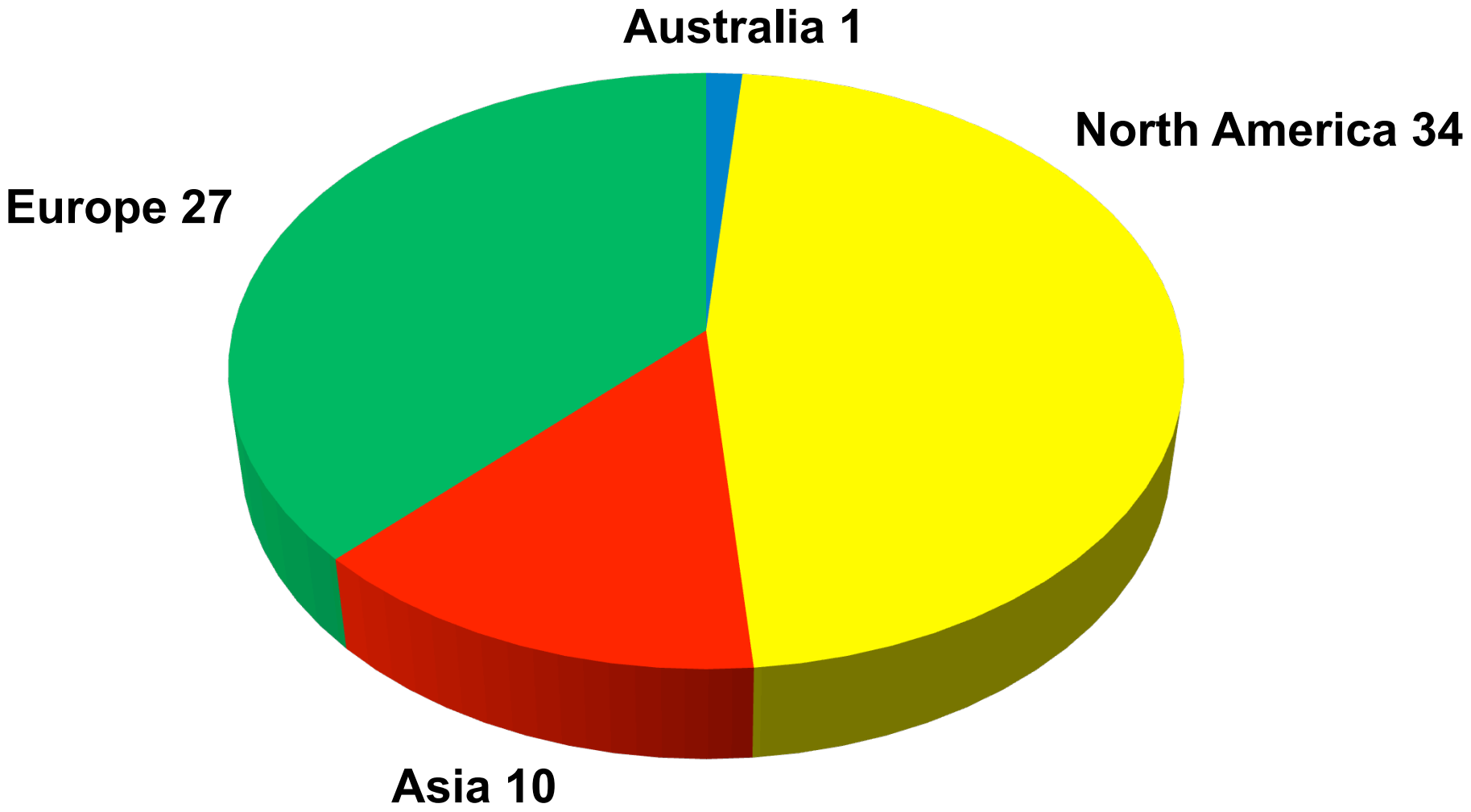
SHARCS 2012
Welcome

Jens-Peter Kaps

GEORGE MASON UNIVERSITY

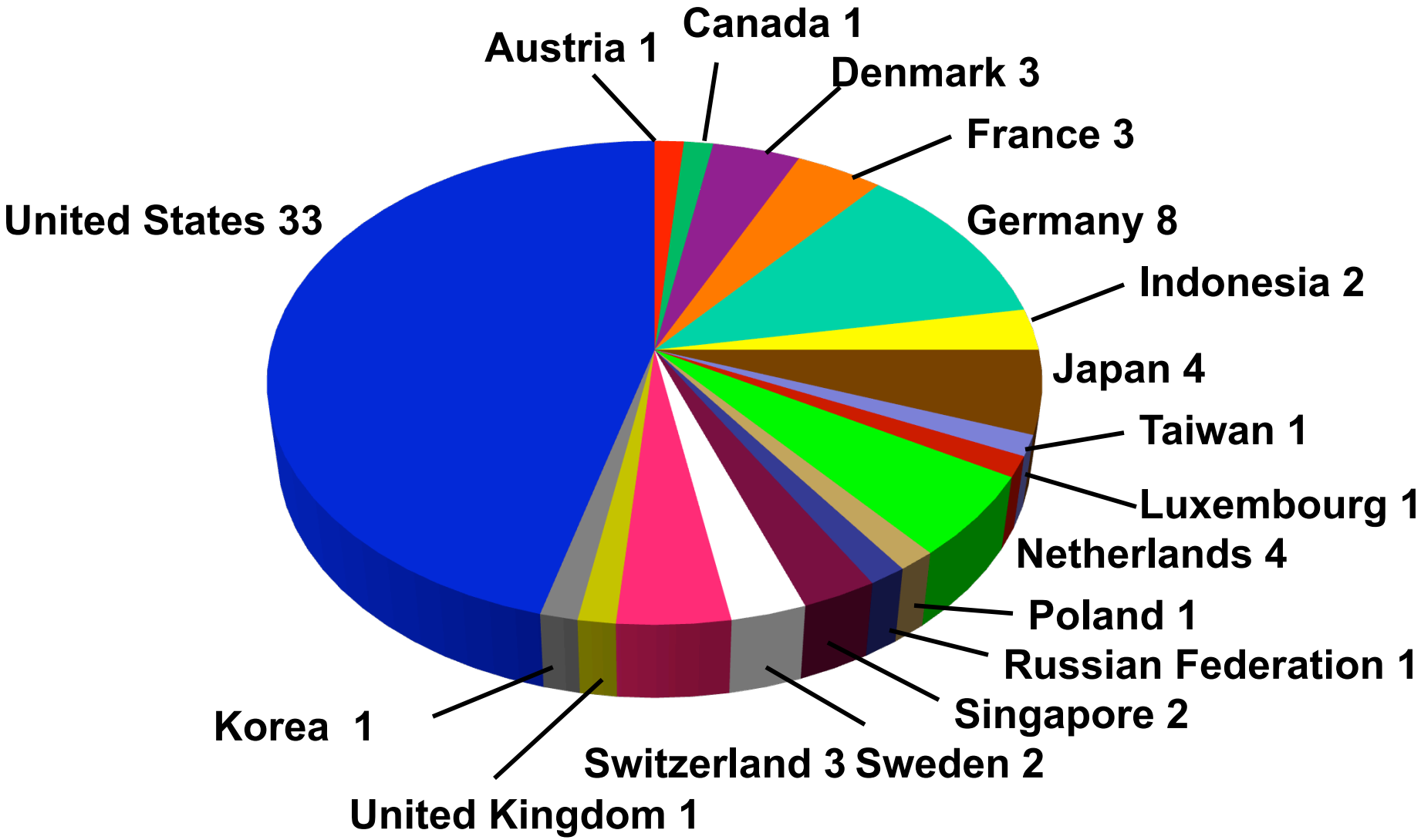
A Few Words About You

4 continents



A Few Words About You

18 countries

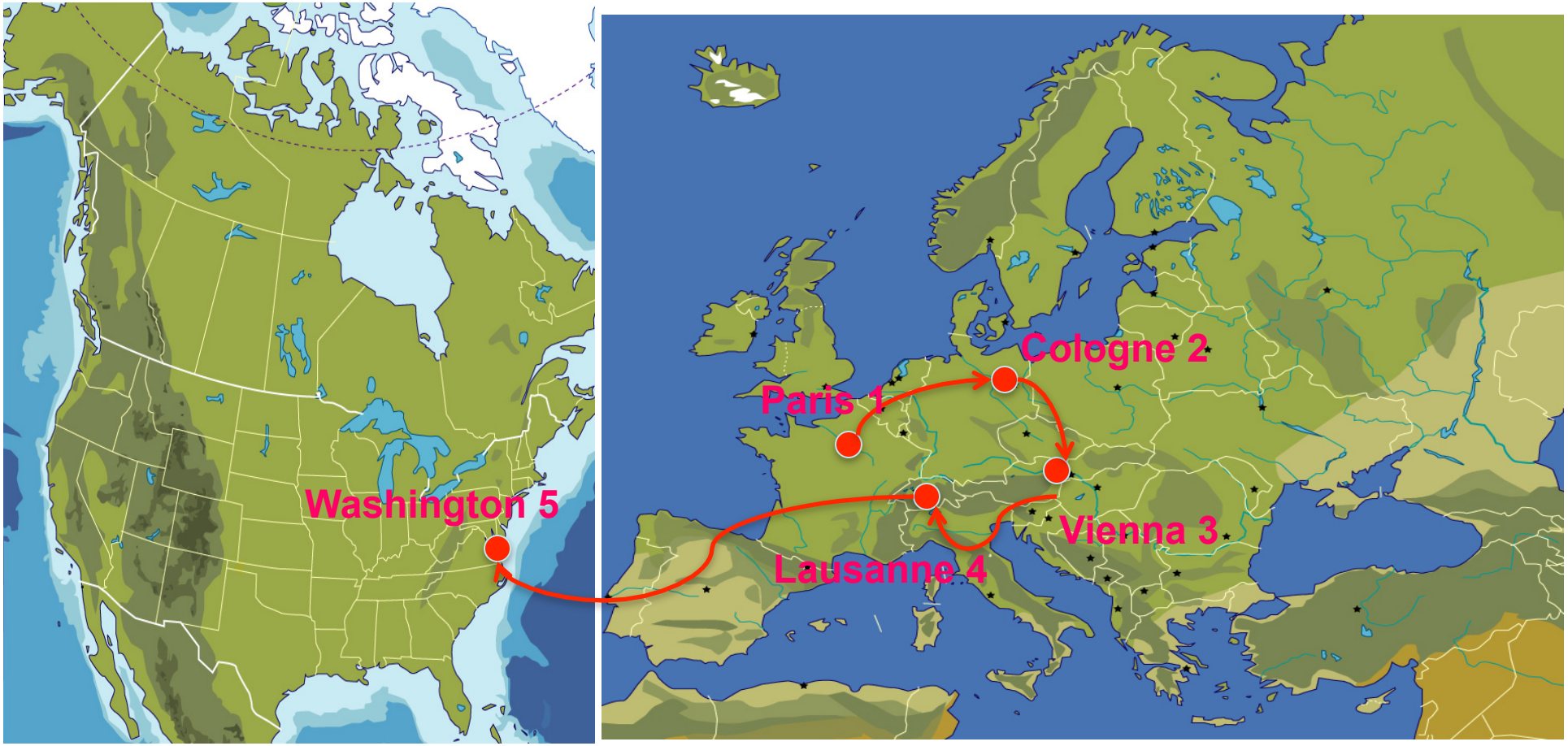


List of Attendees

- distributed on Sunday, after lunch
- if you do not want your name to be listed please let our staff at the registration desk know about it
- if you do not mind your name to be listed please verify your data included in the draft version of the list

  Name:
  Affiliation:
  Address:
  E-mail:

SHARCS Journey 2005-2012



Crypto Triathlon

Saturday-Sunday
March 17-18

Monday-Wednesday
March 19-21

Thursday-Friday
March 22-23

FSE 2012
19th International Workshop on Fast Software Encryption

The Third SHA-3 Candidate Conference

CERG
Cryptographic Engineering Research Group
cryptography.gmu.edu

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

NIST
National Institute of Standards and Technology

Sponsors

Science Applications
International Corporation

Sponsors

hgi
Horst Görtz Institute
for IT-Security

sponsoring
historical talk
by Stephen Budiansky

TU/e Technische Universiteit Eindhoven University of Technology

sponsoring
invited talk
by Marc Stevens

Platinum Sponsor

Sponsoring a significant portion of the venue cost

Statement from Paul Kocher

President, Cryptography Research Inc.

