innovations
for high
performance
microelectronics

Combinatorial logic circuitry as means to protect low cost devices against side channel attacks

Vater, Frank

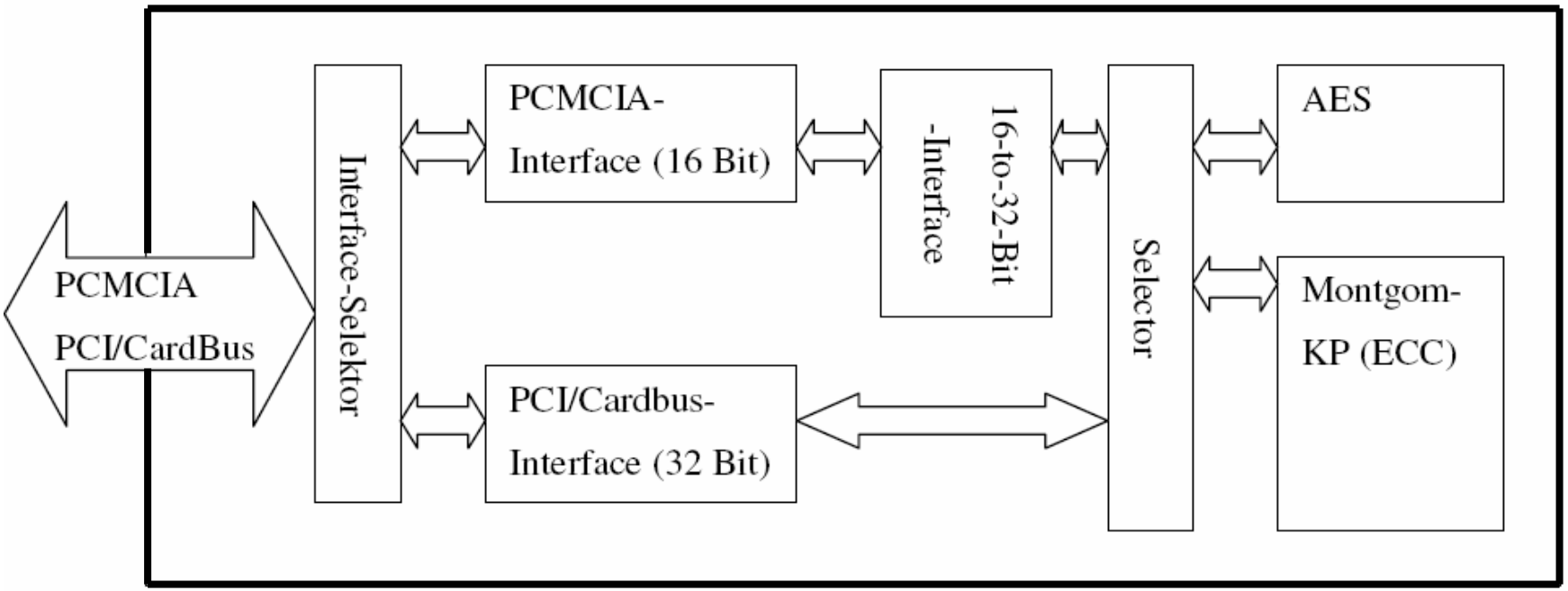
IHP
Im Technologiepark 25
15236 Frankfurt (Oder)
Germany

Overview

- **Dual²-Crypto-Chip**
- **Sucessful side channel attack on AES**
- **Clock Watchdog**
- **Open Problem**
- **Conclusion**

Dual²-Crypto-Chip

- **Dual²-Crypto-Chip:**
  - → **Two interfaces**
  - → **Two crypto cores**
- **Elliptic Curve Cryptographie (ECC) for asymmetric cipher**
- **Advanced Encryption Standard (AES) for symmetric cipher**



Dual²-Crypto-Chip

Side Channel Attack

- **Get informations about internal secrets without destroying**
  Most helpful information: secret key

