Shrnutí aktivit ČVUT, na které projekt AI-SecTools navazuje. Představení use cases.

Workshop NÚKIB, VUT, MUNI, ČVUT

Horoměřice, 01.07.2022

Martin Novotný, ČVUT v Praze, FIT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ČVUT
ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

Čím se zabýváme – ČVUT v Praze, FIT

- FPGA architektury pro kryptografii
  - Software best-practice implementace kryptografických algoritmů pro FPGA - ve formátu IP Core (VUT) (VUT 60% : ČVUT 40%).
- Odběrová analýza
  - Software pro verifikaci bezpečnosti kryptografického zařízení (ČVUT). (ČVUT 60% : VUT 40%)

Čím se zabýváme – ČVUT v Praze, FIT

- **FPGA architektury/techniky pro kryptografii**
  - Software best-practice implementace kryptografických algoritmů pro FPGA - ve formátu IP Core (VUT) (VUT 60% : ČVUT 40%).
- Odběrová analýza
  - Software pro verifikaci bezpečnosti kryptografického zařízení (ČVUT). (ČVUT 60% : VUT 40%)

FPGA architektury/techniky pro kryptografii

- Influence of passive hardware redundancy on resistance against power analysis.
- Dummy rounds as a DPA countermeasure in hardware.
- Dynamic Logic Reconfiguration Based Side-Channel Protection of AES and Serpent.
- High-Level Synthesis of Polymorphic Side-Channel Countermeasures.
- FT & AR: Area-efficient masked and fault-tolerant architectures.
- Versatile Hardware Framework for Elliptic Curve Cryptography.
- Implementation of the Rainbow signature scheme on SoC FPGA.

Čím se zabýváme – ČVUT v Praze, FIT

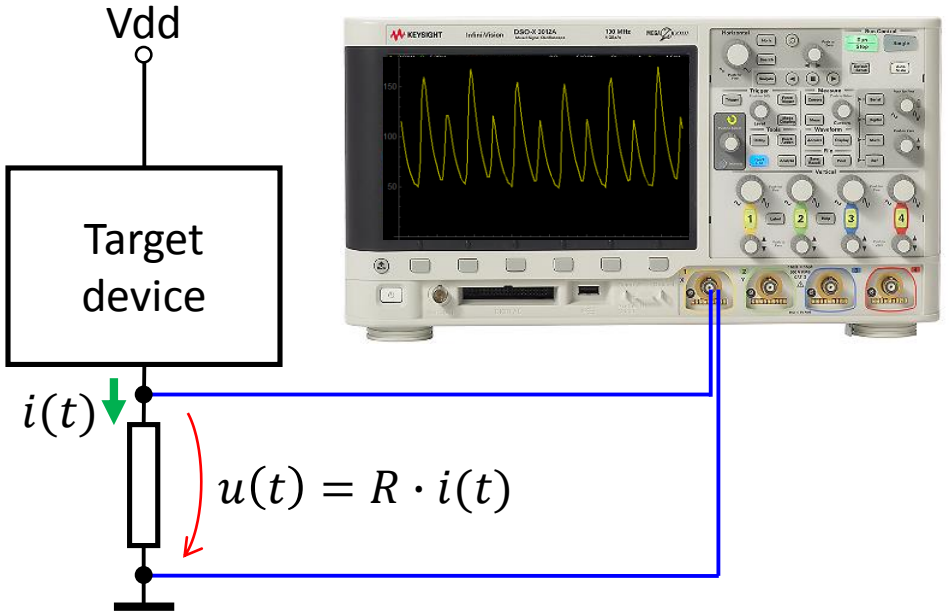
- FPGA architektury pro kryptografii
  - Software best-practice implementace kryptografických algoritmů pro FPGA - ve formátu IP Core (VUT) (VUT 60% : ČVUT 40%).
- **Odběrová analýza**
  - Software pro verifikaci bezpečnosti kryptografického zařízení (ČVUT). (ČVUT 60% : VUT 40%)

Odběrová analýza

- Platformy
- Osciloskopy
- Krypto algoritmy
- Scénáře

Typické use cases

- Correlation Power Analysis (CPA)
  - Symetrické šifry (AES/PRESENT/Serpent)
  - Útok na 1. rundu (MCU) / na poslední rundu (FPGA)
- Test Vector Leakage Assesment (TVLA)
  - Symetrické šifry a post-quantum schémata
  - Welch's t-test / χ^2 test / Neuronové sítě
- Šablonové útoky

