Vampire
Virtual Application and
Implementation Research Lab

ECRYPT
Network of Excellence in Cryptology
IST-2002-507932

Special Purpose Hardware for Attacking Cryptographic Systems (SHARCS ‘06)

Cologne,
April, 03.& 04., 2006

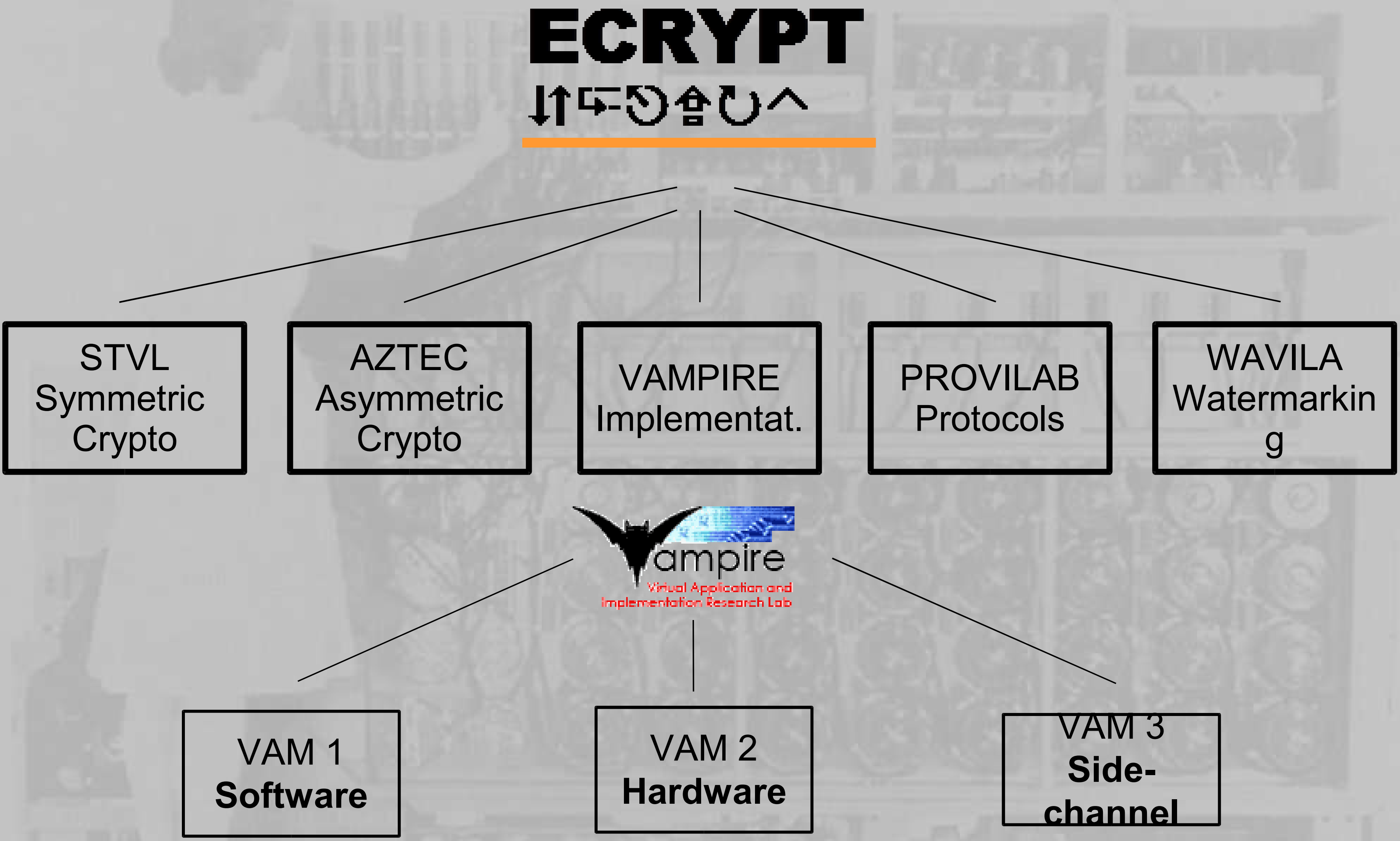
hgi
Horst-Görtz Institut
für IT Sicherheit

DTU

ECRYPT

Network of Excellence in Cryptology
IST-2002-507932

- European Network of Excellence in Cryptology and Watermarking
- EU FP6-IST programme
- February 2004 - July 2008
- Academia: 23; Industry: 9
- 14 countries



ECRYPT

STVL
Symmetric
Crypto

AZTEC
Asymmetric
Crypto

VAMPIRE
Implementat.

