Charalampos (Babis) Papamanthou
Curriculum Vitae
February 26, 2025

414 Arthur K. Watson Hall
51 Prospect Street
New Haven CT 06511

Web: `http://www.cs.yale.edu/homes/cpap/`
Email: charalampos.papamanthou@yale.edu

Research Interests

Computer Security and Applied Cryptography

Academic Appointments

- **Yale University**
  Associate Professor, *Computer Science* 7/21-current
  Co-director, *Yale Applied Cryptography Laboratory* 7/21-current
  Member, *Yale Institute for Foundations of Data Science* 1/23-current
  Faculty Fellow, *Yale Center for Algorithms, Data and Market Design* 9/23-current
- **University of Maryland, College Park**
  Director, *Maryland Cybersecurity Center* (MC2) 12/19-6/21
  Associate Professor, *Electrical and Computer Engineering* 7/19-6/21
  Assistant Professor, *Electrical and Computer Engineering* 8/13-6/19
  Affiliate Faculty, *Computer Science* 8/13-6/21
- **University of California, Berkeley**
  Postdoc, *Electrical Engineering and Computer Sciences* (mentor: Dawn Song) 7/11-7/13

Education

- **Brown University**
  Ph.D., Computer Science 5/11
  Dissertation: *Cryptography for Efficiency: New Directions in Authenticated Data Structures* [93]
  Advisor: Roberto Tamassia
  M.Sc., Computer Science 5/07
  Thesis topic: *Localization in Sensor Networks* [68]
  Advisors: Franco P. Preparata and Roberto Tamassia
- **University of Crete** (Greece)
  M.Sc., Computer Science 7/05
  Thesis topic: *Parameterized st-Orientations of Graphs* [94]
  Advisor: Ioannis G. Tollis
- **University of Macedonia** (Greece)
  B.Sc., Applied Informatics 9/03
  Thesis topic: *Implementation and Computational Study of Network Algorithms* [95]
  Advisor: Konstantinos Paparrizos

Industry Appointments

- **Lagrange Labs, Inc.**, New York NY, USA, Chief Scientist 10/22-current
- **Oasis Labs, Inc.**, Berkeley CA, USA, Research Scientist 7/18
- **Microsoft Research**, Redmond WA, USA, Research Intern (mentor: Seny Kamara) 6/10-8/10
- **Intel Research**, Berkeley CA, USA, Research Intern (mentor: Petros Maniatis) 6/08-8/08

Awards

- ACM CCS Test-of-Time Award, 2022.
- JP Morgan Faculty Research Award, 2022.
- NetApp Faculty Fellowship, 2021.
- Facebook Privacy Research Award (Finalist), 2020.
- 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

Manuscripts

[1] Alexander Chepurnoy, Charalampos Papamanthou, Shravan Srinivasan, and Yupeng Zhang. Edrax: A cryptocurrency with stateless transaction validation. Cryptology ePrint Archive, Report 2018/968, 2018. `https://eprint.iacr.org/2018/968`.

[2] Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou. A zero-knowledge version of vSQL. Cryptology ePrint Archive, Report 2017/1146, 2017. `https://eprint.iacr.org/2017/1146`.

[3] Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, abhi shelat, and Elaine Shi. C∅c∅: A framework for building composable zero-knowledge proofs. Cryptology ePrint Archive, Report 2015/1093, 2015. `https://eprint.iacr.org/2015/1093`.

Refereed conferences

[4] Andreea B. Alexandru, Julian Loss, Charalampos Papamanthou, Giorgos Tsimos, and Benedikt Wagner. Sublinear-round broadcast without trusted setup. In *Proc. ACM-SIAM Symposium on Discrete Algorithms (**SODA**)*, New Orleans LA, USA, 2025.

[5] Arthur Lazzaretti, Charalampos Papamanthou, and Ismael Hishon-Rezaizadeh. Robust double auctions for resource allocation. In *Proc. Int. Financial Cryptography and Data Security Conference (**FC**)*, Miyakojima, Japan, 2025.

[6] Daniel Collins, Sisi Duan, Julian Loss, Charalampos Papamanthou, Giorgos Tsimos, and Haochen Wang. Towards optimal parallel broadcast under a dishonest majority. In *Proc. Int. Financial Cryptography and Data Security Conference (**FC**)*, Miyakojima, Japan, 2025.