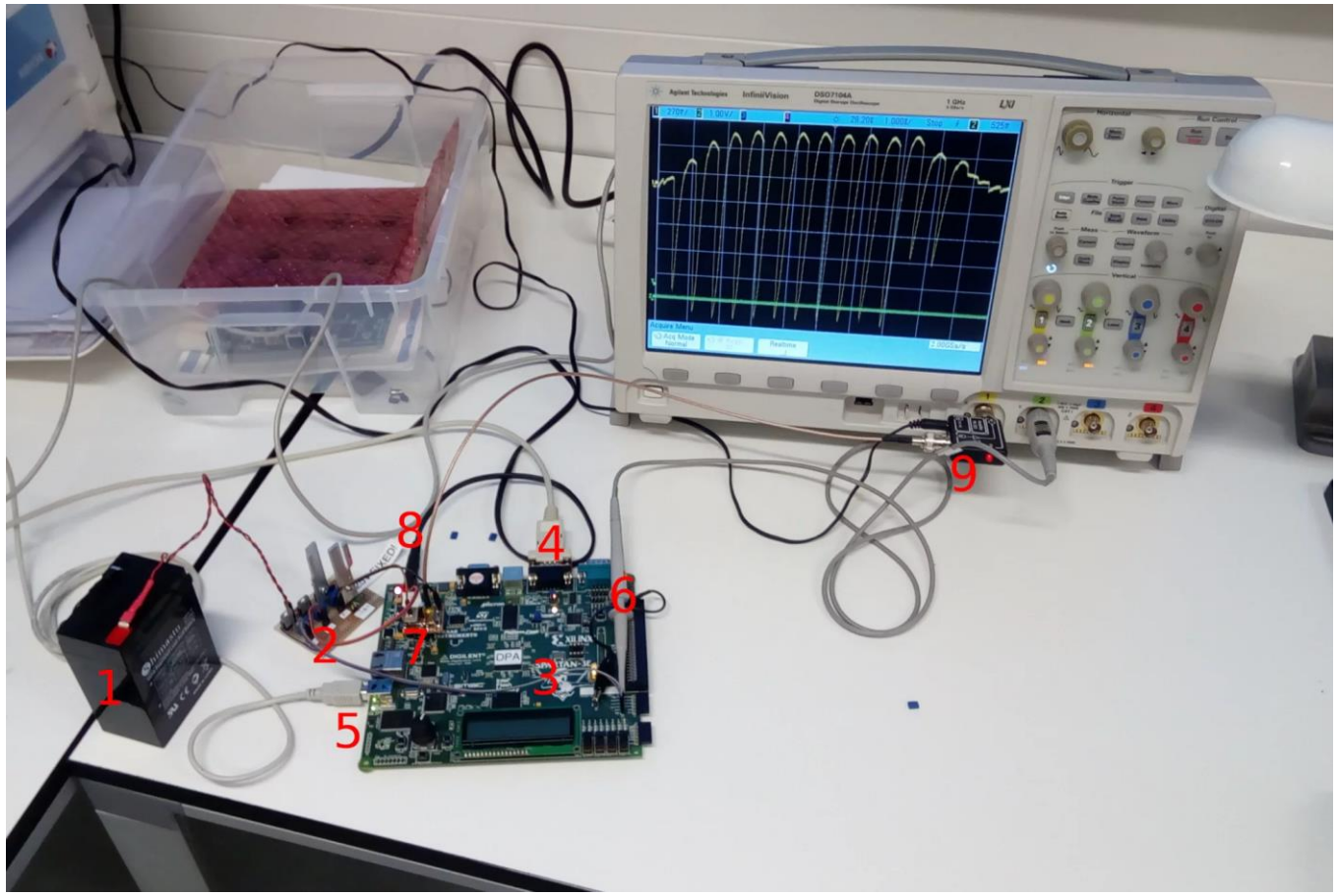


Odběrová analýza

- **Platformy**
- Osciloskopy
- Krypto algoritmy
- Scénáře

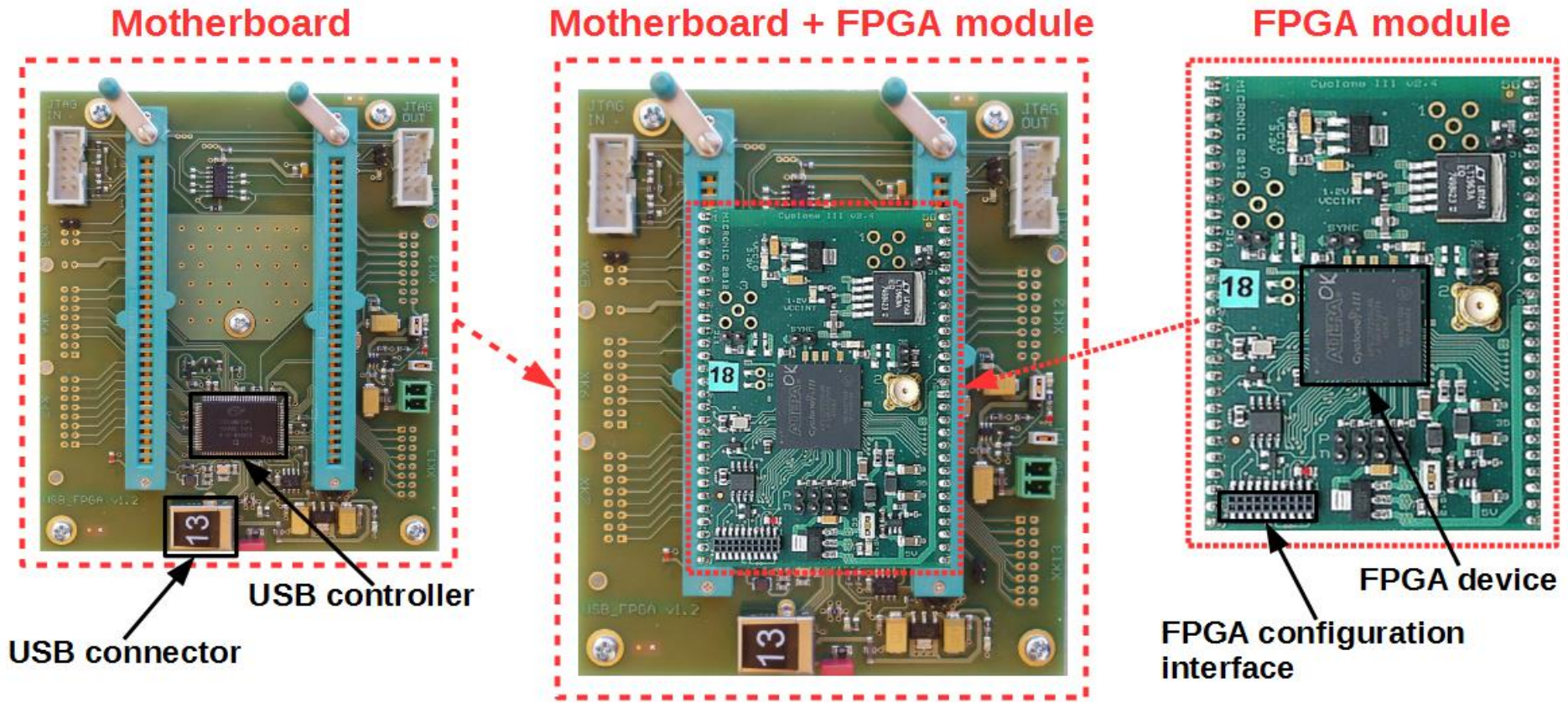
