CHARALAMPOS (BABIS) PAPAMANTHOU

CURRICULUM VITAE

July 31, 2018

3409 A.V. WILLIAMS BUILDING
UNIVERSITY OF MARYLAND, COLLEGE PARK
COLLEGE PARK MD 20742

OFFICE PHONE: 301-405-7212
WEB: http://www.ece.umd.edu/~cpap/
EMAIL: cpap@umd.edu

RESEARCH INTERESTS

Computer Security and Applied Cryptography; Design and Analysis of Algorithms.

PROFESSIONAL APPOINTMENTS

- **UNIVERSITY OF MARYLAND, COLLEGE PARK**, COLLEGE PARK MD, USA 08/13-present
  Assistant professor
  Department of Electrical and Computer Engineering *and* Institute for Advanced Computer Studies
  Department of Computer Science (affiliate position)
- **UNIVERSITY OF CALIFORNIA, BERKELEY**, BERKELEY CA, USA 07/11-07/13
  Postdoctoral researcher
  Department of Electrical Engineering and Computer Sciences (mentor: Dawn Song)

EDUCATION

- **BROWN UNIVERSITY**, PROVIDENCE RI, USA
  - PH.D., COMPUTER SCIENCE 05/11
    Dissertation: *Cryptography for Efficiency: New Directions in Authenticated Data Structures* [62]
    Advisor: Roberto Tamassia
  - M.SC., COMPUTER SCIENCE 05/07
    Thesis topic: *Localization in Sensor Networks* [53]
    Advisors: Franco P. Preparata and Roberto Tamassia
- **UNIVERSITY OF CRETE**, HERAKLION, GREECE
  - M.SC., COMPUTER SCIENCE 07/05
    Thesis topic: *Parameterized st-Orientations of Graphs* [63]
    Advisor: Ioannis G. Tollis
- **UNIVERSITY OF MACEDONIA**, THESSALONIKI, GREECE
  - B.SC., APPLIED INFORMATICS 09/03
    Thesis topic: *Implementation and Computational Study of Network Algorithms* [64]
    Advisor: Konstantinos Paparrizos

INTERNSHIPS

- **MICROSOFT RESEARCH**, REDMOND WA, USA (mentor: Seny Kamara) 06/10-08/10
- **INTEL RESEARCH**, BERKELEY CA, USA (mentor: Petros Maniatis) 06/08-08/08

AWARDS

- National Science Foundation CAREER Award, 2017.
- NetApp Faculty Fellowship, 2016.
- Google Faculty Research Award, 2015.
- Yahoo! Faculty Research and Engagement Program Fellowship, 2015.
- George Corcoran Award for Teaching, University of Maryland, 2015.
- Jimmy Lin Award for Invention, University of Maryland, 2014.
- Invention of the Year Award (one of 3 winners out of 154 disclosures), University of Maryland, 2013.
- van Dam Fellowship, Brown University, 2009.
- Kanellakis Fellowship, Brown University, 2008 and 2010.

PUBLICATIONS

Refereed journals*

[1] **Yupeng Zhang**, Charalampos Papamanthou, and Jonathan Katz. Verifiable graph processing. *ACM Transactions on Privacy and Security (**TOPS**)*, 2018.

[2] Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin. Oblivious network RAM. *Journal of Cryptology (**JoC**)*, 2018.

[3] Daniel Genkin, Dimitrios Papadopoulos, and Charalampos Papamanthou. Privacy in decentralized cryptocurrencies. *Communications of the ACM (**CACM**)*, 61(6):78–88, 2018.

[4] **Ioannis Demertzis**, Stavros Papadopoulos, Odysseas Papapetrou, Antonis Deligiannakis, Minos Garofalakis, and Charalampos Papamanthou. Practical private range search in depth. *ACM Transactions on Database Systems (**TODS**)*, 43(1):2–52, 2018.

