

# ALIN TOMESCU

## PERSONAL INFORMATION

*email* [atom@alum.mit.edu](mailto:atom@alum.mit.edu)  
*website* <http://alinush.org>  
*github* <https://github.com/alinush>  
*twitter* <https://twitter.com/alinush407>

## SHORT BIO

I am interested in applied cryptography, mostly walking the fine line between theory and practice. In the past, I've worked on oblivious RAMs, public-key distribution, authenticated data structures, and threshold cryptography. I especially enjoy implementing and open-sourcing my work. In the present, I am working on anonymous payments, vector commitments, verifiable secret sharing and distributed key generation.

I sometimes blog about my work and muse about other things on my website.

For paper LaTeX and PDFs, slides, code artifacts and talk videos, please see [alinush.github.io/papers.html](http://alinush.github.io/papers.html).

## RESEARCH EXPERIENCE

<i>Research Scientist</i>	<i>2021-present</i> <b>VMWARE RESEARCH</b> Working on anonymous payments and authenticated data structures.
<i>Postdoctoral Researcher</i>	<i>2020-2021</i> <b>VMWARE RESEARCH</b> Worked on aggregatable and maintainable vector commitments, RSA-based authenticated dictionaries, aggregatable distributed key generation, and other applied cryptography topics.
<i>Research Intern</i>	<i>Summer 2017 &amp; 2018</i> <b>VMWARE RESEARCH</b> Worked on multi-party computation protocols via verifiable secret sharing. Worked on scaling byzantine fault tolerance protocols using threshold signatures. Implemented a fast C++ library for RSA and BLS threshold signatures. Designed efficient anonymous cryptocurrencies without zk-SNARKs. <i>Mentors:</i> Ittai ABRAHAM and Dahlia MALKHI
<i>Research Assistant</i>	<i>2013-2020</i> <b>MIT CSAIL</b> Focused on cryptocurrencies, public-key distribution, authenticated data structures, secure communication, anonymity and secure web applications. <i>Lab:</i> Computation Structures Group <i>Advisor:</i> Prof. Srinivas DEVADAS
<i>Research Assistant</i>	<i>2011-2012</i> <b>STONY BROOK UNIVERSITY</b> Worked on access pattern privacy research. Developed PrivateFS, the first oblivious filesystem. <i>Lab:</i> Network Security and Applied Crypto Lab <i>Advisor:</i> Prof. Radu SION

## EDUCATION

<i>Doctor of Philosophy</i>	2015-2019	MASSACHUSETTS INSTITUTE OF TECHNOLOGY	School: Electrical Engineering and Computer Science Thesis: <i>How to Keep a Secret and Share a Public Key (Using Polynomial Commitments)</i> Advisor: Prof. Srinivas DEVADAS
	2013-2015	MASSACHUSETTS INSTITUTE OF TECHNOLOGY	GPA: 4.7 (out of 5) · Major: Computer Science Thesis: <i>PowMail: Want To Fork? Do Some Work.</i> Description: This thesis explored the idea of using cryptographic puzzles computed by email users to prevent equivocation in public key directories. Advisor: Prof. Srinivas DEVADAS
	2008-2012	STONY BROOK UNIVERSITY	GPA: 3.98 (out of 4) · Major: Computer Science <i>Summa Cum Laude</i> · Honors Advisor: Associate Prof. Radu SION
<i>Masters of Science</i>			
<i>Bachelors of Science</i>			
WORK EXPERIENCE			
<i>Head of Research and Development</i>	2012-2013, Summer 2014	PRIVATE MACHINES	Designed, implemented and deployed the first prototype of the CipherRack secure cloud infrastructure. Designed and implemented cryptographic protocols for CipherLocker, a secure searchable cloud file storage engine, as well as other proprietary cryptographic protocols.
	Summer 2011	MICROSOFT	Developed a flexible performance framework in C# for testing critical Microsoft SQL stored procedures used throughout their AdCenter Business Intelligence system. Developed an ASP .NET user interface in C# for charting and graphing performance results across release cycles. Developed an automated code deployment tool for running daily basic viability tests on the latest builds.
<i>Software Development Engineer in Test (Intern)</i>			
<i>Information Technology Specialist</i>	2008-2009	STONY BROOK UNIVERSITY	Developed websites for various programs within the Outreach Division of Stony Brook's Professional Education Program. Developed and maintained Microsoft Access databases. Created and administered LISTSERV mailing lists. Assisted staff with various computer-related issues.

