

# ACM TRANSACTIONS ON RECONFIGURABLE TECHNOLOGY AND SYSTEMS

## CALL FOR PAPERS Special Issue on Security in Reconfigurable Systems Design

The secure operation of computer systems and networks continues to be an important research topic for a variety of applications and infrastructures. Increasingly, these security concerns are extending from the software information-processing domain into the hardware domain and in particular into the reconfigurable computing research community. From a design perspective, security forms a separate dimension in design alongside of constraints on area, performance, and power. By carefully considering security issues in the design of reconfigurable hardware, security can become a basic property of the system implementation rather than being addressed as an afterthought.

This special issue of ACM Transactions on Reconfigurable Technology and Systems solicits papers in the areas of secure design technologies and architectures for reconfigurable devices and novel applications for reconfigurable platforms. Topics of interest include but are not limited to the following areas:

### Design Technologies and Architectures:

- Protection of hardware design intellectual property (e.g. FPGA bitstream).
- Side-channel resistant and fault-resistant design mechanisms.
- The use of Physically Unclonable Functions for authentication and anti-counterfeiting.
- Architectural techniques to mitigate the tradeoffs between power, performance, and area with system security.
- Methods for creating device-unique identifiers from device fabrication properties.
- Architectures that improve component isolation and resistance to physical attacks.
- Secure and formally verifiable/equivalent design automation techniques for reconfigurable hardware.

### Novel Applications:

- Improving the performance or power consumption of software implementations of security algorithms using reconfigurable hardware.
- Acceleration to increase feasibility of brute force attacks on cryptographic algorithms.
- Use of physical partitioning of subsystems to improve secure system design.
- Use of reconfigurable architecture features for resistance to physical attacks.
- Prototyping of novel trusted computing primitives.

Submissions may be based on works that were previously published in refereed conferences such as FPGA or DAC. If the submission is an expanded version of a workshop/conference paper, it should contain at least 30% new material, and the authors should state clearly how the submission differs from and/or expands on the workshop/conference paper. Please submit your paper to <http://mc.manuscriptcentral.com/trets>. Also, please write "SPECIAL ISSUE ON SECURITY IN RECONFIGURABLE SYSTEM DESIGN" on your cover page and in the notes section of the web site submission form. We expect a shorter turnaround time for this special issue.

### Important Dates

Submission Deadline: ~~May 1, 2008~~ **Extended to May 23, 2008**

Acceptance Notice: September 1, 2008

Final Manuscript Due: December 31, 2008

### Guest Editors

Patrick Schaumont  
Virginia Tech  
Blacksburg, VA  
schaum@vt.edu

Alex K. Jones  
University of Pittsburgh  
Pittsburgh, PA  
akjones@ece.pitt.edu

Steve Trimberger  
Xilinx  
San Jose, CA  
steve.trimberger@xilinx.com