[5] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables based on cryptographic accumulators. *Algorithmica (**Algorithmica**)*, 70(4):664–712, 2016.

[6] C. Christopher Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. Dynamic provable data possession. *ACM Transactions on Information and System Security (**TISSEC**)*, 17(4), 2015.

[7] Charalampos Papamanthou, Konstantinos Paparrizos, Nikolaos Samaras, and Angelo Sifaleras. On the initialization methods of an exterior point algorithm for the assignment problem. *International Journal of Computer Mathematics (**Int. J. Comput. Math.**)*, 87(8):1831–1846, 2010.

[8] Charalampos Papamanthou and Ioannis G. Tollis. Applications of parameterized st-orientations. *Journal of Graph Algorithms and Applications (**J. Graph Algorithms Appl.**)*, 14(2):337–365, 2010.

[9] Claire Mathieu and Charalampos Papamanthou. Distortion lower bounds for line embeddings. *Information Processing Letters (**Inform. Process. Lett.**)*, 108(4):175–178, 2008.

[10] Charalampos Papamanthou and Ioannis G. Tollis. Algorithms for computing a parameterized st-orientation. *Theoretical Computer Science (**Theoret. Comput. Sci.**)*, 408:224–240, 2008.

*Papamanthou's PhD students at Maryland are shown in bold.

[11] Charalampos Papamanthou, Konstantinos Paparrizos, Nikolaos Samaras, and Konstantinos Stergiou. Worst case examples of an exterior point algorithm for the assignment problem. *Discrete Optimization (**Discrete Optim.**)*, 5(3):605–614, 2008.

[12] Charalampos Papamanthou, Konstantinos Paparrizos, and Nikolaos Samaras. A parametric visualization software for the assignment problem. *Yugoslav Journal of Operations Research (**Yugosl. J. Oper. Res.**)*, 15(1):147–158, 2005.

[13] Charalampos Papamanthou, Konstantinos Paparrizos, and Nikolaos Samaras. Computational experience with exterior point algorithms for the transportation problem. *Journal of Applied Mathematics and Computation (**Appl. Math. Comput.**)*, 158:459–475, 2004.

Refereed conferences

[14] Evgenios Kornaropoulos, Charalampos Papamanthou, and Roberto Tamassia. Data recovery on encrypted databases with k-nearest neighbor query leakage. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, San Francisco CA, USA, 2019.

[15] Javad Ghareh Chamani, Dimitrios Papadopoulos, Charalampos Papamanthou, and Rasool Jalili. New constructions for forward and backward private symmetric searchable encryption. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Toronto, Canada, 2018. *Acceptance rate:* 16.6%.

[16] **Ioannis Demertzis**, Dimitrios Papadopoulos, and Charalampos Papamanthou. Searchable encryption with optimal locality: Achieving sublogarithmic read efficiency. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Lecture Notes in Computer Science (LNCS), Santa Barbara CA, USA, 2018. *Acceptance rate: %*.

[17] **Ahmed Kosba**, Charalampos Papamanthou, and Elaine Shi. xJsnark: A framework for efficient verifiable computation. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, pages 543–560, San Francisco CA, USA, 2018. *Acceptance rate:* 11%.

[18] **Yupeng Zhang**, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou. vRAM: Faster verifiable RAM with program-independent preprocessing. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, pages 202–220, San Francisco CA, USA, 2018. *Acceptance rate:* 11%.

[19] Lluis Vilanova, Casen Hunger, Charalampos Papamanthou, Yoav Etsion, and Mohit Tiwari. DATS: Refactoring access control out of web applications. In *Proc. ACM Int. Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**)*, pages 722–736, Wiliamsburg VA, USA, 2018. *Acceptance rate:* 17%.

[20] Mohammad Etemad, Alptekin Küpçü, Charalampos Papamanthou, and David Evans. Efficient dynamic searchable encryption with forward privacy. In *Proc. Privacy Enhancing Technologies (**PETS**)*, pages 5–20, Barcelona, Spain, 2018. *Acceptance rate:* 16%.