FPGA: Spartan-3E Starter Kit

- Upravený přípravek



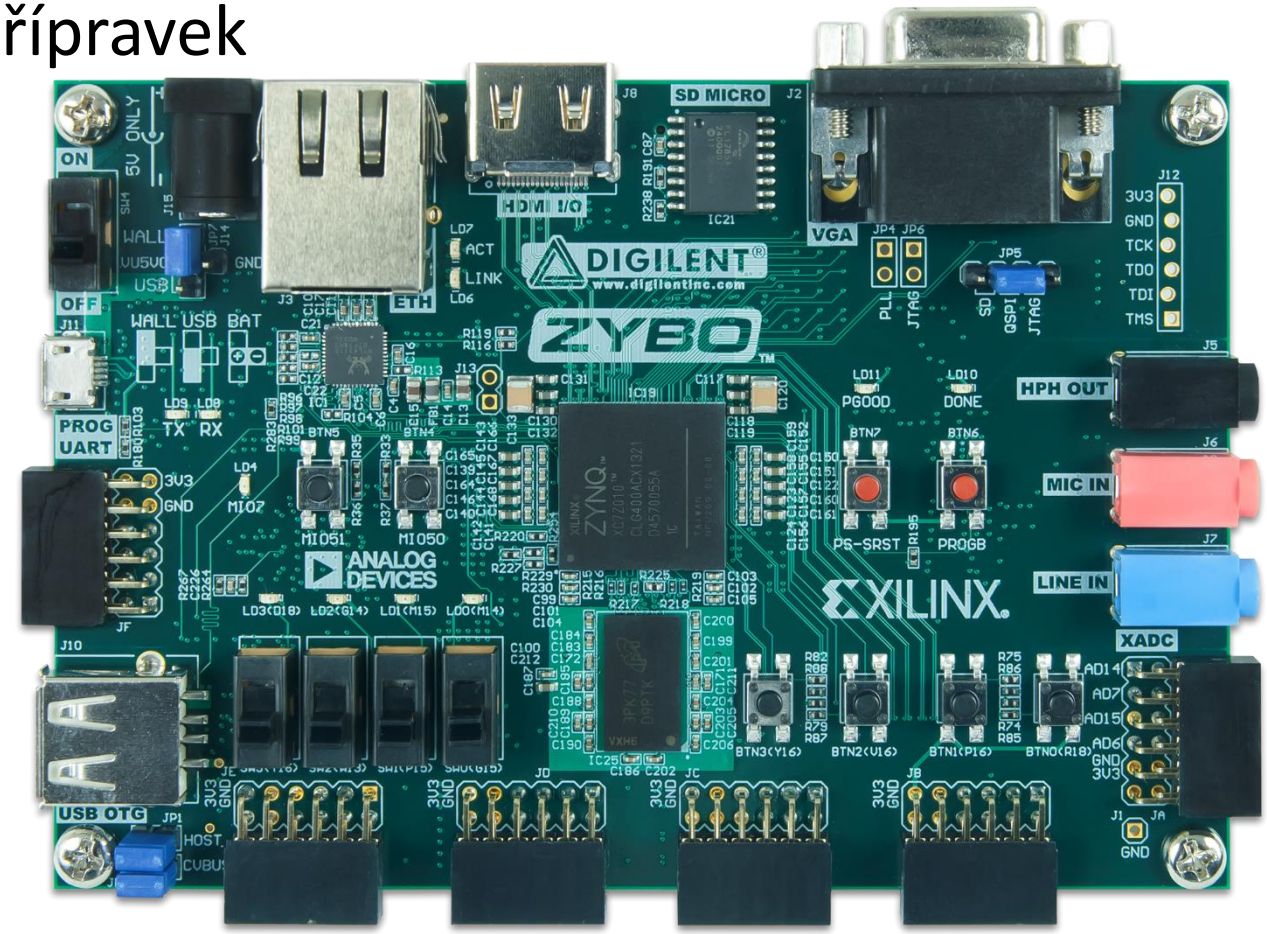
FPGA: Evariste III + Altera Cyclone III

