

Raluca Ada Popa

CSAIL, MIT,
32 Vassar Street, Room 32-G982,
Cambridge, MA 02139.

ralucap@mit.edu
<http://www.mit.edu/~ralucap/>

Education

2010-present: Massachusetts Institute of Technology (MIT), Doctoral candidate. Advisor: Nikolai Zeldovich. GPA: 5.0/5.0.

2009-2010: MIT, Masters of Engineering. Advisor: Hari Balakrishnan. GPA: 5.0/5.0. Thesis: “Provable and Practical Location Privacy for Vehicular and Mobile Systems”.

2006-2009: MIT, two B.S. degrees, Computer Science and Mathematics. Thomas A. Pappas Scholarship GPA: 5.0/5.0. I transferred to MIT after attending Caltech for my freshman year. Research advisors: Prof. Ronald L. Rivest and Prof. Barbara Liskov.

2005-2006: California Institute of Technology (Caltech). GPA: 4.1/4.0.

2001-2005: (High-School) C. N. Gheorghe Lazar, Sibiu, Romania. Valedictorian. School merit scholarship for outstanding academic achievement. GPA: 9.96/10. Baccalaureate: 9.91/10.

Honors and Awards

2011 Google Ph.D. Fellowship, 15 nationwide winners

2010 Charles and Jennifer Johnson award for best CS Masters of Engineering thesis

2010 Morris Joseph Levin Award for best MasterWorks presentation

2009 MIT Irwin and Joan Jacobs Presidential Fellowship for graduate studies (one year)

2009 CRA Outstanding Undergraduate Award for research, Female Winner (one female winner nationwide)

2009 MIT CSAIL Pogogyants Award for Undergraduate Research

2008 Google Anita Borg Scholarship, Winner

2006 Caltech Upper Class Merit Award, Carnation Scholarship

2006 CRA-Women Distributed Mentor Project Award for Summer Research

Earned highest grade in class at MIT for 6.857 (Computer and Networks Security) and *Circuits and Electronics (6.002)* (200 students); Letter of Recognition for *Computation Structures (6.004)* and *Technical Presentation (6.UAT)*, and a few others.

Earned highest grade in class at Caltech for Cs1 (Introduction to Computation), Ma1b (Calculus of One and Several Variables and Linear Algebra), Ph1a (Classical Mechanics and Electromagnetism), and Ph1b (Classical Mechanics and Electromagnetism).

2008 George C. Newton Outstanding Undergraduate Laboratory Project Prize, Third, MIT

2007 Best Game Award for the final project in *Lab in Software Engineering (6.170)*, MIT

Phi Beta Kappa Chapter Xi Honor Society

MIT Electrical and Computer Engineering Honor Society (HKN)

Research Projects and Summer Internships

Current projects:

Secure databases on the cloud. With Professors Nikolai Zeldovich and Hari Balakrishnan, MIT, I designed and built a practical DBMS, CryptDB, whose aim is to preserve the confidentiality of customer databases outsourced to the cloud. CryptDB achieves this goal by enabling the cloud database server to execute queries over encrypted data. It is the first such practical system, supports a wide range of SQL queries, and offloads the whole query execution to the server.

Oblivious outsourced storage (summer 2010). With Professors David Mazières and Dan Boneh from Stanford University, I constructed a novel protocol for guaranteeing strong privacy of customer data stored in a key-value store on a cloud. Besides encrypting the data, our protocol hides even the user access patterns to the data on the cloud. Such access patterns can leak significant information about the content of the data because an adversary can sometimes perform frequency analysis on user requests.

Location Privacy for Mobile Systems (including summer 2008). With Professors Hari Balakrishnan (MIT) and Andrew J. Blumberg (UT Austin), I have been working on two projects about protecting location privacy of individuals in mobile systems applications. The first project, VPriv, enables an untrusted server to compute functions of a driver’s path (e.g., total tolling cost based on path for a month) without learning the path of a driver. The second project, PrivStats, enables a server to compute ag-

gregate statistics over the data from users in social, vehicular, or online review systems without learning any information about any individual's input (preferences, location, reviews) other than the result of the statistics.

Past projects:

Secure Cloud Storage. With Dr. Helen J. Wang and Dr. Jacob R. Lorch from Microsoft Research, Redmond, we designed and built a secure cloud storage system that provides detection and provability of key security properties of user data stored on the cloud; moreover, we proposed mechanisms on top of which one could build cloud Service Level Agreements regarding security.

Electronic Voting (12/2006-06/2009). With Professor Ronald L. Rivest, we developed statistically strong auditing methods for certifying electronic voting systems.

Byzantine Fault Tolerant Systems (06/2007-06/2008, including summer 2007). Under the guidance of Professor Barbara Liskov, I worked on two projects: a Byzantine fault tolerant cooperative caching system (as a part of a larger safe storage system), and a highly-scalable membership management system, Census.

Software Reliability (06/2006-12/2006, including summer 2006). CRA Distributed Mentor Project Award Intern. With Professor Yuanyuan Zhou from University of Illinois at Urbana-Champaign, we studied a new class of bugs (inconsistency bugs) and then developed a tool, MUVI, that detected around 40 real bugs in Unix, Mozilla, and MySQL code.

Research Talks

06/2011 Enabling Security in Cloud Storage SLAs with CloudProof. In the Proceedings of the 2011 USENIX Annual Technical Conference (**Usenix'11**).

04/2011 & 05/2011 Confidentiality for Database Applications with Encrypted Query Processing. Invited talk at Berkeley's Security Seminar, Berkeley's Cloud Computing Seminar, Quanta Research, BBN Technologies, and others.

01/2011 CryptDB: A Practical Encrypted Relational DBMS. New England Database Summit (**NEDB'11**).