[21] Wei Bai, **Ciara Lynton**, Michelle L. Mazurek, and Charalampos Papamanthou. Understanding user tradeoffs for search in encrypted communication. In *Proc. IEEE European Symposium on Security and Privacy (**EUROSSP**)*, page 1, London, UK, 2018. *Acceptance rate:* 23%.

[22] **Ioannis Demertzis**, **Rajdeep Talapatra**, and Charalampos Papamanthou. Efficient searchable encryption through compression. In *Proc. Very Large Databases (**VLDB**)*, Rio de Janeiro, Brasil, 2018. *Acceptance rate: %*.

[23] **Yupeng Zhang**, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou. vSQL: Verifying arbitrary SQL queries over dynamic outsourced databases. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, pages 863–880, San Jose CA, USA, 2017. *Acceptance rate:* 14%.

[24] **Ioannis Demertzis** and Charalampos Papamanthou. Fast searchable encryption with tunable locality. In *Proc. ACM Int. Conference on Management of Data (**SIGMOD**)*, pages 1053–1067, Chicago IL, USA, 2017. *Acceptance rate:* 19%.

[25] **Yupeng Zhang**, Jonathan Katz, and Charalampos Papamanthou. An expressive (zero-knowledge) set accumulator. In *Proc. IEEE European Symposium on Security and Privacy (**EUROSSP**)*, pages 158–173, Paris, France, 2017. *Acceptance rate:* 19%.

[26] Giuseppe Ateniese, Michael T. Goodrich, Vasilis Lekakis, Charalampos Papamanthou, Evripidis Paraskevas, and Roberto Tamassia. Accountable storage. In *Proc. Applied Cryptography and Network Security (**ACNS**)*, volume 10355 of *Lecture Notes in Computer Science (LNCS)*, pages 623–644, Kanazawa, Japan, 2017. *Acceptance rate:* 22.82%.

[27] Sanjam Garg, Payman Mohassel, and Charalampos Papamanthou. TWORAM: Efficient oblivious RAM in two rounds with applications to searchable encryption. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, volume 9816 of *Lecture Notes in Computer Science (LNCS)*, pages 563–592, Santa Barbara CA, USA, 2016. *Acceptance rate:* 25%.

[28] **Yupeng Zhang**, Jonathan Katz, and Charalampos Papamanthou. All your queries are belong to us: The power of file-injection attacks on searchable encryption. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, pages 707–720, Austin TX, USA, 2016. *Acceptance rate:* 16%.

[29] **Ahmed Kosba**, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, pages 839–858, 2016. *Acceptance rate:* 14%.

[30] Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin. Oblivious network RAM and leveraging parallelism to achieve obliviousness. In *Proc. Int. Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**)*, volume 9452 of *Lecture Notes in Computer Science (LNCS)*, pages 121–132, Auckland, New Zealand, 2015. *Acceptance rate:* 25.5%.

[31] **Yupeng Zhang**, Jonathan Katz, and Charalampos Papamanthou. IntegriDB: Verifiable SQL for outsourced databases. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 1480–1491, Denver CO, USA, 2015. *Acceptance rate:* 19%.

[32] Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Practical authenticated pattern matching with optimal proof size. In *Proc. Very Large Databases (**VLDB**)*, pages 750–761, Kohala Coast HI, USA, 2015. *Acceptance rate:* 21%.

[33] T-H. Hubert Chan, Charalampos Papamanthou, and Zhichao Zhao. On the complexity of the minimum independent set partition problem. In *Proc. Int. Computing and Combinatorics Conference (**COCOON**)*, volume 9198 of *Lecture Notes in Computer Science (LNCS)*, pages 121–132, Beijing, China, 2015. *Acceptance rate:* 45%.

[34] **Yupeng Zhang**, Charalampos Papamanthou, and Jonathan Katz. ALITHEIA: Towards practical verifiable graph processing. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 856–867, Scottsdale AZ, USA, 2014. *Acceptance rate:* 19%.