- Upravený přípravek



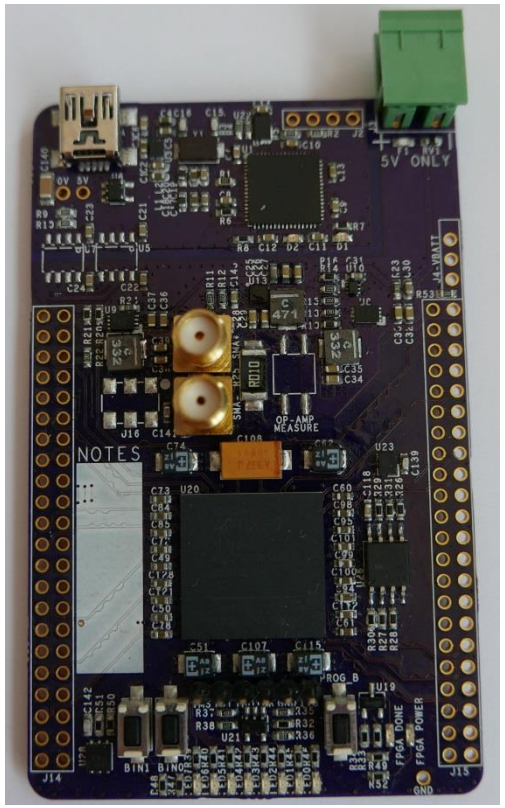
FPGA: ZedBoard

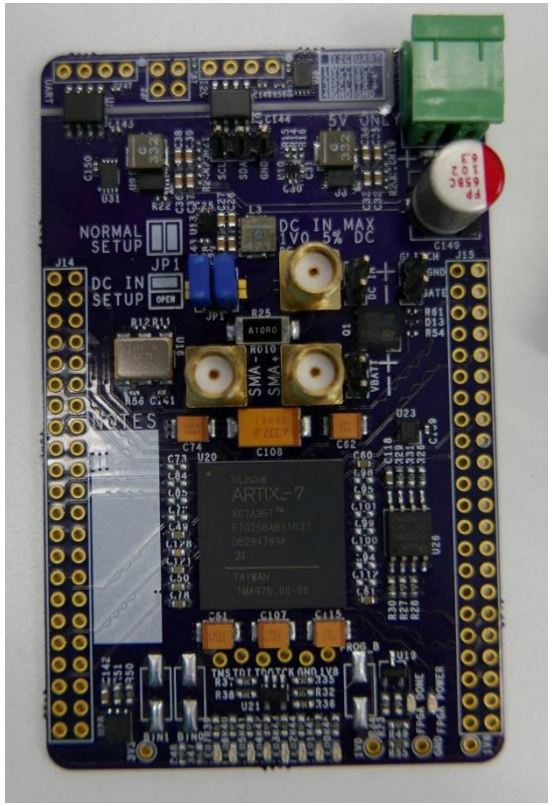
