Fachbereich MATHEMATIK

UNIVERSITÄT SALZBURG

Hash & Stream

The State of the Art for Cryptographic Hash Functions and for Stream Ciphers

Feb. 1 - 2, 2007
Dept. of Mathematics, University of Salzburg

Thursday, Feb. 1		
14:45 - 15:30	Vincent Rijmen (IAIK, TU Graz)	Introduction to Cryptographic Hash Functions
15:30 - 16:00	*Coffee / Tea Break*	
16:00 - 17:15	Vincent Rijmen (IAIK, TU Graz)	Recent Attacks on Hash Functions
17:30 - 18:15	Christian Rechberger (IAIK, TU Graz)	Most Recent Attacks on SHA-1

Friday, Feb. 2		
9:00 - 9:45	Norbert Pramstaller (IAIK, TU Graz)	Practical Impact of the Recent Attacks and What Will Happen Now
10:00 - 10:45	Florian Mendel (IAIK, TU Graz)	Cryptanalysis of Alternative Hash Functions
10:45 - 11:15	*Coffee / Tea Break*	
11:15 - 12.30	Willi Meier (UAS, NW Switzerland)	Design and Recent Analysis of eSTREAM Candidates

Workshop Description
In a compact series of five talks, the state of the art in cryptographic hash functions and for stream ciphers will be reviewed by two leading researchers in this field (Meier, Rijmen) and by three internationally respected young researchers of the IAIK Krypto Group at Graz Technical University (Mendel, Pramstaller, Rechberger).

This workshop is open to anybody familiar with the basic concepts of applied cryptography. Students of mathematics or computer science as well as practitioners in the security industry are particularly welcome.

Attendance of this workshop is free.

Workshop Location
Hörsaal 402
Erdgeschoß, Naturwissenschaftliche Fakultät, Universität Salzburg
Hellbrunner Straße 34, 5020 Salzburg

Workshop Organizer
Peter Hellekalek
Fachbereich Mathematik, Universität Salzburg
Hellbunner Straße 34, 5020 Salzburg
Email: peter.hellekalek@sbg.ac.at
Phone: +43 662 8044 5310

Workshop Sponsors
Universität Salzburg
Fonds zur Förderung der wissenschaftlichen Forschung (FWF)

Getting There by Public Transport
Bus line 22 serves the town center and stops in front of Hellbrunner Straße 34 (bus stop is called "Michael-Pacher-Straße"); it is the "simple but slow" solution to get there.
Bus line 3 serves both the town center and the Central Railway Station (Hauptbahnhof) at much higher frequencies than bus 22; get off at "Faistauergasse" and walk to the university (5 minutes) or change to bus no. 22 at bus stop "Josefiau" (bus 22 stops in the small street left to the post office).
Information in the internet: *http://www.stadtbus.at*

Getting There by Car
Take exit "Salzburg Süd" on highway A10,
then take "Alpenstraße", a two-lane road towards the town center,
until "Michael-Pacher-Straße",
take a half "U"-turn at the little roundabout
at the Alpenstraße - Michael-Pacher-Straße crossing,
following the signs"Landesregierung - Universität".