



Workshop on RFID Security 2006

<http://events.iaik.tugraz.at/RFIDSec06>

July 12-14 2006, GRAZ (Austria)

Important Dates

- *May 22 2006*
Submission deadline
- *June 12 2006*
Notification
- *July 03 2006*
Final version
- *July 12-14 2006*
Workshop

Program Committee

- Vincent Rijmen (chair)
TU Graz, Austria
- Gildas Avoine
MIT, USA
- Christof Paar
RUB, Germany
- Bart Preneel
KULeuven, Belgium
- François-Xavier
Standaert, *UCL, Belgium*
- Johannes Wolkerstorfer
TU Graz, Austria

Organization



European network of
excellence in cryptology

Local organization



Graz University of Technology

Institute for Applied
Information Processing
and Communications

The *Workshop on RFID Security 2006* is the successor of the successful *Workshop on RFID and Light-Weight Crypto 2005*.

Call for Papers

The *Workshop on RFID Security 2006* focuses on approaches to solve security issues in advanced contactless technologies like RFID systems. It stresses implementation aspects imposed by resource constraints.

RFID security issues are a challenge for RFID technologies to become an enabling technology for the Internet of things. The *Workshop on RFID Security 2006* will help to bridge the gap between cryptographic researchers and RFID developers. Therefore, submissions both from academia and industry are appreciated.

Topics of the workshop include but are not limited to:

- *New applications for secure RFID systems*
- *Privacy-enhancing techniques for RFID*
- *Cryptographic protocols for RFID:*
 - *Authentication protocols*
 - *Key update mechanisms*
 - *Scalability issues*
- *Integration of secure RFID systems:*
 - *Middleware and security*
 - *(Public-key) Infrastructures*
- *Resource-efficient implementation of cryptography:*
 - *Small-footprint hardware*
 - *Low-power architectures*

Workshop Proceedings

There will be no formal proceedings. Participants of the workshop will receive a printed handout. Accepted papers can be published elsewhere without restrictions.

Instructions for Authors

Authors are invited to submit papers of at most 12 pages. Latex submissions using the LNCS style (<http://www.springer.de/comp/lncs/authors.html>) are preferred. Papers can be submitted by email or via the web:

Contact and Further Information

Email: RFIDSec06@iaik.tugraz.at

Web: <http://events.iaik.tugraz.at/RFIDSec06>