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

Education

University of California, San Diego (UCSD) — Sep 2007–Fall 2012
Ph.D. in Computer Science – Security and Cryptography group — GPA: 3.95/4.0

National Technical University of Athens (NTUA), Greece — Sep 2001–Jul 2006
Bachelor in Electrical and Computer Engineering — GPA: 9.58/10

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)

• Engineer Intern, **Amazon** (Risk Platform Services), Seattle, WA — Summer 2010
- *Project* 1: Extended command line tool for managing the distributed copying of sensitive data for further processing on Amazon's cloud services (AWS, Ruby, Java)
- *Project* 2: 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
- *Project*: DRM, content and service protection mechanisms for mobile devices.

• Web designer, **Polytechnic University of Hong Kong** — Summer 2005

Computer Skills

Good: Java, Python, C, Linux/Unix

Intermediate: C++, subversion systems, Windows

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

Selected Publications

- *Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions* (with Daniele Micciancio) — CRYPTO'11

- *The Effects of Diversity in Aggregation Games* (with Andrea Vattani and Panagiotis Voulgaris) — ICS'11

- *Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions* (with Scott Yilek), **Best Paper Award** — PKC'10

Selected 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.

Honors and Awards

Best Paper Award, *Public Key Cryptography* (PKC) Conference, Paris, France — 2010

Scholarship for academic excellence in PhD studies, *Gerondelis Foundation* — 2009

Award for ranking in top 2% in class, *Technical Chamber of Greece* — 2004, 2006

Scholarship for ranking in top 1% in class, *National Scholarships Foundation* — 2003, 2004

"Papakyriakopoulos" award for excellence in Mathematics (**NTUA**) — 2002, 2003

Gold medal in math competition *"Euclid"*,*Hellenic Mathematical Society* — 2000, 2001