


2–5 June 2015, New York
Columbia University

The 13th International Conference on Applied Cryptography and Network Security (ACNS 2015) will be held at Columbia University in NYC, New York. The conference seeks submissions presenting novel research on all technical aspects of applied cryptography, network and computer security, and privacy. This includes submissions on traditional cryptography and security areas (e.g., symmetric or public key cryptography, network security, privacy and anonymity), emerging areas (e.g., security and privacy for big data, outsourced computation, or digital currency), and new paradigms or non-traditional perspectives. Submissions may focus on new visions, definitions, security and privacy metrics, provably secure protocols, impossibility results, attacks, industrial challenges, case studies, experimental reports related to implementation and deployment of real-world systems or policies, or any other original research advancing the state of the art.

Submission deadline: 16 January 2015

Notification: 17 March 2015, Camera-ready due: 3 April 2015

General Chairs

Vladimir Kolesnikov (Bell Labs, USA)
Allison Bishop Lewko (Columbia University, USA)
Michalis Polychronakis (Columbia University, USA)

Program Chair

Tal Malkin (Columbia University, USA)

Program Committee

Shweta Agrawal (IIT Delhi, India)
Nuttapong Attrapadung (AIST, Japan)
Alex Biryukov (University of Luxembourg, Luxembourg)
John Black (University of Colorado at Boulder, USA)
Alexandra Boldyreva (Georgia Tech, USA)
Christina Brzuska (MSR Cambridge, UK)
Christian Cachin (IBM Research – Zurich, Switzerland)
Dario Catalano (University of Catania, Italy)
Melissa Chase (MSR Redmond, USA)
Jie Chen (East China Normal University, China)
Liqun Chen (HP Labs, UK)
Seung Geol Choi (US Naval Academy, USA)
Ivan Damgård (Aarhus University, Denmark)
Jean Paul Degabriele (Royal Holloway University of London, UK)
Itai Dinur (ENS, France)
Nelly Fazio (City College, CUNY, USA)
Phillipa Gill (Stony Brook University, USA)
Dov Gordon (ACS, USA)
Shai Halevi (IBM TJ Watson Research Center, USA)
Goichiro Hanaoka (AIST, Japan)
Aggelos Kiayias (University of Athens, Greece)
Ranjit Kumaresan (Technion, Israel)
Kwangsu Lee (Korea University, Korea)
Tancrede Lepoint (CryptoExperts, France)
Adriana Lopez-Alt (Google, USA)
Nasir Memon (NYU Poly, USA)
Andrew Miller (University of Maryland, USA)
Payman Mohassel (Yahoo Labs, USA)
David Naccache (ENS, France)
Kobbi Nissim (Harvard University and Ben-Gurion University, Israel)
Yossef Oren (Columbia University, USA)
Periklis Papakonstantinou (Tsinghua University, China)
Charalampos (Babis) Papamanthou (University of Maryland, USA)
Vasilis Pappas (Appthority Inc., USA)
Mathias Payer (Purdue University, USA)
Thomas Peyrin (Nanyang Technological University, Singapore)
David Pointcheval (ENS, France)
Michalis Polychronakis (Columbia University, USA)
Elizabeth Quaglia (Huawei Technologies, France)
Carla Ràfols (Ruhr-University Bochum, Germany)
Mike Rosulek (Oregon State University, USA)
Emily Shen (MIT Lincoln Laboratory, USA)
Haya Shulman (TU Darmstadt, Germany)
François-Xavier Standaert (UC Louvain, Belgium)
Michael Steiner (IBM Research – Bangalore, India)
Vanessa Teague (University of Melbourne, Australia)
Isamu Teranishi (NEC, Japan)
Stefano Tessaro (UC Santa Barbara, USA)
Arkady Yerukhimovich (MIT Lincoln Laboratory, USA)
Moti Yung (Google and Columbia Univsersity, USA)
Jianying Zhou (Institute for Infocomm Research, Singapore)

http://acns2015.cs.columbia.edu/