

2012 45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops

(MICROW 2012)

**Vancouver, British Columbia, Canada
1-5 December 2012**



IEEE Catalog Number: CFP12MIE-PRT
ISBN: 978-1-4673-4920-8

2012 IEEE/ACM 45th International Symposium on Microarchitecture Workshops

MICROW 2012

Table of Contents

Message from HASP 2012 Organizers.....	vii
HASP 2012 Workshop Organizers.....	viii
HASP 2012 Program Committee.....	ix
HASP 2012 Reviewers.....	x
WNTC 2012 Introduction.....	xi

MICRO-45 Workshops

2012 Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2012)

From Cryptography to Hardware: Analyzing Embedded Xilinx BRAM for Cryptographic Applications	1
<i>Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger</i>	
Power Analysis of Hardware Implementations Protected with Secret Sharing	9
<i>Guido Bertoni, Joan Daemen, Nicolas Debande, Thanh-Ha Le, Michael Peeters, and Gilles Van Assche</i>	
Hardware Prefetchers Leak : A Revisit of SVF for Cache-Timing Attacks	17
<i>Sarani Bhattacharya, Chester Rebeiro, and Debdeep Mukhopadhyay</i>	
PHAP: Password based Hardware Authentication using PUFs	24
<i>Raghavan Kumar and Wayne Burleson</i>	
Wavelet Transform Based Pre-processing for Side Channel Analysis	32
<i>Nicolas Debande, Youssef Souissi, M. Abdelaziz El Aabid, Sylvain Guilley, and Jean-Luc Danger</i>	
An 8-bit AVR-Based Elliptic Curve Cryptographic RISC Processor for the Internet of Things	39
<i>Erich Wenger and Johann Großschadl</i>	
Security Verification of Hardware-enabled Attestation Protocols	47
<i>Tianwei Zhang, Jakub Szefer, and Ruby B. Lee</i>	
Continuous Remote Mobile Identity Management Using Biometric Integrated Touch-Display	55
<i>Tao Feng, Ziyi Liu, Bogdan Carbunar, Dainis Boumber, and Weidong Shi</i>	

Workshop on Near-threshold Computing (WNTC 2012)

Dynamic Acceleration of Multithreaded Program Critical Paths in Near-Threshold Systems	63
<i>Hyoun Kyu Cho and Scott Mahlke</i>	
Low-Latency Mechanisms for Near-Threshold Operation of Private Caches in Shared Memory Multicores	68
<i>Farrukh Hijaz, Qingchuan Shi, and Omer Khan</i>	
Performance and Power Solutions for Caches Using 8T SRAM Cells	74
<i>Mostafa Farahani and Amirali Baniasadi</i>	
Author Index	81