IP Core Protection using Voltage-Controlled Side-Channel Receivers

Peter Samarin[1,2], Kerstin Lemke-Rust[1], and Christof Paar[2]

Bonn-Rhein-Sieg University of Applied Sciences[1]
Ruhr-Universität Bochum[2]
Germany

Bonn-Rhein-Sieg
University of Applied Sciences

RUHR
UNIVERSITÄT
BOCHUM

RUB

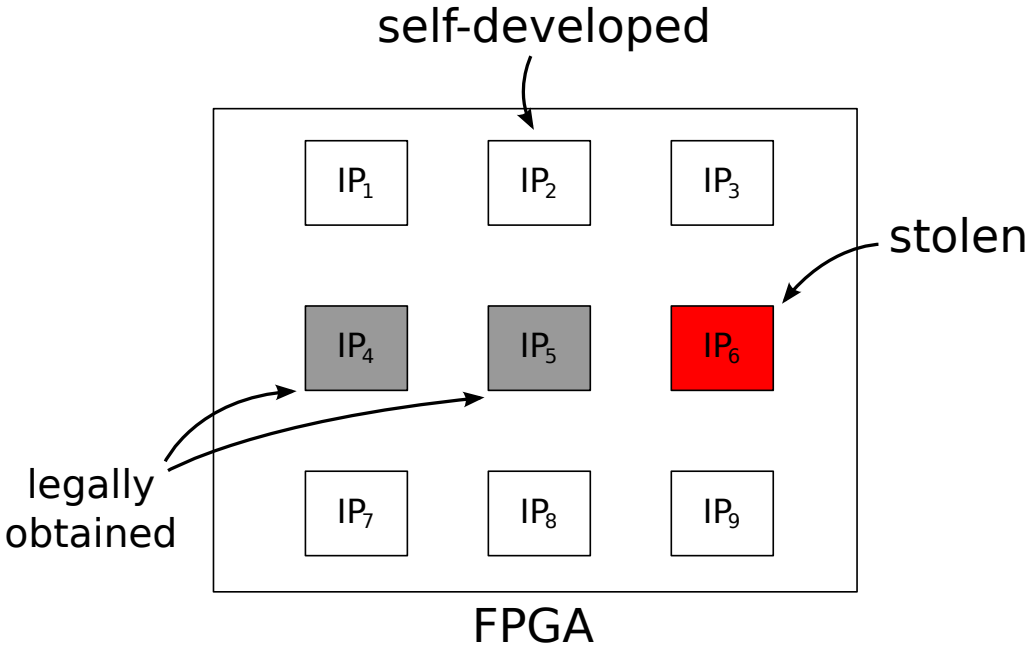
IP Protection on FPGAs

```
(cell yyy (cellType generic)
      (view schematic_ (viewType netlist)
        (interface
          (port CLEAR (direction INPUT))
          (port CLOCK (direction INPUT)) ... )
        (contents
           (instance I_36_1 (viewRef view1 (cellRef dff_4)))
           (instance (rename I_36_3 "I$3") (viewRef view1 (cellRef addsub_4)))
           ...
           (net CLEAR
             (joined
               (portRef CLEAR)
                 (portRef aset (instanceRef I_36_1))
                 (portRef aset (instanceRef I_36_3))))
```

