Journal of Cryptology
Special Issue on Hardware and Security 2009

Call for Papers

The goal of this special issue is to advance research in all areas where cryptography interacts with the physical world. With the advent of pervasive computing, a host of new devices with security needs such as smart cell-phones, RFID tags, medical implants, tiny multimedia players such as the iPod, etc. have arrived. The standard blackbox model in which the attacker is assumed to have only access to the data channels no longer applies, as the opponent will potentially own the platform. The physical implementation provides an attacker with a wealth of information related to the cryptographic implementation, as he/she may listen to and tamper with the physical aspects of the platform. Even the strongest cryptographic scheme with a rigorous security proof in the classical blackbox model may succumb to physical attacks. Specifically, there are information leakages which allows a passive attacker who captures side-channel profiles a means to deduce details of the algorithms and cryptographic keys.

At the same time, the interaction between physical realization and crypto algorithms offers new opportunities for security designers. For instance, subtle variations of the device characteristics can be exploited for key generation or identification. Physical unclonable functions (PUFs) based on manufacturing variations of delays, capacitive load, and on initial memory content are one example for a constructive use of the interaction between the physical platform and the security function. The large, and not particularly well understood, field of tamper resistance is also closely related to the physics of the platform.

Authors with other innovative ideas about relating physics and cryptography are welcome to submit their contribution. Please note that quantum cryptography is not in the scope of this special issue. The topics of the special issue include but are not limited to:

* *Passive and active side-channel attacks: Probing and glitching attacks and countermeasures, side-channel cryptanalysis, tamper-proofing and error detection in cryptographic devices and circuits.*
* *Secure Physical Identification: Identification using physical unclonabls functions (PUFs), secure RF identification.*
* *Physical Security Models: Theoretical models for physical security, techniques for enabling security models.*
* *Trusted Hardware: System and architecture level techniques for establishing trust in hardware devices.*
* *Manufacturing related problems: Hardware Trojans, intellectual property protection, prevention of reverse engineering.*

Guest Editors

All correspondence and/or questions should be directed to either of the Guest Editors:

Christof Paar
Elec. Eng. & Inf. Sciences Dept.
Ruhr-Universität Bochum
Universitätsstraße 150
Bochum, D-44780, Germany
Email: cpaar@crypto.rub.de

Jean-Jacques Quisquater
Advanced Research & Security Center
UCL Crypto Group/DICE
Université Catholique de Louvain
Place du Levant, 3
Email: jjq@dice.ucl.ac.be

Berk Sunar
Elec. and Computer Eng. Dept.
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609-2280, USA
Email: sunar@wpi.edu

Important Dates

Submission deadline:	Decisions & notifications:	Camera-ready version:
September 1st, 2009.	February 1st, 2010.	April 1st, 2010.

Instructions for Authors

Authors are invited to submit original papers. Electronic submission is strongly encouraged. A detailed description of the electronic submission procedure appears on the IACR webpages (see http://www.iacr.org/jofc/guidelines.html).