## MANUSCRIPTS

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · ePrint'21 · Shravan SRINIVASAN, Alex CHEPURNOY, Charalampos PAPAMANTHOU, Alin TOMESCU, Yupeng ZHANG

*Authenticated Dictionaries with Cross-Incremental Proof (Dis)aggregation* · ePrint'20 · Charalampos PAPAMANTHOU, Alin TOMESCU, Yu XIA, Zachary NEWMAN

*How to compute all Pointproofs* · ePrint'20 · Alin TOMESCU

## PUBLICATIONS

*Reaching Consensus for Asynchronous Distributed Key Generation* · PODC'21 · Ittai ABRAHAM, Philipp JOVANOVIĆ, Mary MALLER, Sarah MEIKLEJOHN, Gilad STERN, Alin TOMESCU

*Aggregatable Distributed Key Generation* · EUROCRYPT'21 · Kobi GURKAN, Philipp JOVANOVIĆ, Mary MALLER, Sarah MEIKLEJOHN, Gilad STERN, Alin TOMESCU

*Aggregatable Subvector Commitments for Stateless Cryptocurrencies* · SCN'20 · Alin TOMESCU, Ittai ABRAHAM, Vitalik BUTERIN, Justin DRAKE, Dankrad FEIST, Dmitry KHOVRATOVICH

*Towards Scalable Threshold Cryptosystems* · IEEE S&P'20 · Alin TOMESCU, Robert CHEN, Yiming ZEHNG, Ittai ABRAHAM, Benny PINKAS, Guy Golan GUETA, Srinivas DEVADAS

*Transparency Logs via Append-only Authenticated Dictionaries* · ACM CCS'19 · Alin TOMESCU, Vivek BHUPATIRAJU, Dimitrios PAPADOPOULOS, Charalampos PAPAMANTHOU, Nikos TRIANDOPOULOS, Srinivas DEVADAS

*Efficient Verifiable Secret Sharing with Share Recovery in BFT Protocols* · ACM CCS'19 · Soumya BASU, Alin TOMESCU, Ittai ABRAHAM, Dahlia MALKHI, Michael K. REITER, Emin Gün SIRER

*SBFT: A Scalable and Decentralized Trust Infrastructure* · DSN'19 · Guy Golan GUETA, Ittai ABRAHAM, Shelly GROSSMAN, Dahlia MALKHI, Benny PINKAS, Michael K. REITER, Dragos-Adrian SEREDINSCHI, Orr TAMIR, Alin TOMESCU

*Catena: Efficient Non-equivocation via Bitcoin* · IEEE S&P'17 · Alin TOMESCU, Srinivas DEVADAS

*PriviPK: Certificate-less and secure email communication* · Computer & Security'17 · Mashael ALSABAH, Alin TOMESCU, Ilia LEBEDEV, Dimitrios SERPANOS, Srinivas DEVADAS

*PrivateFS: A Parallel Oblivious Filesystem* · ACM CCS'12 · Peter WILLIAMS, Radu SION, Alin TOMESCU

## PATENTS

*Two-round byzantine fault tolerant (BFT) state machine replication (SMR) protocol with linear authenticator complexity and optimistic responsiveness* · US Patent App · June 2021 Ittai ABRAHAM, Alin TOMESCU, Guy Golan GUETA, Neil GIRIDHARAN, Heidi HOWARD

*Byzantine fault tolerance with verifiable secret sharing at constant overhead* · US Patent US10572352B2 · Feb. 25th, 2020 · Soumya BASU, Alin TOMESCU, Dahlia MALKHI, Michael REITER, Adrian SEREDINSCHI, Ittai ABRAHAM, Guy Golan GUETA

## INVITED TALKS

Some recordings can be found [here](#).

