The 9th Workshop on RFID Security and Privacy 2013

July 09-11, 2013, Graz, Austria

IAIK TU Graz

Conference Program:

<table>
<tr><th></th><th>Tue, 9th July</th><th>Wed, 10th July</th><th>Thu, 11th July</th></tr>
<tr><td>08:30</td><td></td><td></td><td></td></tr>
<tr><td>09:00</td><td rowspan="2">Tutorial 1</td><td>Registration and Welcome</td><td>Registration</td></tr>
<tr><td>09:30</td><td>Invited Talk -
Wayne Burleson</td><td rowspan="2">Technical Sesssion 3</td></tr>
<tr><td>10:00</td><td></td><td></td></tr>
<tr><td>10:30</td><td>Coffee Break</td><td>Coffee Break</td></tr>
<tr><td>11:00</td><td rowspan="3">Tutorial 2</td><td rowspan="3">Technical Sesssion 1</td><td>Coffee Break</td></tr>
<tr><td>11:30</td><td rowspan="2">Invited Talk -
Lejla Batina</td></tr>
<tr><td>12:00</td></tr>
<tr><td>12:30</td><td rowspan="2">Lunch Break</td><td rowspan="2">Lunch Break</td><td rowspan="2">Lunch Break</td></tr>
<tr><td>13:00</td></tr>
<tr><td>13:30</td><td rowspan="3">TAMPRES Workshop
Invited Talk -
Elisabeth Oswald</td><td rowspan="2">Invited Talk - Günther Lackner & Karin Greimel</td><td rowspan="2">Technical Sesssion 4</td></tr>
<tr><td>14:00</td></tr>
<tr><td>14:30</td><td>Coffee Break</td><td>Closing Remarks</td></tr>
<tr><td>15:00</td><td>Coffee Break</td><td rowspan="3">Technical Sesssion 2</td><td></td></tr>
<tr><td>15:30</td><td rowspan="6">TAMPRES Workshop</td><td rowspan="3">Tutorial 3</td><td></td></tr>
<tr><td>16:00</td><td></td></tr>
<tr><td>16:30</td><td></td><td></td></tr>
<tr><td>17:00</td><td></td><td></td><td></td></tr>
<tr><td>17:30</td><td></td><td></td><td></td></tr>
<tr><td>18:00</td><td></td><td></td><td></td></tr>
<tr><td>18:30</td><td colspan="2"></td><td></td></tr>
<tr><td>19:00</td><td colspan="2" rowspan="4">Welcome Reception</td><td rowspan="4">Gala Dinner</td><td rowspan="4">25years IAIK Celebration</td></tr>
<tr><td>19:30</td></tr>
<tr><td>20:00</td></tr>
<tr><td>20:30</td></tr>
</table>

Technical Session 1: NFC & Mobile Security

Time	Paper Title
11:00-11:30	*Deploying OSK on Low-resource Mobile Devices* Authors: Gildas Avoine, Muhammed Ali Bingol, Xavier Carpent, and Süleyman Kardas
11:30-12:00	*Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients* Authors: Mehmet Hilal Özcanhan, Gökhan Dalkiliç, and Semih Utku
12:00-12:30	*Rights Management with NFC Smartphones and Electronic ID Cards: A Proof of Concept for Modern Car Sharing* Authors: Timo Kasper, Alexander Kühn, David Oswald, Christian Zenger, and Christof Paar

Technical Session 2: Protocols and Attacks

Time	Paper Title
15:00-15:30	*The Resistance to Intermittent Position Trace Attacks and Desynchronization Attacks (RIPTA-DA) Protocol Is Not RIPTA-DA* Authors: Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani and Somitra Kumar Sanadhya
15:30-16:00	*Long Distance Relay Attack* Authors: Luigi Sportiello and Andrea Ciardulli
16:00-16:30	*On the Security of two RFID Mutual Authentication Protocols* Authors: Seyed Farhad Aghili, Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya

Technical Session 3: RFID Hardware

Time	Paper Title
09:30-10:00	*Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures* Authors: Lejla Batina, Amitabh Das, Baris Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, and Tolga Yalcin
10:00-10:30	*An Improved Hardware Implementation of the Quark Hash Function* Authors: Shohreh Sharif Mansouri and Elena Dubrova
10:30-11:00	*Analyzing Side-Channel Leakage of RFID-Suitable Lightweight ECC Hardware* Authors: Erich Wenger, Thomas Korak, and Mario Kirschbaum