- Upravený přípravek

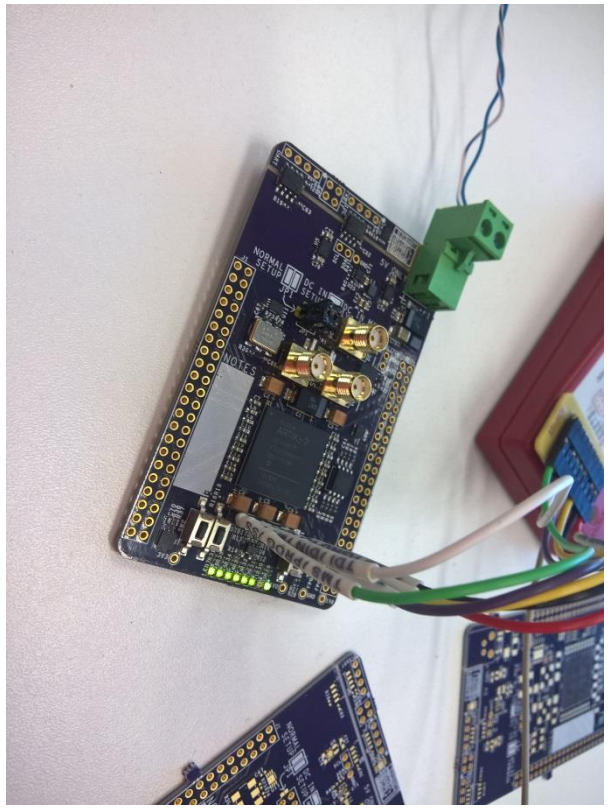


FPGA: DPA board

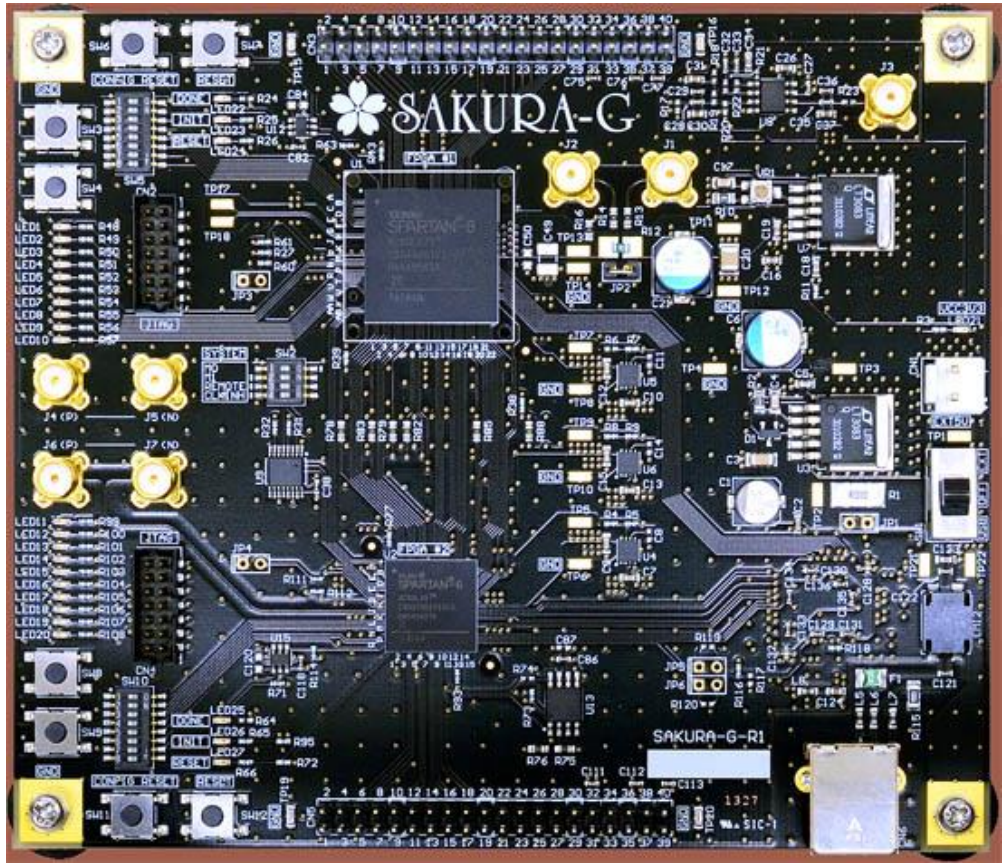
- Vlastní návrh i výroba
