Rachel Miller

32 Vassar Street, 32-G670
Cambridge, MA 02139
H *703 307 5255*
B *r_miller@csail.mit.edu*
http://people.csail.mit.edu/rmiller

Education

2009 - present **Ph.D. computer science**, *Massachusetts Institute of Technology*, Cambridge, MA.
Advised by Prof. Shafi Goldwasser. Studying theory of cryptography.

2008 - 2009 **M.A. mathematics**, *University of Virginia*, Charlottesville, VA.

2005 - 2009 **B.A. computer science, physics**, *University of Virginia*, Charlottesville, VA.
Magna Cum Laude in computer science.

Mihir Bellare, David Cash, and Rachel Miller. **Cryptography Secure Against Related-Key Attacks and Tampering**. To appear in Asiacrypt 2011.

James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. **Goldreichs One-Way Function Candidate Cannot be Inverted by Myopic or Drunk DPLL Backtracking**. Journal Article in submission.

Rachel Miller. **Goldreich's one-way function candidate and drunken backtracking algorithms**. University of Virginia Distinguished Major Thesis with highest honors, May 2009.

James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. **Goldreich's One-Way Function Candidate and Myopic Backtracking Algorithms**. Theory of Cryptography Conference, March 2009.

Positions held

Research Experience

2009 - present **Prof. Shafi Goldwasser**, *MIT Computer Science and Artificial Intelligence Laboratory*, Cambridge, MA.
Research in cryptography, particularly into protocols that tolerate information leakage or tolerate adversarial tampering of secret keys. Also working to apply Lattice-cryptography for privacy in social networks.

2008-2009 **Prof. Abhi Shelat**, *University of Virginia, Department of Compute Science*, Charlottesville, VA.
Worked to develop faster exponentiation algorithms; independently developed a squaring algorithm approximately 20% faster than the commonly used Karatsuba algorithm when used on relatively small numbers.

Summer 2008 **Prof. Luca Trevisan**, *University of Berkeley*, Berkeley, CA.
Worked in complexity theory to show one of the few lower bounds for solving satisfiable k-SAT instances against a subset of attacks; co-author of a resulting paper.

2007 - 2008 **Prof. William Levy**, *University of Virginia, Department of Neuroscience*, Charlottesville, VA.
Used mathematical models of the action potential in neurons to determine how energy efficiency affects the speed and voltage of signals and the physiology of neurons.

Work Experience

Summer 2011 **Software Engineering Intern**, *Facebook*, Palo Alto, CA.
Worked on the Site Integrity team. Independently added machine learning to handle user reports of content differently based on features of the reporter; previously, all reports were handled the same way.

Summer 2006, Winter 2007 and Winter 2008 **Intern**, *SPSS*, Arlington, VA.
Created demonstrations of data mining software for both structured and unstructured data. Solely responsible for creating and presenting a two hour seminar to a local Charlottesville company.

2007 - 2009 **Student Consultant**, *Scholars Lab & Research Computing Lab*, Charlottesville, VA.
Provided support for high performance and research computing, software support, and help with UVA's data sets.

Academic honors

– NDSEG 2009 Fellowship - one of roughly 200 awards in all areas of science
– NSF Graduate Research Fellowship 2009 - one of roughly 1000 awards in all areas of science
– CRA Undergraduate of the Year Finalist 2009 - one of only seven female undergraduates to receive this national distinction for research in computer science
– McShane Prize Winner 2009 - awarded to top three graduating mathematics students at UVA
– Floyd Prize Winner 2008 - awarded for promise in mathematics to three UVA undergraduates a year