Computer and Communications Security (CCS) 2014
    Xiao Shaun Wang, *Kartik Nayak*, Chang Liu, T-H Hubert Chan, Elaine Shi, Emil Stefanov, and Yan Huang

21. **Some Vulnerabilities are Different than Others**
    Published in Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2014
    Kartik Nayak, Daniel Marino, Petros Efstathopoulos, and Tudor Dumitras

Manuscripts

1. **Optimal Good-case Latency for Byzantine Broadcast and State Machine Replication***
   In Submission
   Ittai Abraham, *Kartik Nayak*, Ling Ren, Zhuolun Xiang

2. **Perfectly Secure OPRAM with $O(\log^3 N/\log\log N)$ Overhead*** In Submission
   T-H. Hubert Chan, Wei-Kai Lin, *Kartik Nayak*, and Elaine Shi

3. **Communication Complexity of Byzantine Agreement, Revisited*** In Submission
   Ittai Abraham, T-H. Hubert Chan, Danny Dolev, *Kartik Nayak*, Rafael Pass, Ling Ren, and Elaine Shi

4. **Dfinity Consensus, Explored*** Tech Report
   Ittai Abraham, Dahlia Malkhi, *Kartik Nayak*, and Ling Ren

5. **An Oblivious Parallel RAM with $O(\log^2 N)$ Parallel Runtime Blowup** Tech Report
   Kartik Nayak and Jonathan Katz

AWARDS

2016 Received **Google Ph.D. fellowship in Privacy and Security**
2015 ObliVM won NYU Polytechnic School of Engg's **CSAW Best Applied Security Paper Award** **HLI Award** for Secure Multiparty Computing at the iDash Secure Genome Analysis Competition
2014 Oblivious Data Structures selected in top ten finalists for NYU Polytechnic School of Engineering's **CSAW Best Applied Security Paper Award**
2013 Awarded **Dean's fellowship** at University of Maryland, College Park
2011 Awarded V.J.T.I. **Gold Medal** for obtaining highest GPA among all undergraduate programs
2010 Ranked 18 in Asia Regional Finals of ACM-ICPC at Amritapuri, India
2009 Ranked 24 in Asia Regional Finals of ACM-ICPC at Amritapuri, India

TALKS AND POSTERS

1. **Sync HotStuff: Simple and Practical State Machine Replication System**
   Allerton 2019, Allerton Park, UIUC, IL (09/27/2019)

2. **Communication Complexity of Byzantine Agreement, Revisited**
   Indian Institute of Science (IISc), Bangalore, India, (01/09/2020)

3. **Flexible Byzantine Fault Tolerance**

   (a) Microsoft Research, Bangalore, India, (01/08/2020)

   (b) Indian Institute of Technology, Bombay, India (01/13/2020)

   (c) ACM Computer and Communication Security 2019 (CCS), (11/13/2019)

(d) Simons Workshop on Large-Scale Consensus and Blockchains, (10/23/2019)

(e) Triangle Area Privacy and Security (TAPS), (10/18/2019)

(f) Stanford University, California, USA, (07/23/2019)

4. **Synchronous Byzantine Agreement with Expected $O(1)$ Rounds, Expected $O(n^2)$ Communication, and Optimal Resilience**

   (a) Blockchain Winter School, Shenzhen, China, (12/12/2017)

   (b) Oasis Labs, Berkeley, (08/08/2018)

   (c) Financial Cryptography and Data Security, St. Kitts, (02/19/2019)

5. **Perfectly Secure Oblivious Parallel RAM**
   Theory of Cryptography Conference, Goa, India, (11/14/2018)

6. **More is Less: Perfectly Secure Oblivious Algorithms in the Multi-Server Setting**
   Asiacrypt, Brisbane, Australia, (12/05/2018)

7. **Coco: Confidential Consortium Blockchains**
   Short talk, Blockchain Winter School, Shenzhen, China, (12/11/2017)

8. **HOP: Hardware Makes Obfuscation Practical**

   (a) Network and Distributed System Security 2017 (NDSS), (02/28/17)

   (b) DC Area Privacy and Security (DCAPS) seminar, (02/17/17)

