Workshop on Cryptographic Hardware and Embedded Systems (CHES 2009)

Lausanne, Switzerland
September 6 – 9, 2009
www.chesworkshop.org

sponsored by IACR

Call for Submissions – Hot Topic Session – Hardware Trojans and Trusted ICs

CHES is the premier forum covering all aspects of cryptographic hardware and security in embedded systems.

CHES 2009 will include a Hot Topic Session focused on the emerging research area of "Hardware Trojans and Trusted ICs". A confluence of several trends makes this a timely and important topic. The economic challenges and cost structure of today's semiconductor industry are driving towards increased consolidation of fabrication capabilities and disaggregation of IC and system design houses from foundries. Globalization of both design and fabrication implies that the overall design and manufacturing chain for most ICs often spans across several legislative domains. From the security perspective, this gives rise to new challenges. Most systems rely on correctly designed and fabricated chips (i.e., hardware is not malicious), and consequently most security mechanisms break down when the threat comes from "within the IC". For example, Hardware Trojans could be inserted into ICs prior to manufacturing in order to leak sensitive information or interfere with correct operation (e.g., a "kill switch") once the IC is deployed in an end system. While these concerns are applicable to a broad range of ICs, they are perhaps most critical in ICs used in military systems, which have traditionally been fabricated exclusively through "trusted" foundries and designed using "trusted" components and human resources. However, the cost of maintaining dedicated fabrication channels, and the quality and design time impact of not using the best available IP, is becoming prohibitive. In summary, it is increasingly becoming necessary to ensure the trustworthiness of ICs even when parts of the design and fabrication process are inherently untrusted.

The CHES 2009 committee invites submissions for the Hot Topic session that address any relevant topic, including but not limited to the following:

- Trust / security models for IC design & fabrication
- New challenges & attacks
- Hardware Trojan detection techniques
- Test & validation of ICs fabricated in untrusted foundries
- Trusted re-use models for IP components

Important dates:

Submission:	April 20th, 2009	Final version of papers:	June 15th, 2009
Notification of acceptance:	May 18th, 2009	Presentations:	September 7th – 9th, 2009

For further information, please contact:

CHES '09 Hot Topic Chair: Prof. Anand Raghunathan, School of Electrical and Computer Engineering, Purdue University (USA). Email: raghunathan@purdue.edu

CHES '09 Program co-Chairs:

Christophe Clavier
Université de Limoges &
Institut d'Ingénierie Informatique de Limoges (France)
Email: christophe.clavier@xlim.fr

Kris Gaj
Department of ECE
George Mason University (USA)
Email: kgaj@gmu.edu

CHES '09 Hot Topic Committee (to include):

Farinaz Koushanfar – Rice University
Jim Plusquellic – University of New Mexico
Patrick Schaumont – Virginia Tech
Berk Sunar – Worcester Polytechnic Institute
Pankaj Rohatgi – IBM Watson Research Center