[7] Ben Fisch, Arthur Lazzaretti, Zeyu Liu, and Charalampos Papamanthou. ThorPIR: Single server PIR via homomorphic thorp shuffles. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Salt Lake City UT, USA, 2024.

[8] Charalampos Papamanthou, Shravan Srinivasan, Nicolas Gailly, Ismael Hishon-Rezaizadeh, Andrus Salumets, and Stjepan Golemac. Reckle trees: Updatable merkle batch proofs with applications. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Salt Lake City UT, USA, 2024.

[9] Arthur Lazzaretti and Charalampos Papamanthou. Single pass client-preprocessing private information retrieval. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, Philadelphia PA, USA, 2024.

[10] Fatima Elsheimy, Giorgos Tsimos, and Charalampos Papamanthou. Deterministic byzantine agreement with adaptive $O(n \cdot f)$ communication. In *Proc. ACM-SIAM Symposium on Discrete Algorithms (**SODA**)*, Alexandria VA, USA, 2024.

[11] Fatima Elsheimy, Julian Loss, and Charalampos Papamanthou. Early stopping byzantine agreement in $(1 + \epsilon) \cdot f$ rounds. In *Proc. Int. Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT**)*, Kolkata, India, 2024.

[12] Java Ghareh Chamani, Ioannis Demertzis, Dimitrios Papadopoulos, Charalampos Papamanthou, and Rasool Jalili. GraphOS: Towards oblivious graph processing. In *Proc. Very Large Databases (**VLDB**)*, Guangzhou, China, 2024.

[13] Weijie Wang, Yujie Lu, Charalampos Papamanthou, and Fan Zhang. The locality of memory checking. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Copenhagen, Denmark, 2023.

[14] Arthur Lazzaretti and Charalampos Papamanthou. TreePIR: Sublinear-time and polylog-bandwidth private information retrieval from DDH. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Santa Barbara CA, USA, 2023.

[15] Weijie Wang, Annie Ulichney, and Charalampos Papamanthou. Balanceproofs: Maintainable vector commitments with fast aggregation. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, Anaheim CA, USA, 2023.

[16] Arthur Lazzaretti and Charalampos Papamanthou. Near-optimal private information retrieval with preprocessing. In *Proc. Int. Theory of Cryptography Conference (**TCC**)*, Taipei, Taiwan, 2023.

[17] Shravan Srinivasan, Julian Loss, Giulio Malavolta, Kartik Nayak, Charalampos Papamanthou, and Sri AravindaKrishnan Thyagarajan. Transparent batchable time-lock puzzles and applications to byzantine consensus. In *Proc. Int. Conference on Public Key Cryptography (**PKC**)*, Atlanta GA, USA, 2023.

[18] Shravan Srinivasan, Ioanna Karantaidou, Foteini Baldimtsi, and Charalampos Papamanthou. Batching, aggregation, and zero-knowledge proofs in bilinear accumulators. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Los Angeles CA, USA, 2022.

[19] Evgenios Kornaropoulos, Nathaniel Moyer, Charalampos Papamanthou, and Alexandros Psomas. Leakage inversion: Towards quantifying privacy in searchable encryption. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Los Angeles CA, USA, 2022.

[20] Georgios Tsimos, Julian Loss, and Charalampos Papamanthou. Gossiping for communication-efficient broadcast. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Santa Barbara CA, USA, 2022.

[21] Shravan Srinivasan, Alexander Chepurnoy, Charalampos Papamanthou, Alin Tomescu, and Yupeng Zhang. Hyperproofs: Aggregating and maintaining proofs in vector commitments. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, Boston MA, USA, 2022.

[22] Evgenios Kornaropoulos, Charalampos Papamanthou, and Roberto Tamassia. Response-hiding encrypted ranges: Revisiting security via parametrized leakage-abuse attacks. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, San Francisco CA, USA, 2021.

[23] Ahmed Kosba, Dimitrios Papadopoulos, Charalampos Papamanthou, and Dawn Song. Mirage: Succinct arguments for randomized algorithms with applications to universal zk-snarks. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, Boston MA, USA, 2020.