Netlist

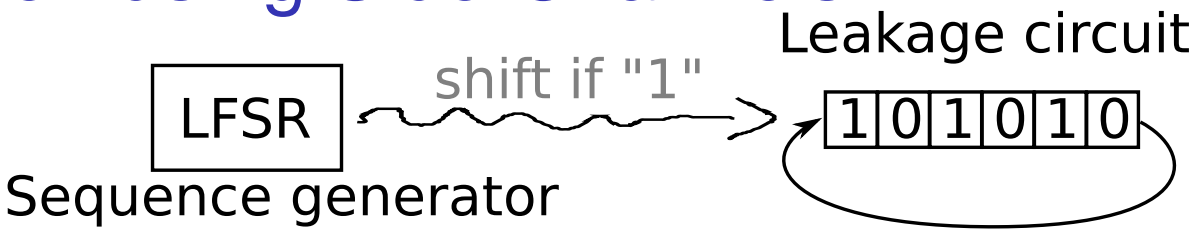
```
01010100100101010111011101000101110101000010011010100100011011111
01010100101010010001010010010101001001010101111011100010111010010
00010011010100100011011111010101001010100100010100100101010010010 1
01011110111010001011101010000100110101001000110111110101010010101 0
01000101001001010100100101010111101110100010111010100001001101010 0
10001101111101010100101010010001010010010101001001010101111011110 10
00101110101000001001101010010001101111101010100101010010001010010 01
01010010010101011110111010001011101010000100110101001000110111110 1
01010010101001000101001001010100100101010111101110100010111010100 0
01001101010010001101111101010100101010010001010010010101001001010 01
01011110111010001011101010000100110101001000110111110101010010101 0
00010100100101010010010101011110111010001010011010010100100101010 10
00110111110101010010101001000101001001010100100101010111101110100 0
10111010100001001101010010001101111101010100101010010001010010010 1
01001001010110111101110100010111010100001001101010010001101111101 01
01001010100100010100100101010010010101011110111010001011101010000 1
00110101001000110111110101010010101001000101001 0
```

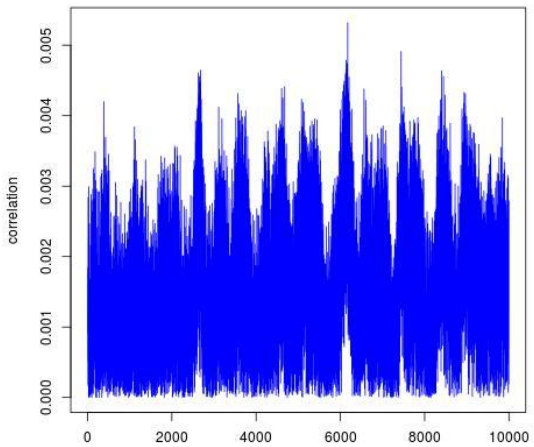
Bitstream



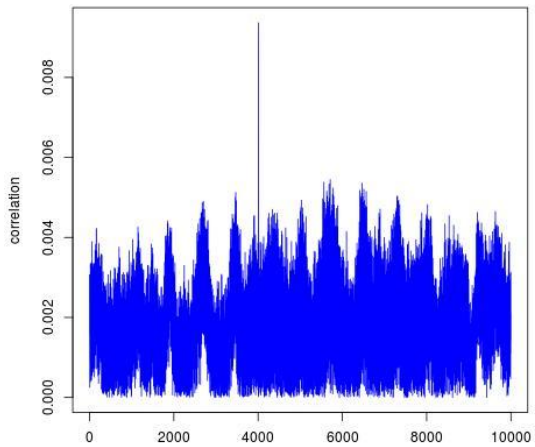
- How to detect illegally used cores *in the field*?
- Challenges
  - Bitstreams are encrypted
  - IP cores are parts of larger systems