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · Protocol Labs · May 28th, 2021

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · Cornell University · April 8th, 2021

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · Cornell University · March 24th, 2021

*Vector Commitments for Stateless Cryptocurrencies* · Duke University · Privacy & Security Seminar · March 9th, 2021

*Towards Scalable Threshold Cryptosystems* · Real World Decentralized Cryptography · January 15th, 2021

*Authenticated Data Structures for Stateless Validation and Transparency logs* · University College London · InfoSec Seminar · November 5th, 2020

*Authenticated Dictionaries with Cross-incremental Proof (Dis)aggregation* · zkStudyClub · October 28th, 2020

*Towards Scalable Threshold Cryptosystems* · Cornell University · June, 2020

*Aggregatable Subvector Commitments* · zkStudyClub · May 13th, 2020

*Towards Scalable Threshold Cryptosystems* · BU Security Seminar · Boston University · January 29th, 2020

*Append-only Authenticated Dictionaries and Their Applications* · MIT Digital Currency Initiative · March 27th, 2019

*Append-only Authenticated Dictionaries and Their Applications* · Xi'an International Workshop on Blockchain 2018 · December 14th, 2018

*Append-only Authenticated Dictionaries and Their Applications* · Modular Approach to Cloud Security (MACS) Project Meeting · December 7th, 2018

*Bandwidth-efficient Transparency Logs via Append-only Authenticated Dictionaries* · VISA Research · July 13th, 2018

*Bandwidth-efficient Transparency Logs via Append-only Authenticated Dictionaries* · Stanford Security Seminar · Stanford University · June 26th, 2018

*Append-only Authenticated Dictionaries and Their Applications* · Oasis Labs · June 21st, 2018

*Append-only Authenticated Dictionaries and Their Applications* · LPD · École Polytechnique Fédérale de Lausanne (EPFL) · January 31st, 2018

*Catena: Efficient Non-equivocation via Bitcoin* · Cambridge Blockchain Meetup · December 13th, 2017

*Append-only Authenticated Dictionaries and Their Applications* · Security Reading Group · University of Maryland · October 27th, 2017

*Secure communication via proof-of-work* · CSAIL Advisory Board · MIT · May 3rd, 2016

*Pulsar: A Space and Bandwidth Efficient, Trustworthy Public Key Directory* · Digital Currency Initiative (DCI) · MIT · April 6th, 2016

#### ACCEPTED TALKS

*Catena: Preventing Lies with Bitcoin* · New England Security Day (NESD) · Worcester Polytechnic Institute · November 28th, 2016

#### PANELS

*On “blockchains”* · TechConnect · Boston University · February 16th, 2018

#### OPEN SOURCE CONTRIBUTIONS

[QEMU](#) · [Eucalyptus](#) · [RELIC](#) · [Concord BFT](#) · [libfqfft](#)

#### PROGRAM COMMITTEES

ACM Advances in Financial Technologies (AFT) · 2021

ACM Cloud Computing Security Workshop (CCSW) · 2020 · 2021

ACM Conference on Computer and Communication Security (CCS) · 2021

Financial Cryptography (FC) · 2021

USENIX Security · 2022

## EXTERNAL REVIEWER

ACM Advances in Financial Technologies (AFT) · 2020

ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) · 2017

ACM ASIA Conference on Computer and Communication Security (AsiaCCS) · 2020

ACM Conference on Computer and Communication Security (CCS) · 2016 · 2020

ACM Symposium on Principles of Distributed Computing (PODC) · 2021

IACR ASIACRYPT · 2020

IACR CRYPTO · 2021

IACR Security and Cryptography for Networks (SCN) · 2016

IACR TCC · 2021

IEEE Security and Privacy (S&P) · 2018 · 2019 · 2020

IEEE Transactions on Information Forensics & Security (TIFS) · 2021

IEEE/ACM International Symposium on Microarchitecture (MICRO) · 2017

Network and Distributed Systems Symposium (NDSS) · 2019

Transactions on Privacy and Security (TOPS) · 2017 · 2019

## TEACHING &amp; MENTORING

*Guest Lectures*

Duke University · Fall 2021 · CS590.02: Cryptocurrency and Cryptography · Aggregatable, Maintainable and Unstealable Vector Commitments

MIT · Spring 2018 · MAS.S62 Cryptocurrency Engineering and Design · Bitcoin-based non-equivocation schemes · [YouTube](#)

2017-2019 MIT PRIMES

*Research Mentor*

Mentored 4 high school students in applied cryptography research. Planned reasonable research projects for students with deliverables. Met with students weekly to assess progress and discuss research topics.

