ALIN TOMESCU

PERSONAL INFORMATION

email	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 commitmments, 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`.

RESEARCH EXPERIENCE

2022-present — Aptos Labs

Research Scientist

Working on applied cryptography for high-throughput smart contract blockchains.

2021-2022 — VMware Research

Research Scientist

Working on anonymous payments and authenticated data structures.

2020-2021 — VMware Research

Postdoctoral Researcher

Worked on aggregatable and maintainable vector commitments, RSA-based authenticated dictionaries, aggregatable distributed key generation, and other applied cryptography topics.

Summer 2017 & 2018 — VMware Research

Research Intern

Worked on multi-party computation protocols via verfiable 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.

2013-2020 — MIT CSAIL

Research Assistant

Focused on cryptocurrencies, public-key distribution, authenticated data structures, secure communication, anonymity and secure web applications.

Lab: Computation Structures Group
Advisor: Prof. Srinivas Devadas

2011-2012 — Stony Brook University

Research Assistant

Worked on access pattern privacy research.
Developed PrivateFS, the first oblivious filesystem.

Lab: Network Security and Applied Crypto Lab
Advisor: Prof. Radu Sion

EDUCATION

2015-2019 **Massachusetts Institute of Technology**

Doctor of Philosophy

School: Electrical Engineering and Computer Science
Thesis: *How to Keep a Secret and Share a Public Key (Using Polynomial Commitments)*
Advisor: Prof. Srinivas Devadas

2013-2015 **Massachusetts Institute of Technology**

Masters of Science

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

2008-2012 **Stony Brook University**

Bachelors of Science

GPA: 3.98 (out of 4) · Major: Computer Science
Summa Cum Laude · Honors
Advisor: Associate Prof. Radu Sion

WORK EXPERIENCE

2012–2013, Summer 2014 **Private Machines**

Head of Research and Development

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**

Software Development Engineer in Test (Intern)

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.

2008–2009 **Stony Brook University**

Information Technology Specialist

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

Distributed Randomness using Weighted VRFs · ePrint'24 · Sourav Das, Benny Pinkas, Alin Tomescu, Zhuolun Xiang

A New Paradigm for Verifiable Secret Sharing · ePrint'23 · Sourav Das, Zhuolun Xiang Alin Tomescu, Alexander Spiegelman, Benny Pinkas, Ling Ren

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

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 Jovanovic, Mary Maller, Sarah Meiklejohn, Gilad Stern, Alin Tomescu

Aggregatable Distributed Key Generation · EUROCRYPT'21 · Kobi Gurkan, Philipp Jovanovic, 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, Srini 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

ACADEMIC TALKS

(Some recordings can be found here**).**

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

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

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

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

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 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

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

Motorcycling · Piano · Philosophy · Weightlifting · Dance

August 30, 2024