Welcome to CHES 2006！

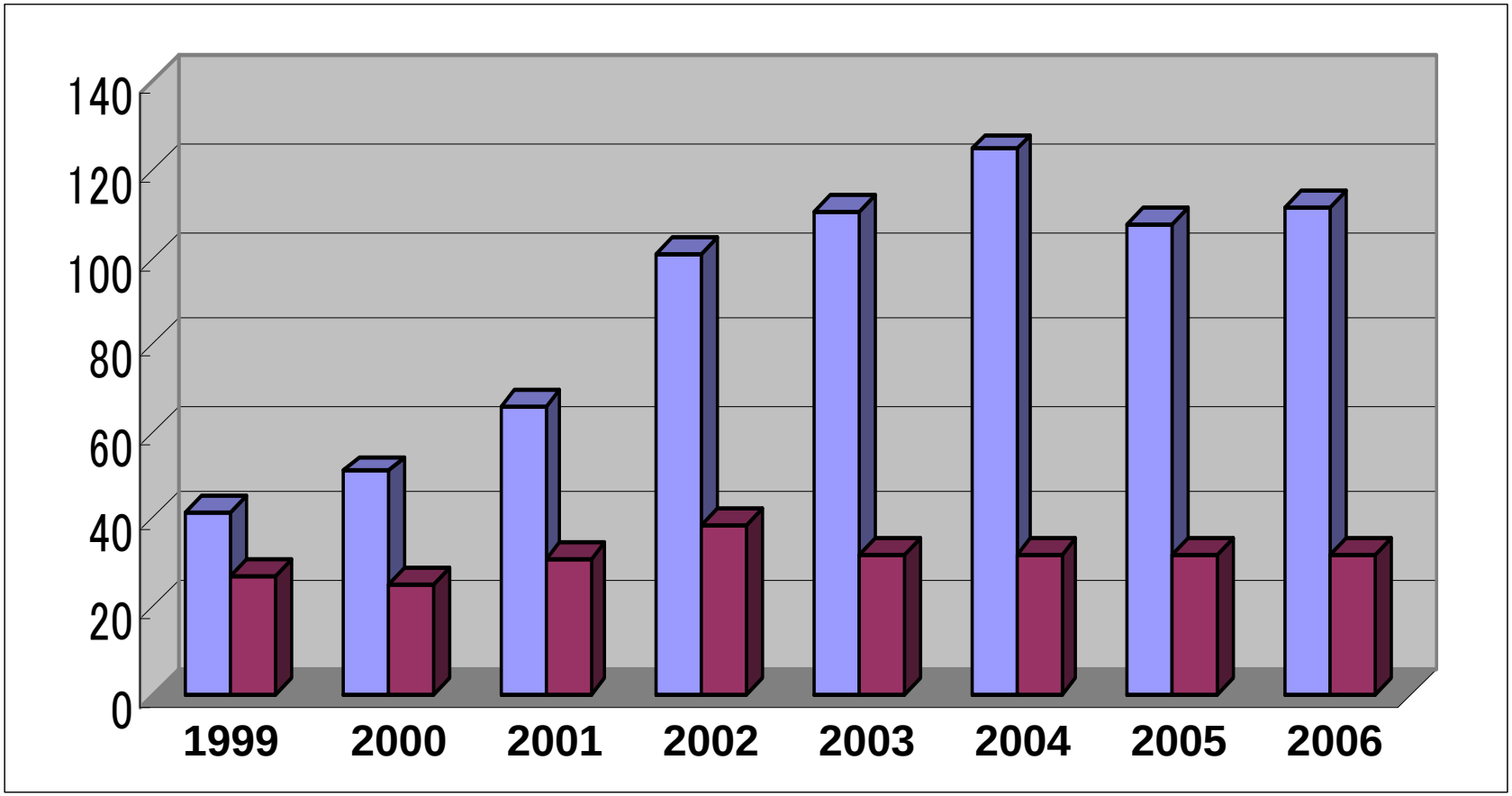
暗号ハードウェアおよび組込みシステム国際会議

Selection process

- **112 papers submitted** (vs 108 last year)
- Program Committee: 26 reviewers
  - Helped by 91 external reviewers
- Each paper carefully read by at least 3 reviewers
  - Submissions with a PC member as a (co-)author read by at least 5 reviewers
- Two week Web discussion process

➔ **32 papers selected for presentation**

CHES1999-2006
of submitted/accepted papers



Program Committee

- Mehdi-Laurent Akkar
- Jean-Sebastien Coron
- Nicolas T. Courtois
- Joan Daemen
- Pierre-Alain Fouque
- Jim Goodman
- Helena Handschuh
- Tetsuya Izu
- Marc Joye
- Seungjoo Kim
- Cetin Kaya Koc
- Pil Joong Lee
- Frederic Muller
- Katsuyuki Okeya
- Elisabeth Oswald
- Christof Paar
- Josyula R. Rao
- Erkay Savas
- Werner Schindler
- Nigel Smart
- Francois-Xavier Standaert
- Berk Sunar
- Frederic Valette
- Ingrid Verbauwhede
- Colin Walter
- Sung-Ming Yen

