

# Prashant Puniya

239 Palisade Avenue, Apt 1  
Jersey City, NJ-07306

puniya@cims.nyu.edu  
<http://www.cs.nyu.edu/~puniya>

---

## Education

- **Ph.D** in Computer Science August 2002 - September 2007  
New York University, New York, NY.
- **Bachelor of Technology**, Computer Science and Engineering July 1998-May 2002  
IIT Bombay, Bombay, India.
  - Ranked 100<sup>th</sup> of over 100,000 students appearing for IIT-JEE 1998.

## Experience

- **JPMorgan, US Fixed Income Strategy (June - August, 2006)**: Worked as part of the *Interest Rate Derivatives* group. Designed and Implemented an *options portfolio evaluator* that evaluates a portfolio consisting of options and futures on a variety of fixed income securities. In particular, this helps in predicting the performance of any portfolio consisting of fixed income options and futures under a variety of future scenarios and possible dynamics for the underlying securities. Also gained valuable experience as part of the *Sales and Trading* summer internship program.
- **Siemens AG, Munich, Germany (May - July, 2001)**: Summer Intern as part of the *Enterprise on Air* project.

## Publications

- *Design Criteria for Hash Functions and Block Ciphers*, PhD Dissertation, Courant Institute, New York University.
- *Getting the best out of Existing Hash Functions*, With Y. Dodis, in *Applied Cryptography and Network Security (ACNS) Conference*, June 2008.
- *A New Mode of Operation for Block Ciphers and Length-Preserving MACs*, With Y. Dodis and K. Pietrzak, in *Advances in Cryptology - Eurocrypt*, April 2008.
- *Feistel Network made Public, and Applications*, With Y. Dodis, in *Advances in Cryptology - Eurocrypt*, May 2007.
- *On the Relation between the Ideal Cipher and Random Oracle Models*, With Y. Dodis, in *Theory of Cryptography Conference (TCC)*, March 2006.
- *Merkle-Damgård Revisited: how to Construct a Hash Function*, With J-S Coron, Y. Dodis and C. Malinaud, *Advances in Cryptology - CRYPTO*, August 2005.
- *A New Design Criteria for Hash-Functions*, With J-S Coron, Y. Dodis and C. Malinaud, NIST Cryptographic Hash Workshop, November 2005.
- *Rake Linking for Suburban Train Services*, With N. Rangaraj, M. Sohoni and J. Garg, in *Opsearch*, Journal of the Operational Research Society of India, June 2006, vol. 43, no. 2.

## Honors

- Recipient of the Henry-MacCracken Fellowship from NYU.
- Ranked 56<sup>th</sup> in the All India Roorkee Engineering Entrance Examination.
- Stood 16<sup>th</sup> in a country-wide programming contest organized by IIT-Kharagpur.

## Technical Skills

- **Languages and Softwares**: C, C++, Java, Python, LISP, MATLAB, Microsoft Excel.

## Course Work

- **Financial Mathematics**: Capital Markets and Portfolio Management, Derivative Securities, Stochastic Calculus.
- **Mathematics**: Probability and Statistics, Linear Algebra, Real Analysis, Ordinary Differential Equations, Optimization, Linear Programming, Topics in Combinatorics, Computational Number Theory and Algebra, Random Graphs.
- **Computer Science**: Introduction to Cryptography, Topics in Cryptography, Elliptic Curve Cryptography, Honors Algorithms, Honors OS, Honors Theory of Computation, Compilers, Programming Languages.