Sergey Gorbunov

Curriculum Vitae

Massachusetts Institute of Technology
Ray and Maria Stata Center Room G32-578,
32 Vassar Street, Cambridge, MA 02139

Email: sergeyg@mit.edu
Homepage: http://people.csail.mit.edu/sergeyg/

Education

Ph.D. Computer Science, Massachusetts Institute of Technology.

- Expected Graduation: Summer 2015
- Advisor: *Vinod Vaikuntanathan*

M.Sc. Computer Science, University of Toronto, 2012.

- Advisor: *Vinod Vaikuntanathan*
- Thesis: "Functional Encryption: Constructions and Lower Bounds"
- Overall GPA: 4.0 (out of 4.0).

H.B.Sc. Computer Science, University of Toronto, 2011.

- Specialist in Information Security with Minor in Mathematics
- With High Distinction
- Overall GPA: 4.0 (out of 4.0).

Interests

Cryptography, Networks, Secure Protocols, Software and Network Security, Privacy.

Honours and Awards

Microsoft PhD Fellowship, *MIT*, 2014-2016. Overall value: $150000.

Alexander Graham Bell Canada Graduate Scholarship (CGS-NSERC-D3), *UofT*, 2013-2016. $105000 (Declined in favor of Microsoft Fellowship starting Fall 2014)

Ontario Graduate Scholarship (OGS), *UofT*, 2012-2013. $15000

Alexander Graham Bell Graduate Scholarship (CGS-NSERC), *UofT*, 2011-2012. $17500

Ontario Graduate Scholarship (OGS) - Declined, 2011-2012. $15000

Dean's Excellence Award in Research, *UofT Mississauga*, 2011. $500

Dean's List, *UofT Mississauga*, 2009-2011

Ken Sevcik Bursary in Computer Science, *UofT*, 2010. $1767.53

NSERC Undergraduate Student Research Award (USRA), *UofT Mississauga*, 2010. $5700

Queen Elizabeth II (Aiming for the Top) Scholarship, *Ryerson University-UofT Mississauga*, 2007-2011. $14000

Mathematical and Computational Science Honour Roll, *UofT Mississauga*, 2009-2011

James H. Rattray Memorial Award for Academic Excellence, *Ryerson University*, 2008. $200

Dean's List, *Ryerson University*, 2007-2009

Entrance Scholarship, *Ryerson University*, 2007-2009. $3000

Employment

Crypto Research Intern, IBM Thomas J. Watson Research Center, June 2013 - August 2013.
- Mentor: *Shai Halevi*

Software Developer, IBM Canada Ltd., May 2009 - August 2009.
- Developed, improved and maintained tools and infrastructures of DB2 reliability, availability, serviceability and problem determination.

Teaching Experience

Course Instructor, *UofT*, Sept 2013 - Dec 2013
- Fall 2013: *CSC347 - Introduction to Information Security.* Teaching introductory topics in information security: software, systems and network security, and cryptography.

Teaching Assistant, *UofT*, Sept 2010 - May 2013
- Winter of 2013: *MAT302 - Algebraic Cryptography.* Instructor: *Vinod Vaikuntanathan.*
- Falls of 2010/2011/2012: *CSC347 - Intro. to Information Security.* Instructor: *Arnold Rosenbloom.*
- Summer of 2012: *CSC373 - Algorithm Design & Analysis.* Instructor: *Siavosh Benabbas.*

Publications

Papers Invited to Special Issues

1. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. **Attribute-Based Encryption for Circuits**. Invited to the SIAM Journal of Computing, special issue on selected papers from the ACM Symposium on the Theory of Computing (STOC) 2013.

Refereed

1. Craig Gentry, Sergey Gorbunov and Shai Halevi. **Graph-Induced Multilinear Maps from Lattices**. In TCC 2015. http://eprint.iacr.org/2014/645

2. Sergey Gorbunov, Vinod Vaikuntanathan, and Daniel Wichs. **Leveled Fully Homomorphic Signatures from Standard Lattices**. In STOC 2015. https://eprint.iacr.org/2014/897.

3. Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan and Dhinakaran Vinayagamurthy. **Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits.** In EUROCRYPT, pages 533 − 556, 2014.

4. Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. **Functional Encryption: New perspectives and Lower Bound.** In CRYPTO, pages 500 − 518, 2013.

5. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. **Attribute-Based Encryption for Circuits**. In STOC, pages 545 − 554, 2013.

6. Sergey Gorbunov, Vinod Vaikuntanathan and Hoeteck Wee. **Functional Encryption with Bounded Collusions via Multi-Party Computation**. In CRYPTO, pages 162 – 179, 2012.

7. Amin Tootoonchian, Sergey Gorbunov, Yashar Ganjali, Martin Casado, Rob Sherwood. **On Controller Performance in Software-Defined Networks**. In USENIX Hot-ICE, 2012.

