FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Low-Cost CMOS Power Consumption Data Dependency Demonstrator Concept

Jan Bělohoubek[1], Robert Vik[2]

[1]jan.belohoubek@fit.cvut.cz, [2]rvik@ket.zcu.cz

[1]Czech Technical University in Prague, Czech Republic
[2]University of West Bohemia in Pilsen, Czech Republic

The 7th Prague Embedded Systems Workshop 2019,
Roztoky u Prahy, Czech republic

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

RESEARCH
CENTER FOR
INFORMATICS
rci.cvut.cz

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Motivation – Novel Vulnerabilities Originating in the Modulated Static Power

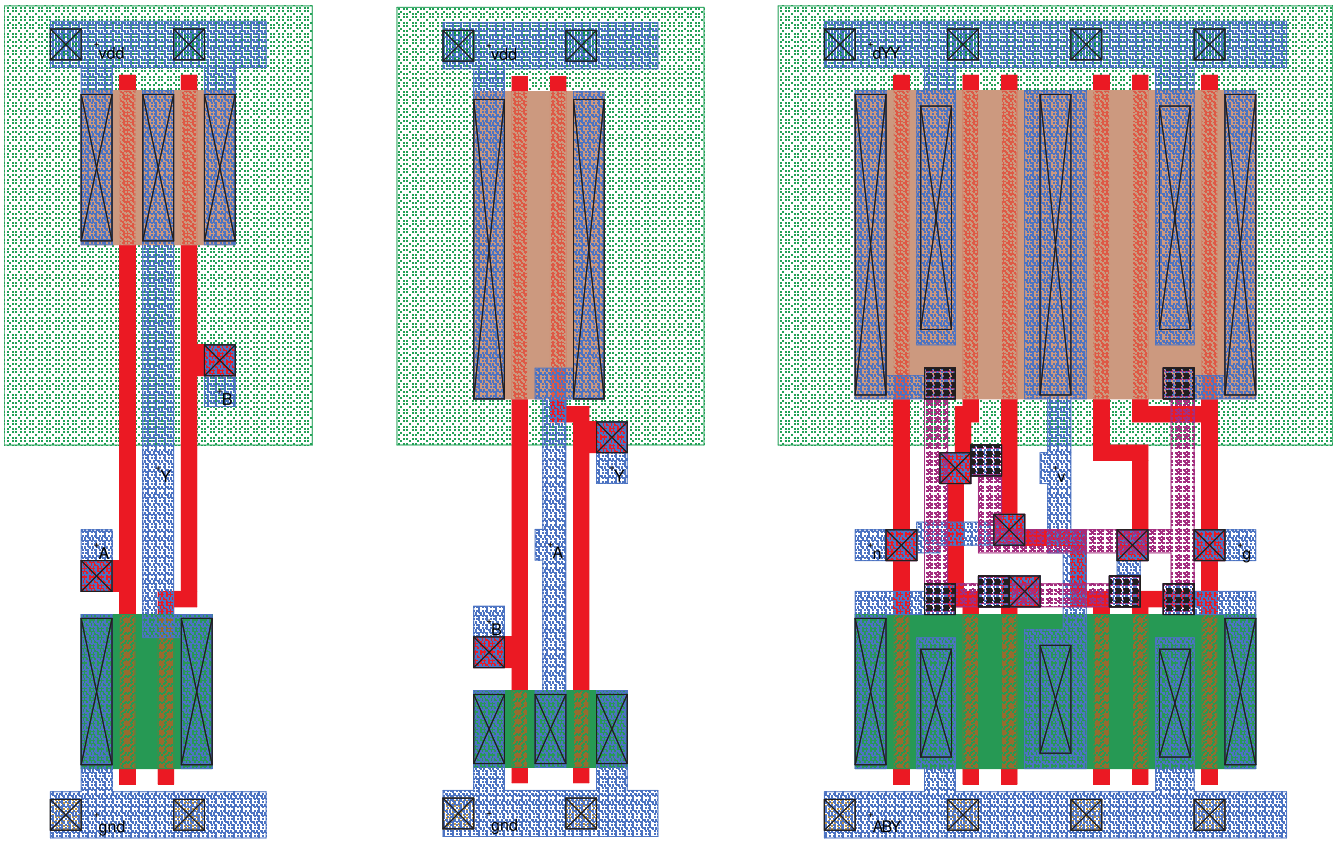
We analyze the data dependency of the photocurrent induced by a laser beam in the illuminated CMOS device:

- → it's like *amplified static power*
- → lasers are often used to induce faults into registers
- → we analyze static current of **combinational circuits** modulated by illumination (a laser beam)

Pros and Cons:

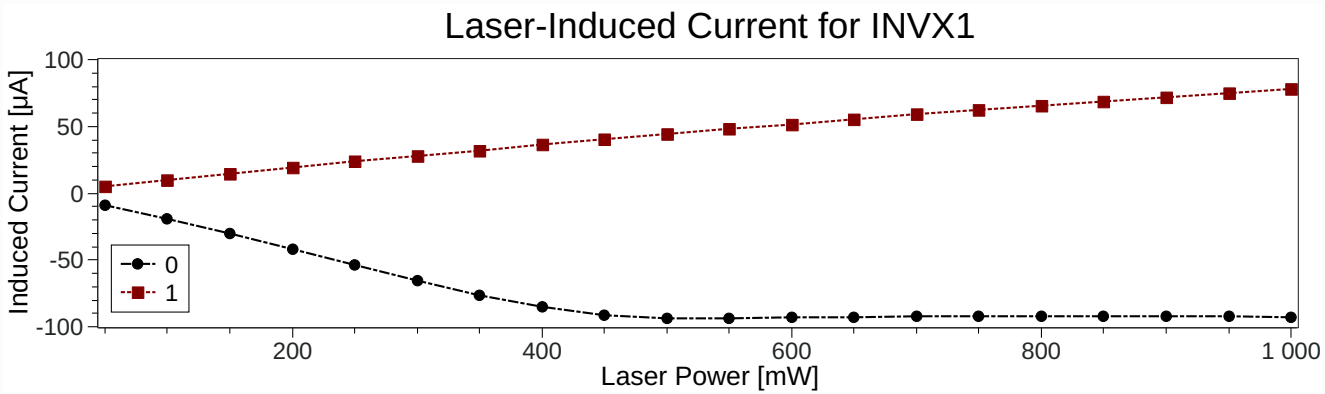
- \+ combinational logic provides **sufficient area** (to target laser beam) even in recent technology nodes
- \+ stored **values remain unaltered**
  - → error detection may not be raised
  - → measurement time may be prolonged
- – advisory values are *mixed together* → **the cocktail effect**
- – possible **attack requirements are strong** – known layout, precise laser beam localization

Data Dependence in CMOS
Conductivity is Influenced by Geometry



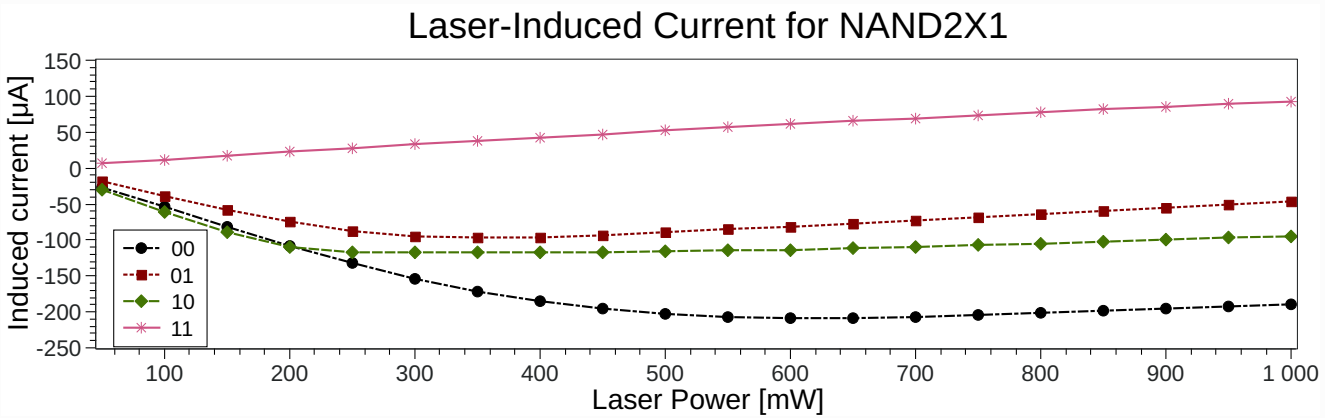
Layout of `NAND2X1` (4 x 10.8 μm), `NOR2X1` (4 x 10.8 μm) and `XOR2X1` (7.2 x 10.8 μm) cells in 180nm TSMC technology

Standard Cell Illumination
INVX1 @ TSMC 180nm (SPICE)