PROVILAB
Protocols

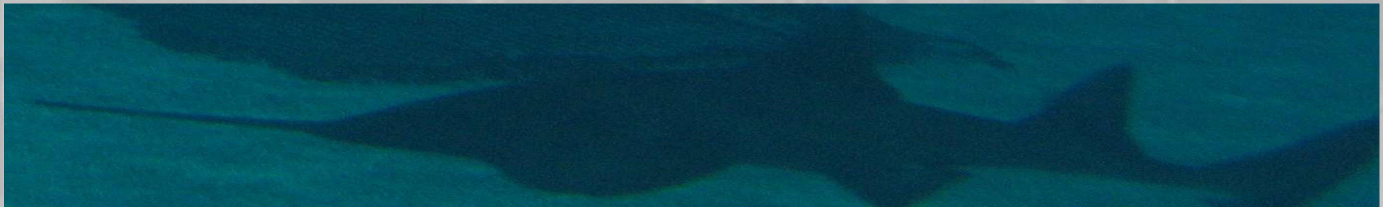
WAVILA
Watermarkin
g

Vampire
Virtual Application and
Implementation Research Lab

VAM 1
Software

VAM 2
Hardware

VAM 3
Side-
channel



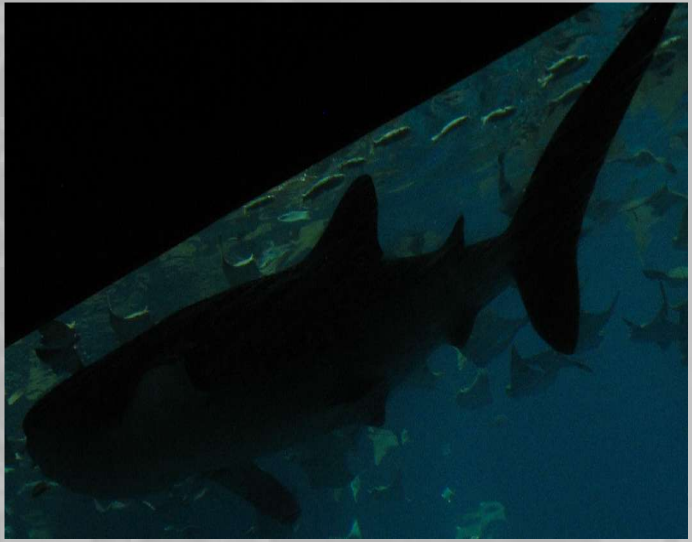
Vampire

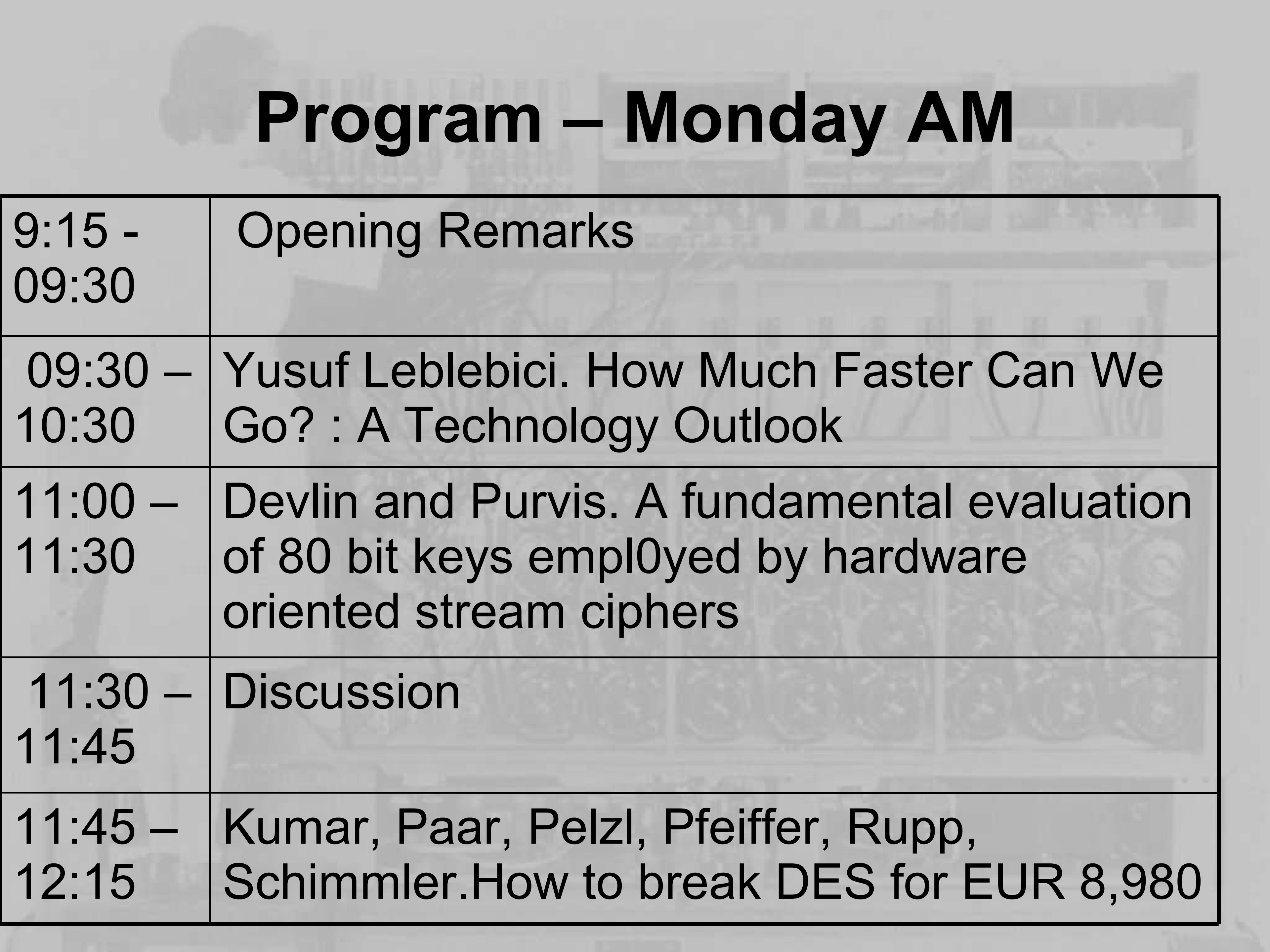
Virtual Application and
Implementation Research Lab