   (c) DIMACS Workshop on Cryptography for RAM Model of Computation, (06/08/2016)

9. **Asymptotically Tight Bounds For Composing ORAMs with PIR**

   (a) Conference on Practice and Theory of Public-Key Cryptography 2017 (PKC), (03/29/2017)

   (b) Microsoft Research, Cambridge, UK, (06/08/2017)

   (c) Microsoft Research, Bangalore, India, (01/06/2017)

10. **Oblivious RAM**
    Google Research, NYC, (10/24/2016)

11. **Stubborn Mining: Generalizing Selfish Mining and Composing with an Eclipse Attack**

    (a) European Symposium on Security and Privacy 2016 (Euro S&P), (03/23/2016)

    (b) Guest Lecture for CS795: Blockchain Technologies, George Mason University, (03/20/2016)

12. **GraphSC: Parallel Secure Computation Made Easy**

    (a) IEEE Security and Privacy 2015 (S&P), (05/19/2015)

    (b) DC Area Privacy and Security Seminar (DCAPS), (11/17/2014)

13. **Oblivious Data Structures**

    (a) ACM Computer and Communication Security 2014 (CCS), (11/04/2014)

    (b) Rump session talk at Crypto 2014, (08/19/2014)

    (c) Poster at IEEE Security and Privacy 2014 (S&P), (05/19/2014)

14. **Some Vulnerabilities are Different than Others**

    (a) Research in Attacks, Intrusions and Defenses 2014 (RAID), (09/18/2014)

(b) Poster at IEEE Security and Privacy 2014 (S&P), (05/19/2014)

(c) Short talk at IEEE Security and Privacy 2014 (S&P), (05/19/2014)

(d) Poster at RAID 2014, (09/18/2014)

TEACHING

Guest Lecture CS 380D: Distributed Systems, UT Austin - Spring 2020

CS590-04: Consensus Protocols in Distributed Computing and Blockchains, Duke University - Fall 2019

Guest Lecture CS294-151: Blockchain and CryptoEconomics, UC Berkeley - Fall 2018

Guest Lecture CS590.01: Privacy and Fairness in Data Science, Duke University - Fall 2018

Guest Lecture CS795: Blockchain Technologies, George Mason University - Spring 2016

Teaching Assistant CMSC351 - Introduction to Algorithms, University of Maryland - Fall 2013

Teaching Assistant CMSC414 - Computer and Network Security, University of Maryland - Spring 2014, Fall 2014, Fall 2015

SERVICE

Organizing Activities

Co-organized Triangle Area Privacy and Security (TAPS), (10/18/2019)

Program Committees and Panels

PC Member, International Conference on Financial Cryptography and Data Security (FC), 2021

PC Member, Proceedings on Privacy Enhancing Technologies (PoPETS), 2021

PC Member, Theory and Application of Cryptology and Information Security (Asiacrypt), 2020

PC Member, Principles of Distributed Computing (PODC), 2020

PC Member, ACM Computer and Communication Security (CCS), 2020

PC Member, Symposium on Foundations and Applications of Blockchain (FAB), 2020

PC Member, Proceedings on Privacy Enhancing Technologies (PoPETS), 2020

PC Member, Theory and Application of Cryptology and Information Security (Asiacrypt), 2019

PC Member, ACM CCS Privacy Preserving Machine Learning, 2019

PC Member, Information Security Conference (ISC), 2019

PC Member, Foundations of Computer Security (FCS), 2019

Panel Member, IEEE Symposium on Privacy-Aware Computing (PAC), 2018

PC Member, Military Communication (MILCOM), 2016-17

Reviewer

Journal of Cryptology, 2018

IEEE Transactions on dependable and secure computing, 2018

European Economic Review, 2018

IEEE Computer Architecture Letters, 2017

Journal of Computer and System Sciences, 2014

Department and University Service

Member, Faculty Search Committee, Duke CS, 2019-2020

Member, Strategic Planning Committee, Duke CS, 2019-2020

Member, Research Initiation Project Committee for Chenghong Wang (2019)

Member, Master of Science Thesis Defense Committee for Shujun Qi (2020)

Member, Master of Science Project Defense Committee for Kehan Lyu (2020)