

**Call for papers:
1st Workshop on Cryptography over Ad hoc Networks
(WCAN 05)**

A SATELLITE WORKSHOP OF WIRELESSCOM 05, [HTTP://SA1.SICE.UMKC.EDU/WC05/](http://sa1.sice.umkc.edu/wc05/)
WORKSHOP DATES: JUNE 15-16

Workshop Location: Sheraton Maui Resort, Kaanapali Beach, Maui, Hawaii, <http://www.sheraton-maui.com>

Wireless ad hoc networks are today receiving a lot of attention for military, commercial and civilian applications, thus raising several challenging security, privacy and anonymity research questions. The security research community has mainly focused on securing routing and is only recently widening its scope of analysis to other security areas. The cryptography research community has mainly focused on standard networks, like the Internet; however, cryptographic protocols for the Internet face serious challenges to be adapted to the ad-hoc, partial-connectivity, mobile, and infrastructureless nature of ad-hoc networks. The aim of this workshop is to help bridging this gap, towards a more comprehensive investigation of security and cryptographic tools, analysis and modeling methodologies over (mobile) ad hoc networks, by bringing together the cryptography, network security, and wireless networking communities. We seek submissions containing original research on all aspects of cryptology in wireless ad hoc networks. Short surveys of sub-areas are also encouraged. Main topics of interest include, but are not limited to the following:

- Ad Hoc Networks and Resources Modeling
- Secure Routing
- Security Bootstrapping
- Trust Establishment
- Distributed Public-Key Infrastructures
- Key Agreement, Management and (Pre)Distribution over Ad Hoc Networks
- Resource-Constrained Cryptography over Ad Hoc Networks
- Threshold Cryptography over Ad Hoc Networks
- Identity-Based Cryptography over Ad Hoc Networks
- Policy-Based Cryptography over Ad Hoc Networks
- Secure Multi-Party Protocols over Ad Hoc Networks
- Security in Distributed Algorithms and Protocols

Important Dates:

- Submission Deadline: May 1, 2005 (Extended)
- Notification of Acceptance: May 8, 2005
- Camera-Ready Papers: May 20, 2005

Program Chair: Giovanni Di Crescenzo, Telcordia, NJ, USA. giovanni@research.telcordia.com

Program Committee: Mike Burmester (Florida State University), David Carman (Johns Hopkins AP Lab), Giovanni Di Crescenzo (Telcordia), Renwei Ge (University of Delaware), Jonathan Katz (University of Maryland), David Naccache (Gemplus), Giuseppe Persiano (University of Salerno), Zulfikar Ramzan (Docomo Labs), Raj Rajagopalan (Hewlett Packard Labs), Ravi Sundaram (Northeastern University), Doug Tygar (UC Berkeley), Serge Vaudenay (Swiss Federal Institute of Technologies), Moti Yung (RSA & Columbia University).

General Chair: Farooq Anjum, Telcordia. fanjum@telcordia.com

Instructions for Authors: Authors are invited to submit surveys or original papers, possibly about work in progress, that deal with both cryptology and ad hoc networks. All submissions will be refereed and must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel. The submissions, preferably in PDF or PS format, must not exceed 6 pages (excluding appendices) nor 12 pages overall. In order to submit a paper, please send your paper as an attachment of an ASCII e-mail to wcan05chair@research.telcordia.com, indicating title of paper, names and affiliations of authors, and full contact information (affiliation, e-mail and phone number) of the contact author. The camera-ready version should not exceed 6 pages in standard double-column IEEE format.

Workshop Proceedings: to be published by IEEE. More details will be provided to the authors.

Hotel Information: Posted at <http://sa1.sice.umkc.edu/wc05/HotelRes.txt>. Early reservation is recommended to benefit from workshop discount.

Registration Information: Forms for authors and non-authors are posted at <http://sa1.sice.umkc.edu/wc05/>. Authors of an accepted paper must guarantee presentation of their paper at the workshop.