- Artix 7

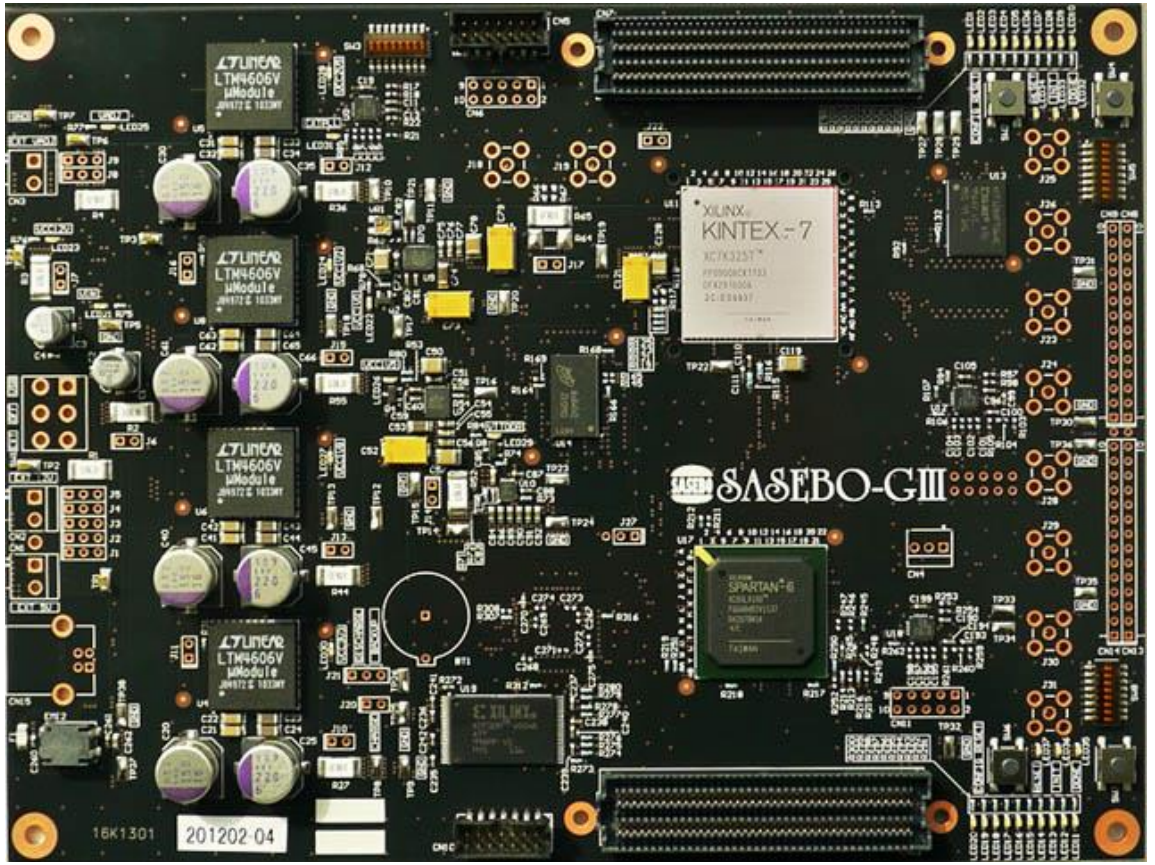




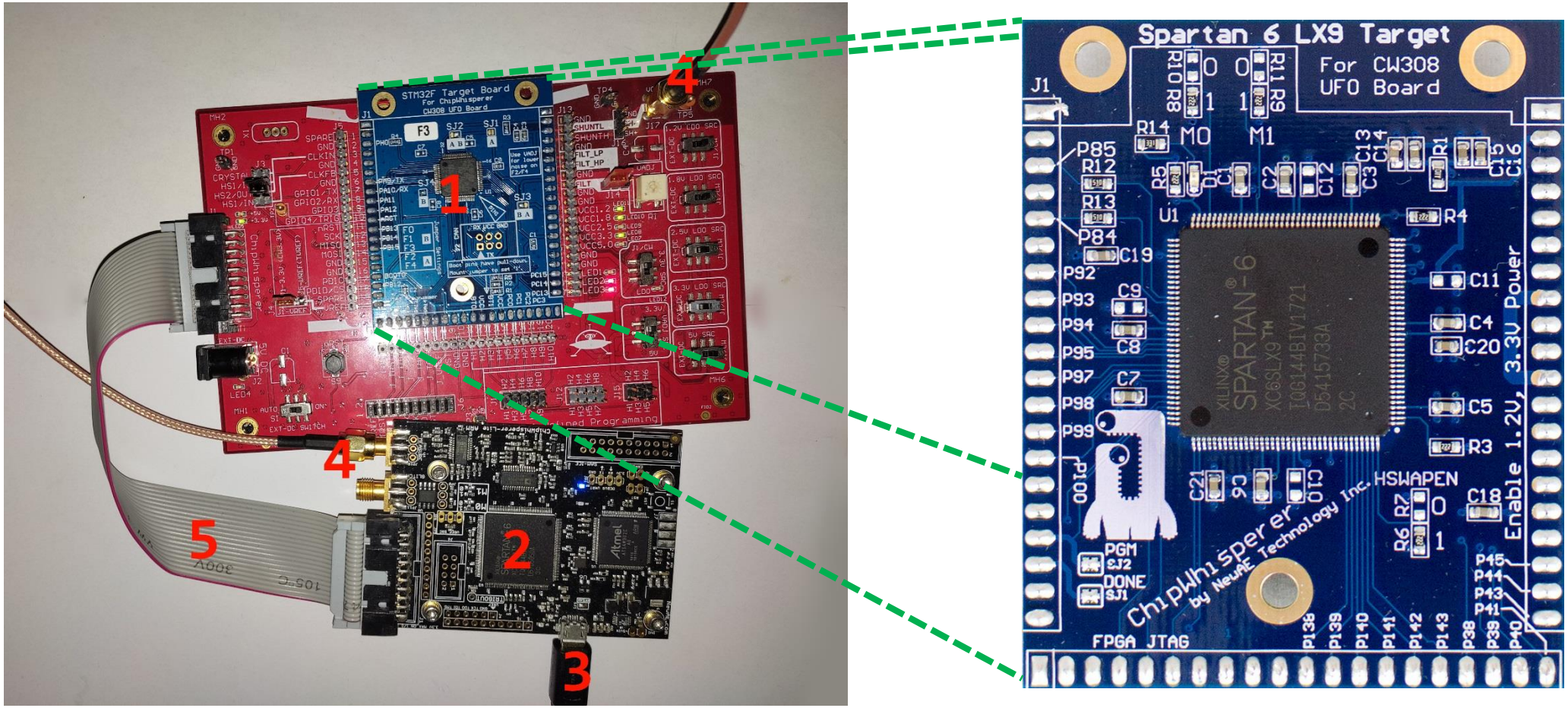


FPGA:
Sakura-G (Spartan 6), Sakura-X (Kintex 7)

