CURRICULUM VITAE
NIKOS TRIANDOPOULOS

Department of Computer Science, Boston University
111 Cummington St., Boston, MA 02215
nikos@cs.bu.edu, www.cs.bu.edu/faculty/nikos/

Current Affiliation

BOSTON UNIVERSITY, DEPT. OF COMPUTER SCIENCE — Boston MA
2010 – today — *Adjunct Assistant Professor* — BUSec Security Group

Research Interests

Broad areas: Security, Privacy & Cryptography

Recent focus areas:
Cloud & Network Security
Verifying computation, secure data outsourcing, reliable transmissions over malicious channels
Mobile & Enterprise Security
Breach-resilient credential/password management, secure analytics-aaS, secure logging
Applied Cryptography & Secure Protocol Design
Private computation, distributed cryptography, security for rational parties

Education

BROWN UNIVERSITY — Providence RI

May 2007 — Ph.D. in Computer Science (completed in Summer 2006)
Thesis Topic: "Efficient Data Authentication"
Advisor: Professor Roberto Tamassia

May 2002 — Sc.M. in Computer Science
Thesis Topic: "Authenticated Data Structures for Graph and Geometric Searching"
Advisor: Professor Roberto Tamassia

NATIONAL & KAPODISTRIAN UNIVERSITY OF ATHENS — Athens, Greece

1999 – 2000 — Studies in Graduate Program in Logic, Algorithms and Computation

UNIVERSITY OF PATRAS — Patras, Greece

June 1999 — Diploma with Honors in Computer Engineering & Informatics
Thesis Topic: "Applications of the Probabilistic Method in Algorithms"
Advisor: Professor Lefteris M. Kirousis

Employment

RSA, THE SECURITY DIVISION OF EMC — Cambridge MA
2010 – 2016 — *Principal Research Scientist* — RSA Laboratories

BOSTON UNIVERSITY, DEPT. OF COMPUTER SCIENCE — Boston MA
2008 – 2010 — *Research Assistant Professor* — Center for Reliable Inf. Systems & Cyber Security

BROWN UNIVERSITY, DEPT. OF COMPUTER SCIENCE — Providence RI
2008 – 2011 — *Adjunct Assistant Professor (Research)*

UNIVERSITY OF AARHUS, DEPT. OF COMPUTER SCIENCE — Aarhus, Denmark
2007 – 2008 — *Research Assistant Professor* — Cryptology & Security Group
Center for Algorithmic Game Theory

DARTMOUTH COLLEGE, DEPT. OF COMPUTER SCIENCE — Hanover NH
2006 – 2007 — *Post-doctoral Research Fellow* — Institute for Security Technology, and Society

Teaching & Advising

	BOSTON UNIVERSITY, DEPT. OF COMPUTER SCIENCE	Boston MA
2011 – today	*Advisor*	Dimitrios Papadopoulos, Ph.D. 2016 (expected)
2014	*(Initial) Co-Advisor*	Emine Ugur Kaynar, PhD student
	RSA LABORATORIES	Cambridge MA
2015	*Mentor*	Yupeng Zhang, Intern
2014	*Mentor*	James Kelley, Intern
	BROWN UNIVERSITY, DEPT. OF COMPUTER SCIENCE	Providence RI
2013 – 2015	*Mentor & Thesis Reader*	James Kelley, Ph.D. 2015
2009 – 2010	*Advisor*	Qiao Xie, Sc.M. 2010
2010	*Instructor*	Intr. to Scientific Comp. & Problem Solving (CS 004, ∼125 enrolled students)
2009	*Instructor*	Intr. to Scientific Comp. & Problem Solving (CS 004, ∼120 enrolled students)

Awards & Honors

2014, 2012	Excellence Award	EMC Corporation
2006 – 2007	Post-doctoral Research Fellowship	Institute for Information Infrastructure Protection
2006	Technological Innovation Award	Brown University
2005	Kanellakis Fellowship	Brown University
2000 – 2002	Kanellakis Fellowship	Brown University
2001	Honorary Distinction Award	Technical Chamber of Greece
1999 – 2000	Fellowship	National & Kapodistrian University of Athens

Research Grants

2010 – today 1. National Science Foundation (NSF), CISE–Trustworthy Computing, Award No. CNS-1012798. *Towards trustworthy interactions in the cloud*. Role: Co-PI. $3M (Total Award). (Status: Active.)