Chronicle / Paul Chinn

Statement from
Paul Kocher
President, Cryptography Research Inc.

On behalf of Cryptography Research, I would like to welcome you to the SHARCS 2012 Workshop. Understanding the limits of cryptographic algorithms is central to all of our efforts to build secure systems. Several years ago, one of our projects was to design the Deep Crack keysearch machine that was built to demonstrate why single-DES needed to be retired.

Today there are still many important security questions where hardware can help us Improve the security, or understand the insecurity, of cryptographic systems.

We're pleased to sponsor the SHARCs workshop as a way of saying "Thank you" for your work, and because we're enthusiastic about research on cryptographic hardware.

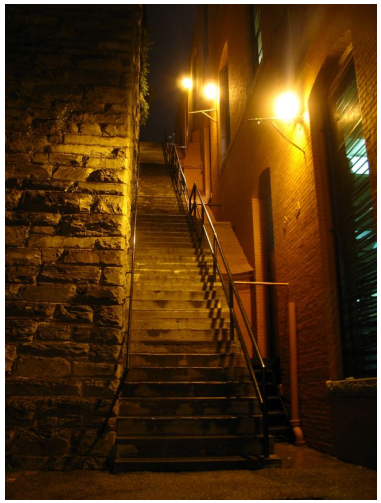
And for the students in the audience -- we are hiring. If you want to work on solving some of the world's most challenging and interesting security problems, visit our website to see our current openings and send us your resume.

Places to See (after SHARCS)