- Vampire public page
  http://www.rub.de/itsc/tanja/vampire

- ECRYPT public page
  http://www.ecrypt.eu.org

- Contains:
  - AES lounge
  - Side-channel analysis lounge

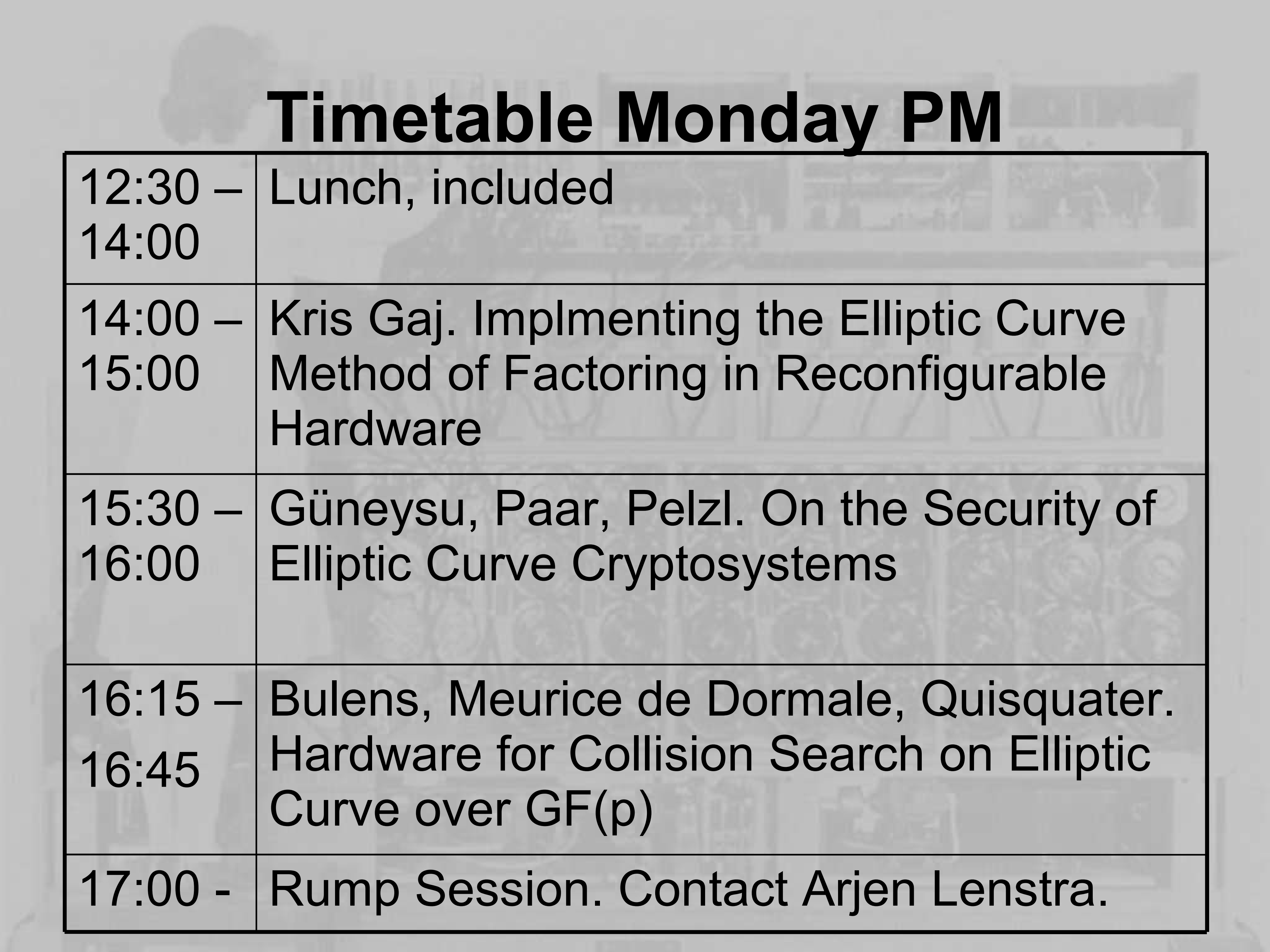




Program – Monday AM

9:15 - 09:30	Opening Remarks
09:30 – 10:30	Yusuf Leblebici. How Much Faster Can We Go? : A Technology Outlook
11:00 – 11:30	Devlin and Purvis. A fundamental evaluation of 80 bit keys empl0yed by hardware oriented stream ciphers
11:30 – 11:45	Discussion
11:45 – 12:15	Kumar, Paar, Pelzl, Pfeiffer, Rupp, Schimmler.How to break DES for EUR 8,980

