Antonio Marcedone

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

Research Interests

Asymmetric cryptography, secure computation, and broadly 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. 2019
Strauss Hawkins Fellowship (2014/2015)

Århus University, Denmark — Aug - Nov 2013

Internship in the cryptography group led by Professor Ivan Damgård.

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.

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

Minimizing Trust in Hardware Wallets with Two Factor Signatures
A. Marcedone, R. Pass, a. shelat. To appear in Proc. of Financial Cryptography and Data Security (FC), USA, 2019.

Outsourcing Private Machine Learning via Lightweight Secure Arithmetic Computation
S. Garg, Z. Ghodsi, A. Marcedone, C. Hazay, Y. Ishai, M. Venkitasubramaniam.
In PPML (NeurIPS workshop), Canada, 2018.

Practical secure aggregation for federated learning on user-held data
K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, K. Seth.
In Computer and Communications Security - CCS, USA, 2017.

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. Keybase, NYC, USA. — Summer 2018
Audited the design of the Keybase app, identifying and fixing some bugs/vulnerabilities (both at the implementation and cryptographic design level). Upgraded and extended the encryption functionality of the Keybase client to allow generating Saltpack encrypted messages for Keybase teams (Golang).

Software Engineering Intern. Snap Inc., LA, USA. — Summer 2017
Contributed to the Google KeyTransparency open source project (prevents MiTM attacks by storing users' public keys in a transparent auditable log) and started developing an Android client app library/app (Golang/Java). Helped design and implement a system for secure distributed machine learning (Java).

Software Engineering Intern. Google, NYC, USA. — Summer 2016
Designed and implemented a new prototype Java library that will be used to perform federated machine learning in a privacy preserving way. This will allow Google to train machine learning models from the data of many users (i.e. to suggest the next word to users typing on their phones) *without* learning the inputs of each user.

Skills

Programming: C, Java (proficient); Python, Golang (some experience); Languages: Italian (native), English (fluent)

Service

Reviewer for the following journals/conferences:
ITCS 2019; FC 2019; CRYPTO 2017, 2015; TCC 2017; FOCS 2015; EUROCRYPT 2014; Theoretical Computer Science (Elsevier)