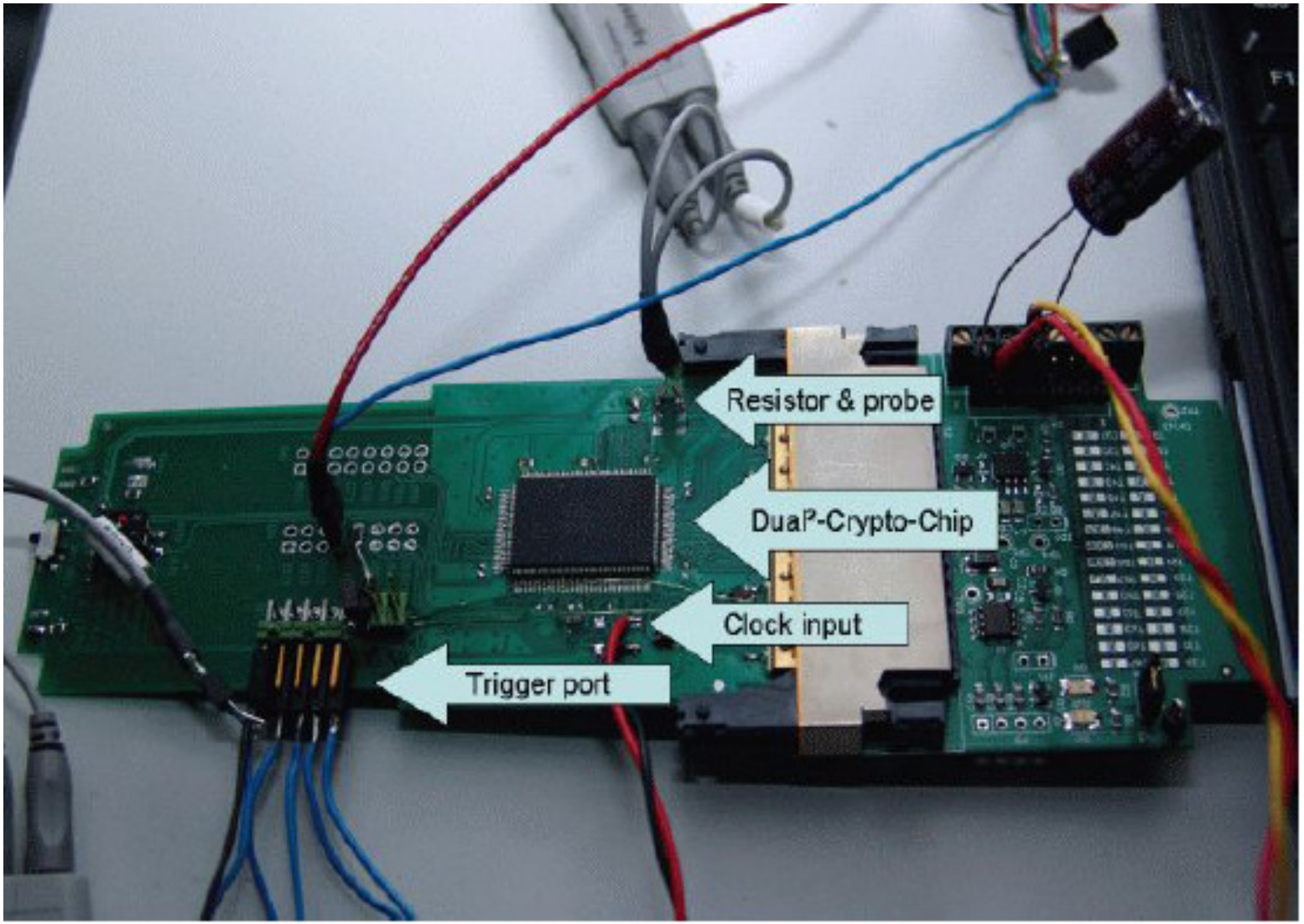
- **Timing analysis**
  Data depending calculation time

- **Power analysis**
  Data depending power consumption

Attacked AES

- White box analysis
  - ⇒ Attacker know implementations details
- Measurement equipment
  - ⇒ High resolution oscilloscope (20GSa) ~ 20 k€
- Time for measurement
  - ⇒ ~ 200,000 single measurements
  - ⇒ ~ 19h full measurement
- Found key bits:
  - ⇒ 121 of 128 bit @ 10 MHz
  - ⇒ 112 of 128 bit @ 50 MHz
- Time for searching last key bits (special hardware)
  - ⇒ 7 bits: ~ 120h
  - ⇒ 16 bits:~ 5.1×10^{11}h
  - ⇒ 6 bits: ~5h