*Student Awards:*

JOHN KUSZMAUL · 2017 Siemens semifinalist  
 ROBERT CHEN · 2017 Siemens semifinalist  
 YIMING ZHENG · 2017 Siemens semifinalist  
 VIVEK BHUPATIRAJU · 2018 Regeneron STS scholar  
 VIVEK BHUPATIRAJU · 2018 ISEF 3rd Special Award (from ACM)  
 VIVEK BHUPATIRAJU · 2018 ISEF 1st Special Award (Science of Security, from NSA)  
 ROBERT CHEN · 2019 Regeneron STS scholar

Spring 2014 INTRODUCTION TO ALGORITHMS (6.006)

*Teaching Assistant at MIT*

Taught four recitation sessions each week.  
 Taught two review sessions before midterm exams.  
 Developed programming assignments for the problem sets.  
 Wrote recitation notes for students.  
 Developed questions for the student exams.

Helped students on the class discussion board and over email.  
 Held biweekly office hours.  
 Provided additional learning resources for my own section students.

*Spring 2011*      **ADVANCED C/C++ PROGRAMMING (CSE230)**

*Teaching Assistant  
at Stony Brook  
University*

Taught four CSE230 lectures on object oriented design in C++.  
 Helped students with C and C++ programming questions during office hours.

*Fall 2009*      **INTRODUCTION TO JAVA (CSE114)**

*Teaching Assistant  
at Stony Brook  
University*

Held biweekly, one-hour and twenty-minutes programming labs.  
 Responsible for overseeing, teaching and grading thirty students in CSE114.  
 Helped and advised students during office hours and over email.

*2009–2012*      **STONY BROOK COMPUTING SOCIETY**

*Exam Reviewer*

Taught review sessions for Java programming, discrete mathematics and data structures exams.

**OTHER INFORMATION**

*Awards*

Avery Ashdown Leadership Award · *Ashdown House, MIT* · 2015 & 2019  
 Academic Excellence in Computer Science · *Computer Science Department at Stony Brook University* · 2012  
 The SUNY Chancellor's Award for Student Excellence · *State University of New York (SUNY)* · 2012  
 Undergraduate Recognition Award for Academic Excellence · *Stony Brook University* · 2012  
 Outstanding Academic Achievement Award · *Stony Brook University* · 2009–2012  
 University Scholars Senior Leadership Award · *Stony Brook University* · 2011  
 February 2011 Student of the Month Award · *National Residence Hall Honorary Chapter at Stony Brook University* · 2011

*Leadership*

Graduate Student Leadership Initiative Fellow & Cambridge Fellow · *Massachusetts Institute of Technology* · Spring 2017  
 Secretary of the Ashdown House Executive Committee · *Massachusetts Institute of Technology* · 2014–2015  
 President of the Romanian Student Association · *Massachusetts Institute of Technology* · 2014–2019  
 Student Ambassador for the Stony Brook Computer Science Department · *Stony Brook University* · 2011–2012  
 Cofounder, Vice-President and President of the Stony Brook Game Developers Club · *Stony Brook University* · 2009–2010

*Communication  
Skills*

Best Computer Science Senior Honors Project Presentation Award · *Stony Brook University* · 2012

*Languages*

ROMANIAN · Native language  
 ENGLISH · Fluent  
 SPANISH · Basic (simple words and phrases only)  
 FRENCH · Basic (simple words and phrases only)

*Interests*

Piano · Philosophy · Weightlifting · Dance

September 28, 2021