Technical Session 4: Implementations

Time	Paper Title
13:30-14:00	*Energy-Architecture Tuning for ECC-based RFID tags* Authors: Deepak Mane and Patrick Schaumont
14:00-14:30	*Speed and size optimized implementations of the PRESENT cipher for tiny AVR devices* Authors: Konstantinos Papagiannopoulos and Aram Verstegen

Tutorials – Program (9th July):

Tutorial 1 (09:00-10:30) - **RFID Introduction and the IAIK DemoTag: A Programmable RFID-Tag Emulator** by Thomas Korak, Raphael Spreitzer, and Hannes Gross (IAIK)

Tutorial 2 (11:00-12:30) **- Side-Channel Attacks and Fault Analysis** by Johann Heyszl (Fraunhofer AISEC) and Thomas Korak (IAIK)

Tutorial 3 (15:30-17:00) - **Cryptographic Hardware Design and Performance Metrics** by Frank K. Gürkaynak (ETH Zurich)

The tutorials will take place at TU Graz (IAIK):

Graz University of Technology,
Inffeldgasse 16a,
8010 Graz

http://www.iaik.tugraz.at/content/about_iaik/how_to_reach_us/

If you would like to reach IAIK from the conference hotel, take the tram #6 (towards direction “St. Peter”) and exit at “Schulzentrum St. Peter”. From there it’s a 5min walk to the institute.

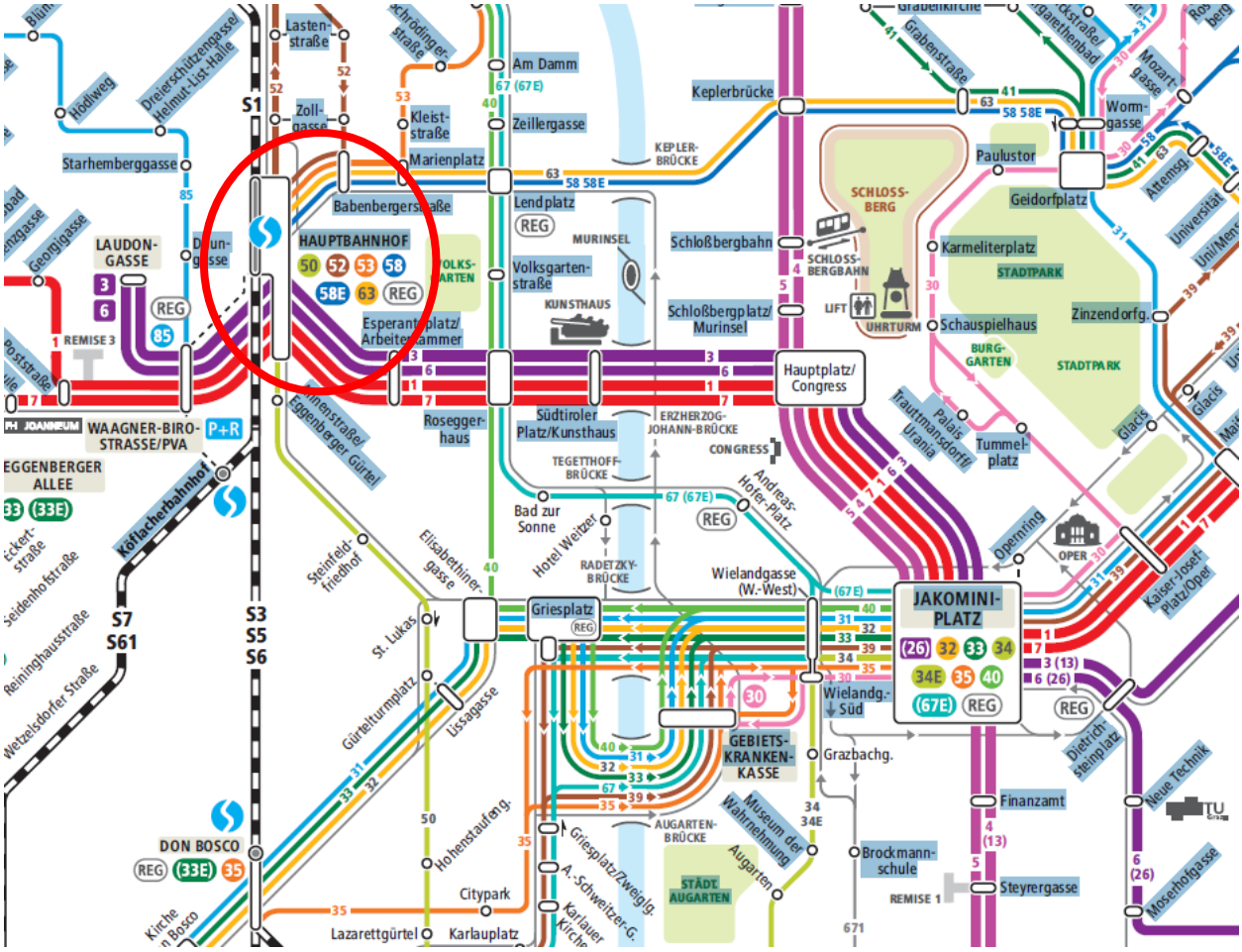
Conference Location:

The conference will take place at the Austria Trend Hotel Graz:

©Austria Trend Hotel Europa

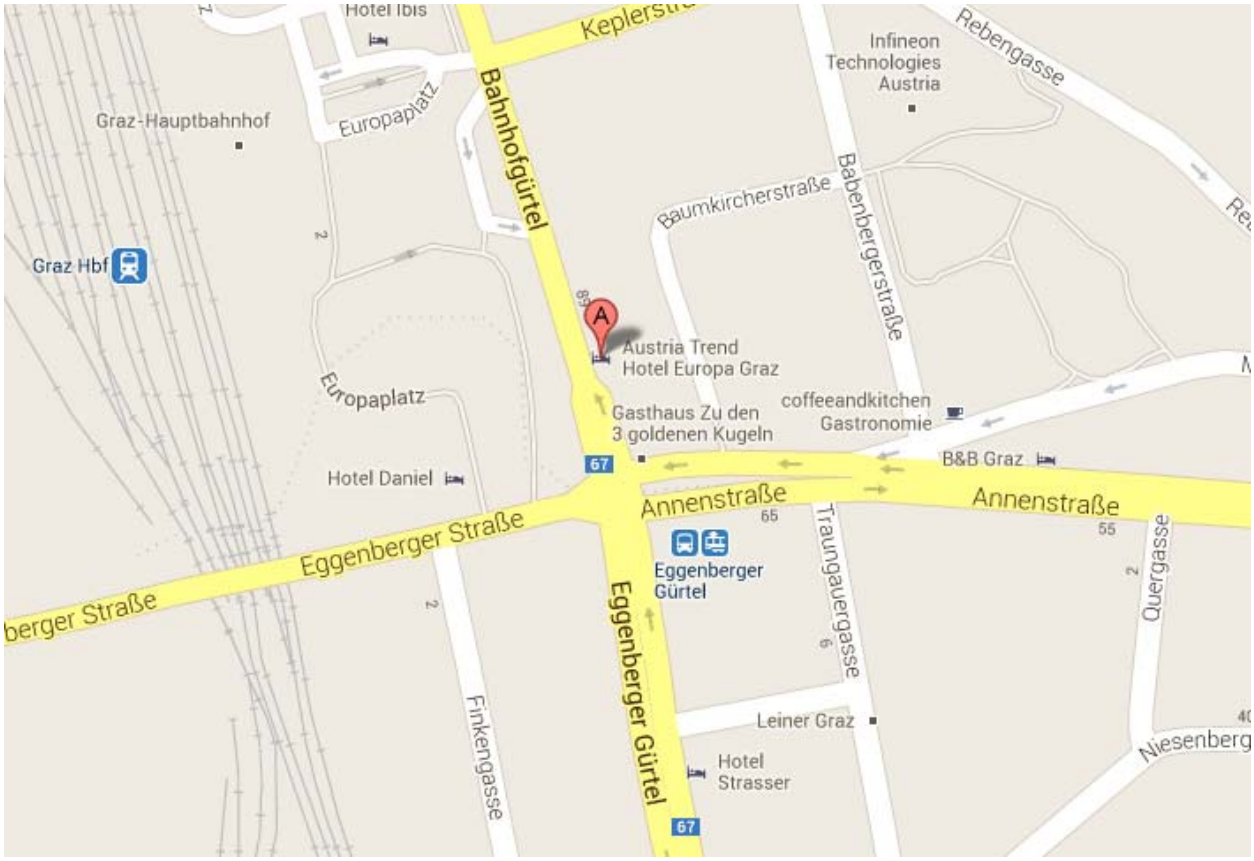
Address:
Bahnhofgürtel 89
8020 Graz
Email: europa.graz@austria-trend.at
Web: http://www.austria-trend.at/hotel-europa-graz/en/

How to reach:
The hotel is right next to the train station of Graz. If you decide to take the tram/street car, you can use the trams 1, 3, 6, and 7; exit at station "Hauptbahnhof" (train station).