Measurement setup

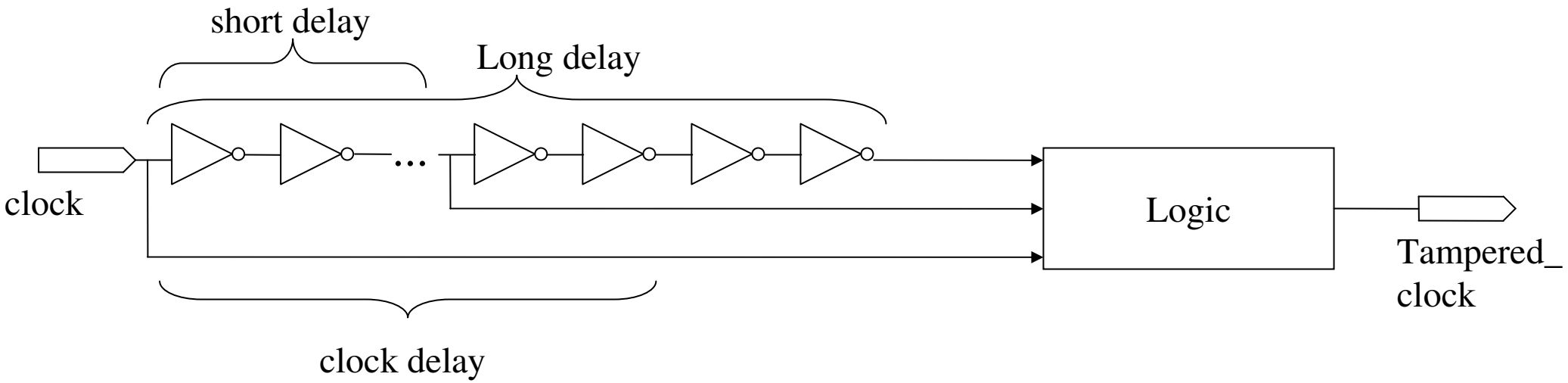


Requirements

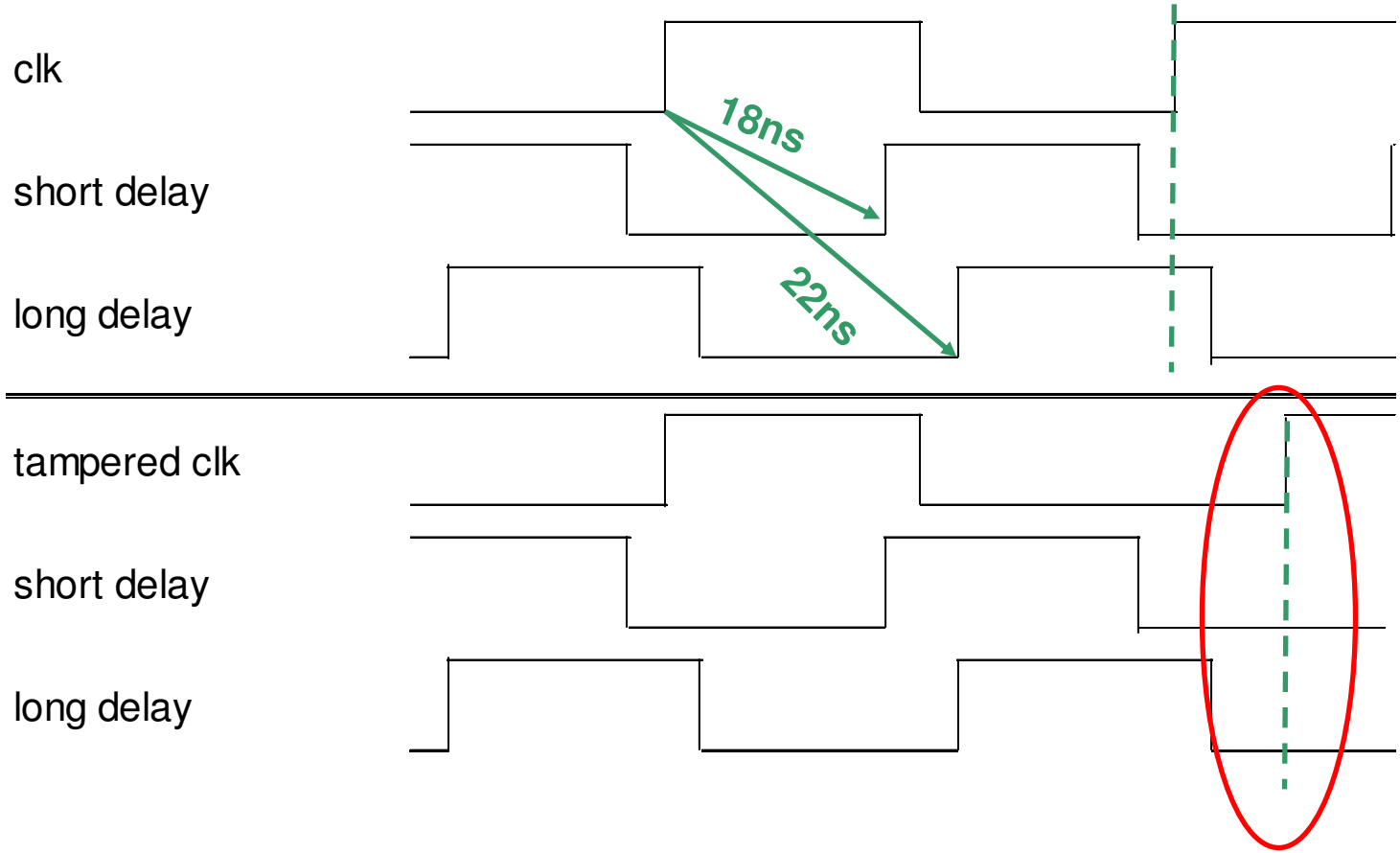
- **Requirements:**
  - **Detecting of a too slow clock „on the fly“**
  - **Low cost: Small area**
    No analog parts

