Problem
- Embedded System market has risen to a multi billion dollar business ⇒ Embedded Systems became a lucrative target for product piracy and intellectual property (IP) theft
- Detecting IP theft in hardware designs is difficult – expensive reverse-engineering needed
- Detecting software theft in embedded microcontrollers is also very difficult – memory read protection prevents reading out program code

Solution:
- Insert a unique and hidden signal into the power consumption of the device ⇒ Easy and cheap detection of IP theft

Side-channel based hardware watermarks

Insert watermark

Original IP block

Watermark

Detect watermark
- Measure the power consumption of the device under test
- The watermark signal is buried in the noise of the power trace
- Use the watermark secret and statistics to recover the hidden watermark signal

Result
- The watermarks can be inserted at the HDL or netlist level but can be detected after manufacturing!
- Watermark hidden in the power consumption – attacker does not know if watermark is present or not
- The side-channel based watermark can be very small and very robust

Side-channel based software watermarks for embedded devices

Insert watermark

Original code

Watermark

Detect watermark
- Measure the power consumption of the suspected device
- Perform statistical analysis of the measured power traces (same technique as side-channel attacks)
- Positive and negative correlation peaks reveal the watermark hidden in the power consumption

Result
- No access to program or data memory needed to detect watermark!
⇒ Memory read protection of microcontrollers no problem any more!
- Watermark consists of only a few assembler instructions
⇒ Very low watermark overhead
- Watermark is hidden in the noise
⇒ Very robust to attacks and code transformations

Acknowledgments: I would like to thank my co-authors Markus Kasper, Amir Moradi and Daehyun Strobel. This project is funded by the National Science Foundation under grant #0916854 and #0923313.