

# SCN 2014

## Ninth Conference on Security and Cryptography for Networks

September 3-5, 2014, Amalfi, Italy

<http://scn.dia.unisa.it>

### CALL FOR PAPERS

#### Scope

The Ninth Conference on Security and Cryptography for Networks (SCN 2014) aims at bringing together researchers in the field of cryptography and information security, practitioners, developers, and users to foster cooperation, exchange techniques, tools, experiences and ideas. The conference seeks submissions from academia, government, and industry presenting novel research on all practical and theoretical aspects of cryptography and information security. All topic areas related to cryptography and information security are of interest and in scope.

**Topics** (suggested topics include but are not restricted to)

Applied Cryptography and Implementations  
Authentication, Identification and Access Control  
Complexity-Theoretic Cryptography  
Information-Theoretic Security  
Security Architectures and Models  
Network, Web and Wireless Security  
Cryptographic Hash Functions  
Cryptographic and Security Protocols  
Digital Signatures and Message Authentication Codes

Anonymity and Privacy  
Block and Stream Ciphers  
Formal Security Methods  
Information Systems Security  
Cryptanalysis  
Physical Cryptography  
Cloud Computing Security  
Distributed Systems Security  
Public-Key Encryption

#### Submissions

Authors are invited to submit electronically (PDF format) a non-anonymous extended abstract. The extended abstract should be typeset using 11-point or larger fonts, in a single-column, single-spacing format, and reasonable margins. Submissions deviating significantly from these guidelines risk rejection without consideration of their merits. The length of the submission should be at most 14 pages excluding the title page, bibliography and appendices. Referees are not required to read appendices; the paper should be intelligible without them. Submissions must not substantially duplicate work that was published elsewhere, or work that any of the authors has submitted in parallel to a journal or to any other conference or workshop with proceedings.

#### Best Paper Award

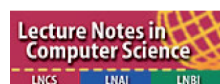
All submissions are eligible for the Best Paper award. The committee may decide to split the award between multiple papers, or to decline to make an award.

#### Dates and Deadlines

Submission: **April 14, 2014**  
Notification to authors: **June 9, 2014**  
Camera-Ready Version: **June 23, 2014**  
Conference: **September 3-5, 2014**

#### Presentation

Authors of accepted papers must guarantee that their paper will be presented at the conference.



#### Proceedings

Proceedings will be published by Springer in the Lecture Notes in Computer Science (LNCS) series.

This event is organized in cooperation with the International Association for Cryptologic Research

IACR



#### Program Chair

Michel Abdalla, *ENS Paris, France*

#### Program Committee

Masayuki Abe, *NTT, Japan*  
Giuseppe Ateniese, *Rome University, Italy*  
Carlo Blundo, *Università di Salerno, Italy*  
Elette Boyle, *Technion, Israel*  
Jean-Sébastien Coron, *Univ. of Luxembourg, Luxembourg*  
Stefan Dziembowski, *University of Warsaw, Poland*  
Dario Fiore, *IMDEA, Spain*  
Marc Fischlin, *Darmstadt University of Technology, Germany*  
Pierre-Alain Fouque, *University of Rennes, France*  
Brett Hemenway, *UPenn, USA*  
Stanislaw Jarecki, *UCI, USA*  
Gaëtan Leurent, *Université Catholique de Louvain, Belgium*  
Daniele Micciancio, *UCSD, USA*  
Michael Naehrig, *Microsoft Research, USA*  
Adam O'Neill, *Georgetown University, USA*  
Claudio Orlandi, *Aarhus University, Denmark*  
Carles Padro, *Nanyang Technological University, Singapore*  
Christopher Peikert, *Georgia Institute of Technology, USA*  
Giuseppe Persiano, *Università di Salerno, Italy*  
Thomas Peyrin, *Nanyang Technological University, Singapore*  
Emmanuel Prouff, *ANSSI, France*  
Christian Rechberger, *DTU, Denmark*  
Vincent Rijmen, *K.U. Leuven, Belgium*  
Christian Schaffner, *Univ. of Amsterdam, The Netherlands*  
Thomas Shrimpton, *Portland State University, USA*  
Francois-Xavier Standaert, *UCL, Belgium*  
Stefano Tessaro, *UCSB, USA*  
Mehdi Tibouchi, *NTT, Japan*  
Damien Vergnaud, *ENS, France*  
Ivan Visconti, *Università di Salerno, Italy*  
Bogdan Warinschi, *University of Bristol, UK*

#### General Chair

Roberto De Prisco, *Università di Salerno, Italy*

#### Local organization

Luigi Catuogno, *Università di Salerno, Italy*  
Aniello Castiglione, *Università di Salerno, Italy*  
Paolo D'Arco, *Università di Salerno, Italy*

#### Steering Committee

Carlo Blundo, *Università di Salerno, Italy*  
Alfredo De Santis, *Università di Salerno, Italy*  
Ueli Maurer, *ETH Zurich, Switzerland*  
Rafail Ostrovsky, *UCLA, USA*  
Giuseppe Persiano, *Università di Salerno, Italy*  
Jacques Stern, *ENS, France*  
Douglas Stinson, *University of Waterloo, Canada*  
Gene Tsudik, *University of California - Irvine, USA*  
Moti Yung, *Google, USA*