

# ALIN TOMESCU

## PERSONAL INFORMATION

<i>email</i>	<a href="mailto:atom@alum.mit.edu">atom@alum.mit.edu</a>
<i>website</i>	<a href="http://alinush.org">http://alinush.org</a>
<i>github</i>	<a href="https://github.com/alinush">https://github.com/alinush</a>
<i>twitter</i>	<a href="https://twitter.com/alinush407">https://twitter.com/alinush407</a>

## 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 &amp; Head of Cryptography</i>	<i>2022-present</i> <b>APTOS LABS</b> Working on applied cryptography for high-throughput smart contract blockchains.
<i>Research Scientist</i>	<i>2021-2022</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>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

*Doctor of Philosophy*      2015-2019      MASSACHUSETTS INSTITUTE OF TECHNOLOGY  
 School: Electrical Engineering and Computer Science  
 Thesis: *How to Keep a Secret and Share a Public Key (Using Polynomial Commitments)*  
 Advisor: Prof. Srinivas DEVADAS

*Masters of Science*      2013-2015      MASSACHUSETTS INSTITUTE OF TECHNOLOGY  
 GPA: 4.7 (out of 5) · Major: Computer Science  
 Thesis: *PowMail: Want To Fork? Do Some Work.*  
 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

*Bachelors of Science*      2008-2012      STONY BROOK UNIVERSITY  
 GPA: 3.98 (out of 4) · Major: Computer Science  
*Summa Cum Laude* · Honors  
 Advisor: Associate Prof. Radu SION

## WORK EXPERIENCE

*Head of Research and Development*      2012-2013,  
*Summer*      PRIVATE MACHINES  
 2014  
 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.

*Software Development Engineer in Test (Intern)*      *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.

*Information Technology Specialist*      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.

## ACADEMIC MANUSCRIPTS

UTT: *Decentralized Ecash with Accountable Privacy* · ePrint'22 · Alin TOMESCU, Adithya BHAT, Benny APPLEBAUM, Ittai ABRAHAM, Guy GUETA, Benny PINKAS, Avishay YANAI

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

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

## ACADEMIC PUBLICATIONS

- Distributed Randomness using Weighted VRFs* · EUROCRYPT'25 · Sourav DAS, Benny PINKAS, Alin TOMESCU, Zhuolun XIANG
- Verifiable Secret Sharing Simplified* · IEEE S&P'25 · Sourav DAS, Zhuolun XIANG, Alin TOMESCU, Alexander SPIEGELMAN, Benny PINKAS, Ling REN
- Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · USENIX Security'22 · Shravan SRINIVASAN, Alex CHEPURNOY, Charalampos PAPAMANTHOU, Alin TOMESCU, Yupeng ZHANG
- 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 TRIANOPOULOS, 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 · Mashaël ALSABAH, Alin TOMESCU, Ilia LEBEDEV, Dimitrios SERPANOS, Srinivas DEVADAS
- PrivateFS: A Parallel Oblivious Filesystem* · ACM CCS'12 · Peter WILLIAMS, Radu SION, Alin TOMESCU

## PATENTS

- Accountable decentralized anonymous payments* · US Patent US20240265373A1 · August 2023 Alin TOMESCU, Adithya BHAT, Ittai ABRAHAM, Guy Golan GUETA, Binyamin PINKAS, Avishay YANAI,
- Two-round byzantine fault tolerant (BFT) state machine replication (SMR) protocol with linear authenticator complexity and optimistic responsiveness* · US Patent 20240028612 · Jan 2024 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

## ACADEMIC TALKS

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

*Keyless blockchain accounts from ZKPs* · Universitat Pompeu Fabra · May 12th, 2025

*The latency price of threshold cryptosystems in blockchains* · FC'25 · April 17th, 2025

*Keyless blockchain accounts from ZKPs* · Northeastern University · February 28th, 2025

*Keyless blockchain accounts from ZKPs* · MIT CSAIL Security Seminar · February 27th, 2025

*Keyless blockchain accounts from ZKPs* · NoirCon 1 · February 24th, 2025

*Distributed randomness using weighted VRFs* · IOHK Research & Development Seminar · February 10th, 2025

*Distributed randomness using weighted VRFs* · Bay Area Crypto Day · November 1st, 2024

Invited talk: *How should a blockchain keep a secret?* · Schloss Dagstuhl · Seminar on Secure Distributed Computing · September 2nd, 2024

*Distributed randomness using weighted VRFs* · Science of Blockchain Conference (SBC) · August 8th, 2024

*Aptos Keyless: Blockchain Accounts without Secret Keys* · zkSummit'11 (ZK11) · April 10th, 2024