IP Protection using Side-Channels

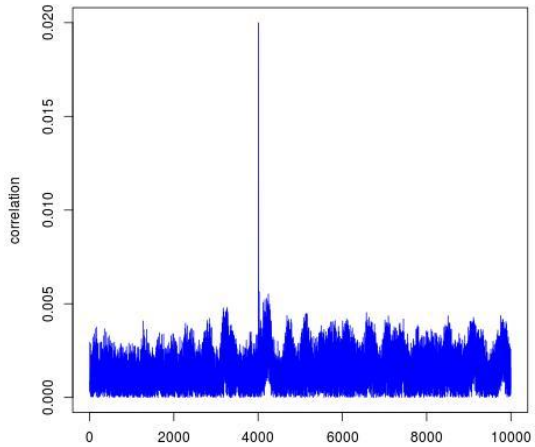




Width: 16



Width: 32



Width: 64

Verification

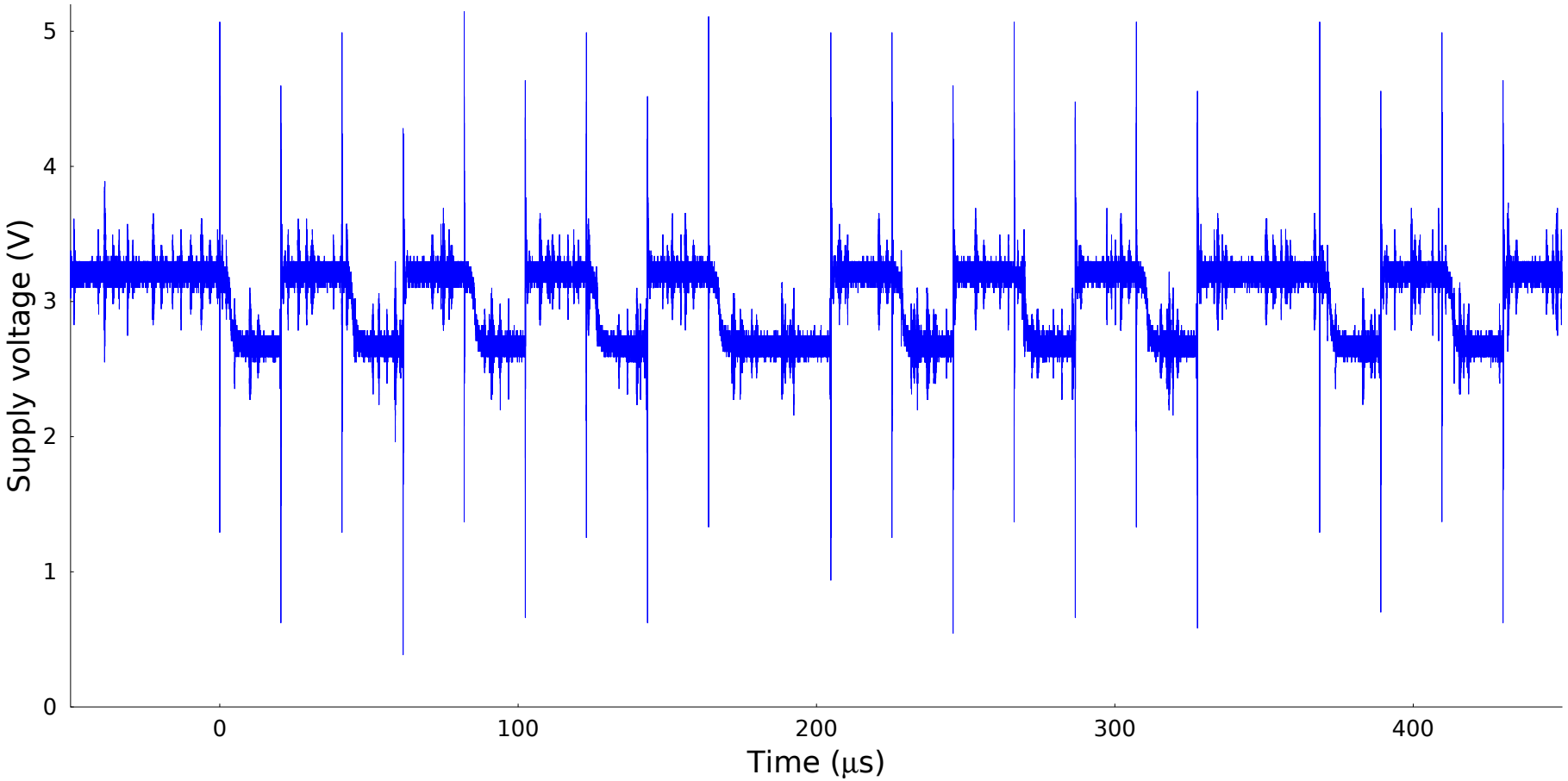
- Measure the power consumption
- Correlate the known LFSR sequence to the measurement

(Becker et al., 2010)

