ARISTEIDIS TENTES

OFFICE ADDRESS
Courant Institute at New York University
Office 408
251 Mercer Street
New York
NY 10012
+1 212 998 3311

PERMANENT ADDRESS
3419 29th Street
Apartment 5A
Astoria, New York
NY 11106
+1 347 925 7268

RESEARCH INTEREST

My research is mainly in Cryptography and Complexity. More specifically I have studied the limits of provable security of popular Digital Signature Schemes and Universal One Way Hash Functions. Moreover, I have done research regarding the construction of Pseudorandom Functions. However, I am also interested in Security and real world applications of Cryptography.

EDUCATION

- Courant Institute of Mathematical Sciences,
  New York University
  PhD student in the Computer Science program — September 2008 - present
  - Advisor: Yevgeniy Dodis

- Graduate Program in Logic and Algorithms (MPLA),
  National Technical University of Athens
  University of Athens
  University of Patras
  MSc — September 2006 - September 2008

- School of Applied Mathematical and Physical Sciences
  National Technical University of Athens
  Diploma — September 2000 - September 2006

CONFERENCE PUBLICATIONS AND WORK IN PROGRESS

- "On the Instantiability of Hash and Sign RSA Signatures"
  Yevgeniy Dodis, Iftach Haitner, Aris Tentes
  9th Theory of Cryptography Conference (**TCC 2012**)
- "Hardness Preserving Constructions of Pseudorandom Functions"
  Abhishek Jain, Krzysztof Pietrzak, Aris Tentes
  9th Theory of Cryptography Conference (**TCC 2012**)
- "On the Connection between Interval Size Functions and Path Counting"
  Evangelos Bampas, Andreas-Nikolas Göbel, Aris Pagourtzis, Aris Tentes
  6th conference on Theory and Applications of Models of Computation (**TAMC 2009**)
- "An Optimal Monte Carlo Type Byzantine Agreement Protocol"
  Aris Tentes
  11th Panhellenic Conference on Informatics (**PCI 2007**)
- "Commitements and Efficient Zero-Knowledge from Hard Learning Problems"
  Abhishek Jain, Krzysztof Pietrzak, Aris Tentes
  In Preparation
- "On the Black-Box Optimality of Shoups Domain Extension of UOWHFs"
  Iftach Haitner, Aris Tentes
  In Preparation
- "On the Uninstantiability of BLS Signatures" Yevgeniy Dodis, Aris Tentes
  In Preparation

EXTERNAL RESEARCH AND VISITS

- 17 January - 3 February 2012
  Tel Aviv University/ Checkpoint Institute
  Invited by Iftach Haitner
- 1 - 10 August 2011
  Institute of Science and Technology Austria (IST Austria)
  Invited by Krzysztof Pietrzak
- 22 May - 31 July 2011
  Centrum voor Wiskunde en Informatica (CWI Amsterdam)
  Invited by Krzysztof Pietrzak
- Spring Semester 2011
  Tel Aviv University/ Checkpoint Institute
  invited by Iftach Haitner
- 17 - 31 May 2010
  Microsoft Research - New England Lab. Cambridge, MA USA
  Gratis Visitor of Iftach Haitner

HONORS AND AWARDS

- NYU Henry M. MacCracken Fellowship, (full tuition and stipend) 2008-2013
- MPLA Mytilinaios Prize for distinguished performance, 2008

TALKS-PRESENTATIONS

- **National Technical University of Athens** - 10 January 2012
  "Hardness Preserving Constructions of Pseudorandom Functions"
- **University of Maryland** - 14 December 2011
  "Hardness Preserving Constructions of Pseudorandom Functions"
- **Tel-Aviv University, Greater Tel Aviv Area Theory Talks** - 7 April 2011
  "On the (In)Security of RSA Signatures"
- **Ben Gurion University** - 12 April 2011
  "On the (In)Security of RSA Signatures"
- **University of Athens** - 11 January 2011
  "On the (In)Security of RSA Signatures"
- **5th Athens Colloquium on Algorithms and Complexity (ACAC)** - 26-27 August 2010
  "On the (In)Security of RSA Signatures"
- **8th Panhellenic Conference in Algebra, Number Theory and Applications** - 29 May 2008
  "Algebraic Techniques in Byzantine Agreement Protocols"
- **6th Panhellenic Conference on Informatics** - 19-21 May 2007
  "An Optimal Monte Carlo Type Byzantine Agreement Protocol"

COMPUTER SKILLS

- Programming Languages: Java
- Other: Matlab

TEACHING EXPERIENCE

- "Number Theory, Cryptography and Complexity"
  Class for 5th year students in National Technical University of Athens (Fall 2007)
  Teaching Assistant, Lecturer of half of the lectures
- "Introduction to Programming"
  Lab Course in Pascal for first year students in National Technical University of Athens (Fall 2007)
  Responsible for a group of 15 students
- "Number Theory, Cryptography and Complexity"
  Class for 5th year students in National Technical University of Athens (Fall 2006)
  Teaching Assistant, Lecturer of half of the lectures
- "Introduction to Programming"
  Lab Course in Pascal for first year students in National Technical University of Athens (Fall 2006)
  Responsible for a group of 15 students

REFERENCES

- Professor Yevgeniy Dodis (advisor)
  New York University
  email: dodis@cs.nyu.edu
  homepage: `http://cs.nyu.edu/~dodis`
- Professor Iftach Haitner
  Tel Aviv University
  email: iftach.haitner@cs.tau.ac.il
  homepage: `http://www.cs.tau.ac.il/~iftachh`
- Professor Krzysztof Pietrzak
  IST Austria
  email: pietrzak@ist.ac.at
  homepage: `http://homepages.cwi.nl/~pietrzak` (old)

LANGUAGES

- Greek (native)
- English (Proficiency of Michigan)
- German (Abitur)

WEBPAGE

`http://cs.nyu.edu/~tentes`