

Dimitrios (Dimitris) Papadopoulos CV

Address: 111 Cummington Mall, Boston MA 02215 USA

Tel: +1 (617) 435-0070

Email: dipapado@bu.edu

Website: cs-people.bu.edu/dipapado

Education

<i>2011 - present</i>	PhD program in Computer Science, Boston University Advisor: Nikos Triandopoulos Thesis Title: Practical Verifiable Computation: Function-specific constructions and a composition framework
<i>2010</i>	Diploma in Applied Mathematics, School of Applied Mathematics & Physical Sciences, National Technical University of Athens (NTUA) Advisor: Antonios Symvonis Thesis Title: Design and development of application for the implementation of mixed map labeling algorithms

Research Interests

My research areas span theory and applications of cryptography and computer and network security. I am interested in the development and implementation of practical cryptographic solutions for verifiable computation, secure Internet protocols, authenticated database queries, and privacy of data stored in the cloud. In particular, I focus on constructions that are not only provably secure but also efficient, aiming for adoption in practice. Other interests include economic aspects of secure cloud computing and the practical impact of security extensions of core Internet protocols.

Publications (authors listed in alphabetic order)

<i>VLDB 2015</i>	Practical Authenticated Pattern Matching with Optimal Proof Size Dimitrios Papadopoulos, Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos
<i>NDSS 2015</i>	NSEC5: Provably Preventing DNSSEC Zone Enumeration Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin, Sachin Vasant, Asaf Ziv
<i>ACM CCS 2014</i>	Taking Authenticated Range Queries to Arbitrary Dimensions Dimitrios Papadopoulos, Stavros Papadopoulos, Nikos Triandopoulos
<i>USENIX Security 2014</i>	TRUESET: Faster Verifiable Set Computations Ahmed Kosba, Dimitrios Papadopoulos, Charalampos Papamanthou, Mahmoud Sayed, Elaine Shi, Nikos Triandopoulos
<i>PKC 2014</i>	Verifiable Set Operations over Outsourced Databases Ran Canetti, Omer Paneth, Dimitrios Papadopoulos, Nikos Triandopoulos
<i>SOFSEM 2011</i>	Combining Traditional Map Labeling with Boundary Labeling Michael Bekos, Michael Kaufmann, Dimitrios Papadopoulos, Antonios Symvonis
<i>ePrint Archive (Jan 2016)</i>	NSEC5 from Elliptic Curves Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin
<i>under submission</i>	Practical Secure Computation for Online Social Networks Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos, Alessandra Scaffuro, Nikos Triandopoulos
<i>under submission</i>	Zero-Knowledge Accumulators and Set Algebra Esha Ghosh, Olga Ohrimenko, Dimitrios Papadopoulos, Roberto Tamassia, Nikos Triandopoulos
<i>BU Tech. Report (Jan 2015)</i>	Stretching NSEC3 to the Limit: Efficient Zone Enumeration Attacks on NSEC3 Variants Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin, Sachin Vasant, Asaf Ziv

Work Experience

<i>Jun - Sep 2015</i>	Research Intern at Verisign Labs, Reston VA, USA (Mentor: Duane Wessels)
<i>Jun - Sep 2014</i>	Research Intern at IBM Research, Zurich, Switzerland (Mentor: Christian Cachin)
<i>June 2010 - November 2010</i>	Junior Software Engineer at Datamine Ltd., Athens Greece (Internship)
<i>June 2008 - October 2008</i>	National Statistical Survey of Greece, National Accounts, Athens Greece (Internship)

Selected Invited Talks

<i>University of Maryland (Sep. 2015)</i>	NSEC5: Provably Presenting DNSSEC Zone Enumeration
<i>IBM Research Zurich (Jul. 2014)</i>	Multi-Writer Authenticated Data Structures
<i>Athecrypt 2015</i>	Verifiable Dataset Queries: Cryptographic Tools and Constructions for Specific Functions
<i>Athecrypt 2014</i>	Verifiable Computation Can Be Practical – The Case of Set Operations
<i>Athecrypt 2013</i>	Efficient & Parallelizable Authenticated Pattern Matching and XML Search

Teaching

<i>Spring 2014, 2015</i>	Teaching Assistant for CS558 Network Security (taught by Prof. Sharon Goldberg, BU)
<i>Fall 2012</i>	Teaching Assistant for CS237 Probability in Computing (taught by Prof. Sharon Goldberg, BU) <i>received the departmental Teaching Fellow Award</i>
<i>Spring 2010</i>	Lab Assistant for Software Applications in Java (taught by Prof. Antonios Symvonis, NTUA)

Awards

Boston University Computer Science Research Excellence Award (2015)
Boston University Computer Science Teaching Fellow Award (2013)
Gatzoyiannis Scholarship (2012-2015)
Outstanding Academic Performance Scholarship, Gerondelis Foundation (2012)

Patents

Authenticated hierarchical set operations and applications, US Patent No. 9049185, Mar. 2013
D. Papadopoulos, R. Canetti, N. Triandopoulos
Authenticated Pattern Matching and Exact Path Queries, US Patent (pending)
C. Papamanthou, D. Papadopoulos, R. Tamassia, E. Tremel, N. Triandopoulos

Academic Service

External Reviewer/Sub-reviewer:	Eurocrypt'16, EuroS&P'16, SIGMOD'16,'14,'13, SIGCOMM-CCR'16, TCC'15, ACM-CCS'15,'14, ACNS'15, CANS'15, TKDE'15, Crypto'14, ICALP'14, SIGCOMM'14, NSDI'14, CCSW'14, ICDE'14, ISC'14, BalkanCryptSec'14, IJIS'14, IEE S&P Magazine'13, ICJ'13, HotCloud'12
Local Organizing Committee Volunteer	Eurocrypt'13

REFERENCES PROVIDED UPON REQUEST