May 4, 2016

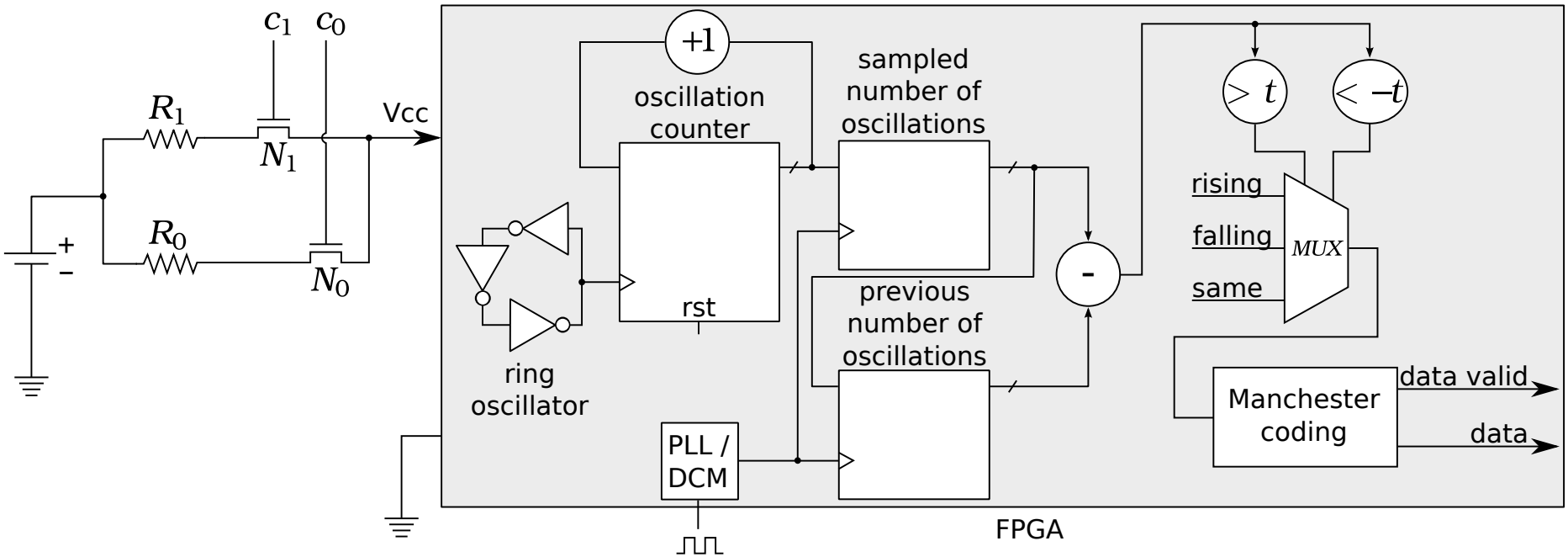
Our Contribution

- Establish an input side channel to individual IP Cores using voltage modulation
- (Sun et al., 2011) used temperature (several bits/s)