Schematic of Clock Watchdog

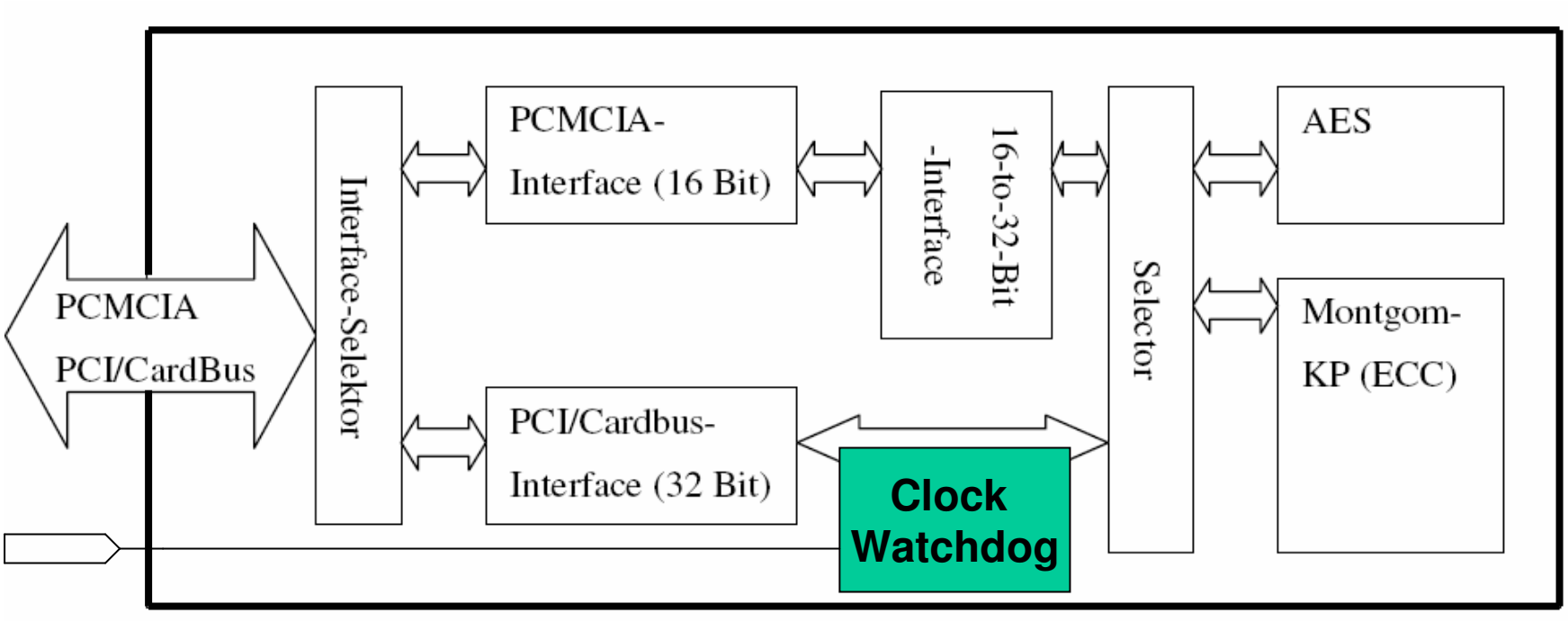
- **Solution:**
  - Using the known delay of digital components
  - Building up an delay element – delay time: ~ clk_period / 2
  - Comparing delay with incoming clock
  - Enabling signal, if clock is tampered



