In cooperation with

In association with

Call for Papers

International Conference on Security, Privacy and Applied Cryptography Engineering

SPACE 2012

November 2-3, 2012, Chennai, India

http://space.cse.iitm.ac.in/

SPACE is an annual international conference covering various aspects of security, privacy, applied cryptography, and cryptographic engineering. SPACE 2012 is organized by IIT Madras in cooperation with IACR (International Association for Cryptologic Research) and in association with SETS (Society for Electronic Transactions and Security). Original papers are invited on any aspect that SPACE 2012 covers. The core topics of SPACE 2012 include but are not limited to the following:

Topics

Symmetric-key algorithms and cryptanalysis
Cryptographic implementations
Side channel analysis and countermeasures
Fault tolerance of cryptosystems
Physically uncloneable functions
Public-key schemes and cryptanalysis
Analysis and design of security protocols
Security of systems and applications
High-performance computing in cryptology
Cryptography in ubiquitous devices
Trusted computing
Anonymity and privacy
Data base security
Operating system security
Cloud and grid security
Network security, botnets, intrusion detection

Program Committee

Rafael Accorsi, University of Freiburg (Germany)
Toru Akishita, Sony Corporation (Japan)
Elena Andreeva, KU Leuven (Belgium)
Rajat Subhra Chakraborty, IIT Kharagpur (India)
Carlos Cid, Royal Holloway, University of London (UK)
Donghoon Chang, NIST (US)
Abhijit Das, IIT Kharagpu (India)
Kris Gaj, George Mason University (US)
Craig Gentry, IBM Watson Research Center (US)
Dieter Gollmann, TUHH (Germany)
Johann Grossschaedl, Univ. of Luxembourg (Luxembourg)
Tim Gueneysu, Ruhr University Bochum (Germany)
Tibor Jager, Karlsruhe Institute of Technology (Germany)
Marc Joye, Technicolor (France)
Stefan Katzenbeisser, TU Darmstadt (Germany)
Ilya Kizhvatov, Riscure (The Netherlands)
Cetin Koc, UCSB (US)
Tanja Lange, TU Eindhoven (The Netherlands)
Gregor Leander, DTU Mathematics (Denmark)
Kerstin Lemke-Rust, FH Bonn-Rhein-Sieg (Germany)
Dongdai Lin, Chinese Academy of Sciences (China)
Keith Martin, Royal Holloway, University of London (UK)
Debdeep Mukhopadhyay, IIT Kharagpur (India)
David Naccache, ENS Paris (France)
Arpita Patra, ETH Zurich (Switzerland)
Joachim Posegga, University of Passau (Germany)
Bart Preneel, KU Leuven (Belgium)
Francesco Regazzoni, University of Lugano (Switzerland)
Vincent Rijmen, TU Graz (Austria) and KU Leuven (Belgium)
Matt Robshaw, Orange (France)
Bimal Roy, ISI Kolkata (India)
Pierangela Samarati, University of Milan (Italy)
Sumanta Sarkar, University of Calgary (Canada)
Martijn Stam, University of Bristol (UK)
François-Xavier Standaert, UCL (Belgium)
Berk Sunar, Worcester Polytechnic Institute (US)
Michael Tunstall, University of Bristol (UK)
Gilles Van Assche, STMicroelectronics (Belgium)
Bo-Yin Yang, Academia Sinica (Taiwan)
Jianying Zhou, Institute for Infocomm Research (Singapore)

Conference Organizers

C. Pandurangan, IIT Madras (Hon. General Chair)
S. Burman, CAIR Bangalore (General Chair)
V. Kamakoti, IIT Madras (General Chair)
S. Bhunia, Case West. Res. Univ. (Publicity Chair)
S. Balachandran, IIT Madras (Organizing Chair)

Program Chairs

Andrey Bogdanov, KU Leuven (Belgium)
Somitra Sanadhya, IIIT Delhi (India)

Important Dates

Submission deadline:	**July 3, 2012, 23:59 IST (GMT+5:30)**
Acceptance notification:	August 17, 2012
Final version due:	August 31, 2012
Conference presentations:	November 2-3, 2012

Instructions for Authors

Authors are invited to submit original papers via electronic submission. Details of the electronic submission procedure will be posted on the conference webpage. The submission must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The paper should be at most 12 pages (excluding the bibliography and clearly marked appendices), and at most 18 pages in total, using at least 11-point font and reasonable margins. Submissions not meeting these guidelines risk rejection without consideration of their merits. All submissions will be blind-refereed. Only original research contributions will be considered. Submissions which substantially duplicate work that any of the authors have published elsewhere, or have submitted in parallel to any other conferences or workshops that have proceedings, will be instantly rejected. The IACR Policy on Irregular Submissions (http://www.iacr.org/irregular.html) will be strictly enforced.

Conference Proceedings

The proceedings will be published in Springer's Lecture Notes in Computer Science (LNCS). Accepted papers should follow the LNCS author instructions http://www.springer.de/comp/lncs/authors.html. In order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the conference.

Location and Stay

The conference will be held at IIT Madras, Chennai. The city of Chennai is one of the major cities in the southern part of India and is well connected by international and domestic flights as well as trains and buses from all over India. Every attempt will be made to accommodate the delegates attending the conference within IIT Madras campus or nearby places. Information about travel and stay will be updated on the conference website.

Contact

For any further clarification, please mail:
V. Kamakoti and S. Burman (kama@cse.iitm.ac.in and sanjayburman@gmail.com) or
Andrey Bogdanov and Somitra Sanadhya (andrey.bogdanov@esat.kuleuven.be and somitra@iiitd.ac.in).

Last updated: 20 June 2012