2010 – today 2. National Science Foundation (NSF), CISE–Trustworthy Computing, Award No. CNS-1012910. *Securing the open softphone*. Role: Senior Personnel. $3M. (Status: Active.)

2006 – 2007 3. U.S. Department of Homeland Security, Office of Science and Technology. *Algorithms for high assurance in cyber-security*. Role: PI. $150K. (Status: Completed.)

Industrial Research

Innovation & Technology Transfer

2014 – 2015	Breach-resilient credential-management and user-authentication systems
2013 – 2014	Integrity and privacy protections for security alert systems and secure logging
2011 – 2013	Anti-cloning and anti-breach protections for two-factor authenticators
2010 – 2012	Integrity and confidentiality mechanisms for secure cloud services and reliable cloud auditing

Academic Activities

Program Committee Member

2016	ACM CCS, IEEE EuroS&P
2015	ACM CCS
2014	ACM CCSW, BalkanCryptSec, IACR CANS, ICDCS
2013	ACM SIGMOD
2012	IEEE GLOBECOM (ManSec-CC)
2011	CT-RSA

Organizing Committee Member

2013 EUROCRYPT Sponsorship Chair

Panelist

2013 European Commission Workshop on Cloud Computing Security

2012 NSF Trustworthy Computing Program

2011 Advanced Cyber Security Center Second Annual Working Conference

New England Faculty Summit on Cyber Security

Co-organizer

2008 Summer School on Rational Cryptography, PROVILAB, Bertinoro, Italy.

2004 32nd IPP Symposium on Trusted Computing, Brown University.

Publications

Conference

1. Ari Juels, James Kelley, Roberto Tamassia, and Nikos Triandopoulos. *Falcon codes: Fast, authenticated LT codes (Or: Making Rapid Tornadoes unstoppable)*. In *Proceedings of ACM Conference on Computer and Communications Security* **(CCS)**, pp. 1032–1047, Denver, CO, October, 2015.
2. Dimitrios Papadopoulos, Stavros Papadopoulos, and Nikos Triandopoulos. *Taking authenticated range queries to arbitrary dimensions*. In *Proceedings of ACM Conference on Computer and Communications Security* **(CCS)**, pp. 819–830, Scottsdale, AZ, November, 2014.
3. Kevin D. Bowers, Catherine Hart, Ari Juels, and Nikos Triandopoulos. *PillarBox: Combating next-generation malware with fast forward-secure logging*. In *Proceedings International Symposium on Research in Attacks, Intrusions and Defenses* **(RAID)**, pp. 46–67, Gothenburg, Sweden, September, 2014.
4. Ahmed E. Kosba, Dimitrios Papadopoulos, Charalampos Papamanthou, Mahmoud F. Sayed, Elaine Shi, and Nikos Triandopoulos. *TRUESET: faster verifiable set computations*. In *Proceedings of USENIX Security Symposium* **(USENIX Security)**, pp. 765–780, San Diego, CA, August, 2014.
5. Ran Canetti, Omer Paneth, Dimitrios Papadopoulos, and Nikos Triandopoulos. *Verifiable set operations over outsourced databases*. In *Proceedings of Int. Conference on Practice and Theory of Public-Key Cryptography* **(PKC)**, pp. 113–130, Buenos Aires, Argentina, March, 2014.
6. Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. *Delegateable pseudorandom functions and applications*. In *Proceedings of ACM Conference on Computer and Communications Security* **(CCS)**, pp. 669–684, Berlin, Germany, November 2013.
7. Kevin D. Bowers, Marten van Dijk, Robert Griffin, Ari Juels, Alina Oprea, Ronald L. Rivest, and Nikos Triandopoulos. *Defending against the unknown enemy: Applying* FLIPIT *to system security*. In *Proceedings of Conference on Decision and Game Theory for Security* **(GameSec)**, LNCS, Vol. 7638, Springer, pp. 248–263, Budapest, Hungary, November 2012.
8. Marten van Dijk, Ari Juels, Emil Stefanov, Alina Oprea, Ronald L. Rivest, and Nikos Triandopoulos. *Hourglass schemes: How to prove that cloud files are encrypted*. In *Proceedings of ACM Conference on Computer and Communications Security* **(CCS)**, pp. 265–280, Raleigh, NC, USA, October 2012.
9. James Kelley, Roberto Tamassia, and Nikos Triandopoulos. *Hardening access control and data protection in GFS-like file systems*. In *Proceedings of European Symposium on Research in Computer Security* **(ESORICS)**, LNCS, Vol. 7459, Springer, pp. 19–36, Pisa, Italy, September 2012.
10. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. *Optimal authentication of operations on dynamic sets*. In *Proceedings of Annual International Cryptology Conference* **(CRYPTO)**, LNCS, Vol. 6841, Springer, pp. 91–110, Santa Barbara CA, USA, August 2011.

11. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. *Optimal authenticated data structures with multilinear forms*. In *Proceedings of International Conference on Pairing-based Cryptography* **(Pairing)**, LNCS, Vol. 6487, Springer, pp. 246–264, Yamanaka, Japan, December 2010.
12. Roberto Tamassia and Nikos Triandopoulos. *Certification and authentication of data structures*. In *Proceedings of Alberto Mendelzon International Workshop on Foundations of Data Management* **(AMW)**, Buenos Aires, Argentina, May 2010.
13. Michael T. Goodrich, Jonathan Z. Sun, Roberto Tamassia, and Nikos Triandopoulos. *Reliable resource searching in P2P networks*. In *Proceedings of International Conference on Security and Privacy in Communication Networks* **(SecureComm)**, LNICST, Vol. 19, Springer, pp. 437–447, Athens, Greece, September 2009.
14. Peter Bro Miltersen, Jesper Buus Nielsen, and Nikos Triandopoulos. *Privacy-enhancing auctions using rational cryptography*. In *Proceedings of Annual Int. Cryptology Conference* **(CRYPTO)**, LNCS, Vol. 5677, Springer, pp. 541–558, Santa Barbara CA, USA, August 2009.
15. Apu Kapadia, David Kotz, and Nikos Triandopoulos. *Opportunistic sensing: Security challenges for the new paradigm*. In *Proceedings of 1st International Conference on Communication Systems and Networks* **(COMSNETS)**, pp. 1–10, Bangalore, India, January 2009. (Invited paper.)
16. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. *Authenticated hash tables*. In *Proceedings of ACM Conference on Computer and Communications Security* **(CCS)**, pp. 437–448, Alexandria VA, USA, October 2008.
17. Michael T. Goodrich, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. *Athos: Efficient authentication of outsourced file systems*. In *Proceedings of Information Security Conference* **(ISC)**, LNCS, Vol. 5222, Springer, pp. 80–96, Taipei, Taiwan, September 2008.
18. Cory Cornelius, Apu Kapadia, David Kotz, Daniel Peebles, Minho Shin, and Nikos Triandopoulos. *AnonySense: Privacy-aware people-centric sensing*. In *Proceedings of ACM/USENIX International Conference on Mobile Systems, Applications, and Services* **(MobiSys)**, pp. 211–224, Breckenridge CO, USA, June 2008.
19. Apu Kapadia, Nikos Triandopoulos, Cory Cornelius, Daniel Peebles, and David Kotz. *AnonySense: Opportunistic and privacy-preserving context collection*. In *Proceedings of International Conference on Pervasive Computing* **(Pervasive)**, LNCS, Vol. 5013, Springer, pp. 280–297, Sydney, Australia, May 2008.
20. Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. *Super-efficient verification of dynamic outsourced databases*. In *Proceedings of RSA Conference - Cryptographers Track* **(CT-RSA)**, LNCS, Vol. 4964, Springer, pp. 407–424, San Francisco CA, USA, April 2008.
21. Apu Kapadia and Nikos Triandopoulos. *Halo: High-assurance locate for distributed hash tables*. In *Proceedings of Annual Network & Distributed System Security Symposium* **(NDSS)**, pp. 61–79, San Diego CA, USA, February 2008.
22. Yi Ouyang, Zhengyi Le, Yurong Xu, Nikos Triandopoulos, Sheng Zhang, James Ford, and Fillia Makedon. *Providing anonymity in wireless sensor networks*. In *Proceedings of IEEE International Conference on Pervasive Services* **(ICPS)**, Istanbul, Turkey, July 2007.
23. Roberto Tamassia and Nikos Triandopoulos. *Efficient content authentication in peer-to-peer networks*. In *Proceedings of International Conference on Applied Cryptography and Network Security* **(ACNS)**, LNCS, Vol. 4521, Springer, pp. 354–372, Zhuhai, China, June 2007.
24. Anna Lysyanskaya and Nikos Triandopoulos. *Rationality and adversarial behavior in multi-party computation*. In *Proceedings of Annual International Cryptology Conference* **(CRYPTO)**, LNCS, Vol. 4117, Springer, pp. 180–197, Santa Barbara CA, USA, August 2006.

