Petros Mol

UCSD CSE, EBU3B 4242
9500 Gilman Drive
La Jolla, CA 92093-0404

(347) 200 1443
pmol@cs.ucsd.edu
http://cseweb.ucsd.edu/∼pmol

Research Interests

My interests lie broadly in both the theoretical foundations and the applications of cryptography. My research has focused mostly on studying the use of learning problems and lattices in the construction of cryptographic primitives. Recently, I have been interested in lightweight cryptography and especially in understanding the security challenges related to Radio Frequency IDentification (RFID) systems.

Education

University of California, San Diego — Fall 2007–Fall 2012 (expected)
Ph.D. in Computer Science and Engineering
Advisor: Prof. Daniele Micciancio
GPA: 3.95/4.0 (Major: 4.0/4.0)

National Technical University of Athens (NTUA), Greece — Fall 2001–Summer 2006
Bachelor in Electrical and Computer Engineering
Thesis Supervisor: Prof. Stathis Zachos
GPA: 9.58/10 (Ranked 3rd out of ∼400 students)

Conference Proceedings

- *Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions* — CRYPTO'11
  Daniele Micciancio, Petros Mol
  In Proc. of 31^{st} *International Cryptology Conference*
- *The Effects of Diversity in Aggregation Games* — ICS'11
  Petros Mol, Andrea Vattani, Panagiotis Voulgaris
  In Proc. of 2^{nd} *Symposium on Innovations in Computer Science*
- *Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions* — PKC'10
  Petros Mol, Scott Yilek
  In Proc. of 13^{th} *Int'l Conf. on Practice and Theory in Public Key Cryptography*
  Received Best Paper Award
- *Recovering NTRU Secret Key from Inversion Oracles* — PKC'08
  Petros Mol, Moti Yung
  In Proc. of 11^{th} *Int'l Conf. on Practice and Theory in Public Key Cryptography*

Manuscripts

- *Symmetric Authentication Beyond the Challenge-Response Paradigm: Definitional Issues and New Protocols*
  Petros Mol, Stefano Tessaro
  under submission
- *Leakage-Resilient Cryptography: A Survey of Recent Advances*
  Petros Mol
  Research Exam, UC San Diego, May 2010
- *Lattices and Their Applications to RSA Cryptosystem*
  Petros Mol
  Diploma thesis, National Technical University of Athens, July 2006

Teaching Experience

Introduction to the Theory of Computation, Teaching Assistant, UCSD	Fall 2011
Computability and Complexity, Teaching Assistant, UCSD	Fall 2008
Number Theory and Cryptography, Teaching Assistant, NTUA	Fall 2006
Algorithms and Complexity, Grader, NTUA	Fall 2005

Working experience

- Research Intern, **INRIA/ENS**, Paris (Hosts: V. Lyubashevsky, O. Regev) Summer 2011
  - *Project*: Worked both on algorithms and on the construction of cryptographic protocols based on learning problems (Learning Parity with Noise and Learning With Errors)
- Software Engineer Intern, **Amazon** (Risk Platform Services), Seattle, WA Summer 2010
  - Extended command line tool for managing the distributed copying of sensitive data for further processing on Amazon's cloud services (AWS, Ruby, Java)
  - Developed service that coordinated metadata exchanged between applications that produced or consumed the variables used in Amazon's fraud detection models (Java, Hibernate)
- Engineering Intern, **Qualcomm** (MediaFLO), San Diego, CA Summer 2008
  - DRM, content and service protection mechanisms for mobile devices.
- Web designer, **Polytechnic University of Hong Kong** Summer 2005

Professional Activities

External Reviewer: WSDM 2013, PKC 2012, TCC 2012, PQCRYPTO 2011, ACNS 2011, CRYPTO 2011, STOC 2011, EUROCRYPT 2011, PKC 2011, FSE 2010, TCC 2009, ACNS 2009, The Computer Journal (COMPJ) 2009

Honors and Awards

Best Paper Award in *Public Key Cryptography* (PKC)	2010
Scholarship by the *Gerondelis Foundation* for academic excellence in PhD studies	2009
Award by the *T*echnical Chamber of Greece for academic excellence	2004, 2006
Scholarship by the *Greek State Scholarships Foundation* for academic excellence	2003, 2004
"Papakyriakopoulos" Award for excellence in Mathematics	2002, 2003
Gold medal in math competition *"Euclid"* held by *Hellenic Mathematical Society*	2000, 2001

Computer Skills

Good: Java, Python, C, Linux/Unix, Latex

Intermediate: C++, subversion systems, Windows

Previous Experience: Ruby, Matlab, SQL, Prolog, Hibernate, HTML

Sample Projects

• *Artificial Intelligence* (Java): Implemented strategies that allow multi-agent populations navigate in unknown territory and collect resources. The implementation employed several optimizations (fast path-finding, diversification of roles, knowledge exchange) that drastically reduced the number of steps required to collect all the resources.

• *Finance* (Python): Implemented various portfolio-selection algorithms and evaluated their performance using simulations based on real historical data from Yahoo! Finance. Two main families of algorithms were considered: mean-reversion and trend-following. Surprisingly, the former outperformed (often significantly) the latter in practice.

• *Cryptography* (C/C++/NTL): Evaluated the concrete security of cryptographic primitives based on hard learning problems (LPN, LWE). The evaluation is backed by both theoretical analysis and concrete implementation (in C++, NTL). The findings of the analysis are expected to lead to a publication.

• *Security* (Wireshark): Security evaluation of Instant Messengers (MSN, Yahoo!, Gtalk etc) against sniffing and Man in the Middle attacks.

Selected Talks

- *Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions* July 2011
  Invited talk, INRIA, Paris, France
- *Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions* May 2010
  Int'l Conf. on Practice and Theory in Public Key Cryptography, Paris, France.
- *Lattices and Cryptography: An Overview of Recent Results with Emphasis on RSA and NTRU Cryptosystems* Fall 2006
  NYU Crypto Seminar