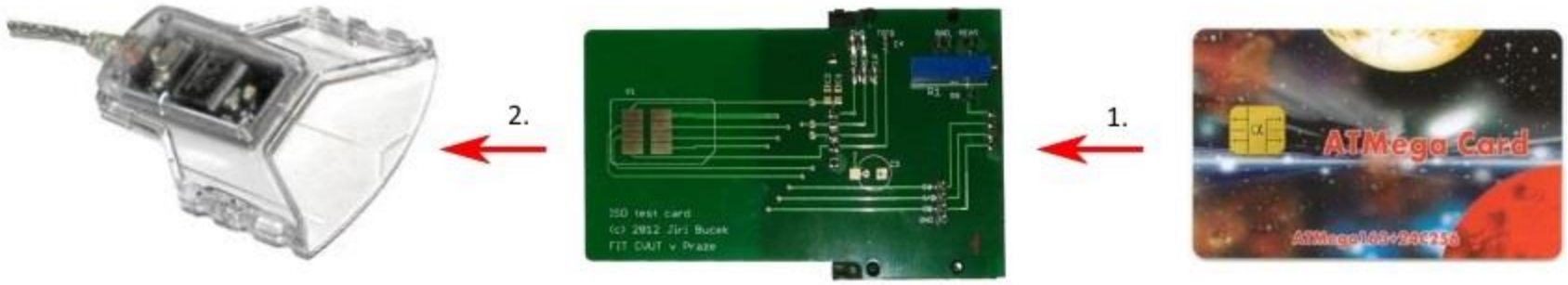




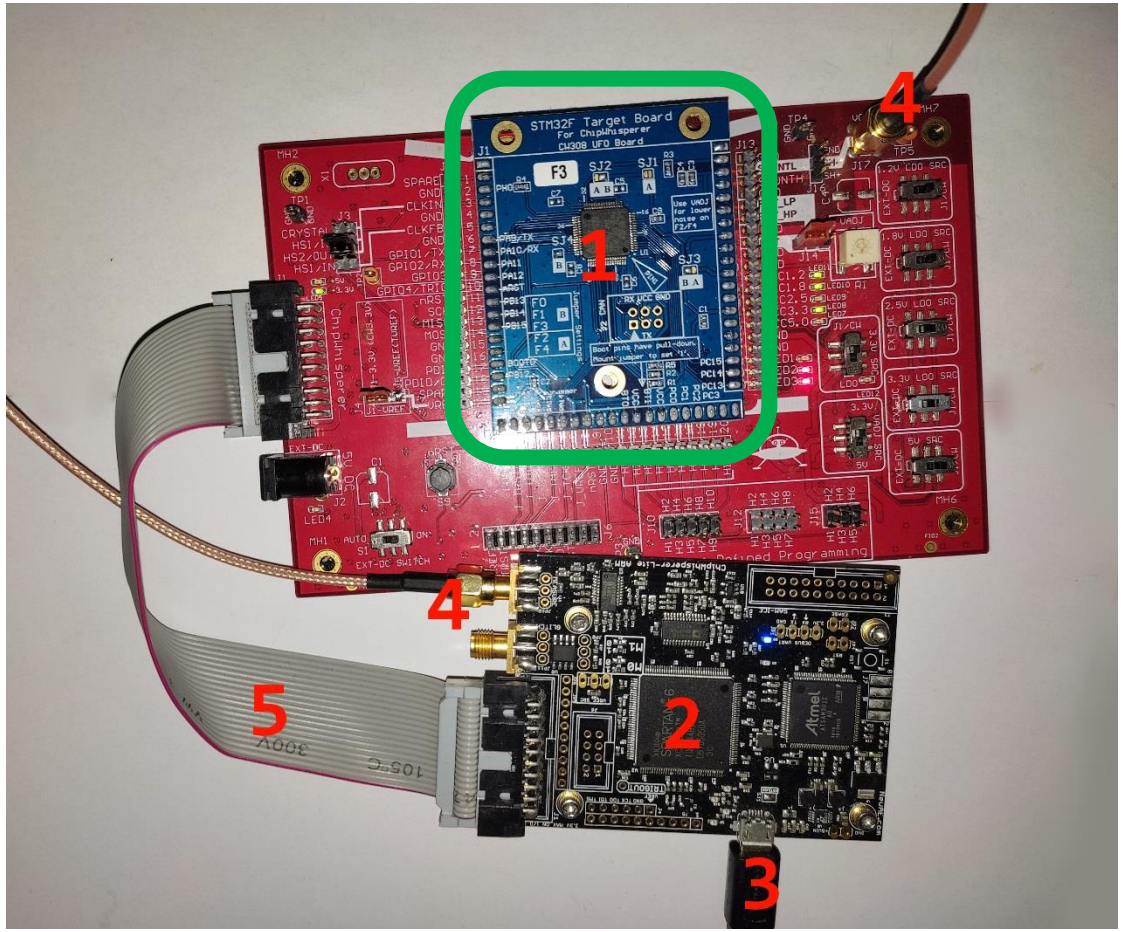
FPGA: Sada ChipWhisperer + Spartan 6

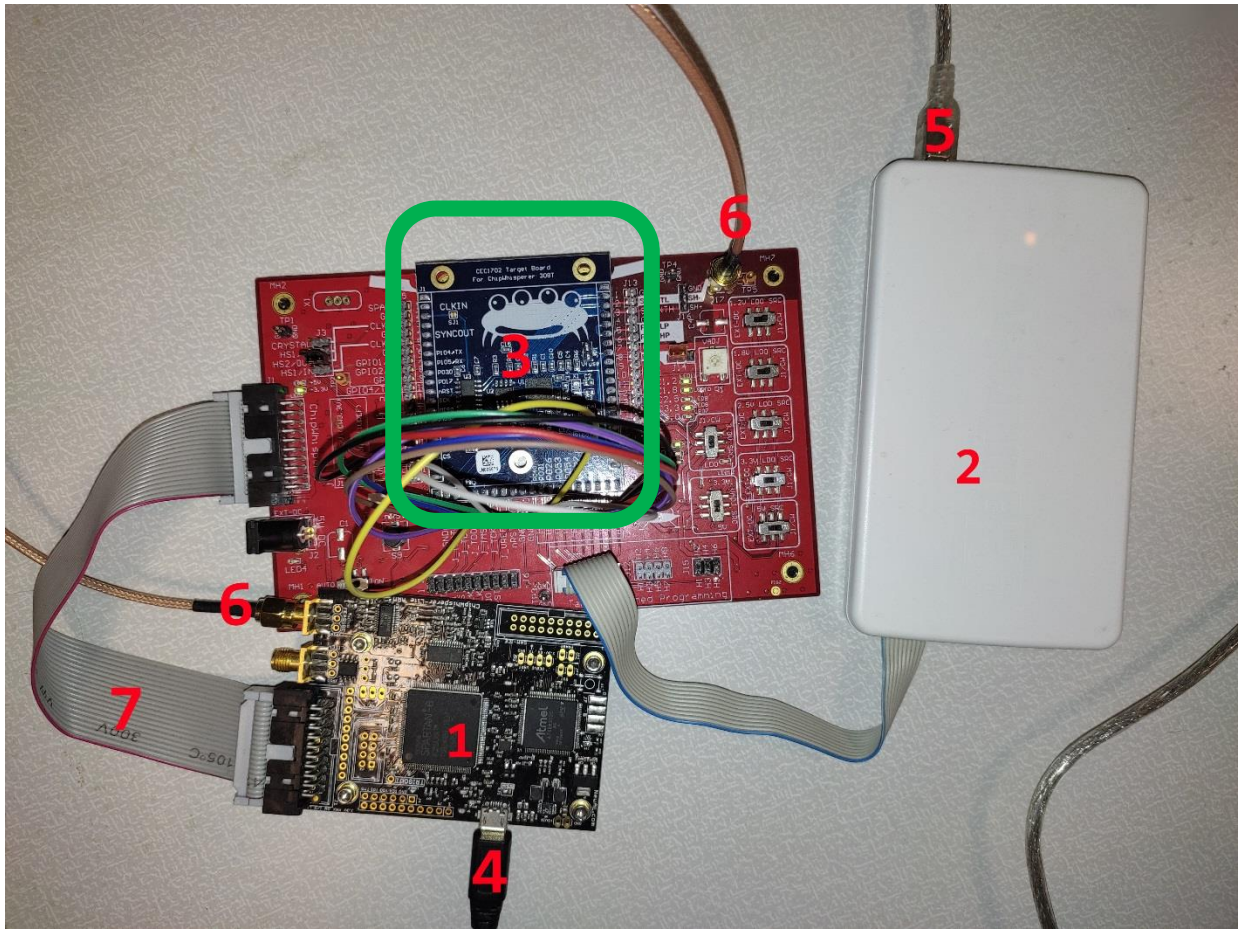


MCU: AVR SmartCard

