Hardware Trojans
Detect and React?

A. Dabrowski, P. Fejes, J. Ullrich, K. Krombholz, H. Hobel, E. Weippl

Future Work
- Enhancement of the development process to mitigate the threat of Hardware Trojans
- Provision of the Trojan kit to the scientific community

Methodology: Malware Structures
- An analysis on HDL/RTL as well as netlist level showed that the following characteristic structures are of interest for Hardware Trojan detection:
  - Asynchronous latches
    - unlocked, self-clocked or externally clocked flip-flops
  - Gated wire or output signals
    - signal which is influenced by means of a gate
  - Ring oscillator
    - combinational loop without constant frequency
  - Unused pins or bond wires
    - convient for covert channel dissemination
  - Additional states
    - dependent on the encoding scheme
  - Gated reset signal
    - resets, which are independent from the global reset
  - Local or gated clocks
    - clocks, which are independent from the global clock

Methodology: Hardware Trojan Kit
- The kit is assembled in a modular way and it bases on four characteristics: activation, covert communication, payload and detection.