



CHES 2009
September 6th – 9th

Switzerland

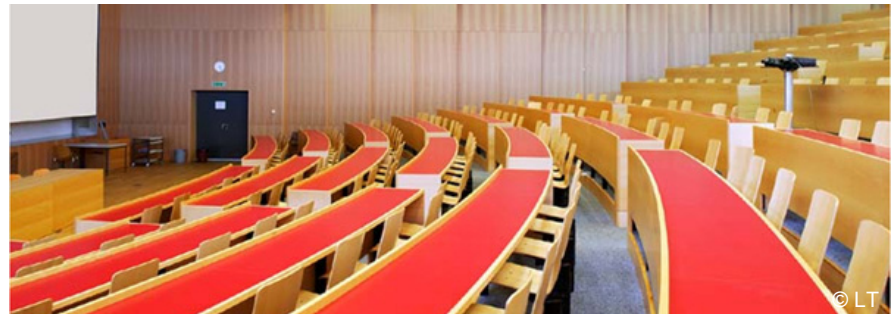






Ecole Polytechnique Fédérale de Lausanne

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE



Christophe Clavier (Program co-Chair)
Université de Limoges &
Institut d'Ingénierie Informatique de Limoges
(France)

Kris Gaj (Program co-Chair)
George Mason University (US)

Marcelo Kaihara (General Chair)
Ecole Polytechnique Fédérale de Lausanne
(Switzerland)

Çetin Kaya Koç (Publicity Chair)
University of California Santa Barbara (US)

Submission deadline: **Monday, March 16th, 2009.**

Acceptance notification: Monday, May 18th, 2009.

Final version due: Monday, June 15th, 2009.

Workshop presentations: Monday - Wednesday, September 7th - 9th, 2009.

Since its first workshop in 1999 in Worcester, Massachusetts, USA...

10th year anniversary of CHES

Gala dinner
on Lake Geneva

Rump Session in the
Casino Montbenon





Workshop on Cryptographic Hardware and Embedded Systems 2009 (CHES 2009)

Lausanne, Switzerland

Sunday September 6th - Wednesday 9th, 2009

Co-located with [6th Workshop on Fault Diagnosis and Tolerance in Cryptography](#)
- FDTC 2009, Sunday September 6th.

Preliminary Call For Papers

(in [PDF format](#))

The focus of this workshop is on all aspects of cryptographic hardware and security in embedded systems. The workshop is a forum for new results from the research community as well as from the industry. Of special interest are contributions that describe new methods for secure and efficient hardware implementations, and high-speed or leak-resistant software for embedded systems, e.g. smart cards, microprocessors, DSPs, etc. The workshop helps to bridge the gap between the cryptography research community and the application areas of cryptography. Consequently, we encourage submissions from academia, industry, and other organizations. All submitted papers will be reviewed. The topics of CHES 2009 include but are not limited to

Cryptographic Hardware

- Hardware architectures for public-key & secret-key cryptography
- Special-purpose hardware for cryptanalysis
- Cryptographic processors and co-processors
- Hardware accelerators for security protocols (security processors, network processors, etc.)
- True and pseudorandom number generators
- Physically Unclonable Functions (PUFs)



GOLD SPONSORS



SPONSORS



[CHES Home](#)

[CALL FOR SPONSORS](#)

[VENUE](#)

[Preliminary CFP](#)

[AUTHOR INSTRUCTIONS](#)

[DATES](#)

[MAILING LIST](#)

[PROGRAM COMMITTEE](#)

[CONTACT INFORMATION](#)

[HISTORY OF CHES](#)

[FORMER CHES INFO](#)

[SPONSORS](#)