*UTT: Sensibly-Anonymous Decentralized Payments from Randomizable Signatures* · Stanford Security Seminar · November 16th, 2023

*UTT: Sensibly-Anonymous Decentralized Payments without zkSNARKs* · Science of Blockchain Conference (SBC) · August 29th, 2023

*UTT: Fast, Accountable, Anonymous Payments without zkSNARKs* · UC Santa Cruz · April 27th, 2023

*UTT: Fast, Accountable, Anonymous Payments without zkSNARKs* · ACE Symposium at Yale University · April 21st, 2023

*UTT: Decentralized Ecash with Accountable Privacy* · a16z Crypto · November 17th, 2022

*Fantastic Trees and How to Hash Them* · Protocol Labs VC Day · March 24th, 2022

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · Duke · September 27th, 2021

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

*Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments* · Axelar · 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

*Aggregatable Subvector Commitments* · SCN'20 · September 14th, 2020

*Towards Scalable Threshold Cryptosystems* · Cornell University · June 16th, 2020

*Towards Scalable Threshold Cryptosystems* · IEEE S&P'20 · May 19th, 2020

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

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

*Transparency Logs via Append-only Authenticated Dictionaries* · ACM CCS'19 · November 13th, 2019

*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

*Catena: Efficient Non-equivocation via Bitcoin* · IEEE S&P'17 · May 23rd, 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

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

## PUBLIC SPEAKING

**Panel** · *Emerging Research in On-chain Randomness* · 3rand Workshop · Supra Oracles · June 19th, 2024

**Podcast** · *Distributed On-Chain Randomness and Keyless Accounts* · ZeroKnowledge Podcast · March 20th, 2024

**Podcast** · *Keyless Accounts, Randomness and ZKPs* · Absolutely Zero Knowledge · February 15th, 2024

**Tutorial** · *How to Use Aptos Roll – Aptos' On-Chain Randomness API* · Aptos Network · February 1st, 2024

**Twitter Space** · *zk: zero knowledge proofs* · Flipside · May 24th, 2023

**Panel** · *zkPrivacy* · zkWeek · Jump Crypto · May 19th, 2023

**Podcast** · *Stateless Validation* · ZeroKnowledge Podcast · November 18th, 2020

**Panel** · *On "blockchains"* · TechConnect · Boston University · February 16th, 2018

## OPEN SOURCE CONTRIBUTIONS

**Aptos Core** · **Move language** · **RELIC** · **libfqfft** · **Concord BFT** · **QEMU** · **Eucalyptus**

## 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 · 2022

Financial Cryptography (FC) · 2021

IACR CRYPTO · 2023

IEEE Security & Privacy (Oakland) · 2023 · 2026

Science of Blockchain Conference (Stanford's SBC) · 2023 · 2024 · 2025

USENIX Security · 2022 · 2025

VMware R&D Innovation Offsite (RADIO) · 2022

Workshop on Cryptography Applied to Transparency Systems (CATS) · 2023

#### EXTERNAL REVIEWER

ACM Advances in Financial Technologies (AFT) · 2020 · 2022

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 · 2022

IACR ASIACRYPT · 2020

IACR CRYPTO · 2021

IACR RWC · 2025

IACR Security and Cryptography for Networks (SCN) · 2016

IACR TCC · 2021

IEEE Security and Privacy (S&P) · 2018 · 2019 · 2020 · 2024

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

USENIX Security · 2023

#### TEACHING & 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 officer 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*

Best Reviewer Award · ACM CCS · 2021 · 2022  
 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  
 Best Computer Science Senior Honors Project Presentation Award · Stony Brook University · 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

<i>Leadership</i>	Graduate Student Leadership Initiative Fellow & Cambridge Fellow · <i>Massachusetts Institute of Technology</i> · Spring 2017
	Secretary of the Ashdown House Executive Committee · <i>Massachusetts Institute of Technology</i> · 2014–2015
	President of the Romanian Student Association · <i>Massachusetts Institute of Technology</i> · 2014–2019
	Student Ambassador for the Stony Brook Computer Science Department · <i>Stony Brook University</i> · 2011–2012
	Cofounder, Vice-President and President of the Stony Brook Game Developers Club · <i>Stony Brook University</i> · 2009–2010
<i>Languages</i>	ROMANIAN · Native language
	ENGLISH · Fluent
	SPANISH · Basic (simple words and phrases only)
	FRENCH · Basic (simple words and phrases only)
<i>Interests</i>	Motorcycling · Piano · Philosophy · Weightlifting · Dance

July 22, 2025