[24] Ioannis Demertzis, Dimitrios Papadopoulos, Charalampos Papamanthou, and Saurabh Shintre. SEAL: Attack mitigation on encrypted databases via adjustable leakage. In *Proc. Usenix Security Symposium (**USENIX SECURITY**)*, Boston MA, USA, 2020.

[25] Ioannis Demertzis, Javad Ghareh Chamani, Dimitrios Papadopoulos, and Charalampos Papamanthou. Dynamic searchable encryption with small client storage. In *Proc. Int. Network and Distributed System Security Symposium (**NDSS**)*, San Diego CA, USA, 2020.

[26] Evgenios Kornaropoulos, Charalampos Papamanthou, and Roberto Tamassia. The state of the uniform: Attacks on encrypted databases beyond the uniform query distribution. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, San Francisco CA, USA, 2020.

[27] Alin Tomescu, Vivek Bhupatiraju, Dimitrios Papadopoulos, Charalampos Papamanthou, Nikos Triandopoulos, and Srinivas Devadas. Transparency logs via append-only authenticated dictionaries. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, London, UK, 2019.

[28] Tiancheng Xie, Jiaheng Zhang, Yupeng Zhang, Charalampos Papamanthou, and Dawn Song. Libra: Succinct zero-knowledge proofs with optimal prover computation. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Santa Barbara CA, USA, 2019.

[29] 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.

[30] 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.

[31] Ioannis Demertzis, Dimitrios Papadopoulos, and Charalampos Papamanthou. Searchable encryption with optimal locality: Achieving sublogarithmic read efficiency. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Santa Barbara CA, USA, 2018.

[32] Ahmed Kosba, Charalampos Papamanthou, and Elaine Shi. xJsnark: A framework for efficient verifiable computation. In *Proc. IEEE Symposium on Security and Privacy (**SSP**)*, San Francisco CA, USA, 2018.

[33] 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**)*, San Francisco CA, USA, 2018.

[34] 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**)*, Wiliamsburg VA, USA, 2018.

[35] 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%.

[36] 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**)*, London, UK, 2018.

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

[38] 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**)*, San Jose CA, USA, 2017.

[39] Ioannis Demertzis and Charalampos Papamanthou. Fast searchable encryption with tunable locality. In *Proc. ACM Int. Conference on Management of Data (**SIGMOD**)*, Chicago IL, USA, 2017.

[40] Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. An expressive (zero-knowledge) set accumulator. In *Proc. IEEE European Symposium on Security and Privacy (**EUROSSP**)*, Paris, France, 2017.

[41] Giuseppe Ateniese, Michael T. Goodrich, Vasilis Lekakis, Charalampos Papamanthou, Evripidis Paraskevas, and Roberto Tamassia. Accountable storage. In *Proc. Applied Cryptography and Network Security (**ACNS**)*, Kanazawa, Japan, 2017.

[42] 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**)*, Santa Barbara CA, USA, 2016. *Acceptance rate:* 25%.

[43] 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**)*, Austin TX, USA, 2016.

[44] 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**)*, San Jose CA, USA, 2016.

[45] 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**)*, Auckland, New Zealand, 2015.

[46] Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. IntegriDB: Verifiable SQL for outsourced databases. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Denver CO, USA, 2015.

[47] Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Practical authenticated pattern matching with optimal proof size. In *Proc. Very Large Databases (**VLDB**)*, Kohala Coast HI, USA, 2015.

[48] 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**)*, Beijing, China, 2015.

[49] Yupeng Zhang, Charalampos Papamanthou, and Jonathan Katz. ALITHEIA: Towards practical verifiable graph processing. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Scottsdale AZ, USA, 2014.

[50] 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**)*, Scottsdale AZ, USA, 2014.

[51] 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**)*, San Diego CA, USA, 2014.

[52] 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.

[53] Elaine Shi, Emil Stefanov, and Charalampos Papamanthou. Practical dynamic proofs of retrievability. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Berlin, Germany, 2013.

[54] 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**)*, Athens, Greece, 2013.

[55] Seny Kamara and Charalampos Papamanthou. Parallel and dynamic searchable symmetric encryption. In *Proc. Int. Financial Cryptography and Data Security Conference (**FC**)*, Okinawa, Japan, 2013.

[56] Charalampos Papamanthou, Elaine Shi, and Roberto Tamassia. Signatures of correct computation. In *Proc. Int. Theory of Cryptography Conference (**TCC**)*, Tokyo, Japan, 2013.

