

ADRIANA M. PALACIO – CURRICULUM VITAE

Computer Science Department
Bowdoin College
8650 College Station
Brunswick, ME 04011-8486

Phone: (207) 798-4220
Fax: (207) 725-3750
apalacio@bowdoin.edu
<http://academic.bowdoin.edu/faculty/A/apalacio>

RESEARCH INTERESTS

Cryptography and Information Security

EDUCATION

Ph.D. in Computer Science, *University of California, San Diego* June 2006
Advisor: Mihir Bellare
M.S. in Computer Science, *University of California, San Diego* June 2004
B.S. in Mathematics, *Universidad de los Andes*, Bogotá, Colombia September 1998
B.S. in Systems and Computer Engineering, with honors, March 1998
Universidad de los Andes, Bogotá, Colombia

RESEARCH AND PROFESSIONAL EXPERIENCE

Assistant Professor, Computer Science Department, July 2006 - Present
Bowdoin College.

Doctoral Research, Department of Computer Science & Engineering, 2001 - 2006
University of California, San Diego. Advisor: Mihir Bellare.

- Conducted research on various topics in cryptography, including identification protocols, encryption, signatures, and zero-knowledge protocols.

Undergraduate Research, Department of Mathematics, 1997 - 1998
Universidad de los Andes. Advisor: Dr. Luis Jaime Corredor.

- Studied the specification language called the “Temporal Language of Transitions” (TLT), a framework for the specification and verification of concurrent distributed systems, developed at Siemens Corporate Research and Development, and independently proved the equivalence of the three representations of TLT specifications.

Undergraduate Research, Department of Systems and Computer Engineering, 1997 - 1998
Universidad de los Andes. Advisor: Dr. Olga Mariño.

- Designed a language to represent data types and constraints with a semantics based on default reasoning.

Software Engineer, *OPUS Ingeniería Ltda.*, Bogotá, Colombia. 1998 - 2000

- Contributed to the requirements analysis, design and implementation of a distributed loan management system.
- Lead a team of 8 software engineers.

PUBLICATIONS¹ (Authors are in alphabetical order)

Refereed Conference Papers

- [1] M. BELLARE AND A. PALACIO. “GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks.” In *Advances in Cryptology - Crypto 2002 Proceedings*, Lecture Notes in Computer Science Vol. 2442, M. Yung ed., Springer-Verlag, 2002.
- [2] M. BELLARE, A. BOLDYREVA, AND A. PALACIO. “An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem.” In *Advances in Cryptology - Eurocrypt 2004 Proceedings*, Lecture Notes in Computer Science Vol. 3027, C. Cachin and J. Camenisch eds, Springer-Verlag, 2004.
- [3] M. BELLARE AND A. PALACIO. “The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols.” In *Advances in Cryptology - Crypto 2004 Proceedings*, Lecture Notes in Computer Science Vol. 3152, M. Franklin ed., Springer-Verlag, 2004.
- [4] M. BELLARE AND A. PALACIO. “Towards Plaintext-Aware Public-Key Encryption without Random Oracles.” In *Advances in Cryptology - Asiacrypt 2004 Proceedings*, Lecture Notes in Computer Science Vol. 3329, P. J. Lee ed., Springer-Verlag, 2004.
- [5] A. BOLDYREVA, M. FISCHLIN, A. PALACIO, AND B. WARINSCHI. “A Closer Look at PKI: Security and Efficiency.” To appear in *International Conference on Theory and Practice of Public-Key Cryptography (PKC) 2007 Proceedings*.

Refereed Journal Papers

- [6] M. BELLARE AND A. PALACIO. “Protecting against Key Exposure: Strongly Key-Insulated Encryption with Optimal Threshold.” *Applicable Algebra in Engineering, Communication and Computing*, Vol. 16, No. 6, Springer-Verlag, 2006.

