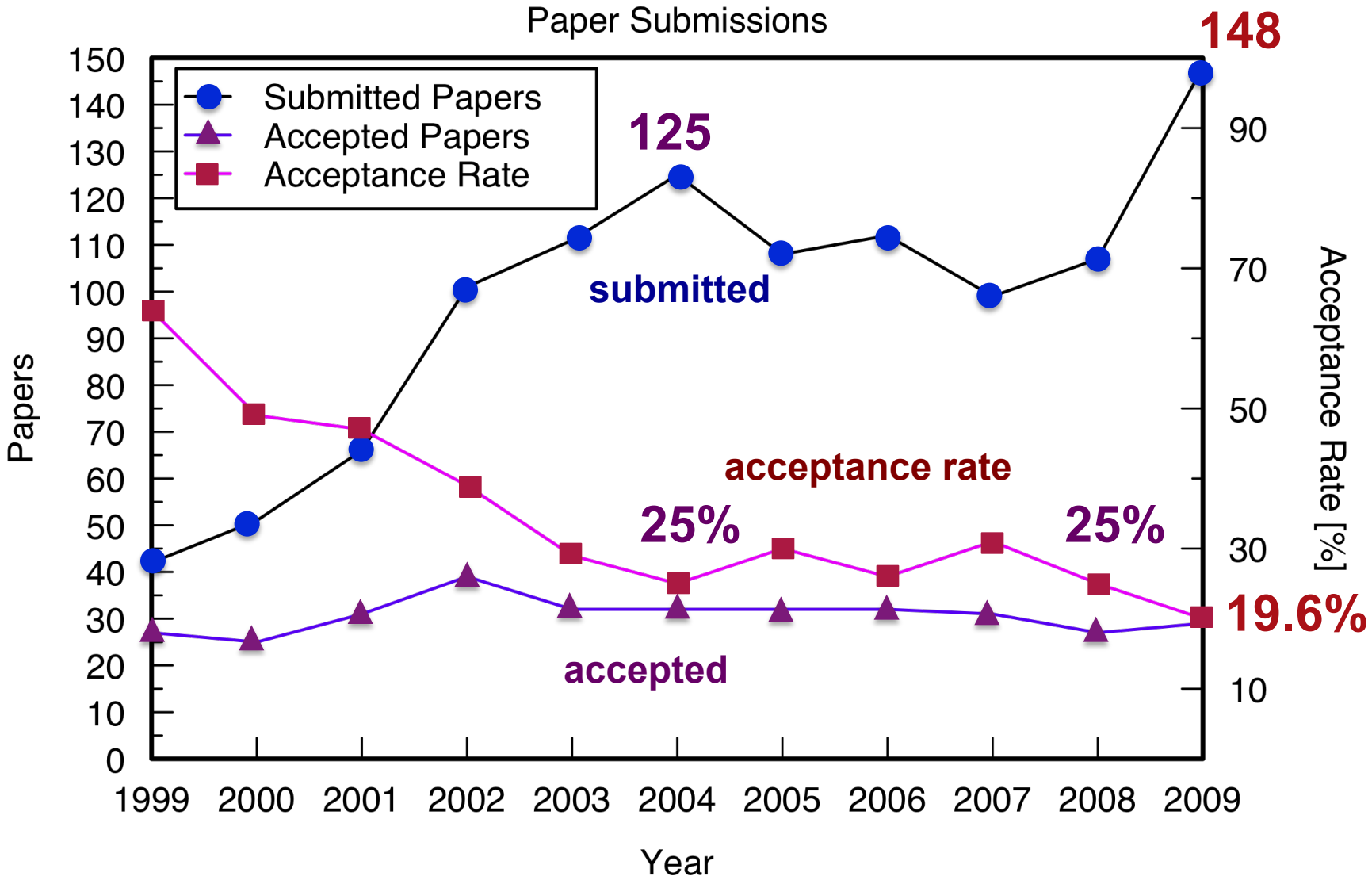
Christophe Clavier
Kris Gaj
CHES 2009 Program Co-chairs