INTERNATIONAL SPY MUSEUM

White House

The Mall

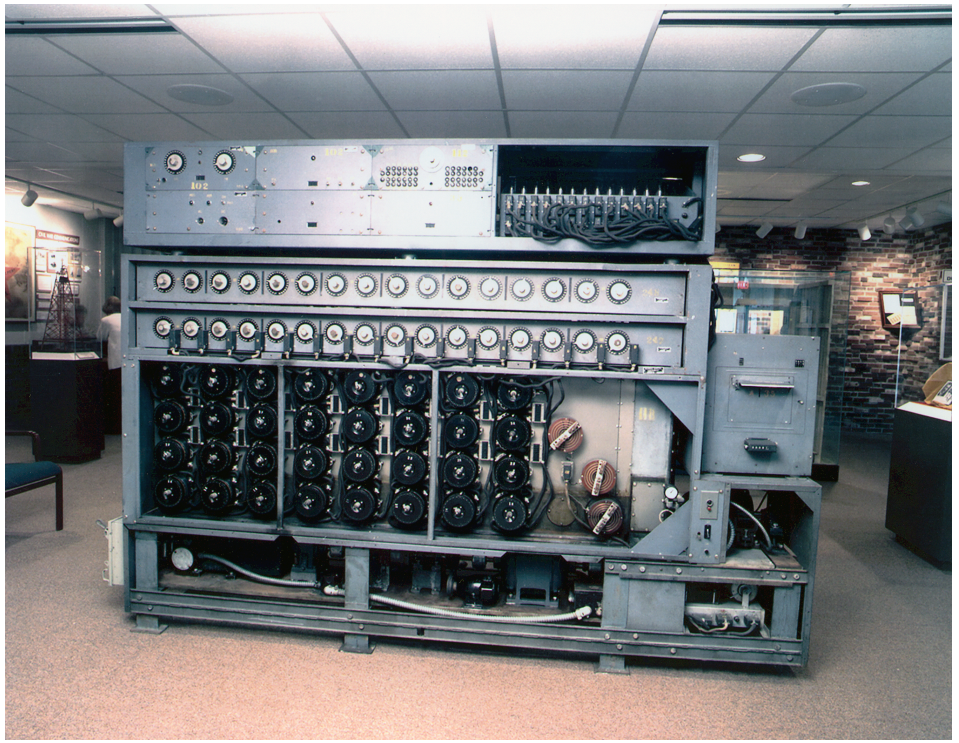


Georgetown

Kennedy Center

Newseum

National Cryptologic Museum
Fort Meade, MD



- 45-minute drive by car
- Open M-F, 9:00-16:00

SHARCS 2012 Program

Daniel J Bernstein

UIC
UNIVERSITY OF ILLINOIS AT CHICAGO

Kris Gaj

GEORGE MASON UNIVERSITY

Program Committee

- Daniel J. Bernstein, University of Illinois at Chicago, USA
- Duncan A. Buell, University of South Carolina, USA
- Kris Gaj, George Mason University, USA
- Tim Güneysu, Ruhr-Universität Bochum, Germany
- Tetsuya Izu, Fujitsu Laboratories, Japan
- Tanja Lange, Technische Universiteit Eindhoven, Netherlands
- Christof Paar, Ruhr-Universität Bochum, Germany
- Christian Rechberger, Danmarks Tekniske Universitet, Denmark
- Rainer Steinwandt, Florida Atlantic University, USA
- Eran Tromer, Tel Aviv University, Israel
- Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium
- Michael Wiener, Irdeto, Canada
- Bo-Yin Yang, Academia Sinica, Taiwan

All papers evaluated by at least 3 members of the PC

Subreviewers

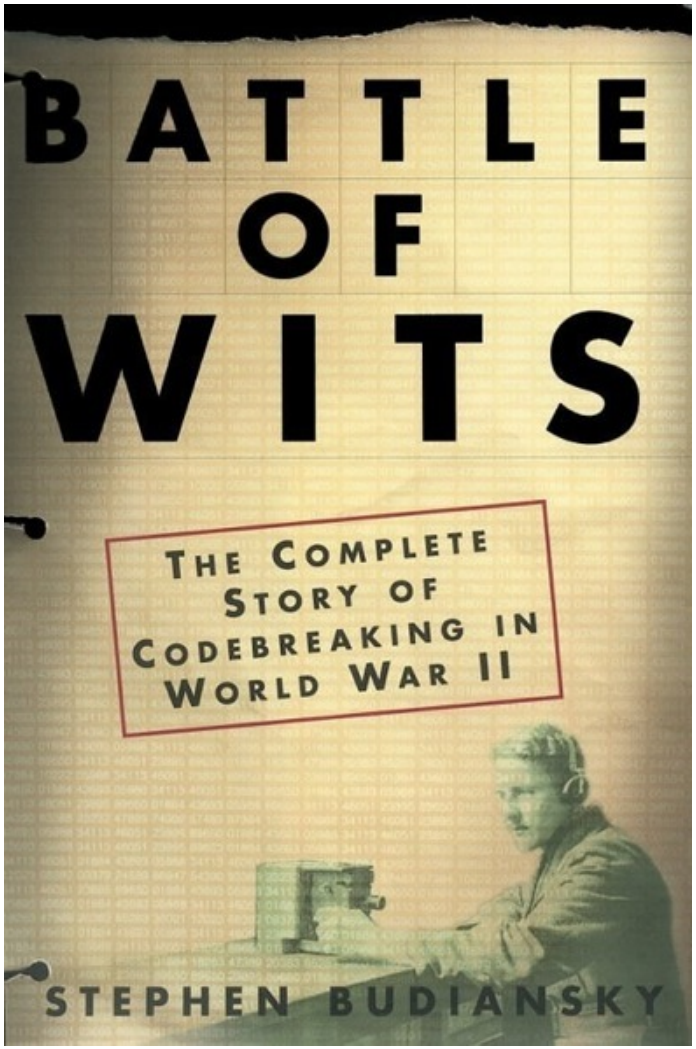
Jens Hermans
Markus Kasper
Nele Mentens
Amir Moradi
Anthony Van Herrewege
Frederik Vercauteren
Christopher Wolf
Tolga Yalcin
Ralf Zimmermann

Invited Historical Talk
Saturday, 17:15

Stephen Budiansky

"Codebreaking with IBM machines in World War II"