[35] Yi Qian, **Yupeng Zhang**, Xi Chen, and Charalampos Papamanthou. Streaming authenticated data structures: Abstraction and implementation. In *Proc. ACM Int. Workshop on Cloud Computing Security (**CCSW**)*, pages 920–931, Scottsdale AZ, USA, 2014. *Acceptance rate:* 33%.

[36] **Ahmed E. Kosba**, Dimitrios Papadopoulos, Charalampos Papamanthou, Mahmoud F. Sayed, Elaine Shi, and Nikos Triandopoulos. TRUESET: Faster verifiable set computations. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, pages 765–780, San Diego CA, USA, 2014. *Acceptance rate:* 19%.

[37] Emil Stefanov, Charalampos Papamanthou, and Elaine Shi. Practical dynamic searchable encryption with small leakage. In *Proc. Int. Network and Distributed System Security Symposium (**NDSS**)*, San Diego CA, USA, 2014. *Acceptance rate:* 18%.

[38] Elaine Shi, Emil Stefanov, and Charalampos Papamanthou. Practical dynamic proofs of retrievability. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 325–336, Berlin, Germany, 2013. *Acceptance rate:* 19%.

[39] Charalampos Papamanthou, Elaine Shi, Roberto Tamassia, and Ke Yi. Streaming authenticated data structures. In *Proc. Int. Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT**)*, volume 7881 of *Lecture Notes in Computer Science (LNCS)*, pages 353–370, Athens, Greece, 2013. *Acceptance rate:* 20%.

[40] Seny Kamara and Charalampos Papamanthou. Parallel and dynamic searchable symmetric encryption. In *Proc. Int. Financial Cryptography and Data Security Conference (**FC**)*, volume 7859 of *Lecture Notes in Computer Science (LNCS)*, pages 258–274, Okinawa, Japan, 2013. *Acceptance rate:* 20%.

[41] Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia. Signatures of correct computation. In *Proc. Int. Theory of Cryptography Conference (**TCC**)*, volume 7785 of *Lecture Notes in Computer Science (LNCS)*, pages 222–242, Tokyo, Japan, 2013. *Acceptance rate:* 37%.

[42] Prateek Mittal, Charalampos Papamanthou, and Dawn Song. Preserving link privacy in social network-based systems. In *Proc. Int. Network and Distributed System Security Symposium (**NDSS**)*, San Diego CA, USA, 2013. *Acceptance rate:* 18.8%.

[43] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 965–976, Raleigh NC, USA, 2012. *Acceptance rate:* 18.9%.

[44] Michael T. Goodrich, Duy Nguyen, Olga Ohrimenko, Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos, and Cristina Videira Lopes. Efficient verification of web-content searching through authenticated web crawlers. In *Proc. Very Large Databases (**VLDB**)*, pages 920–931, Istanbul, Turkey, 2012. *Acceptance rate:* 20.3%.

[45] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal verification of operations on dynamic sets. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, volume 6841 of *Lecture Notes in Computer Science (LNCS)*, pages 91–110, Santa Barbara CA, USA, 2011. *Acceptance rate:* 18%.

[46] Petros Maniatis, Michael Dietz, and Charalampos Papamanthou. MOMMIE knows best: Systematic optimizations for verifiable distributed algorithms. In *Proc. ACM Int. Workshop on Hot Topics in Operating Systems (**HOTOS**)*, Napa CA, USA, 2011. *Acceptance rate:* not available.

[47] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal authenticated data structures with multilinear forms. In *Proc. Int. Conference on Pairing-Based Cryptography (**PAIRING**)*, volume 6487 of *Lecture Notes in Computer Science (LNCS)*, pages 246–264, Ishikawa, Japan, 2010. *Acceptance rate:* not available.