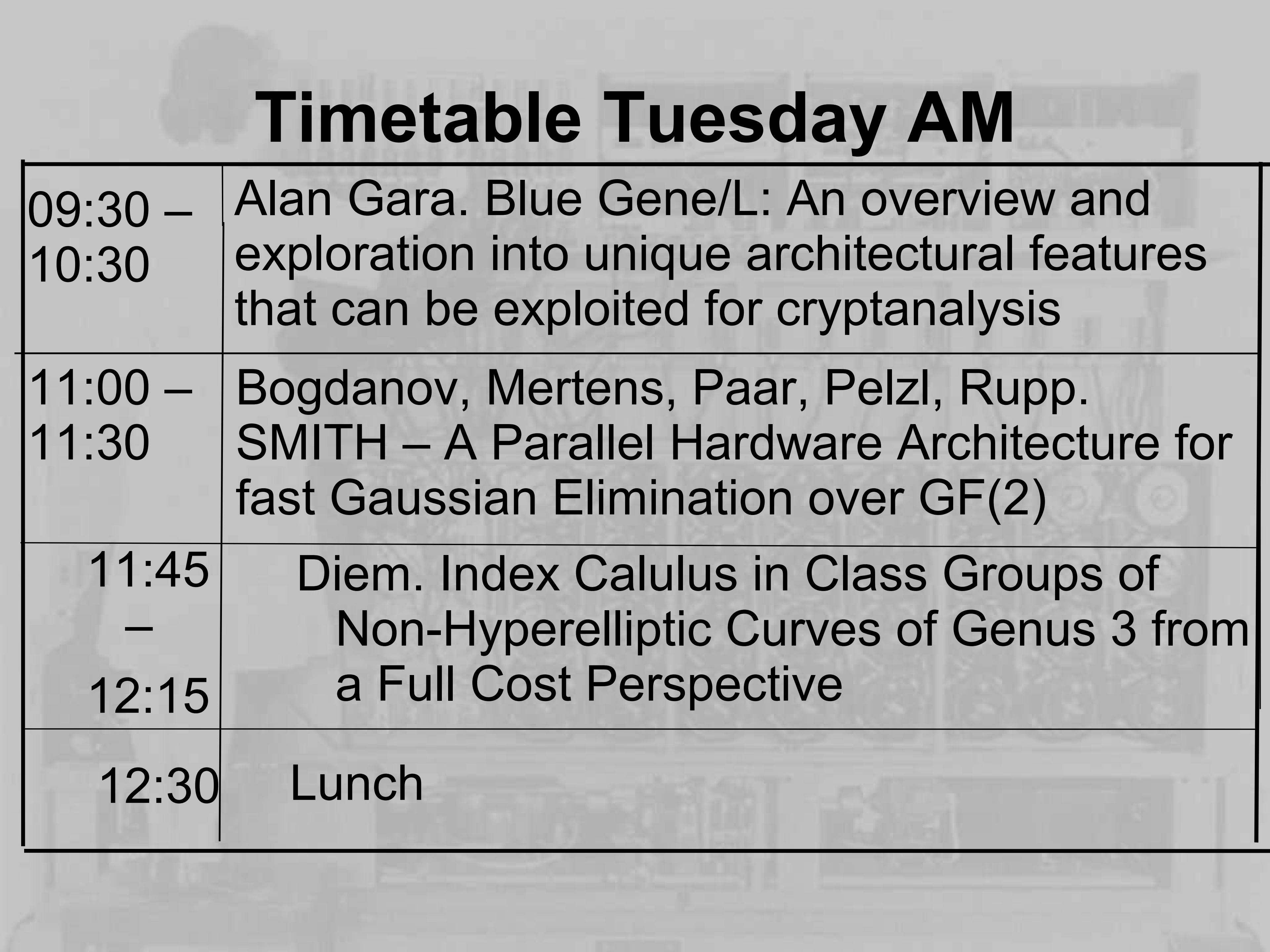
Timetable Monday PM



12:30 – 14:00	Lunch, included
14:00 – 15:00	Kris Gaj. Implmenting the Elliptic Curve Method of Factoring in Reconfigurable Hardware
15:30 – 16:00	Güneysu, Paar, Pelzl. On the Security of Elliptic Curve Cryptosystems
16:15 – 16:45	Bulens, Meurice de Dormale, Quisquater. Hardware for Collision Search on Elliptic Curve over GF(p)
17:00 -	Rump Session. Contact Arjen Lenstra.