External reviewers

- Onur Aciicmez
- Manfred Aigner
- Toru Akishita
- Frederic Amiel
- Cedric Archambeau
- Lejla Batina
- Kamel Bentahar
- Guido Bertoni
- Regis Bevan
- Arnaud Boscher
- Donald R. Brown
- Cecile Canovas
- Chien-Ning Chen
- Benoit Chevallier-Mames
- Jessy Clediere
- Eric Dahmen
- Yasin Demirbas
- Loic Duflot
- Takashi Endo
- Pooya Farshim
- Benoit Feix
- Kris Gaj
- Christophe Giraud
- Aline Gouget
- Rob Granger
- Johann Grossschald
- Jorge Guajardo
- Frank Guerkaynak
- Tim Guneysu
- Adnan Gutub
- DongGuk Han
- Christoph Herbst
- Yong Ho Hwang
- Kouichi Itoh
- Charantjit Jutla
- Jin Ho Kim
- Tae Hyun Kim
- Young Hwan Kim
- Thorsten Kleinjung
- Sandeep Kumar
- Noboro Kunihiro
- Sebastien Kunz-Jacques
- Eun Jeong Kwon
- Soonhak Kwon
- Kerstin Lemke-Rust
- Wei-Chih Lien
- Manfred Lochter
- Francois Mace
- Pascal Manet
- Stefan Mangard
- Marian Margraf
- Gwenaelle Martinet
- John McNeill
- Nele Mentens
- Guerric Meurice de Dormale
- Andrew Moss
- Francis Olivier
- Berna Ors
- Dan Page
- Jung Hyung Park
- Fabrice Pautot
- Eric Peeters
- Jan Pelzl
- Thomas Peyrin
- Thomas Popp
- Axel Poschmann
- Emmanuel Prouff
- Jean-Luc Rainard
- Arash Reybani-Masoleh
- Francisco Rodriguez-Henriquez
- Kazuo Sakiyama
- Gokay Saldamli
- Akashi Satoh
- Sven Schage
- Daniel Schepers
- Kai Schramm
- Jae Woo Seo
- Jong Hoon Shin
- Alexei Tchoulkine
- Alexandre F. Tenca
- Stefan Tillich
- Elena Trichina
- Pim Tuyls
- Francois Vacherand
- Camille Vuillaume
- Takashi Watanabe
- Jun Yajima
- Yeon Hyeong Yang
- Hirotaka Yoshida
- Masayaki Yoshino
- Dae Hyun Yum

Invited Speakers

- Kazumaro Aoki (NTT)
  - “Integer Factoring Utilizing PC Cluster”
- Ari Juels (RSA Labs)
  - “The Outer Limits of RFID Security”
- Ahmad Sadeghi (Ruhr University Bochum)
  - “Challenges for Trusted Computing”

The program at a glance

- Wednesday, October 11
  - Side Channels I (Chair: Marc Joye)
  - Low Resources (Chair: Elena Trichina)
  - Hardware Attacks and Countermeasures I (Chair: Pierre-Alain Fouque)
  - Special Purpose Hardware (Chair: Tetsuya Izu)
  - Efficient Algorithms for Embedded Processors (Chair: Berk Sunar)
- Thursday, October 12
  - Side Channels II (Chair: Erkay Savas)
  - Hardware Attacks and Countermeasures II (Chair: Ingrid Verbauwhede)
  - Efficient Hardware I (Chair: Akashi Satoh)
  - Trusted Computing (Chair: Shiho Moriai)
- Friday, October 13
  - Side Channels III (Chair: Katsuyuki Okeya)
  - Hardware Attacks and Countermeasures III (Chair: Frederic Valette)
  - Efficient Hardware II (Chair: Francois-Xavier Standaert)

All speakers: please contact the chair of your session before the session !

Rump Session: Wednesday Evening

What?

- recent results
- work in progress
- can be funny

How?

- max. ½ page abstract
- **drop an abstract off at registration desk by 10:45**

Presentations?

- chaired by Christof Paar
- **5 minutes** max

Special thanks to

- Those who wrote papers
  - All the authors who submitted papers to CHES 2006
- Those who read papers
  - The program committee members
  - All the external reviewers
- The one who maintained the Web review system
  - Jens-Peter Kaps (Our dedicated webmaster)
- The CHES 2006 organizing committee
  - Tsutomu Matsumoto (General Chair and local organizer)
  - Cetin Kaya Koc (Publicity Chair)
- Our academic supporters
  - The IACR (International Association for Cryptologic Research)
  - The CHES steering committee

And to the local committee !

- Akashi Satoh (Secretary – IBM Japan Ltd.)
- Toru Akishita (Sony Corporation)
- Tetsuya Izu (Fujitsu Laboratories Ltd.)
- Masanobu Koike (Toshiba Solutions Corporation)
- Kazuto Matsuo (Institute of Information Security)
- Natsume Matsuzaki (Matsushita Electric Industrial Co., Ltd.)
- Shiho Moriai (Sony Computer Entertainment Inc.)
- Sumio Morioka (NEC Corporation)
- Hanae Nozaki (Toshiba Corporation)
- Kenji Ohkuma (IPA)
- Katsuyuki Okeya (Hitachi Ltd.)
- Shunsuke Ota (Hitachi Ltd.)
- Yasuyuki Sakai (Mitsubishi Electric Corporation)
- Junji Shikata (Yokohama National University)
- Daisuke Suzuki (Mitsubishi Electric Corporation)
- Yukiyasu Tsunoo (NEC Corporation)
- Takanari Ueno (IPA)
- Takshi Watanabe (Hitachi Ltd.)
- Atsuhiro Yamagashi (IPA)

Thanks to the financial supporters

150th Anniversary of the Opening of the Port of Yokohama

Enjoy the conference !