The photocurrent for `INVX1` for different input patters and increasing laser power. The 0 and 1 input patterns are easy to distinguish

Standard Cell Illumination
NAND2X1 @ TSMC 180nm (SPICE)



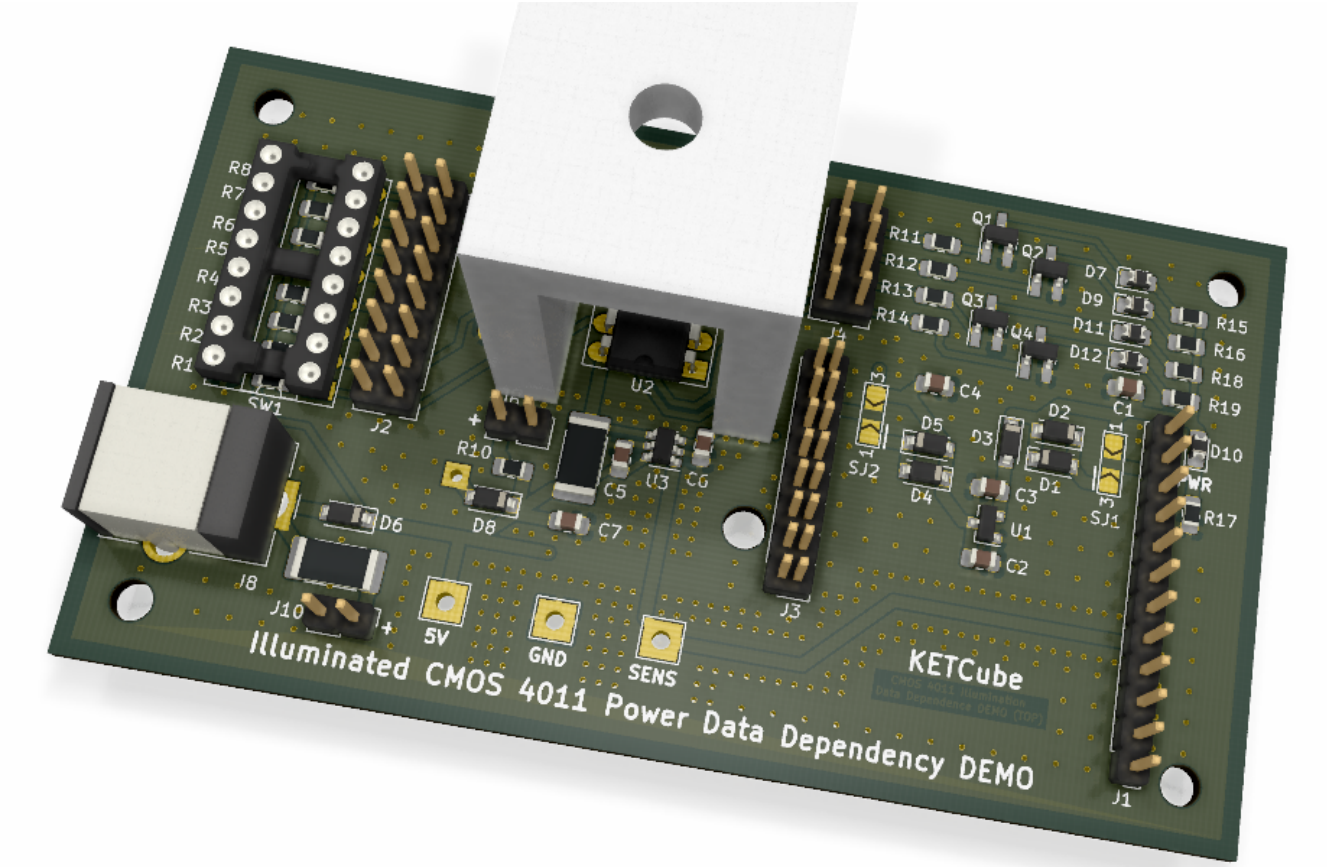
The photocurrent for `NAND2X1` for different input patters and increasing laser power. The 00 and 11 input patterns are easy to distinguish; patterns 01 and 10 cause similar currents, although the 20μA difference (for 100mW and above) is still distinguishable

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Data Dependency Demonstrator Concept
Low Cost CMOS 4011 Based Demonstrator