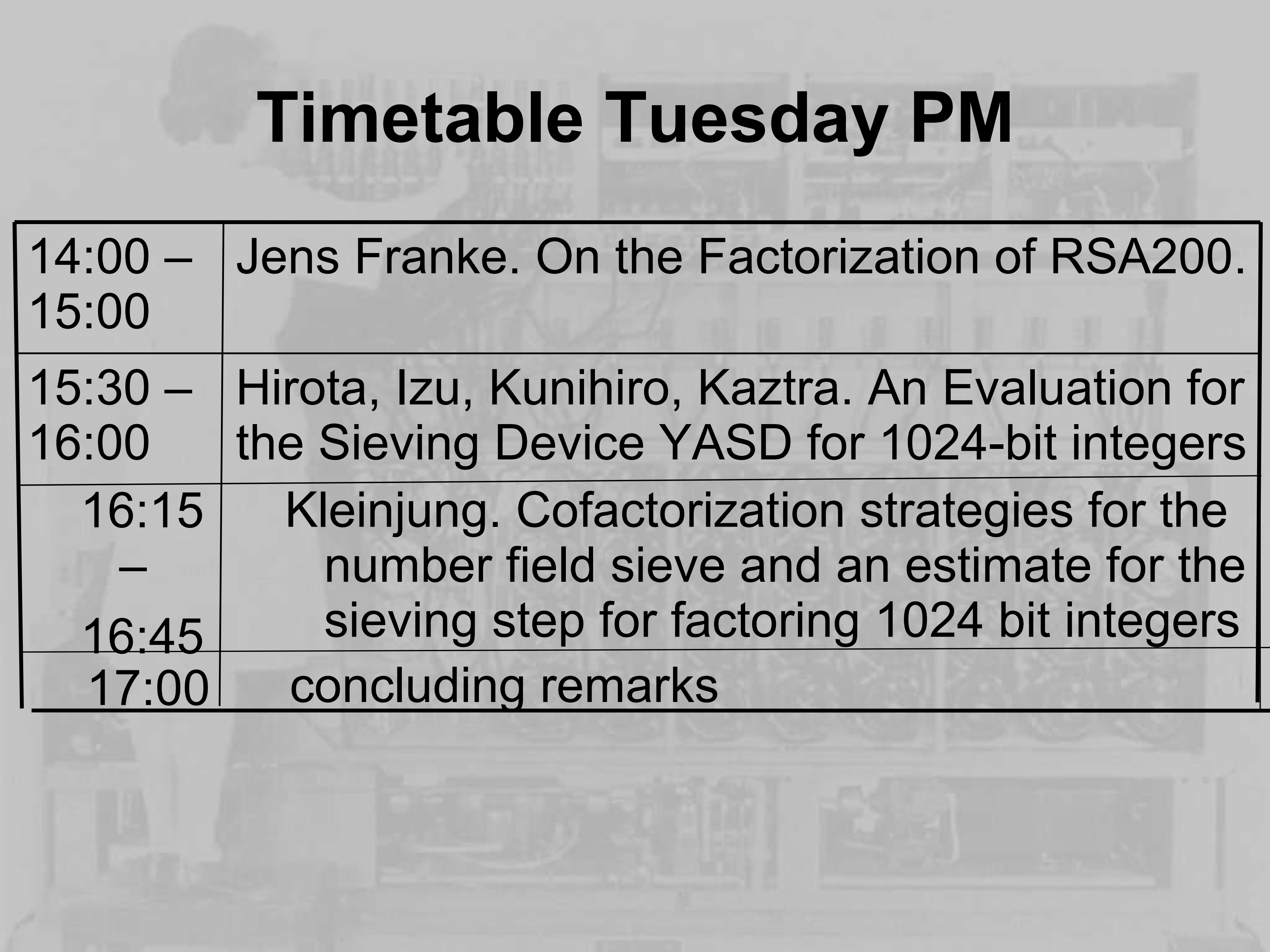
Dinner – 19:30

- Hotel Hilton Cologne
- Very close to the Main Station.
- Map is available at the reception desk.
- Joint walk at 19:00 from Dorint Hotel.



Timetable Tuesday AM

09:30 – 10:30	Alan Gara. Blue Gene/L: An overview and exploration into unique architectural features that can be exploited for cryptanalysis
11:00 – 11:30	Bogdanov, Mertens, Paar, Pelzl, Rupp. SMITH – A Parallel Hardware Architecture for fast Gaussian Elimination over GF(2)
11:45 – 12:15	Diem. Index Calulus in Class Groups of Non-Hyperelliptic Curves of Genus 3 from a Full Cost Perspective
12:30	Lunch



Timetable Tuesday PM

14:00 – 15:00	Jens Franke. On the Factorization of RSA200.
15:30 – 16:00	Hirota, Izu, Kunihiro, Kaztra. An Evaluation for the Sieving Device YASD for 1024-bit integers
16:15 – 16:45	Kleinjung. Cofactorization strategies for the number field sieve and an estimate for the sieving step for factoring 1024 bit integers
17:00	concluding remarks

Enjoy SHARCS'06