09/2009 Enabling Security in Cloud SLAs. End of internship talk at Microsoft Research, Redmond.

08/2009 VPriv: Protecting Privacy in Location-Based Vehicular Services. Talk at the 18th USENIX Security Symposium, Montreal, Canada, (**USENIX SEC'09**).

04/2009 Protecting Privacy in Location-Based Vehicular Services. Poster at the 6th USENIX Symposium on Networked Systems Design and Implementation.

11/2008 Protecting Privacy in Location-Based Vehicular Services. Invited talk at University of Massachusetts, Amherst, Security Seminar.

06/2008 On Auditing Elections When Precincts Have Different Sizes. 2008 USENIX ACCURATE Electronic Voting Technology Workshop (**EVT'08**).

09/2007 Byzantine Fault Tolerant Cooperative Caching. 3rd CSAIL Student Workshop, MIT.

08/2007 On Estimating the Size and Confidence of a Statistical Audit. 2007 USENIX ACCURATE Electronic Voting Technology Workshop (**EVT'07**).

Papers

1. **Raluca Ada Popa**, Catherine M.S. Redfield, Nikolai Zeldovich, and Hari Balakrishnan. *CryptDB: Protecting Confidentiality with Encrypted Query Processing*. In the Proceedings of the 23rd ACM Symposium on Operating Systems Principles (**SOSP'11**).
2. **Raluca Ada Popa**, Hari Balakrishnan, Andrew J. Blumberg and Frank H. Li. *Privacy and Accountability for Location-Based Aggregate Statistics*. In the Proceedings of the 18th ACM Conference on Computer and Communications Security (**CCS'11**).
3. **Raluca Ada Popa**, Helen J. Wang, Jacob R. Lorch, David Molnar, and Li Zhuang. *Enabling Security in Cloud Storage SLAs with CloudProof*. In proceedings of the 2011 USENIX Annual Technical Conference (**Usenix'11**).
4. Carlo Curino, Evan P.C. Jones, **Raluca Ada Popa**, Nirmesh Malviya, Eugene Wu, Sam Madden, Hari Balakrishnan, and Nikolai Zeldovich. *Relational Cloud: A Database-as-a-Service for the Cloud*. 5th Biennial Conference on Innovative Data Systems Research (**CIDR'11**).
5. **Raluca Ada Popa**, Helen J. Wang, Jacob R. Lorch, David Molnar, and Li Zhuang. *Enabling Security in Cloud Storage SLAs with CloudProof*. TechReport MSR-TR-2010-46. Patent pending.
6. **Raluca Ada Popa**, Hari Balakrishnan, and Andrew J. Blumberg. *VPriv: Protecting Privacy in Location-Based Vehicular Services*. In the proceedings of the 18th USENIX Security Symposium (**UsenixSec'09**).

7. James Cowling, Dan Ports, Barbara Liskov, **Raluca Ada Popa**, and Abhijeet Gaikwad. *Census: Location-Aware Membership Management for Large-Scale Distributed Systems*. In the proceedings of the 2009 USENIX Annual Technical Conference (**Usenix'09**).
8. Javed A. Aslam, **Raluca Ada Popa**, and Ronald L. Rivest. *On Auditing Elections When Precincts Have Different Sizes*, In the Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (**EVT'08**).
9. Javed A. Aslam, **Raluca Ada Popa**, and Ronald L. Rivest. *On Estimating the Size and Confidence of a Statistical Audit*. In the Proceedings of the 2007 USENIX/ ACCURATE Electronic Voting Technology Workshop (**EVT'07**) held in conjunction with the 16th USENIX Security Symposium , August 2007.
10. Shan Lu, Soyeon Park, Chongfeng Hu, Xiao Ma, Weihang Jiang, Zhenmin Li, **Raluca Ada Popa**, Yuanyuan Zhou. *MUVI: Automatically Inferring Multi-Variable Access Correlations and Detecting Related Semantic and Concurrency Bugs*. In the Proceedings of the 21st ACM Symposium on Operating Systems Principles, (**SOSP'07**).

In submission/preparation

11. Dan Boneh, David Mazières, and Raluca Ada Popa. *Remote Oblivious Storage: Making Oblivious RAM practical*.
12. Raluca Ada Popa, Alessandro Chiesa, Tural Badirkhanli, and Muriel Médard. *Going Beyond Pollution Attacks: Forcing Byzantine Clients to Code Correctly*.

Leadership

02/2010 - present Founded the *Security seminar/discussion group*. The purpose of the group is to bring together systems and cryptography faculty and students from MIT and other institutions/research labs.

06/2008-06/2010 Women's Outreach Program for MIT EECS Honor Society (HKN), Chair. We organized events to attract women to computer science and electrical engineering. Our activities included freshman outreach, graduate school guidance for upperclassmen, as well as many social and networking events.

Teaching Experience

10/2007-06/2009 Undergraduate Tutor for the Office of Minority Education, MIT. Tutored individual students weekly for introductory mathematics and computer science classes.

Graduate Course Work, MIT (Grade: all A or A+)

Computer Systems and Security, 6.857; Cryptography and Cryptanalysis, 6.875; Distributed Systems, 6.824; Advanced Algorithms, 6.854; Operating Systems, 6.828; Computer Networks, 6.829; Database Systems, 6.830; Machine Learning, 6.867; Network Coding, 6.989; Quantum Complexity Theory, 6.845; Laboratory in Mathematics, 18.821; New Developments in Cryptography, 6.889; Cloud Computing Seminar, 6.897

Miscellaneous

Programming Languages: C & C++, C#, Java, SQL, Javascript, Python, Scheme, MatLab, Pascal, Unix Programming, Web Programming, Perl, PHP, and others.

Languages: Romanian, English, French, Italian, Spanish.