- Employs **CMOS 4011** by Texas Instruments
  - Low cost, well known CMOS circuit in PDIP (Plastic Dual-In-Line Package)
  - Datasheet contains design details including metal layer geometry
  - Illuminated by power diode
- Highly Configurable
  - Battery-Powered samples
  - MicroAmps are expressed as millivolts (SENS pin)
  - Measurement by MCU or by multimeter (accuracy of tens of millivolts)
- Measurements
  - Static/Leakage Power
  - Static power data dependency

Data Dependency Demonstrator Concept
Low Cost Demonstrator Visualization



FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

CMOS 4011 Decapsulation
Traditional Chemical Process

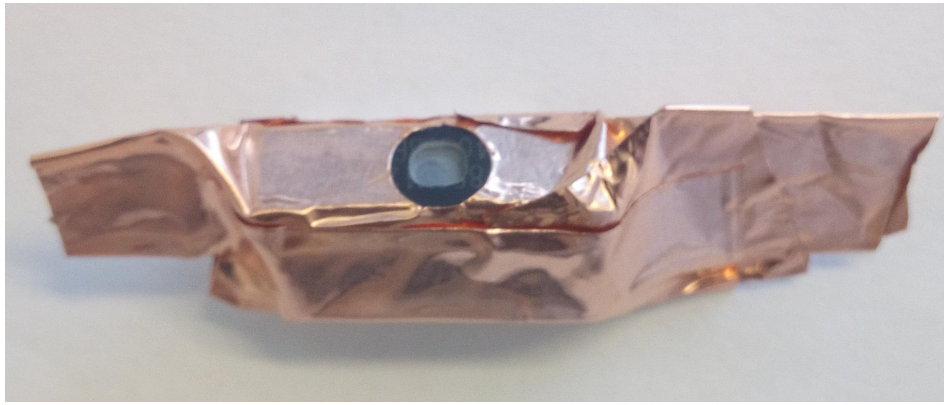
- Fuming HNO_3 is used (above 86%)
- Cu bonding was dissolved, DIE remains OK
- After bonding recovery (bonding machine), the circuit was operational

But:

- Bonding recovery takes too much time

CMOS 4011 Decapsulation
Electro-Chemical Process – Prerequisites

- Concentrated H_2SO_4 (1 part) + red fuming HNO_3 (3 parts)
- Device was milled above DIE to speed-up decapsulation
- Device was covered using conductive copper tape



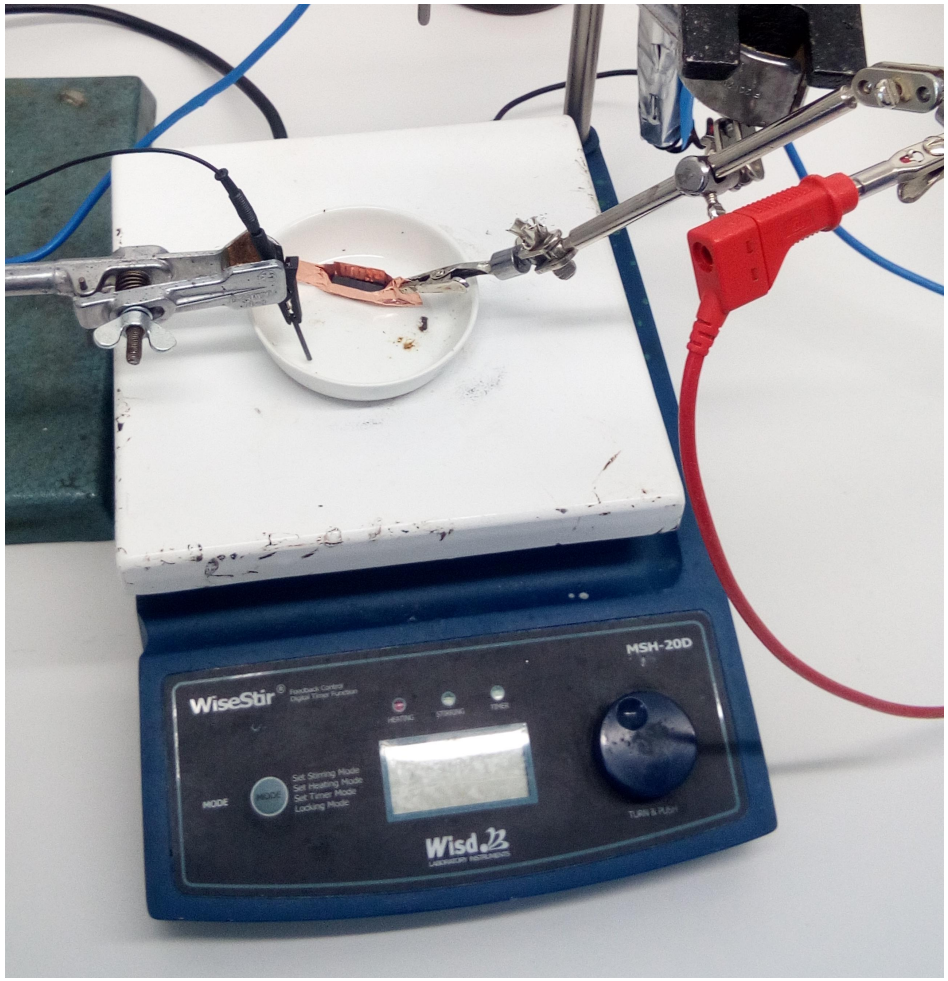
FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

