Preliminary program

Sunday, May 9

16:00 – 19:00	Registration

Monday, May 10

8:30 - 9:45	Registration / Coffee
9:45 - 10:00	Welcome
10:00 – 11:00	**Invited talk** Cyclic Properties of AES Round Functions *Yvo Desmedt (Florida State University)*
11:00 – 12:30	Presentations I More dual Rijndaels *Håvard Raddum* Boomerang attack on 5- and 6-round AES *Alex Biryukov* A three rounds property of the AES *Marine Minier*
12:30	Lunch
14:00 - 15:00	**Invited talk** Representations of Rijndael *Vincent Rijmen (IAIK, Graz University of Technology and Cryptomathic)*
15:00	Coffee break
15:30 - 17:00	Presentations II Efficient AES implementations on ASICs and FPGAs *Sandra Dominikus, Stefan Mangard, Norbert Pramstaller, Johannes Wolkerstorfer* Small size, low power, side channel-immune AES coprocessor *Elena Trichina, Tymur Korkishko* A CAM based associative processor array for parallel implementation of AES *Hua Li, Hang N. Zhang, Jianzhou Li*

Tuesday, May 11

9:00 - 10:00	**Invited talk** Some Algebraic Aspects of the Advanced Encryption Standard *Carlos Cid (Royal Holloway, University of London)*
10:00	Coffee break
10:30 – 12:00	Presentations III DFA on AES *Christophe Giraud*

Refined analysis of bounds related to linear and differential cryptanalysis for the AES
Liam Keliher
Linearity of the AES key schedule
Frederik Armknecht, Stefan Lucks

12:00 - 13:00 **Invited talk**
General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers
Nicolas T. Courtois (Axalto Smart Cards)

13:00 Lunch

16:00 – 18:00 Guided Tour in Arithmeum
Institute for Discrete Mathematics
Lennestrasse 2
53113 Bonn
http://www.arithmeum.de/

19:00 Social event / Banquet

Wednesday, May 12

9:00 - 10:00 **Invited talk**
To be named
Jean-Charles Faugere (University of Paris VI / INRIA, France)

10:00 Coffee break

10:30 – 12:00 Presentations IV

An algebraic interpretation of AES-128
Ilia Toli, Alberto Zanoni
The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers
Nicolas T. Courtois

12:00 - 13:00 **Invited talk**
NIST and AES in 2004
John Kesley (NIST)

13:00 - 14:00 Discussion (open to the public)

Moderation:
Peter Welchering (Wissenschaftspressekonferenz)

Participants:
Nicolas T. Courtois (Axalto Smart Cards)
Hans Dobbertin (ITS, Ruhr-University Bochum / HGI)
John Kelsey (NIST)
Vincent Rijmen (IAIK, Graz University of Technology and Cryptomathic)

14:00 Lunch

16:00 End