MANUSCRIPTS

- [7] A. BOLDYREVA, A. PALACIO, AND B. WARINSCHI. “Secure Proxy Signature Schemes for Delegation of Signing Rights.” Cryptology ePrint Archive: Report 2003/096, May 2003. <http://eprint.iacr.org/2003/096/>.
- [8] A. PALACIO. “Deniable Zero-Knowledge Sets.” In preparation.

¹Full versions of my papers are available via <http://academic.bowdoin.edu/faculty/A/apalacio/>.

TEACHING EXPERIENCE

Assistant Professor , <i>Bowdoin College</i>	
<i>Introduction to Computer Science</i>	Spring 2007, Fall 2006
<i>Theory of Computation</i>	Spring 2007
<i>Cryptography and Network Security</i>	Fall 2006
Lecturer , <i>Universidad de los Andes</i>	
<i>Foundations of Cryptography: Provable Security</i>	Summer 2005
<i>Introduction to Algorithms</i>	Spring 2000
Summer Graduate Teaching Fellow , <i>University of California, San Diego</i>	Summer 2004
<i>Theory of Computability</i>	
GRE and GMAT Mathematics Program Director , <i>Kaplan Educational Center - Colombia</i>	1999 - 2000
<i>GRE and GMAT math test preparation courses</i>	
Teacher , <i>Kaplan Educational Center - Colombia</i>	1998 - 1999
<i>GRE and GMAT math test preparation courses</i>	
Instructor , <i>Universidad de los Andes</i>	
<i>Geometry Lessons II</i> (a course for architecture majors)	Spring 1997
<i>Integral Calculus</i>	Summer 1996
Teacher-in-Training , <i>Universidad de los Andes</i>	
<i>Integral Calculus</i>	Spring 1996
<i>Analytical Geometry</i>	Fall 1995
Teaching Assistant , <i>University of California, San Diego</i>	Spring 2002
<i>Theory of Computability</i>	

AWARDS, HONORS AND FELLOWSHIPS

National Science Foundation Graduate Research Fellowship	2002 - 2005
Summer Graduate Teaching Fellow appointment, <i>UCSD</i>	Summer 2004
Minority Access to Science, Engineering and Mathematics Fellowship, <i>UCSD</i>	2000
<i>Universidad de los Andes</i> 40 year Anniversary Scholarship	1991 - 1997

CONFERENCE PRESENTATIONS

- GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. Crypto 2002, Santa Barbara, CA, August 2002.

PROFESSIONAL ACTIVITIES

Program Committee Member, Theory of Cryptography Conference (TCC) 2008.

Conference Reviewer, Crypto 2003, High-Performance Distributed Computing (HPDC) 2003, TCC 2004, Eurocrypt 2004, Asiacrypt 2004, Eurocrypt 2006, International Conference on Theory and Practice of Public Key Cryptography (PKC) 2006, Eurocrypt 2007.

Journal Reviewer, Journal of Cryptology.

Membership, The International Association for Cryptologic Research (IACR).

CITIZENSHIP

U.S. citizen

REFERENCES

PROFESSOR MIHIR BELLARE
Computer Science Department
University of California, San Diego
9500 Gilman Drive, Mail Code 0404
La Jolla, CA 92093-0404
Phone: (858) 534-4544
Fax: (207) 725-3750
mihir@cs.ucsd.edu
<http://www.cse.ucsd.edu/~mihir>

PROFESSOR PHILLIP ROGAWAY
Department of Computer Science
University of California, Davis
3063 Kemper Hall
Davis, CA 95616-8562
Phone: (530) 752-7583
Fax: (530) 752-4767
rogaway@cs.ucdavis.edu
<http://www.cs.ucdavis.edu/~rogaway>

PROFESSOR DANIELE MICCIANCIO
Computer Science Department
University of California, San Diego
9500 Gilman Drive, Mail Code 0404
La Jolla, CA 92093-0404
Phone: (858) 822-2577
Fax: (207) 725-3750
daniele@cs.ucsd.edu
<http://www.cse.ucsd.edu/~daniele>

Additional references available upon request.