CMOS 4011 Decapsulation
Electro-Chemical Process – Setup[1]

- Positive electrode – device being decapsulated
- Negative electrode – platinum is recommended in literature
- Negative electrode – low cost alternatives:
  - Graphite electrode (originally from a pencil) – it works, but it dissolves due to fillers
  - Stainless electrode provides satisfactory results (stainless steel screw was used)
- Potential: 5V (current was about 50 - 100 mA)
- Acid temperature: 70 - 80 °C
- Decapsulation time: $>$ 1 minute

[1] Endoh, Hirohiko, and Takuya Naoe. "Copper wire bonding package decapsulation using the anodic protection method." Microelectronics Reliability 55.1 (2015): 207-212.

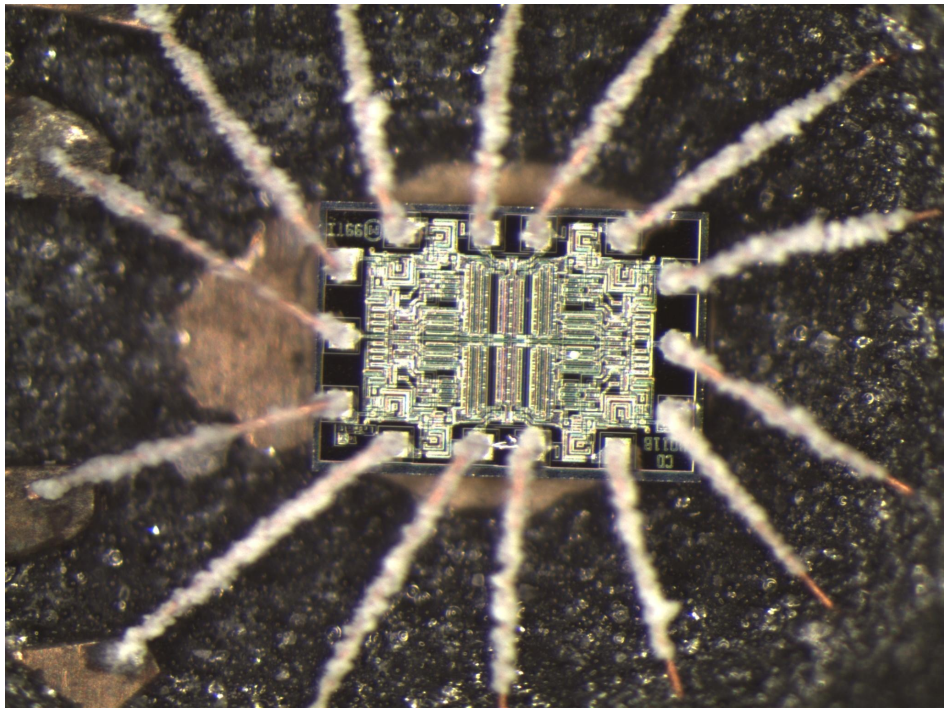
CMOS 4011 Decapsulation
Electro-Chemical Process – Illustration

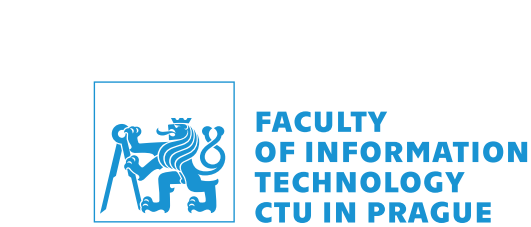


CMOS 4011 Decapsulation
Electro-Chemical Process – Postprocessing

- Decapsulated device was washed in acetone
- The process residual are the Cu^{2+} salts ($CuSO_4$, $Cu(NO_3)_2$)