25. Roberto Tamassia and Nikos Triandopoulos. *Computational bounds on hierarchical data processing with applications to information security*. In *Proceedings of International Colloquium on Automata, Languages and Programming* **(ICALP)**, Track C: *Security and Cryptography Foundations*, LNCS, Vol. 3580, Springer, pp. 153–165, Lisbon, Portugal, July 2005.

26. Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. *Multicast authentication in fully adversarial networks*. In *Proceedings of IEEE Symposium on Security and Privacy* **(S&P - Oakland)**, pp. 241–255, Oakland CA, USA, May 2004.

27. Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos, and Robert Cohen. *Authenticated data structures for graph and geometric searching*. In *Proceedings of RSA Conference - Cryptographers Track* **(CT-RSA)**, LNCS, Vol. 2612, Springer, pp. 295–313, San Francisco CA, USA, April 2003.

Journal

28. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos, *Authenticated hash tables based on cryptographic accumulators*. **Algorithmica**, 74(2):664–712, 2016.

29. Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. *Practical authenticated pattern matching with optimal proof size*. In *Proceedings of the VLDB Endowment* **(PVLDB)**, 8(7): 750–761, Kohala Coast, HI, September, 2015.

30. Minho Shin, Cory Cornelius, Apu Kapadia, Nikos Triandopoulos, and David Kotz. *Location privacy for mobile crowd sensing through population mapping*. **Sensors**, June 2015. DOI: 10.3390/s150715285.

31. 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 *Proceedings of the VLDB Endowment* **(PVLDB)**, 5(10):920–931, Istanbul, Turkey, August 2012.

32. Michael T. Goodrich, Roberto Tamassia, and Nikos Triandopoulos. *Efficient authenticated data structures for graph connectivity and geometric search problems*. **Algorithmica**, 60(3):505–552, 2011.

33. Minho Shin, Cory Cornelius, Apu Kapadia, David Kotz, Dan Peebles, and Nikos Triandopoulos. *AnonySense: A system for anonymous opportunistic sensing*. *Journal of Pervasive and Mobile Computing* **(PMC)**, 7(1):16–30, 2011.

34. Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. *Authenticated error-correcting codes with applications to multicast authentication. ACM Transactions on Information and System Security* **(TISSEC)**, 13(2), 2010.

