* DAC
  + 2013
    1. The Undetectable and Unprovable Hardware Trojan Horse
  + 2014
    1. Circuit Camouflage Integration for Hardware IP Protection
    2. FIGHT-Metric: Functional Identification of Gate-Level Hardware Trustworthiness
    3. Hardware Trojan Detection through Golden Chip-Free Statistical Side-Channel Fingerprinting
    4. High-Level Synthesis for Run-Time Hardware Trojan Detection and Recovery
  + 2015
    1. A Practical Circuit Fingerprinting Method Utilizing Observability Don't Care Conditions
    2. Detecting Hardware Trojans Using Backside Optical Imaging of Embedded Watermarks
    3. Detecting Malicious Modifications of Data in Third-Party Intellectual Property Cores
* DATE
  + 2014
    1. EDA Tools Trust Evaluation through Security Property Proofs
  + 2015
    1. A high efficiency Hardware Trojan detection technique based on fast SEM imaging
    2. A Score-Based Classification Method for Identifying Hardware-Trojans at Gate-Level Netlists
    3. Fault-based Attacks on the Bel-T Block Cipher Family
    4. Functional Locking Modules for Design Protection of Intellectual Property Cores
    5. Hardware Trojan Detection for Gate-level ICs Using Signal Correlation Based Clustering
    6. Hardware Trojan Detection by Delay and Electromagnetic Measurements
    7. Hardware Trojans in TRNGs
    8. Introduction to Hardware Trojan Detection Methods
    9. New Testing Procedure for Finding Insertion Sites of Stealthy Hardware Trojans
* HOST
  + 2013
    1. Cycle-Accurate Information Assurance by Proof-Carrying Based Signal Sensitivity Tracing
    2. On Hardware Trojan Design and Implementation at Register-Transfer Level
    3. Malicious Circuitry Detection Using Fast Timing Characterization via Test Points
    4. WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates
  + 2014
    1. A Chaotic Ring Oscillator based Random Number Generator
    2. Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter
    3. Countering the Effects of Silicon Aging on SRAM PUFs
    4. Entropy Loss in PUF-based Key Generation Schemes: The Repetition Code Pitfall
    5. On Design of a Highly Secure PUF based on Non-Linear Current Mirrors
    6. Power supply glitch attacks: design and evaluation of detection circuits
  + 2015
    1. Evaluating the Security of Logic Encryption Algorithms
    2. Hacking and Protecting IC Hardware
    3. Toward Automatic Proof Generation for Information Flow Policies in Third-Party Hardware IP
    4. GDS-II Trojan Detection using Multiple Supply Pad VDD and GND IDDQs in ASIC Functional Units
  + 2016
    1. A New Approach for Rowhammer Attacks
    2. Robust Privacy-Preserving Fingerprint Authentication
* IC CAD
  + 2012
    1. Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC
    2. Provably Complete Hardware Trojan Detection Using Test Point Insertion
  + 2013
    1. A Primer on Hardware Security: Models, Methods, and Metrics
    2. A Proof-Carrying Based Framework for Trusted Microprocessor IP
    3. A Write-Time Based Memristive PUF for Hardware Security Applications
  + 2014
    1. Hardware Obfuscation using PUF-based Logic
    2. On Trojan Side Channel Design and Identification
    3. Protecting Integrated Circuits from Piracy with Test-aware Logic Locking
  + 2015
    1. A Flexible Architecture for Systematic Implementation of SoC Security Policies
    2. BoardPUF: Physical Unclonable Functions for Printed Circuit Board Authentication
    3. ConFirm: Detecting Firmware Modifications in Embedded Systems using Hardware Performance Counters
    4. Detecting Hardware Trojans in Unspecified Functionality Using Mutation Testing
    5. PUF-Based Authentication
    6. Quantifying Timing-Based Information Flow in Cryptographic Hardware
    7. RRAM Based Lightweight User Authentication
    8. Security Policy Enforcement in Modern SoC Designs