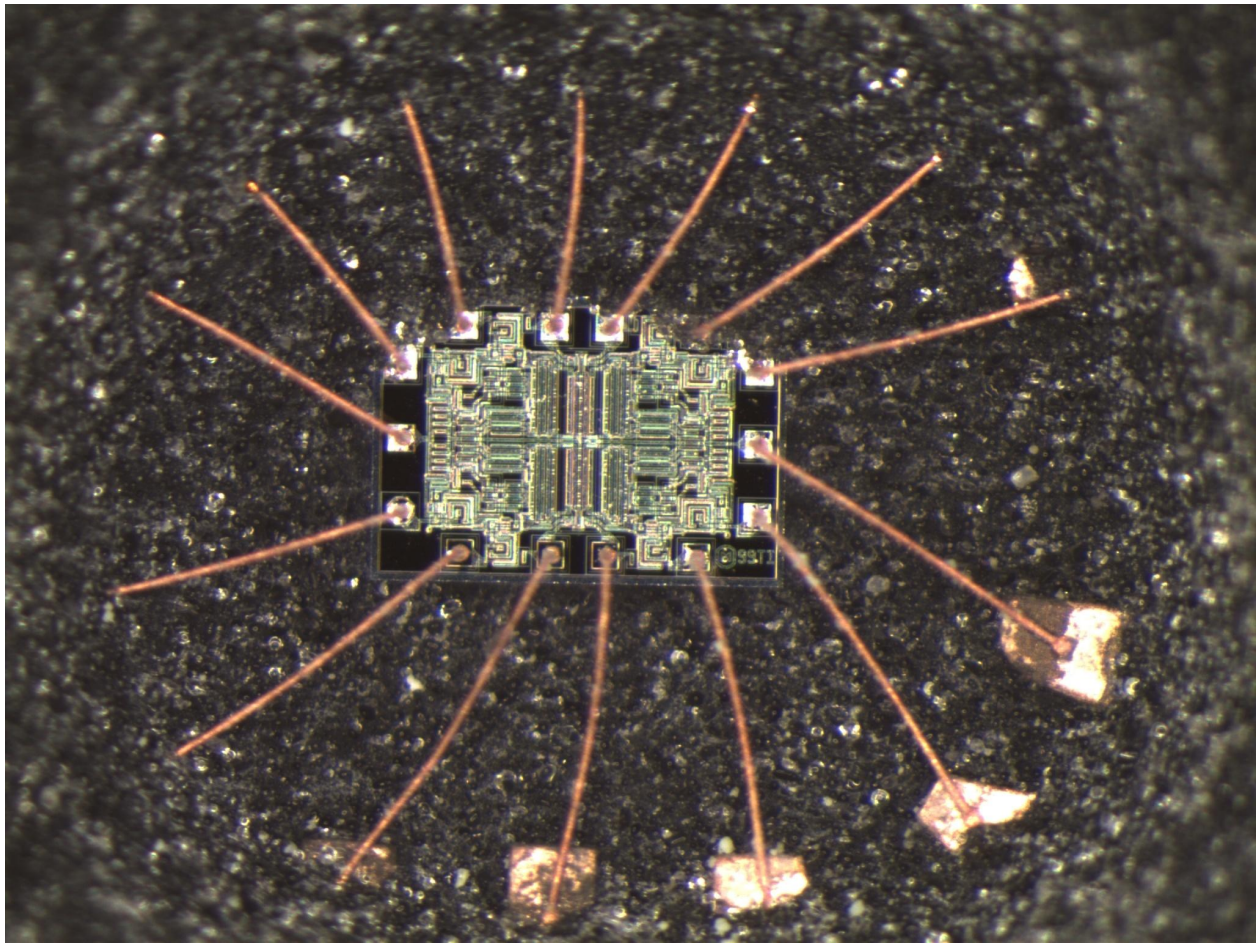
→ salts were dissolved in the distilled water





FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

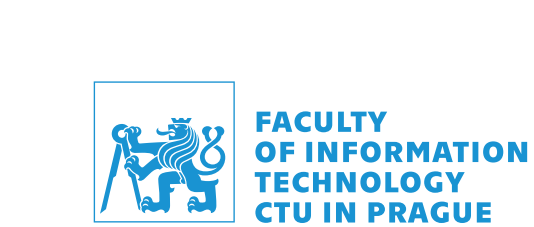
CMOS 4011 Decapsulation
Decapsulated and Operational CMOS 4011