[57] 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.

[58] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Raleigh NC, USA, 2012.

[59] 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**)*, Istanbul, Turkey, 2012.

[60] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal verification of operations on dynamic sets. In *Proc. Int. Cryptology Conference (**CRYPTO**)*, Santa Barbara CA, USA, 2011.

[61] 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.

[62] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal authenticated data structures with multilinear forms. In *Proc. Int. Conference on Pairing-Based Cryptography (**PAIRING**)*, Ishikawa, Japan, 2010.

[63] 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**)*, Chicago IL, USA, 2009.

[64] Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Authenticated hash tables. In *Proc. ACM Int. Conference on Computer and Communications Security (**CCS**)*, Alexandria VA, USA, 2008.

[65] Michael T. Goodrich, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Athos: Efficient authentication of outsourced file systems. In *Proc. Int. Information Security Conference (**ISC**)*, Taipei, Taiwan, 2008.

[66] 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**)*, Alexandria VA, USA, 2008.

[67] 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**)*, Boston MA, USA, 2008.

[68] 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**)*, Reykjavik, Iceland, 2008.

[69] Roberto Tamassia, Bernardo Palazzi, and Charalampos Papamanthou. Graph drawing for security visualization. In *Proc. Int. Conference on Graph Drawing (**GD**)*, Heraklion, Greece, 2008.

[70] 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**)*, Zhengzhou, China, 2007.

[71] 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**)*, Rome, Italy, 2007.

[72] Charalampos Papamanthou and Ioannis G. Tollis. Parameterized st-orientations of graphs: Algorithms and experiments. In *Proc. Int. Conference on Graph Drawing (**GD**)*, Karlsrühe, Germany, 2006.

[73] Charalampos Papamanthou and Ioannis G. Tollis. Applications of parameterized st-orientations in graph drawing algorithms. In *Proc. Int. Conference on Graph Drawing (**GD**)*, pages 355–367, Limerick, Ireland, 2005.

[74] 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**)*, New York City NY, USA, 2004.

[75] 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**)*, Thessaloniki, Greece, 2003.

Refereed journals

[76] Brice Minaud and Charalampos Papamanthou. Generalized cuckoo hashing with a stash, revisited. *Information Processing Letters (**Inform. Process. Lett.**)*, 181, 2023.

[77] Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin. Oblivious network RAM. *Journal of Cryptology (**J. Cryptology**)*, 32(3):941–972, 2019.

[78] Yupeng Zhang, Charalampos Papamanthou, and Jonathan Katz. Verifiable graph processing. *ACM Transactions on Privacy and Security (**TOPS**)*, 21(4):1–23, 2018.

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

[80] 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.

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

[82] 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.

[83] 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.

[84] 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.

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

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

[87] 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.

[88] 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.

[89] 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.

Book chapters and edited volumes

[90] Zhiqiang Lin, Charalampos Papamanthou, and Michalis Polychronakis, editors. *Proceedings of the Information Security Conference* (ISC), New York City NY, USA. Springer, 2019.

[91] Radu Sion and Charalampos Papamanthou, editors. *Proceedings of the Cloud Computing Security Workshop* (CCSW), London, UK. ACM, 2019.

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

Other

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

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

[95] 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 and Corporate Gifts

Total amount of funding to Papamanthou: $3,494,819.

