Ananth Raghunathan

Curriculum Vitæ

Department of Computer Science
#492 Gates, 353 Serra Mall
Stanford University, Stanford CA 94305
http://crypto.stanford.edu/~ananthr/

119 Quillen Court
Apt. No. 301
Stanford CA 94305
ananthr@stanford.edu

Research Interests

- *Cryptography & Security:* I am interested in all aspects of cryptography. I work on robust constructions of deterministic and searchable encryption schemes. I also look at problems related to building novel cryptogrpahic primitives using lattice-based cryptography. Additionally, I am interested in exploring problems in cryptography motivated by privacy.

  I have worked on constructions and applications of pseudorandom and verifiable random functions. In the distant past, I also worked on program obfuscation and verifiable secret sharing.

Education

Stanford University — Sep 2009 – present
PhD candidate in Computer Science — Stanford, CA
Advisor: Prof. Dan Boneh.
CGPA: **4.02 / 4**

Indian Institute of Technology, Madras — Aug 2005 – July 2009
B.Tech. Computer Science and Engineering with minor in Physics — Chennai, India
Advisor: Prof. C. Pandu Rangan.
CGPA: **9.83 / 10**

Publications

1. **Function-Private Subspace Membership Encryption and Its Applications**
   with Dan Boneh and Gil Segev
   In Advances in Cryptology – ASIACRYPT 2013
2. **Function-Private Identity-Based Encryption: Hiding the Function in Functional Encryption**
   with Dan Boneh and Gil Segev
   In Advances in Cryptology – CRYPTO 2013
3. **Message-Locked Encryption for Lock-Dependent Messages**
   with Martin Abadi and Dan Boneh and Ilya Mironov and Gil Segev
   In Advances in Cryptology – CRYPTO 2013
4. **Key-Homomorphic PRFs and Their Applications**
   with Dan Boneh and Kevin Lewi and Hart Montgomery
   In Advances in Cryptology – CRYPTO 2013
5. **Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions**
   with Gil Segev and Salil Vadhan
   In Advances in Cryptology – EUROCRYPT 2013
6. **Algebraic Pseudorandom Functions with Improved Efficiency from the Augmented Cascade**
   with Dan Boneh and Hart Montgomery
   In proceedings of the 17^{th} *ACM conference on Computer and Communications Security (CCS)* 2010
7. **Obfuscating Straight Line Arithmetic Programs**
   with Srivatsan Narayanan and Ramarathnam Venkatesan
   In proceedings of the 9^{th} *annual ACM workshop on Digital Rights Management (DRM)* 2009
8. **Privately Identifying Location Hotspots**
   with Dan Boneh and Peter Chien

9. **Lower Bounds for Round and Communication Complexities of Unconditional Verifiable Secret Sharing**
   with Srivatsan Narayanan and Pandu Rangan
   Technical report.
10. **Bilinear Maps in Verifiable Random Functions**
    Technical report, CS259C/MATH 250: Elliptic Curves in Cryptography

WORK EXPERIENCE

Research Intern Jun 2012 – Sep 2012
– *Security and Privacy group, Microsoft Research (MSR) Silicon Valley* Mountain View, CA
Advisors: Dr. Ilya Mironov and Dr. Gil Segev

Worked on improving the security definitions and more robust constructions of deterministic encryption schemes. In addition, looked at problems (including on-going research) related to secure deduplication of encrypted data and authenticated differential privacy.

Course Assistant Jan 2011 – Apr 2011, Jan 2012 – Apr 2012
– *Department of Computer Science, Stanford University* Stanford, CA
CS255: Introduction to Cryptography

Work included help setting problem sets, teaching additional topics in sections, and grading.
In 2012, I also helped with the online offering at `http://crypto-class.org/` particularly with setting problems and answering questions and clarifications in forums.

Research Intern May 2008 – Aug 2008
– *Cryptography, Security and Algorithms group, Microsoft Research (MSR) India* Bangalore, India
Advisors: Dr. Satya Lokam and Dr. Ramarathnam Venkatesan

Worked on problems related to program obfuscation and white-boxing of code.

ACADEMIC TALKS

– *Searching on Encrypted Data without Revealing the Search Predicate*
Invited talk, IT Security Entrepreneur's Forum Workshop, Stanford, Mar. 2013
Invited talk, Stanford Computer Forum Security Workshop, Apr. 2013
Stanford Security Lunch, Apr. 2013
– *Randomness Extractors in Cryptography: The Leftover Hash Lemma and Its Variants*
Stanford Security Lunch, Mar. 2013
– *Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions*
EUROCRYPT 2013 conference, Athens, Greece, May 2013
End-of-internship talk, Microsoft SVC, Oct. 2012
Stanford Security Lunch, Oct. 2012
– *Recent results and new directions in constructing Succinct Non-Interactive Arguments*
PhD Qualifying Exam talk, Stanford University, May 2012
– *Signature schemes from Lattices*
Invited talk, Indo-US workshop on lattice based cryptography, ISI Kolkata, Jan. 2012
Microsoft Research India, Jan. 2012
– *Algebraic Pseudorandom Functions with Improved Efficiency from Augmented Cascade*
ACM CCS 2010 conference, Chicago, Il., Oct. 2010
Stanford Theory Lunch, June 2010
Microsoft Research India, Dec. 2010
Theoretical Computer Science Lab, IIT-Madras, Dec. 2010

PROGRAMMING SKILLS

– Good knowledge of C/C++, Python
– Strong foundations in algorithms and data structures and past experience in socket and assembly programming
– Past experience in Perl, MySQL, x86 Assembly language, Prolog, LISP, Lex, Yacc

– Familiar with Windows, Linux, and Mac environments

Selected Undergraduate Projects

– *Camouflage (Spring* 2008*)*
Wrote a software to hide plain text data in images in a manner that is imperceptible to the naked eye. This software used the latest algorithms and techniques to preserve security of protected data including world-class algorithms like AES and the SHA family of hash functions, ratified by the U.S. Govt.
– *A Pascal Compiler (Autumn* 2007*)*
Wrote a compiler from scratch for a subset of Pascal, with help from Lex and Yacc software. This covered functions, procedures, recursion and other common features of Pascal as part of our *Language Translators* course.
– *Implementation of OS functionalities in* GeekOS *kernel (Autumn* 2007*)*
Written code to implement loader, scheduler and semaphores to the GeekOS skeleton. Also implemented paging, device drivers and other functionalities in the GeekOS kernel as part of the *Operating Systems* course.

Academic Honors and Achievements

– Received the *Stanford School of Engineering Fellowship* for the period 2009 – 2010.
– Ranked *second* in the graduating class of 2009 from the Indian Institute of Technology, Madras.
– Received an All India Rank of *139* in IIT-JEE 2005 among over 170,000 students.
– Secured a *Gold Medal* for being among the *top 25 students* in India at the 2005 *International Physics Olympiad Training Camp, Bombay*.
– Awarded the *Kishore Vaigyanik Prothsahan Yojana* fellowship for the period 2003-05. KVPY is a prestigious fellowship offered to around 50 students a year all over the country to nurture scientific talent and promote research in Science.
– Was a *National Talent Search Exam (NTSE)* scholar for the period 2003-05, with a state rank of *3*.