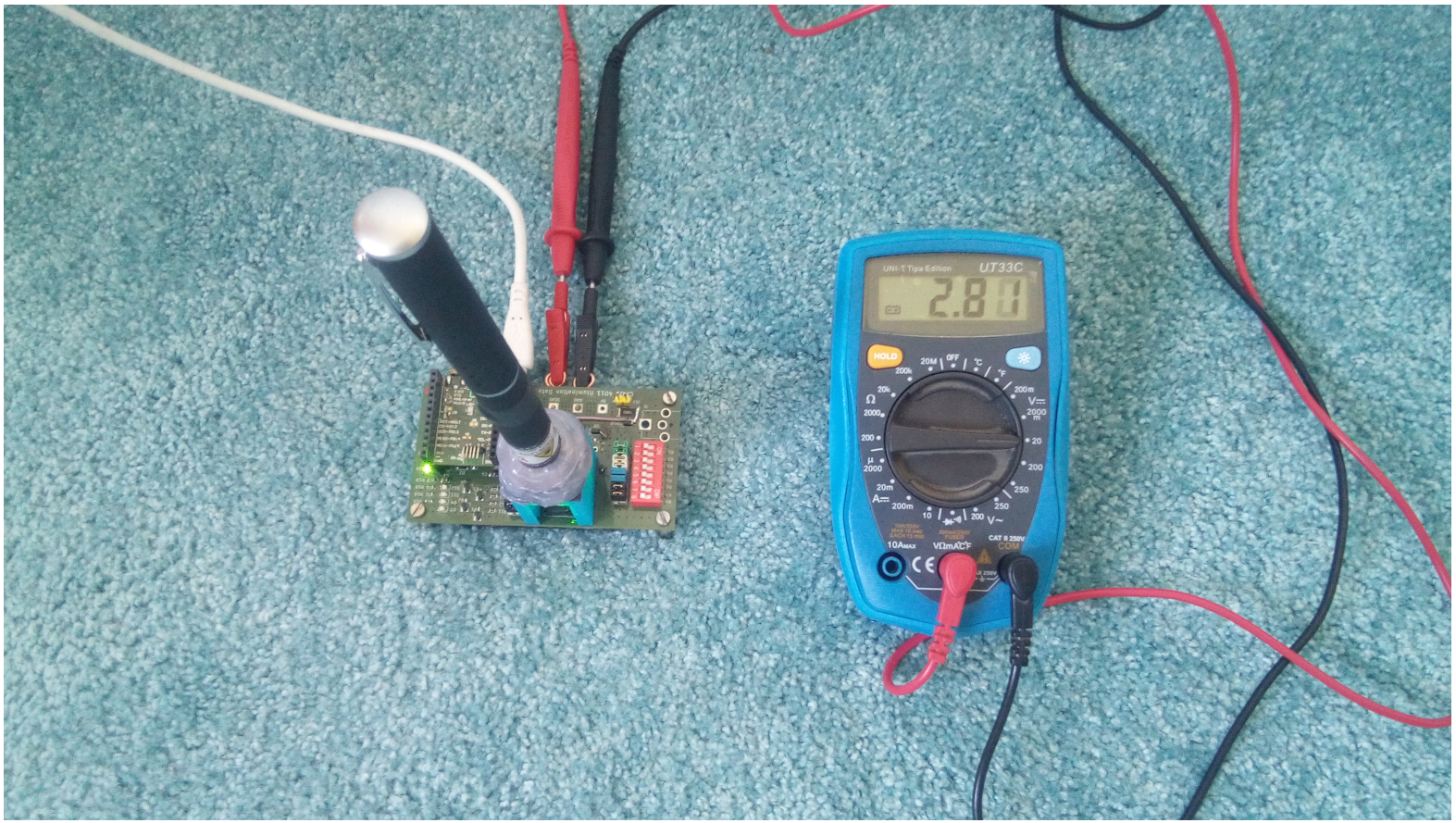
FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

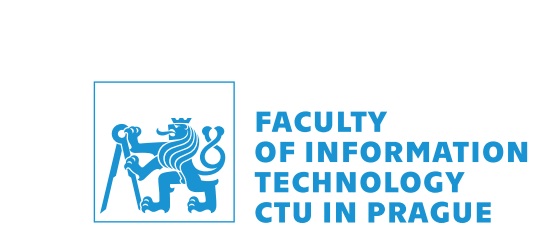
CMOS 4011 Live Demo

Live Demo . . . Later :-)