Technical report

35. Peter Johnson, Apu Kapadia, David Kotz, and Nikos Triandopoulos. *People-centric urban sensing: Security challenges for the new paradigm*. Technical Report TR2007–586, Dartmouth College, Computer Science, Hanover, NH, February 2007.

36. Roberto Tamassia and Nikos Triandopoulos. *On the cost of authenticated data structures*. Technical Report, Center for Geometric Computing, Brown University, 2003.

Manuscript/ Under submission

37. Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos, Alessandra Scafuro, and Nikos Triandopoulos. *Practical secure computation for online social networks*, 2016.

38. Esha Ghosh, Olga Ohrimenko, Dimitrios Papadopoulos, Roberto Tamassia, and Nikos Triandopoulos. *Zero-knowledge accumulators and set operations*. *IACR Cryptology ePrint Archive 2015: 404*, 2015.

39. Kevin D. Bowers, Panagiotis Ipeirotis, Ari Juels, Guoying Luo, Ronald L. Rivest, Nikos Triandopoulos, and Matt Weir. *Honeywords in practice: Generating effective fake passwords*, 2013.

40. Ivan Damgård and Nikos Triandopoulos. *Supporting non-membership proofs with bilinear-map accumulators*. *IACR Cryptology ePrint Archive 2008: 538*, 2008.

Issued Patents

1. U.S. Patent 9,256,725: *Credential recovery with the assistance of trusted entities*, February, 2016.
2. U.S. Patent 9,225,717: *Event-based data signing via time-based one-time authentication tokens*, December, 2015.
3. U.S. Patent 9,160,539: *Methods and apparatus for secure, stealthy and reliable transmission of alert messages from a security alerting system*, October, 2015.
4. U.S. Patent 9,152,716: *Techniques for verifying search results over a distributed collection*, October, 2015.
5. U.S. Patent 9,118,661: *Methods and apparatus for authenticating a user using multi-server one-time passcode verification*, August, 2015.
6. U.S. Patent 9,098,725: *Cryptographic accumulators for authenticated hash tables*, August, 2015.
7. U.S. Patent 9,083,515: *Forward secure pseudorandom number generation resilient to forward clock attacks*, July, 2015.
8. U.S. Patent 9,049,185: *Authenticated hierarchical set operations and applications*, June, 2015.
9. U.S. Patent 9,021,553: *Methods and apparatus for fraud detection and remediation in knowledge-based authentication*, April, 2015.
10. U.S. Patent 9,009,844: *Methods and apparatus for knowledge-based authentication using historically aware questionnaires*, April, 2015.
11. U.S. Patent 9,008,303: *Method and apparatus for generating forward secure pseudorandom numbers*, April, 2015.
12. U.S. Patent 8,997,198: *Techniques for securing a centralized metadata distributed filesystem*, March, 2015.
13. U.S. Patent 8,984,609: *Methods and apparatus for embedding auxiliary information in one-time passcodes*, March, 2015.
14. U.S. Patent 8,954,728: *Generation of exfiltration-resilient cryptographic keys*, February, 2015.
15. U.S. Patent 8,875,263: *Controlling a soft token running within an electronic apparatus*, Oct., 2014.
16. U.S. Patent 8,819,769: *Managing user access with mobile device posture*, August, 2014.
17. U.S. Patent 8,817,988: *Variable epoch scheduler for proactive cryptography systems*, Aug., 2014.
18. U.S. Patent 8,813,234: *Graph-based approach to deterring persistent security threats*, Aug., 2014.
19. U.S. Patent 8,788,817: *Methods and apparatus for secure and reliable transmission of messages over a silent alarm channel*, July, 2014.
20. U.S. Patent 8,752,156: *Detecting soft token copies*, June, 2014.
21. U.S. Patent 8,752,146: *Providing authentication codes which include token codes and biometric factors*, June, 2014.
22. US Patent 8,726,034: *Cryptographic accumulators for authenticated hash tables*, May, 2014.
23. US Patent 8,683,570: *Scheduling soft token data transmission*, March, 2014.
24. US Patent 8,683,563: *Soft token posture assessment*, March, 2014.
25. US Patent 8,572,385: *System and method for optimal verification of operations on dynamic sets*. October, 2013.
26. US Patent 7,974,221: *Efficient content authentication over distributed hash tables*, July, 2011.