Evolution of CHES

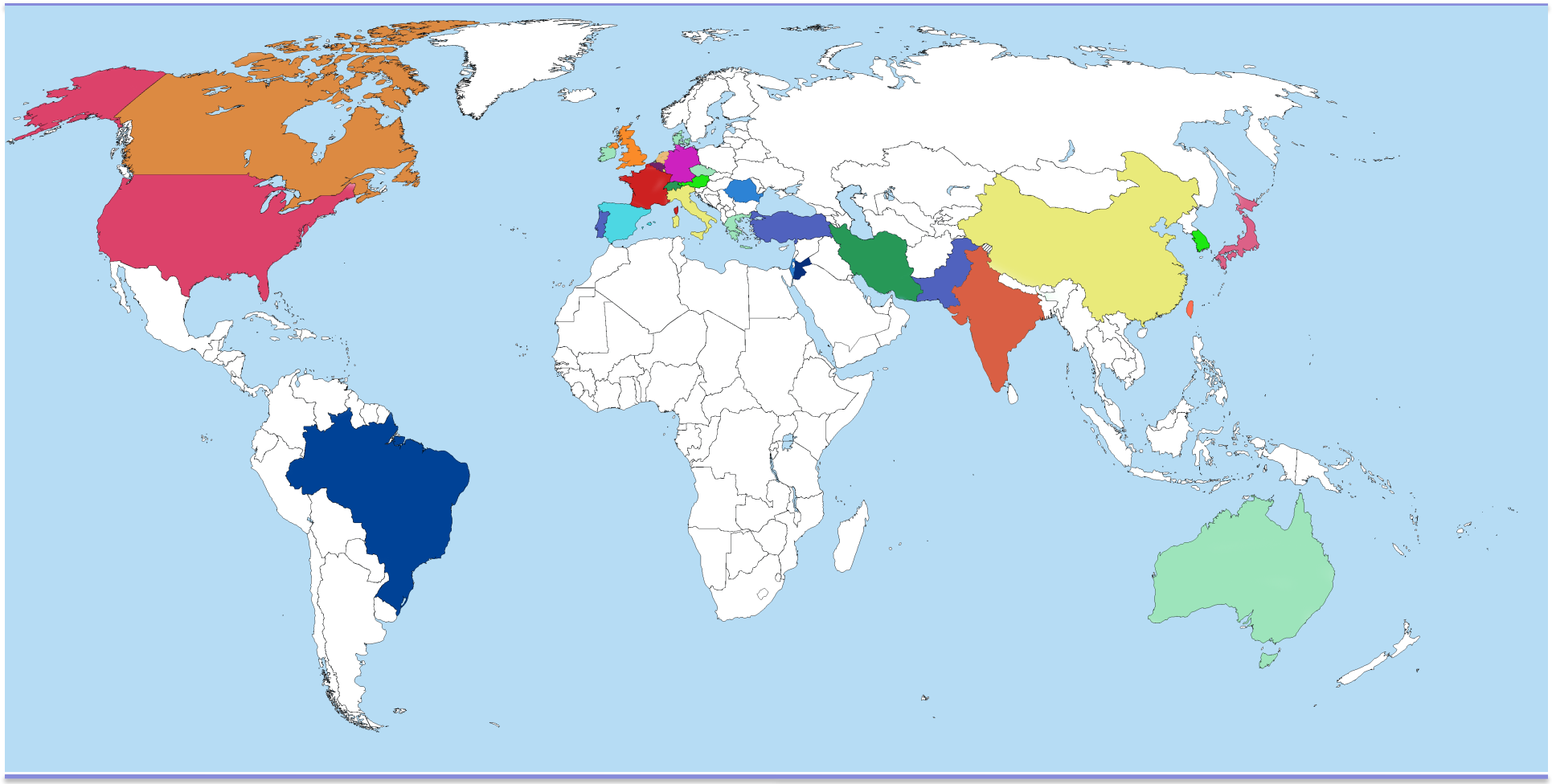
record number of submissions
smallest acceptance rate



Submissions by a Country of the Contact Author

1. USA, France – 20 each
2. Japan – 15
3. Germany – 13
4. Belgium – 12
5. Canada – 11
6. UK – 9
7. India, Netherlands – 5 each
8. China, Italy, Taiwan – 4 each
9. Austria, Korea – 3 each
10. Iran, Luxembourg, Switzerland – 2 each
11. Australia, Brazil, Czech Republic, Denmark, Greece, Ireland, Israel, Jordan, Pakistan, Portugal, Romania, Spain, Turkey – 1 each