- **PI**, 2024-2025, Yale KIAT City: *Security of Machine Learning and Artificial Intelligence (Feasibility Study)*, $50,970.00.
- **PI**, 2024-2025, Protocol Labs: *Advancing Metadata-Private Technologies: Improving Concrete Performance of Private Information Retrieval for Real-World Systems*, $100,000.
- **PI**, 2023-2026, National Science Foundation (NSF): *Medium: Cryptographic Accumulators and Revocation of Credentials* (with Foteini Baldimtsi, Taejoong Chung, Anna Lysyanskaya and Alan Mislove), $1,200,000. $240,000 to Papamanthou.
- **PI**, 2023-2024. Protocol Labs: *Private Retrieval of Data*, $102,273.
- **PI**, 2023-2024, Yale Ventures Roberts Innovation Fund: *Non-Interactive State Proofs*, $75,000 ($25,000 in Amazon credits).
- **PI**, 2022-2024, Protocol Labs: *Updatable Vector Commitments with Natural Aggregation Algorithms*, $198,032.
- **PI**, 2022-2023, Algorand Foundation: *PAVE Algorand Center of Excellence: Privacy, Accountability, Verification, and Economics of Blockchain systems* (with Tal Malkin, Rosario Gennaro, Bryan Ford, Joan Feigenbaum, Ben Fisch, Zhong Shao, Gur Huberman, Eran Tromer), $1,150,000. $122,012 to Papamanthou.
- **PI**, 2023-2023, JP Morgan: *New Zero-Knowledge Arguments for Cryptocurrencies*, $110,000.
- **PI**, 2022-2025, National Science Foundation (NSF): *Medium: The Next Generation of Leakage Attacks and Defenses for Encrypted Databases* (with Evgenios Kornaropoulos and Roberto Tamassia), $1,200,000. $400,000 to Papamanthou.
- **PI**, 2021-2022, NetApp: *New Directions in Expressive Searchable Encryption* (with Roberto Tamassia), $64,090 (NetApp Faculty Fellowship). $34,090 to Papamanthou.
- **PI**, 2021-2022, Protocol Labs: *Advances in Vector Commitments: Updatability, Aggregation and New Assumptions*, $56,820.

- **PI**, 2021-2022, Ethereum Foundation: *A Proposal for Advancing Tree-Based Vector Commitments*, $64,000.
- **PI**, 2021-2024, VMware: *Authenticated Data Structures and Zero-Knowledge Arguments*, $225,000.
- **co-PI**, 2019-2021, National Institute of Standards and Technology (NIST): *Next-Generation Cryptography* (continuation) (with Jonathan Katz and Dana Dachman-Soled), $600,000. $200,000 to Papamanthou.
- **PI**, 2018-2019, Ergo Platform (through Blockchain Institute): *Stateless Cryptocurrency Transaction Validation*, $50,000.
- **PI**, 2017-2022, National Science Foundation (NSF): *CAREER: Towards Practical Systems for Trustworthy Cloud Computing*, $450,000.
- **PI**, 2016-2017, NetApp: *Secure Deduplication and Compression for Big Data* (with Roberto Tamassia), $60,000 (NetApp Faculty Fellowship). $30,000 to Papamanthou.
- **PI**, 2015-2016, Yahoo!: *Searchable Encryption For More Functional End-to-End Encrypted Email*, $25,000 (Faculty Research Engagement Program).
- **PI**, 2015-2016, Google: *Pmail: Private Gmail with Search*, $49,764 (Google Faculty Research Award).
- **PI**, 2015-2017, National Science Foundation (NSF): *Small: 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: 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: *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.

MENTORING

1. *Postdoctoral researchers*
   - Varun Madathil, (2024-).
   - Daniel Genkin, (2016-2018), now Assistant Professor at University of Michigan.
   - Dimitrios Papadopoulos, (2016-2017), now Assistant Professor at HKUST.
2. *Ph.D. Theses*
   - Fatima Elsheimy, Yale (2022-).
   - Arthur Lazzarreti[*], Yale (2021-).
   - Weijie Wang[†], Yale (2021-).

[*] Protocol Labs PhD fellowship
[†] Protocol Labs PhD fellowship

- Giorgos Tsimos, UMD (2019-).
- Shravan Srinivasan, PhD, 2023 (UMD). Now research scientist at Lagrange Labs.
- Ioannis Demertzis[‡], PhD, 2020 (UMD). Now faculty at University of California Santa Cruz.
- Ahmed Kosba, PhD, 2018 (co-advised with E. Shi, UMD). Now faculty at Alexandria University (Egypt).
- Yupeng Zhang[§], PhD, 2018 (co-advised with J. Katz, UMD). Now faculty at University of Illinois Urbana-Champaign.