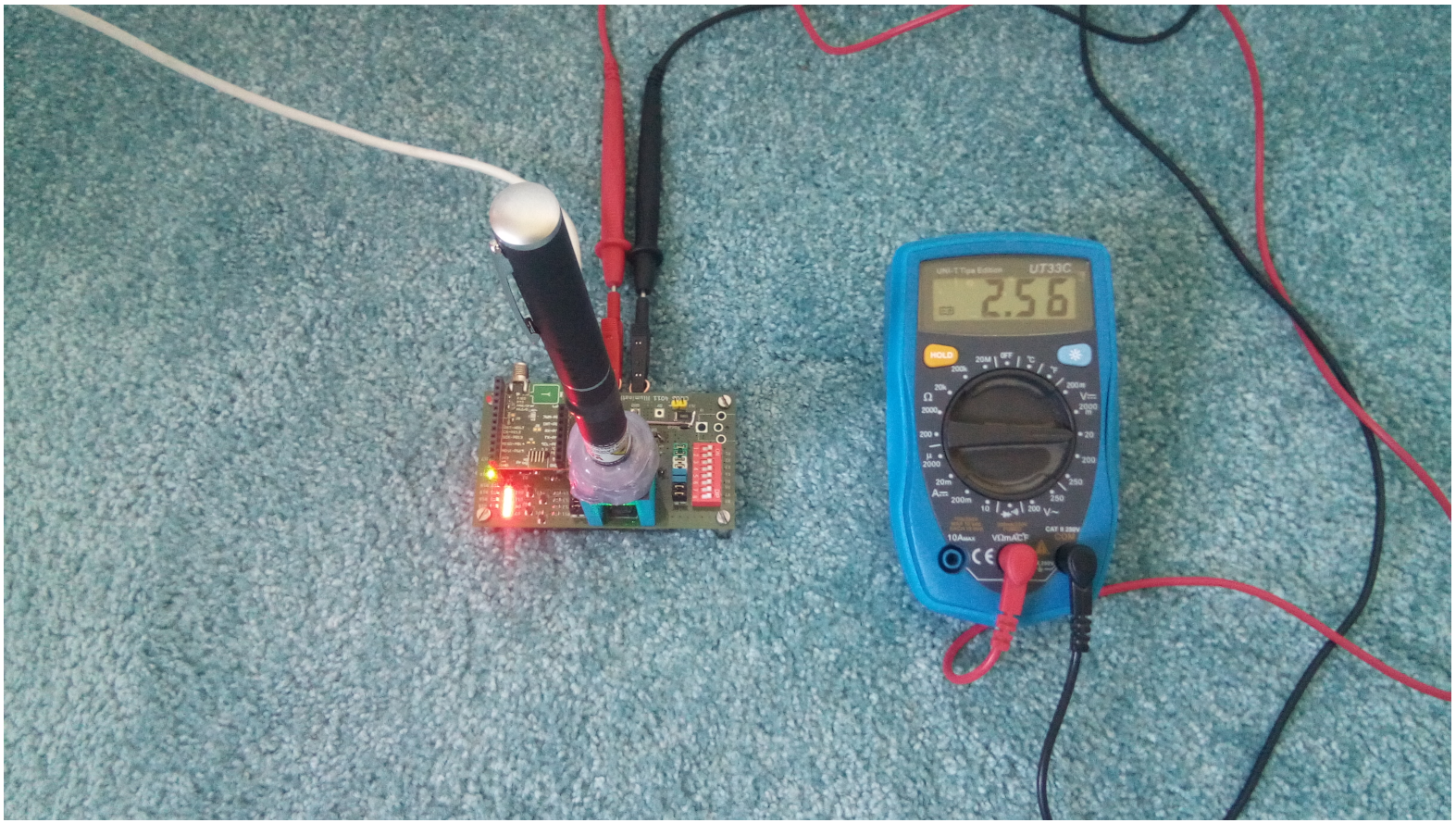
CMOS 4011 Demo – Experiments
All-1 inputs; 50mW laser: 2810 μA





FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

CMOS 4011 Demo – Experiments
All-0 inputs; 50mW laser: 2560 μA



FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Thank You!
Work-In-Progress and Future Work

Future Work is related to submicron technology and applications of the phenomena in the security area:

- research of the "cocktail effect" influence
- modulated static current variability modeling and simulation
- measurements using devices manufactured by using corresponding (in the field) technologies
- attack scenario formulation and validation

The author [1] *acknowledges the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics" and the CTU grant SGS17/213/OHK3/ 3T/18.*