[48] C. Christopher Erway, Alptekin Küpçü, Charalampos Papamanthou, and Roberto Tamassia. Dynamic provable data possession. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 213–222, Chicago IL, USA, 2009. *Acceptance rate:* 18.4%.

[49] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, pages 437–448, Alexandria VA, USA, 2008. *Acceptance rate:* 18.1%.

[50] Michael T. Goodrich, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Athos: Efficient authentication of outsourced file systems. In *Proc. Int. Information Security Conference (**ISC**)*, volume 5222 of *Lecture Notes in Computer Science (LNCS)*, pages 80–96, Taipei, Taiwan, 2008. *Acceptance rate:* 23%.

[51] Alexander Heitzmann, Bernardo Palazzi, Charalampos Papamanthou, and Roberto Tamassia. Efficient integrity checking of untrusted network storage. In *Proc. ACM Int. CCS Workshop on Storage Security and Survivability (**STORAGESS**)*, pages 43–54, Alexandria VA, USA, 2008. *Acceptance rate:* not available.

[52] Alexander Heitzmann, Bernardo Palazzi, Charalampos Papamanthou, and Roberto Tamassia. Effective visualization of file system access-control. In *Proc. IEEE Int. Workshop on Security Visualization (**VIZSEC**)*, volume 5210 of *Lecture Notes in Computer Science (LNCS)*, pages 18–25, Boston MA, USA, 2008. *Acceptance rate:* 67%.

[53] Charalampos Papamanthou, Franco P. Preparata, and Roberto Tamassia. Algorithms for location estimation based on RSSI sampling. In *Proc. Int. ICALP Workshop on Algorithms for Sensor Networks (**ALGOSENSORS**)*, volume 5389 of *Lecture Notes in Computer Science (LNCS)*, pages 72–86, Reykjavik, Iceland, 2008. *Acceptance rate:* 40%.

[54] Roberto Tamassia, Bernardo Palazzi, and Charalampos Papamanthou. Graph drawing for security visualization. In *Proc. Int. Conference on Graph Drawing (**GD**)*, volume 5417 of *Lecture Notes in Computer Science (LNCS)*, pages 2–13, Heraklion, Greece, 2008. *Acceptance rate:* not available.

[55] Charalampos Papamanthou and Roberto Tamassia. Time and space efficient algorithms for two-party authenticated data structures. In *Proc. Int. Conference on Information and Communications Security (**ICICS**)*, volume 4861 of *Lecture Notes in Computer Science (LNCS)*, pages 1–15, Zhengzhou, China, 2007. *Acceptance rate:* not available.

[56] Michael T. Goodrich, Charalampos Papamanthou, and Roberto Tamassia. On the cost of persistence and authentication in skip lists. In *Proc. Int. Workshop on Experimental Algorithms (**WEA**)*, volume 4525 of *Lecture Notes in Computer Science (LNCS)*, pages 94–107, Rome, Italy, 2007. *Acceptance rate:* 24%.

[57] Charalampos Papamanthou and Ioannis G. Tollis. Parameterized st-orientations of graphs: Algorithms and experiments. In *Proc. Int. Conference on Graph Drawing (**GD**)*, volume 4372 of *Lecture Notes in Computer Science (LNCS)*, pages 220–233, Karlsrühe, Germany, 2006. *Acceptance rate:* not available.

[58] Charalampos Papamanthou and Ioannis G. Tollis. Applications of parameterized st-orientations in graph drawing algorithms. In *Proc. Int. Conference on Graph Drawing (**GD**)*, volume 3843 of *Lecture Notes in Computer Science (LNCS)*, pages 355–367, Limerick, Ireland, 2005. *Acceptance rate:* not available.

[59] Charalampos Papamanthou, Ioannis G. Tollis, and Martin Doerr. 3D visualization of semantic metadata models and ontologies. In *Proc. of the Int. Conference on Graph Drawing (**GD**)*, volume 3383 of *Lecture Notes in Computer Science (LNCS)*, pages 377–388, New York City NY, USA, 2004. *Acceptance rate:* not available.