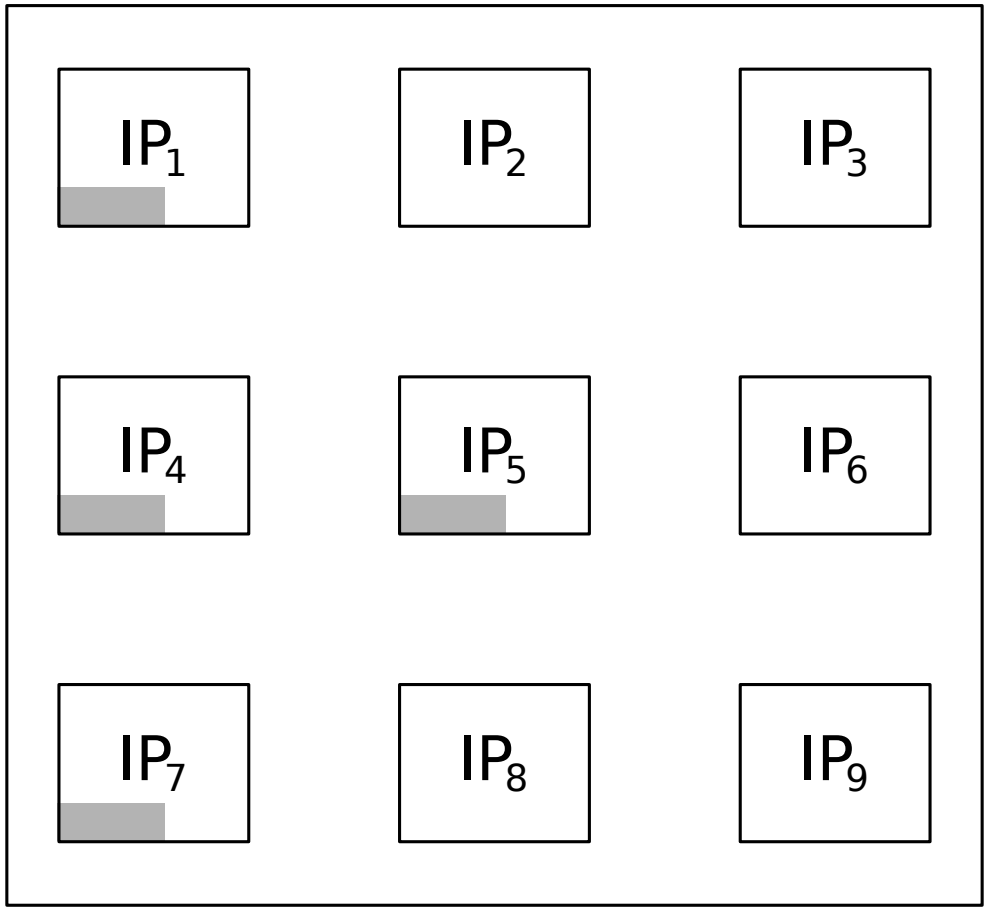
May 4, 2016

Voltage-Based Side-Channel Receivers



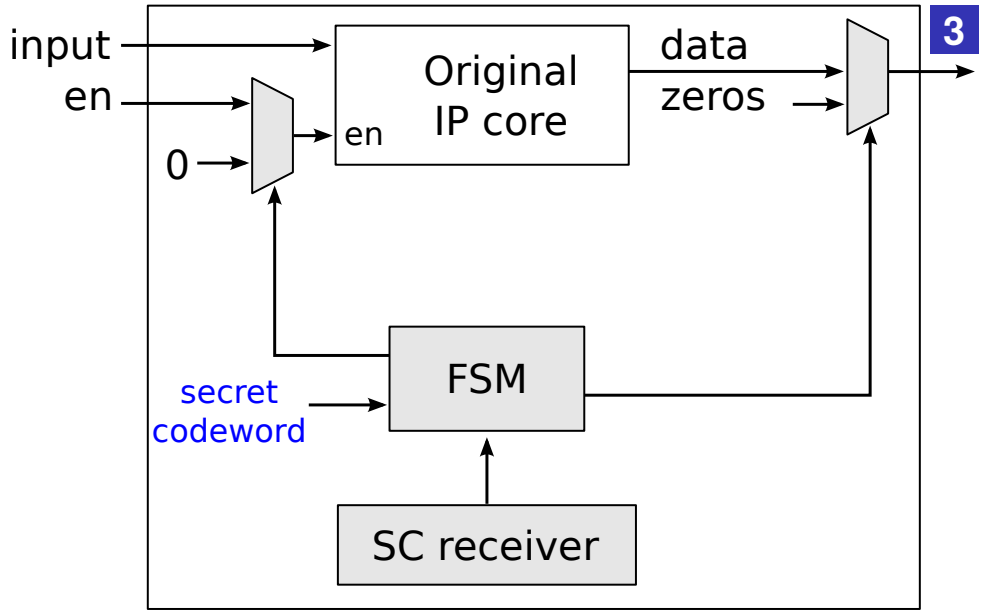
1. Supply voltage control
   - 3 Voltage levels: V_{reset}, V_0, V_1 (V_2 is not used)
2. Detection of changes in supply voltage
   - Ring oscillator sampled by a fixed clock
   - Relative threshold to find rising and falling edges
   - Manchester coding

IP Protection

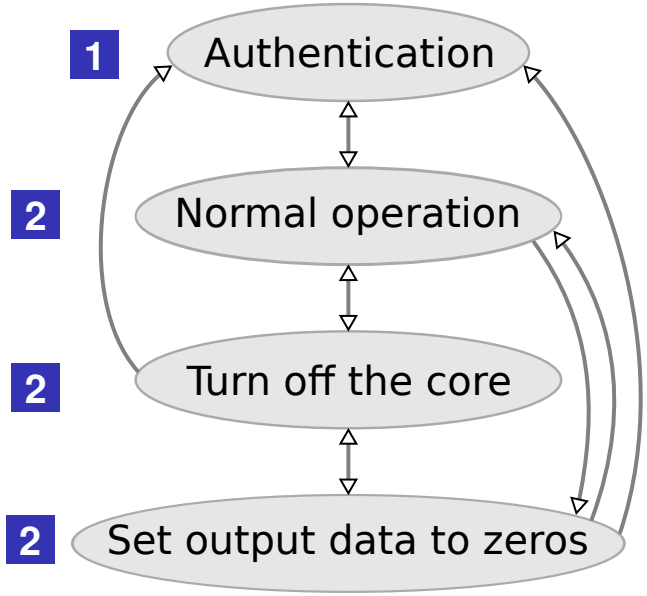


- Embed an SC-receiver into each protected IP core
- Send commands to protected IP cores