Simulation



Integration



Dual²-Crypto-Chip

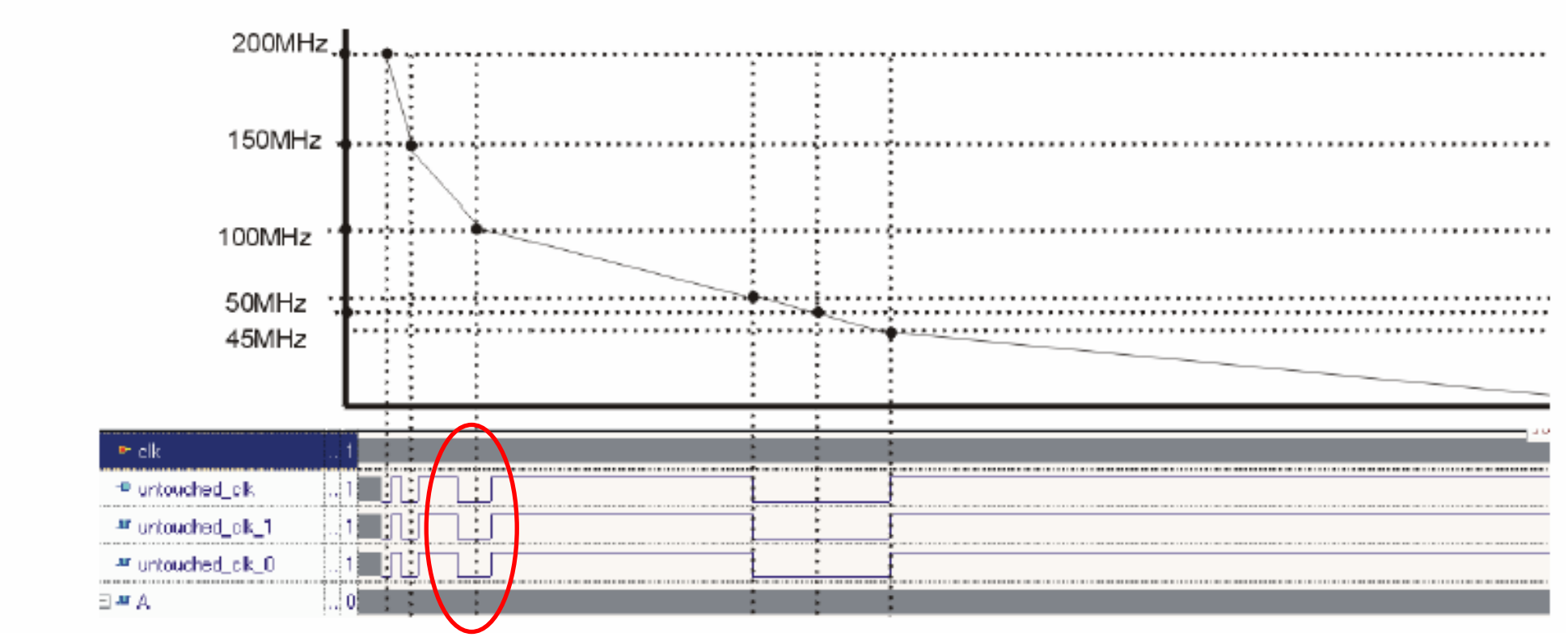
Properties

- **Clock Watchdog 45 – 55 MHz in 0.25µm CMOS**
- **Easy to implement**
- **Area:**
  - **Delay chain (240 inverter): 3,800 µm²**
  - **Analyze logic: 380 µm²**
- **Designer task:**
  - **Responding to event:**
    - **Stop crypto core**
    - **zeroisation**
    - **self destroying**

Problems

- **Influence of voltage and temperature**
- **Detecting of too fast clock not reliable:**

  Multiplies of allowed freqency are „correct“



Conclusion & Future work

- **Especially detecting of too slow clock**
- **small area => low cost:**
  4,200µm² <-> AES core 430.000 µm²
- **No analog parts => low cost**
- **Fast detecting of too slow clock**
- **Future work:**
  Development of temperature or voltage detection bases on the digital components
  Too fast clock detection

Questions?

- **Thank you for your attention**