Invited Lectures

1. *Falcon Codes: Fast, Authenticated LT-Codes*. Workshop on Secure Cloud Computing & Storage, organized by Boston University & MIT Lincoln Labs, Hariri Institute, Boston University, Boston, MA, USA, May 2015.
2. *Falcon Codes: Fast, Authenticated LT-Codes*. Department of Computer Science, Aarhus University, Aarhus, Denmark, September 2014.

3. *Falcon Codes: Fast, Authenticated LT-Codes*. 4th CryptoSec Day Workshop, Department of Informatics, Athens University of Economics and Business, Athens, Greece, July 2014.
4. *'2nd-Wave' Advanced Threats: Preparing for Tomorrow's Sophisticated Attacks*. RSA Conference - Analytics & Forensics Track, San Fransisco, CA, USA, February 2014.
5. *Confidentiality and Integrity in the Cloud*. European Commission Workshop on Cloud Computing Security, organized by EUs European Commission (DG Communications Networks, Content and Technology), Brussels, Belgium, May 2013.
6. *Position Statement on "Cybersecurity R&D Grand Challenges"*. Advanced Cyber Security Center Second Annual Working Conference, Federal Reserve Bank of Boston, Boston, MA, November 2012.
7. *Hourglass Schemes: How to Prove that Cloud Files are Encrypted*. Department of Computer Science, UMass Boston, Boston, MA, USA, October 2012.
8. *PillarBox: Protecting the Chain of Custody in Security Alerting Systems*. Department of Computer Science, UC Berkeley, Berkeley, CA, USA, May 2012.
9. *Optimal Verification of Operations on Dynamic Sets*. Theory Seminar, Department of Informatics, Athens University of Economics and Business, Athens, Greece, June 2011.
10. *Efficient Protocols for Trustworthy Outsourced Computations*. RSA Laboratories, Cambridge, MA, USA, March 2010.
11. *Efficient Protocols for Trustworthy Outsourced Computations*. Department of Computer Science, UMass Boston, Boston, MA, USA, February 2010.
12. *Privacy-Enhancing Auctions Using Rational Cryptography*. Algorithms Seminar, Department of Informatics and Telecommunications, University of Athens, Athens, Greece, September 2009.
13. *Privacy-Enhancing Auctions Using Rational Cryptography*. CS/RISCS Colloquium, Boston University, Boston MA, USA, May 2009.
14. *Authentication Hash Tables*. Department of Computer Science, Aarhus University, Aarhus, Denmark, November 2008.
15. *Efficient Data Authentication in Distributed Environments*. CS/RISCS Colloquium, Boston University, Boston MA, USA, October 2008.
16. *Mixed-behavior Models in Multi-party Computation*. Summer School on Rational Cryptography, ECRYPT, Bertinoro, Italy, June 2008.
17. *Protocols for Efficient Data Authentication*. Computer Science and Engineering Colloquium, University of Texas, Arlington TX, USA, March 2007.
18. *Efficient Data Authentication*. Institute for Security Technology Studies, Dartmouth College, Hanover NH, USA, October 2006.
19. *Computing Without Honesty*. Computer Science departmental retreat, Brown University, Providence RI, USA, May 2006.
20. *Rationality and Adversarial Behavior in Multi-party Computation*. Department of Computer Science, Aarhus University, Aarhus, Denmark, May 2006.

Professional Societies

Institute of Electrical and Electronics Engineers, International Association for Cryptologic Research, Association for Computing Machinery.