8. Sergey Gorbunov and Arnold Rosenbloom. **AutoFuzz: Automated Network Protocol Fuzzing Framework**. In IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

In Submission/Preparation

1. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. **Predicate Encryption for Circuits from LWE**. In Submission. http://eprint.iacr.org/2015/029

2. Sergey Gorbunov and Dhinakaran Vinayagamurthy. **Riding on Asymmetry: Efficient ABE for Branching Programs**. In Submission. http://eprint.iacr.org/2014/819

3. Sergey Gorbunov and Yael Tauman Kalai. **Platcoin: Collusion Resistant Bitcoin Protocol with Useful Mining**. In Preparation.

4. Sergey Gorbunov and Vinod Vaikuntanathan. **Streaming Delegation for Regular Languages**. In Preparation.

Technical Reports

1. Sergey Gorbunov. **Functional Encryption: Constructions and Lower Bounds**. M.Sc. Thesis. 2012.

2. Sergey Gorbunov and Charles Rackoff. **On the Security of Cipher Block Chaining Message Authentication Code**. *UofT*. September 2010.

3. Sergey Gorbunov and Sami Guirguis. **Analyzing web-servers for malicious content using Monkey-Spider honeyclient**. The Honeynet Project. October 2009.

Selected Talks

1. **Predicate Encryption for Circuits from LWE**.
   (a) MIT Cryptography and Information Security Seminar, October 2014.
   (b) The National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program meeting, October 2014.

2. **(Leveled) Fully Homomorphic Signatures from Standard Lattices**.
   (a) Mathematical Research Institute of Oberwolfach, Cryptography Workshop, July 2014.
   (b) DARPA Proceed Program Meeting, September 2014.

3. **Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits**.
   (a) IBM T.J. Watson Cryptography Seminar, April 2014.
   (b) MIT Cryptography and Information Security Seminar, May 2014.
   (c) Ecole normale superieure (ENS) Cryptography Seminar, May 2014.

(d) Mathematical Research Institute of Oberwolfach, Cryptography Workshop, July 2014.

4. **Attribute-Based Encryption for Circuits**.
   (a) IBM T.J. Watson Cryptography Seminar, August 2013.
   (b) China Theory Week, Department of Computer Science, Aarhus University, Denmark. July 2013.
   (c) University of Toronto Theory Seminar, Toronto, ON. December 2012.
5. **Functional Encryption: Constructions and Lower Bounds**.
   (a) Crypto Day, New York, NY. September, 2012.
   (b) University of Toronto Student Theory Seminar, Toronto, ON. March 2012.
6. **On the selective-opening attack on encryption schemes**. University of Toronto Student Theory Seminar, Toronto, ON. April 2013.
7. **On the Dining Cryptographers Problem**. University of Toronto Student Theory Seminar, Toronto, ON. November 2012.
8. **Cryptography: The Science of Secrecy**. University of Toronto High School Visit Day, Toronto, ON. December 2012, March 2013.

Systems Projects

1. **Distributed Computation Protocols** , *UofT*, May 2011 - Aug 2011.
   Advisor: *Peter Marbach*
   Researched and developed communication protocols/systems for distributed computing.
2. **Software Defined Networks**, *UofT*, Jan 2011 - June 2011.
   Advisors: *Yashar Ganjali, Amin Tootoonchian*
   Worked on optimizing and measuring performance characteristics of SDN controllers. Worked on software implementations for state reconstruction of OpenFlow controllers.
3. **Secure IP-based Geolocation Tracking**, *UofT*, May 2011 - Aug 2011.
   Advisors: *Yashar Ganjali, Phillipa Gill*
   Research on delay-based geolocation tracking schemas.
4. **AutoFuzz: Automated Network Protocol Fuzzing Framework** , *UofT Mississauga*, Jan 2010 - Aug 2010.
   Advisor: *Arnold Rosenbloom*
   Designed and implemented a framework for testing network protocols for design and implementation flaws.
5. **Honeynets and Honeyclients**, The Honeynet Project, May 2009 - Feb 2011.
   Researched and improved Honeyclient systems designed to automate collection and analysis of the Internet Threats.

Personal

Languages - English, Russian
Citizenship - Canadian, Russian

References

Vinod Vaikuntanathan (advisor)
Assistant Professor, Computer Science, MIT
+1 (617) 324-8444
vinodv@mit.edu

Shafi Goldwasser
Professor, Computer Science, MIT
+1 (617) 253-5914
shafi@theory.csail.mit.edu

Shai Halevi
Researcher, IBM T. J. Watson Research Center
+1 (914) 945-2706
shaih@alum.mit.edu

Hoeteck Wee
Researcher, École Normale Supérieure
+33 (144) 32-2050
hoeteck@alum.mit.edu

Yael Tauman Kalai
Researcher, Microsoft Research
+1 (857) 453-6322
yael@microsoft.com

Last updated: February 25, 2015