3. *MSc students*
   - Rajdeep Talapatra, ECE MSc (2016-2021), now Silicon Design Engineer at AMD.
   - Ciara Lynton, ECE MSc (2016-2018), now Systems Engineer at Boeing.
4. *Undergraduate students*
   - Annie Ulichney, Yale undergraduate (Project: Vector commitments, led to a publication [15]). Spring 2023.
   - Israel Yolou, Yale undergraduate (Project: Locality in searchable encryption). Spring 2022.
   - Thomas Quinn, UMD undegraduate (Project: Smart contracts). Spring 2016.
   - Josh Pruncal, UMD undergraduate (Project: Searchable encryption). Spring 2016.
   - Daven Patel, UMD undergraduate (Project: Searchable encryption). Fall 2015.
   - Connor Bruso, UMD undegraduate (Project: Private email). Spring 2015.
   - Chicka Nna, UMD undergraduate (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).

Teaching

- *Mathematical Tools for Computer Science* (CPSC 202): Spring 25 (Yale)
- *Advanced Topics in Cryptography: Cryptography and Computation* (CPSC 417): Fall 24 (Yale)
- *Introduction to Cryptography* (CPSC 467): Spring 23 (Yale).

[‡] 2018 Symantec Research Fellowship, 2020 ACM SIGSAC Dissertation Award (runner-up), ECE Distinguished Dissertation Award.
[§] 2017 Google PhD Fellowship, 2019 ACM SIGSAC Dissertation Award (runner-up), 2019 ECE Distinguished Dissertation Award.

- *Cryptography and Computer Security* (CPSC 467): Spring 22 (Yale).
- *Cryptography* (ENEE 456): Spring 21.
- *Bitcoin and Cryptocurrency Technologies* (ENPM809V): Fall 19.
- *Blockchain and Cryptocurrency Technologies* (ENEE 759-F/CMSC 818-C): Spring 18.
- *Introduction to ECE* (ENEE 101 cybersecurity section): Fall 17, Spring 18, Fall 18, Spring 19, Fall 19, Spring 20, Fall 20, Spring 21.
- *Algorithms and Data Structures* (ENEE 351): Spring 16, Spring 17, Spring 20.
- *Digital Logic Design* (ENEE 244): Spring 15.
- *Cloud Computing Security* (ENEE 759-L/CMSC 818-L): Spring 14.
- *Computer Systems Security* (ENEE 457): Fall 13, Fall 14, Fall 15, Fall 16, Fall 18.

TALKS

- *Recproofs: Vector Commitments with Updatable Batch Proofs and their Applications:*
  Science of Blockchain Conference, Stanford, August 2023.
- *Leakage Abuse Attacks in Encrypted Databases:*
  National Technical University of Athens, December 2020.
  Carnegie Mellon University, April 2021.
- *Distributed Authenticated Data Structures and their Applications:* Decrypto Seminar, January 2021.
- *Blockchains from an Academic Perspective:* General Motors, June 2019.
- *Trustworthy and Private Computation in Adversarial Environments:*
  Technical University of Crete, August 2019.
  Yale University, April 2019.
  Duke University, February 2019.
  Helmholtz Center for Information Security (CISPA), February 2019.
  Yale Institute for Network Science, **Distinguished Lecture**, November 2018.
- *Applications of Verifiable Computation in Blockchains and Cryptocurrencies:*
  University of Macedonia, June 2018.
  Symposium on Foundations and Applications of Blockchain, **Keynote**, 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

- **Chair**: 2022 SIGSAC Doctoral Dissertation Award committee.

- **Editorial Board:** Computer Science Review (2021-2022).

- **Invited Proposal Reviewer:** UC Multicampus Research Programs and Initiatives (2024), National Science Foundation (2016, 2017, 2025), Research Grants Council (RGC) of Hong Kong (2014, 2015, 2017, 2018), Luxembourg National Research Fund (2015).

- **Program Committees:** CCS 2025, CRYPTO 2025, EUROCRYPT 2025, SSP (OAKLAND) 2025, CRYPTO 2024, CCS 2024, AFT 2023, CCS 2023, PKC 2023, FC 2023, CCS 2022, CCS 2021, CT-RSA 2021, PETS 2020, PKC 2020, DSC 2020, CRYPTO 2019, ISC 2019, CCSW 2019, 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:** (Organizer) 2nd Yale Symposium on Privacy, Accountability, Verification and Economics of Blockchain Systems (2025), (Organizer) 1st Yale Symposium on Privacy, Accountability, Verification and Economics of Blockchain Systems (2023), CCSW 2019 (program co-chair), ISC 2019 (program co-chair), ICERM Topical Workshop on Encrypted Search, June 2019 (co-organizer); 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).