Antonio Marcedone

411 Gates Hall, Cornell University, Ithaca NY 14853 | (315) 351-2686 | marcedone@cs.cornell.edu | www.marcedone.it

Research Interests

Exploring all aspects of **asymmetric cryptography, provable security and security protocols' design**, as well as the application of cryptographic techniques to solve practical problems.

Education

Cornell University, NY, USA

Doctoral Candidate, Computer Science. Advisor: Prof. Rafael Pass — Aug 2014 - exp. 2018
Strauss Hawkins Fellowship (2014/2015)

Århus University, Denmark — Aug - Nov 2013

Internship in the cryptography group led by Professor Ivan Damgård.
Was invited back in Feb 2014. Lead to a publication.

University of Catania, Italy

M.S., Mathematics. 110/110 *cum laude* (max grade). Advisor: Prof. Dario Catalano — 2012 - 2014

B.S., Mathematics. 110/110 *cum laude* (max grade). Advisor: Prof. Dario Catalano — 2009 - 2012

Fellow of the **Scuola Superiore di Catania** — 2009 - 2015
Covers both B.S. and M.S., includes funds for travel and early research experience.
First place at the admission's test.

Honors and Awards

"Premio di Studio" scolarship (2010) - National fellowship by INDAM (National Inst. for Higher Mathematics) (Refused. 2009) - Silver Medal (2009), Bronze Medal (2008), Honourable Mention (2006) in the national Italian Mathematical Olympiads

Papers Published

Bounded KDM Security from iO and OWF
A. Marcedone, R. Pass, a. shelat. In Proc. of Security and Cryptography for Networks (SCN), Italy, 2016.

Linearly Homomorphic Structure Preserving Signatures: New Methodologies and Applications
D. Catalano, A. Marcedone, O. Puglisi. In Advances in Cryptology - ASIACRYPT 2014, Taiwan, 2014.

Obfuscation $\Rightarrow$ (IND-CPA Security $\not\Rightarrow$ Circular Security)
A. Marcedone, C. Orlandi. In Proc. of Security and Cryptography for Networks (SCN), Italy, 2014.

Relevant Experiences

Software Engineering Intern. Google, NYC, USA. — Summer 2016
I designed and implemented a new prototype (Java) library that uses a practical multiparty computation protocol to perform federated machine learning in a privacy preserving way.

Teaching Assistant - Introduction to Cryptography. Cornell University, USA. — Fall 2015
Designed homeworks, held office hours and occasional make up lectures, graded.

Teaching Assistant - C Programming. University of Catania, Italy. — Winter 2013/2014
Designed and lectured (30 hours) practical "Labs" and review sessions.

Skills

Programming: C, Java (proficient); C++, Python, HTML, CSS, PHP, MySQL (prior experience)
Languages: Italian (fluent), English (fluent), spoken French (basic)

Relevant Projects

Grad Course Project: Cloud Based Password Manager — 2015
Implemented a cloud-based password manager using Java, in a team of 4. Used libraries for SSL session management, encryption and signatures. Wrote extensive security documentation including threat analysis, goals, assurances.

Course Project: Genetic algorithms for multi-modal optimization. — 2010
Implemented a genetic algorithm for the simultaneous optimization of numerical functions (hundreds of variables). Used C and displayed results using gnuplot.

Course Project: Tetris Game — 2009
Implemented a Tetris game. Used Python and the pygame library.

Service

Reviewer for the following journals/conferences:
CRYPTO 2015, EUROCRYPT 2014, Theoretical Computer Science (Elsevier)