© http://www.holding-graz.at

Conference Venue Location:



© Google.com

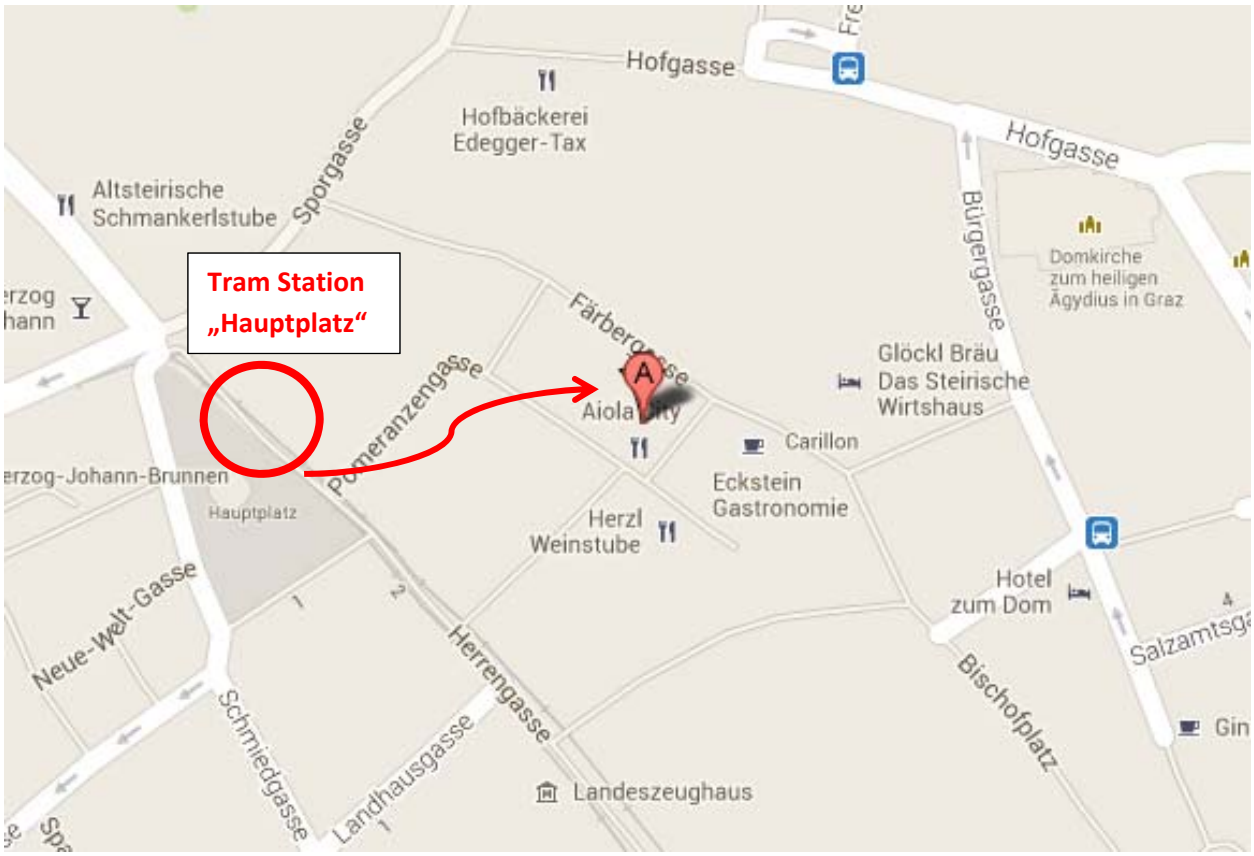
Welcome Reception:

The welcome reception will take place at the M1 bar in the center of Graz.

Address:
Färberplatz 1
A-8010 Graz

© M1 bar

How to reach:
If you take the tram/street car, you have to stop at station „Hauptplatz“. From the Hauptplatz, it’s a 5min walking distance.



© Google.com

Graz - City Overview:

© Google.com

Sponsors:

SFG
Im Auftrag des Wirtschaftslandesrates

GRAZ
www.graz.at

Das Land Steiermark
Wissenschaft

NXP

NXP Semiconductors N.V. (NASDAQ: NXPI) provides High Performance Mixed Signal and Standard Product solutions that leverage its leading RF, Analog, Power Management, Interface, Security and Digital Processing expertise. These innovations are used in a wide range of automotive, identification, wireless infrastructure, lighting, industrial, mobile, consumer and computing applications. A global semiconductor company with operations in more than 25 countries, NXP posted revenue of 4,36 mio $ in 2012. Additional information can be found by visiting www.nxp.com.

NXP is the trusted partner for authenticating identities, securing transactions and providing convenient interactions through our complete identification solutions.