[60] Charalampos Papamanthou and Konstantinos Paparrizos. A visualization of the primal simplex algorithm for the assignment problem. In *Proc. ACM Int. Conference on Innovation and Technology in Computer Science Education (**ITICSE**)*, page 267, Thessaloniki, Greece, 2003. *Acceptance rate:* not available.

Chapters in books

[61] Olga Ohrimenko, Charalampos Papamanthou, and Bernardo Palazzi. Computer security. In *Handbook of Graph Drawing and Visualization (Roberto Tamassia, editor), CRC press*, 2013.

Other

[62] Charalampos Papamanthou. *Cryptography for Efficiency: New Directions in Authenticated Data Structures*. PhD thesis, Brown University, Providence RI, USA, May 2011.

[63] Charalampos Papamanthou. *Computing Longest Path Parameterized st-Orientations of Graphs: Algorithms and Applications*. Master's thesis, University of Crete, Heraklion, Greece, July 2005.

[64] Charalampos Papamanthou. *Effective Programming, Computational Study and Internet Visualization of Network Programming Problems Algorithms*. Bachelor's thesis, University of Macedonia, Thessaloniki, Greece, September 2003.

RESEARCH GRANTS

Total amount of funding to Papamanthou: $1,548,440.

- **PI**, 2018-2019, Ergo Platform (through Blockchain Institute): *Stateless Cryptocurrency Transaction Validation*, $50,000. $50,000 to Papamanthou.
- **PI**, 2017-2022, National Science Foundation (NSF): *CAREER: Towards Practical Systems for Trustworthy Cloud Computing*, $450,000. $450,000 to Papamanthou.
- **co-PI**, 2016-2017, NetApp, Inc.: *Secure Deduplication and Compression for Big Data* (with Roberto Tamassia), $60,000 (NetApp Faculty Fellowship). $30,000 to Papamanthou.
- **PI**, 2015-2016, Yahoo!, Inc.: *Searchable Encryption For More Functional End-to-End Encrypted Email*, $25,000 (Faculty Research Engagement Program). $25,000 to Papamanthou.
- **PI**, 2015-2016, Google, Inc.: *Pmail: Private Gmail with Search*, $49,764 (Google Faculty Research Award). $49,764 to Papamanthou.
- **PI**, 2015-2017, National Science Foundation (NSF): *TWC: Small: Collaborative: Practical Security Protocols via Advanced Data Structures* (with Roberto Tamassia and Michael T. Goodrich), $500,000. $167,000 to Papamanthou.
- **PI**, 2015-2018, National Science Foundation (NSF): *TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing* (with Jonathan Katz, Elaine Shi, and Amol Desphande), $1,162,868. $290,717 to Papamanthou.
- **co-PI**, 2015-2018, National Institute of Standards and Technology (NIST): *Next-Generation Cryptography* (with Jonathan Katz and Dana Dachman-Soled), $1,097,937. $365,979 to Papamanthou.
- **co-PI**, 2014-2016, National Security Agency (NSA): *Understanding Developers Reasoning about Privacy and Security* (with Elaine Shi, Katie Shilton and Mohit Tiwari), $451,355. $112,838 to Papamanthou.
- **co-PI**, 2015-2017, Amazon, Inc.: *Cybersecurity for Big Data* (with Michael Hicks, Jonathan Katz, Dave Levin, Michelle Mazurek, Tudor Dumitras and Elaine Shi), $50,000 (Amazon Web Services credit fund). $7,142 to Papamanthou.