Book Signing
Saturday, 18:15-19:00



Stephen Budiansky

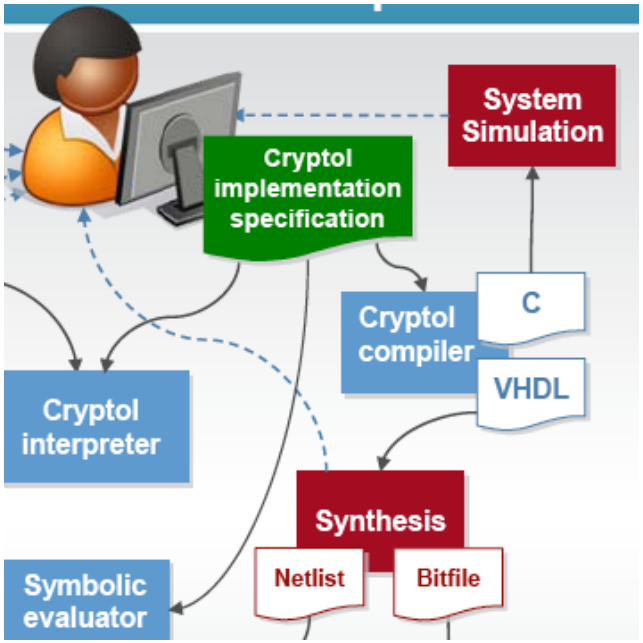
Where: table in front of the conference room

Books available for purchase at the registration desk.

Invited Talk
Sunday, 9:00

Joe Hurd and Sally A. Browning
Galois, Inc.

Cryptol: The Language of
~~Cryptography~~ Cryptanalysis

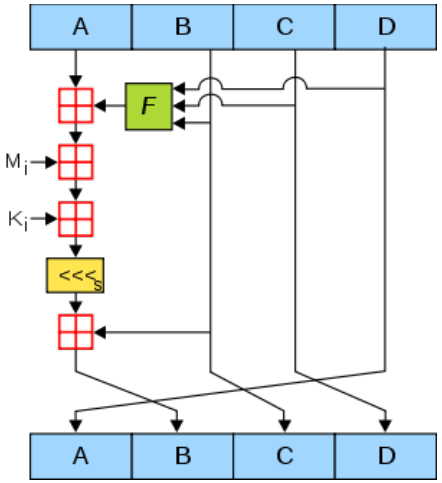


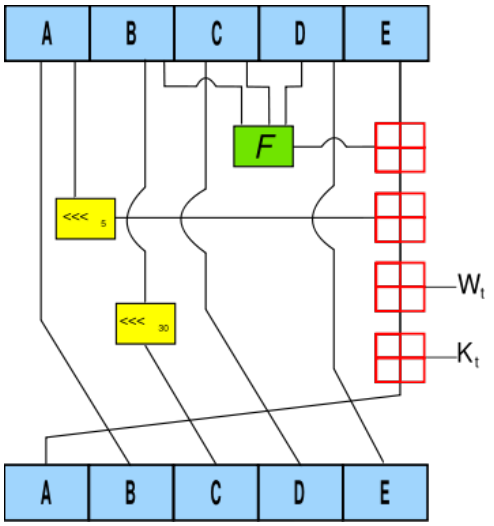
Invited Talk
Sunday, 13:30

Marc Stevens

Centrum voor Wiskunde en Informatica (CWI)

Cryptanalysis of MD5 and SHA-1





Four Sessions Based on Regular Submissions

Saturday

15:15-16:45 **Session 1: Better than brute force**

Chair: Bo-Yin Yang

Sunday

10:30-12:00 **Session 4: Discrete logarithms**

Chair: Tanja Lange

14:30-15:30 **Session 6: Algebraic attacks**

Chair: Nicolas Courtois

16:00-17:00 **Session 7: Tools**

Chair: Christian Rechberger

Guidelines for Speakers

- Upload your slides to the presenter's laptop
  at least 10 minutes before the start of your session
  Helpers: Marcin on Saturday
  Rabia on Sunday
- Introduce yourself to the Session Chair
  before the start of your session
- Pay attention to signs indicating the amount of
  time left till the end of your talk
  25 minutes for the talk, 5 minutes for Q&A

Enjoy the Workshop!