CHES Map of the World (based on a contact author affiliation)



Submissions by Category

1. ATTACKS AGAINST IMPLEMENTATIONS AND COUNTERMEASURES AGAINST THESE ATTACKS
   - 70 submissions
2. CRYPTOGRAPHIC HARDWARE
   - 45 submissions
3. CRYPTOGRAPHIC SOFTWARE FOR EMBEDDED SYSTEMS
   - 12 submissions
4. HARDWARE TROJANS AND TRUSTED ICs – 8 submissions
5. APPLICATIONS AND IMPLEMENTATION ENVIRONMENTS
   - 6 submissions
6. OTHER - 7 submissions

Selection Process

- **148 Submissions**
  - **30 countries, 5 continents**
- **53 Program Committee Members**
  - **20 countries, 5 continents**
- **150 External Reviewers**
- **582 Reviews**
  - **On average 3.93 per paper**

Program Committee by Country

France : 10

USA : 9

Belgium, Germany, UK : 4 each

Japan, Switzerland : 3 each

Canada, Italy, Korea : 2 each

Austria, Brazil, India, Ireland, Luxembourg, Mexico, Netherlands, New Zealand, Taiwan, Turkey: 1 each

Accepted Papers by a Country of the Contact Author

1. Belgium – 8 (out of 12)
2. Germany – 4 (out of 13)
3. France, USA – 4 (out of 20)
4. Luxembourg – 2 (out of 2)
5. Japan – 2 (out of 15)
6. Czech Republic, Portugal – 1 (out of 1)
7. Taiwan – 1 (out of 4)
8. UK – 1 (out of 9)
9. Canada – 1 (out of 10)

Technical Program

- **9 Regular Sessions**
  - **3 each day, 27 regular talks**
- **3 Special Sessions**
  - Monday: **DPA Contest**
  - Tuesday: **Benchmarking of Cryptographic Hardware**
  - Wednesday: **Hot Topic Session: Hardware Trojans and Trusted ICs**
- **3 Invited Talks**
- **Poster Session & Rump Session**

Invited Talks

Monday, 10:50 - 11:50

Srini Devadas, MIT, USA
Physical Unclonable Functions and Secure Processors

Tuesday, 10:55 - 11:55

Christof Paar, Ruhr-Universität Bochum, Germany
Crypto Engineering: Some History and Some Case Studies
This talk marks 10 years after the first CHES at WPI in Worcester, Massachusetts, USA, organized by Christof Paar and Cetin Koc.

Wednesday, 10:30 - 11:30

Randy Torrance and Dick James, Chipworks Inc., Canada
The State-of-the-Art in IC Reverse Engineering

Hot Topic Session

Motivation:

Enhance the list of traditional CHES topics with one or more new "hot" topics every year, and thus also attract a new group of authors and new audience to CHES

This Year's Hot Topic:

Hardware Trojans and Trusted ICs

Special Session Chair:

Anand Raghunathan, Purdue University, USA

Session Chairs

- **Monday, Sep. 7**
  - Session 1: **Guido Bertoni**
  - Session 2: **Helena Handschuh**
  - Session 3: **Marc Joye**
  - Special Session 1: **Elisabeth Oswald**
- **Tuesday, Sep. 8**
  - Session 4: **Catherine Gebotys**
  - Session 5: **Erkay Savas**
  - Session 6: **Luca Breveglieri**
  - Special Session 2: **Patrick Schaumont**
- **Wednesday, Sep. 9**
  - Session 7: **Jorge Guajardo**
  - Hot Topic Session: **Anand Raghunathan**
  - Sessions 8 & 9: **Louis Goubin**

Best Paper Awards

Presentation of Best Paper Awards

Tuesday, 20h15 - Casino Montbenon
(just before the start of the Rump Session)

Program Committee & External Reviewers

Special Presentation of the Program Committee and all External Reviewers

Tuesday, 22h00 - Casino Montbenon (just after the end of the Rump Session)

Enjoy the Workshop!!!