STUDENTS AND POSTDOCS MENTORING

1. *Postdoctoral researchers*
    - Daniel Genkin, (2016-2018), now Assistant Professor at University of Michigan.
    - Dimitrios Papadopoulos, (2016-2017), now Assistant Professor at HKUST.
2. *PhD students*
    - Lambros Mertzanis, ECE PhD (2018-).
    - Shravan Srinivasan, CS PhD (2018-).
    - Rajdeep Talapatra, ECE PhD (2016-).
    - Ioannis Demertzis[†], ECE PhD (2015-).
    - Ahmed E. Kosba, CS PhD, graduated 2018 (co-advised with Elaine Shi). Now Postdoc at UC Berkeley.
    - Yupeng Zhang[‡], ECE PhD, graduated 2018 (co-advised with Jonathan Katz). Now Postdoc at UC Berkeley.
3. *MSc students*
    - Ciara Lynton, ECE MSc, graduated 2018. Now Systems Engineer at Boeing.
4. *Undergraduate students*
    - Thomas Quinn, ECE undegraduate (ENEE 499 project: Smart contracts). Spring 2016.
    - Josh Pruncal, ECE undergraduate (URF project: Searchable encryption). Spring 2016.
    - Daven Patel, ECE undergraduate (URF project: Searchable encryption). Fall 2015.
    - Connor Bruso, ECE undegraduate (ENEE 499 project: Private email). Spring 2015.
    - Chicka Nna, ECE undergraduate (ENEE 499 project: E-voting privacy). Fall 2013.

PATENTS

- *Techniques for verifying search results over a distributed collection*, United States Patent no. 9152716, 2015 (with Michael T. Goodrich, Duy Nguyen, Olga Ohrimenko, Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos and Cristina Videira Lopes).
- *Cryptographic accumulators for authenticated hash tables*, United States Patent no. 9098725, 2015 (with Roberto Tamassia and Nikos Triandopoulos).
- *Dynamic symmetric searchable encryption*, United States Patent no. 8930691, 2015 (with Seny Kamara).
- *Apparatus, methods, and computer program products providing dynamic provable data possession*, United States Patent no. 8978155, 2015 (with C. Christopher Erway, Alptekin Küpçü and Roberto Tamassia).
- *System and method for optimal verification of operations on dynamic sets*, United States Patent no. 8572385, 2013 (with Roberto Tamassia and Nikos Triandopoulos).

[†] Awarded 2018 Symantec Research Fellowship.
[‡] Awarded 2017 Google PhD Fellowship.

TEACHING

- Computer Systems Security (ENEE 457), UMD, Fall 2018.
- Introduction to ECE (ENEE 101, Cybersecurity Section), UMD, Fall 2018.
- Blockchain and Cryptocurrency Technologies (ENEE 759-F/CMSC 818-C), UMD, Spring 2018 (24 students)
- Introduction to ECE (ENEE 101, Cybersecurity Section), UMD, Spring 2018 (120 students).
- Introduction to ECE (ENEE 101, Cybersecurity Section), UMD, Fall 2017 (108 students).
- Algorithms and Data Structures (ENEE 351), UMD, Spring 2017 (8 students).
- Computer Systems Security (ENEE 457), UMD, Fall 2016 (44 students).
- Algorithms and Data Structures (ENEE 351), UMD, Spring 2016 (11 students).
- Computer Systems Security (ENEE 457), UMD, Fall 2015 (33 students).
- Digital Logic Design (ENEE 244), UMD, Spring 2015 (76 students).
- Computer Systems Security (ENEE 457), UMD, Fall 2014 (31 students).
- Cloud Computing Security (ENEE 759-L/CMSC 818-L), UMD, Spring 2014 (11 students).
- Computer Systems Security (ENEE 457), UMD, Fall 2013 (30 students).