Verification



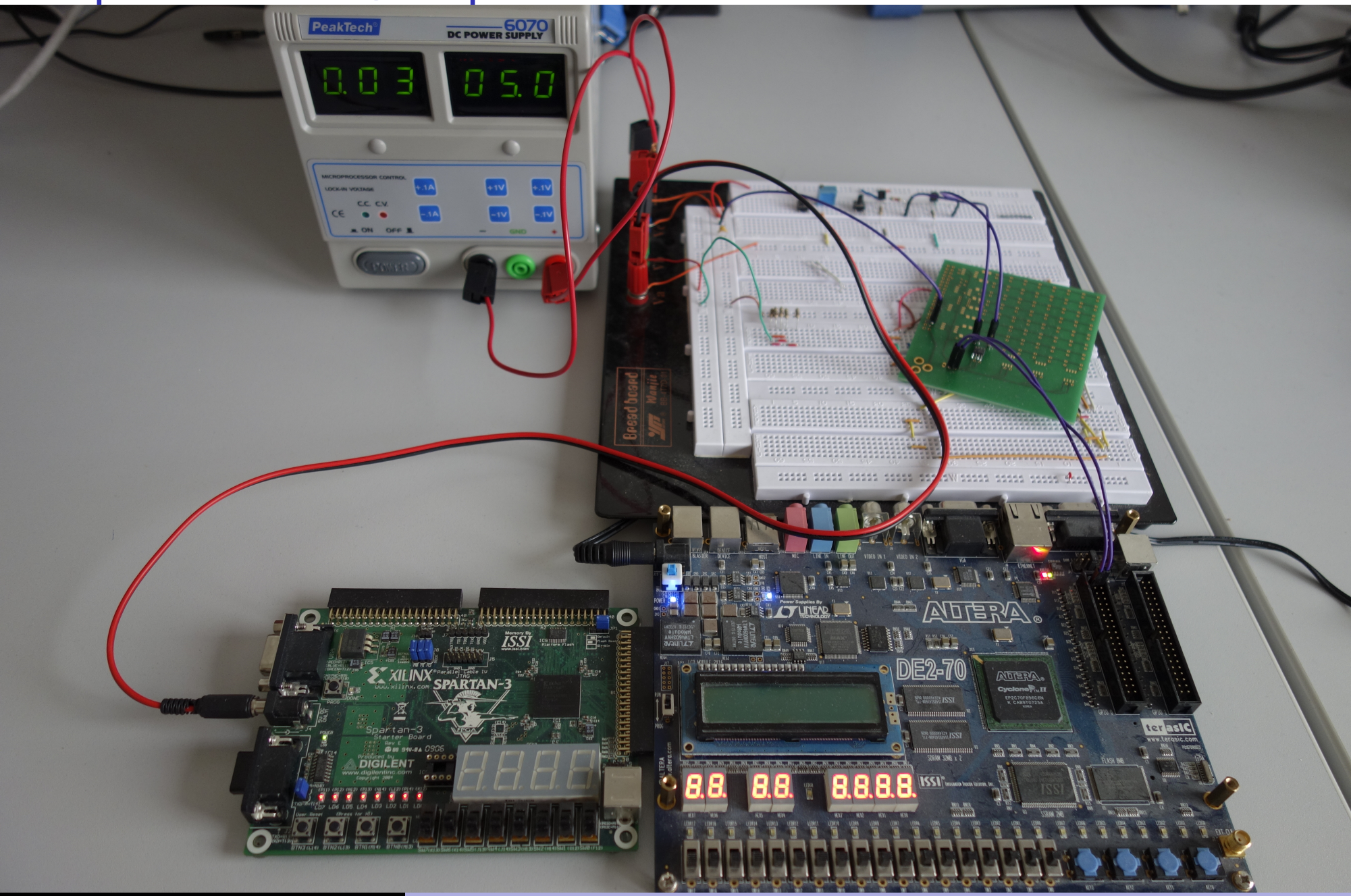
Protected IP core



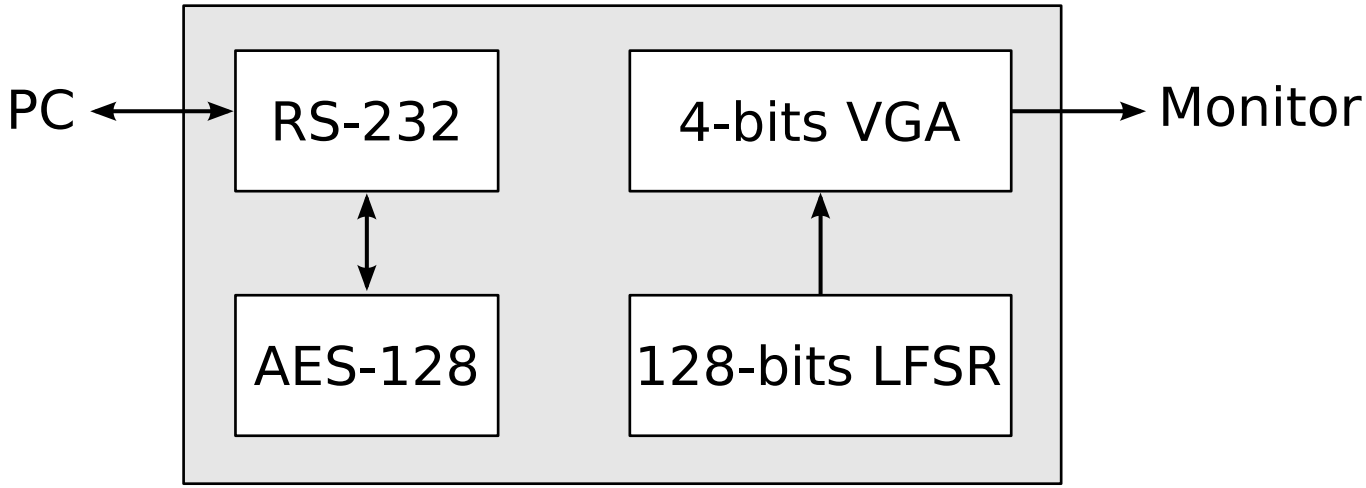
FSM

1. Send a core-dependent secret codeword
2. Send commands, observe the behavior of the chip:
   - Turn off the core
   - Set output data to zeros
   - Return to normal operation
   - Deselect core
3. If the behavior is unusual then stop, else goto step 2

Experimental Setup



A Proof-of-Concept Implementation



- Digilent board with a Spartan 3 (XC3S200) FPGA[1]
- 50MHz external clock
- Voltage control by a breadboard circuit
- Voltage levels V_{reset} = 0V, V_0 = 2.8V, V_1 = 3.2V
- Transmission rate 2.4 KBits/s
- 32-Bit codewords

[1] http://store.digilentinc.com/spartan-3-board-retired/

The Price to Pay

Codeword size (bits)	N. of slices
32	49
64	70
80	81
128	111

- Need to try several codewords (in the worst case all)
- Cannot measure once and try them all just on the data
- Cores without clock cannot be protected

- More recent work on SASEBO-GII board[2]
  - Spartan 3 FPGA for control
  - Virtex 5 (XC5VLX50) FPGA for measurements
  - *Same breadboard circuit didn't work* (voltage regulator)

[2] http://satoh.cs.uec.ac.jp/SASEBO/en/board/sasebo-g2.html

May 4, 2016

Summary and Future Work

- Voltage-controlled side-channel receiver on FPGAs
  - IP protection of individual cores
  - Strong proof of IP ownership
- Other applications
  - Hardware trojans triggered by a codeword
  - Protection against counterfeits
- Future work
  - Testing other FPGAs and boards
  - Adressing voltage regulators
  - Two-way side-channel communication

References

Becker, G., Kasper, M., Moradi, A., and Paar, C. (2010). Side-channel based watermarks for integrated circuits. In *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, pages 30–35.

Sun, J., Bittner, R., and Eguro, K. (2011). FPGA side-channel receivers. In *Proceedings of the 19th ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, FPGA '11, pages 267–276, New York, NY, USA. ACM.