TALKS

- ***Keynote:*** *Applications of Verifible Computation in Blockchains and Cryptocurrencies:*
  2018 Symposium on Foundations and Applications of Blockchain, March 2018.
- *Verifiable Computation: From Polynomials and Graphs to Databases and RAM Programs:*
  MIT, March 2018.
  UC San Diego, February 2018.
- *Searchable Encryption Through Compression:*
  NetApp, March 2018.
- *Private Smart Contracts on the Blockchain: Challenges and New Advances:*
  Laboratory for Telecommunications Sciences, October 2017.
- *Searchable Encryption for Data on Disk:*
  George Mason University, November 2017.
  DIMACS Workshop on Outsourcing Computation Securely, July 2017.
  Maryland Cybersecurity Center Symposium, December 2016.
- *IntegriDB: Verifiable SQL for Outsourced Databases:*
  DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures, July 2016.
- *How to Search Encrypted Data:*
  Maryland Cybersecurity Center Symposium, December 2015.
  Koç University, August 2015.
  Yahoo! Labs, May 2015.
  Laboratory for Telecommunications Sciences, February 2015.
  University of Crete, July 2014.

- *Practical Dynamic Proofs of Retrievability:*
  University of Athens, December 2013.
  Brown University, October 2013.
- *Secure and Private Cloud Computing:*
  New York Colloqium on Algorithms and Complexity, November 2013.
  Laboratory for Telecommunications Sciences, September 2013.
- *Trustworthy Computing with Untrusted Resources:*
  Saarland University, December 2015.
  UC Berkeley, April 2015.
  University of Maryland, College Park, April 2013.
  Stony Brook University, March 2013.
  University of California, Santa Barbara, March 2013.
  Oregon State University, February 2013.
  University of Utah, February 2013.
- *Signatures of Correct Computation:*
  University of California, Irvine, June 2012.
  Boston University, April 2012.
- *CS2: A Cryptographic Cloud Storage System:*
  Brown University, April 2012.
  RSA Labs, April 2012.
- *Optimal Verification of Operations on Dynamic Sets:* Palo Alto Research Center (PARC), September 2011.
- *Authenticated Data Structures: Efficient Verification of Data and Computations in the Cloud:*
  Boston University, February 2011.
  University of Athens, December 2010.
- *Efficient Verification of Outsourced Data and Computations:* Microsoft Research, August 2010.
- *Secure and Efficient Cloud Computing:* IBM Research, May 2010.

PROFESSIONAL ACTIVITIES

- **Invited Proposal Reviewer:** National Science Foundation (2016, 2017), Research Grants Council (RGC) of Hong Kong (2014, 2015, 2017, 2018), Luxembourg National Research Fund (2015).
- **Program Committees:** PETS 2019, SIGMOD 2019, FC 2018, NDSS 2017, FC 2017, CCS 2016, SCN 2016, SCC 2016, CCSW 2015, CCS 2015, SCC 2015, ACNS 2015, CCS 2014, CCSW 2014, WPES 2014, ISC 2014, BalkanCryptSec 2014, ICDE 2014, SIGMOD 2013, ASIACCS 2013, SCC 2013.
- **Conference Reviewing:** CCS 2017, CRYPTO 2014, EUROCRYPT 2014, EUROCRYPT 2013, FC 2013, CCSW 2012, ICDE 2012, CCSW 2011, CT-RSA 2011, PacificVis 2009, WADS 2007, GD 2007, PCI 2005, SOFSEM 2005.
- **Journal Reviewing:** Journal of Cryptology, International Journal of Information Security, Information Processing Letters, VLDB Journal, ACM Transactions on Information and System Security, ACM Transactions on Data and Knowledge Engineering, SIAM Journal on Discrete Mathematics, IEEE Transactions on Computing.
- **Service to the Community:** DSSP: Workshop on Data Science for Secure and Privacy-Aware Large Data Management and Mining, September 2016 (co-organizer along with Feifei Li and Rachel Lin); FOCS: 48th conference on Foundations of Computer Science, October 2007 (member of the organizing committee); Francofest: A late festschrift for Franco P. Preparata, November 2006 (member of the organizing committee).

LANGUAGES

Greek (native), *English* (Certificate of Proficiency in English, University of Cambridge and University of Michigan), *German* (Zentrale Mittelstufenprüfung, Goethe Institut), *French* (basic knowledge).