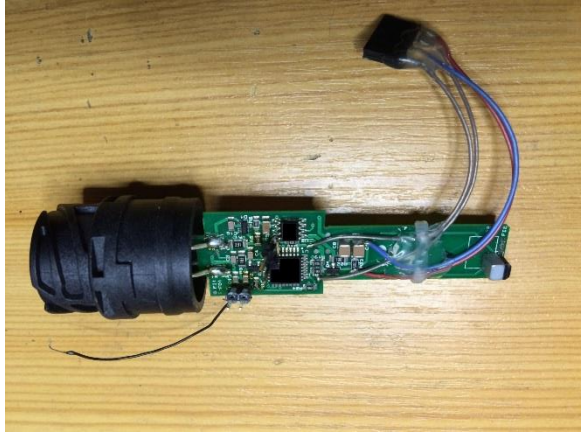


MCU: Sada ChipWhisperer
+ STM32, CEC1702, …

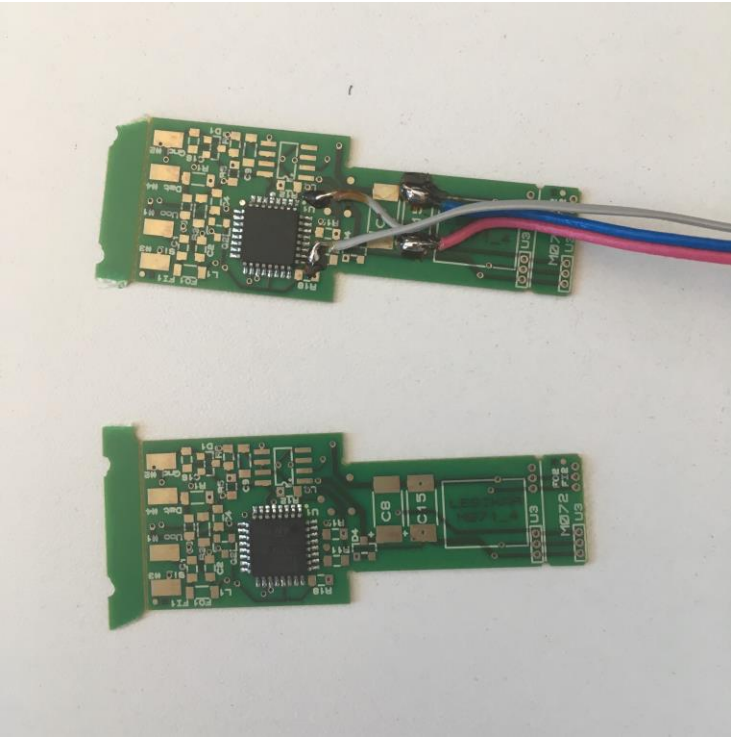




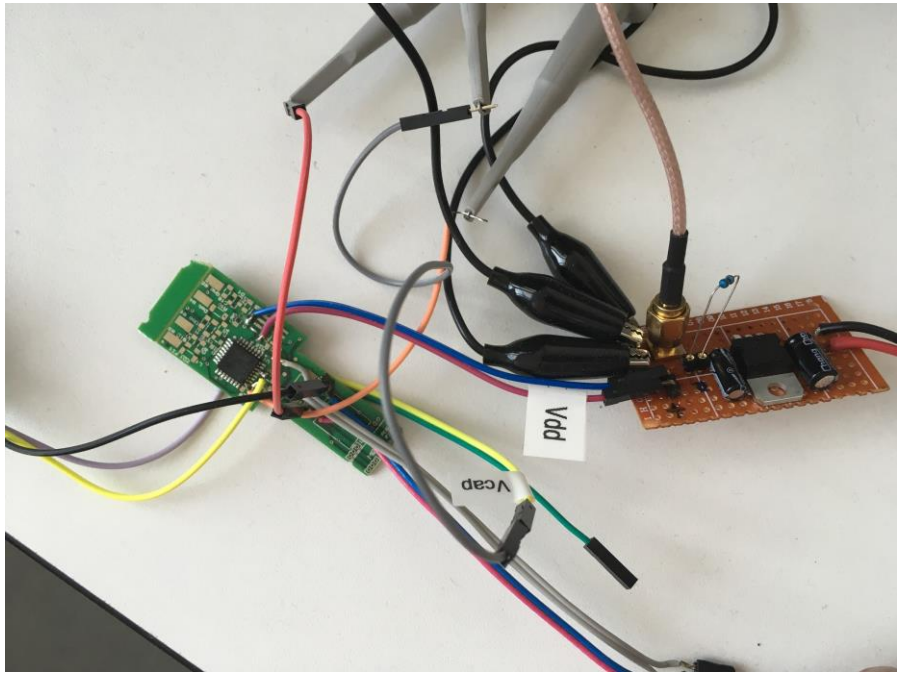
MCU: Koncové zařízení



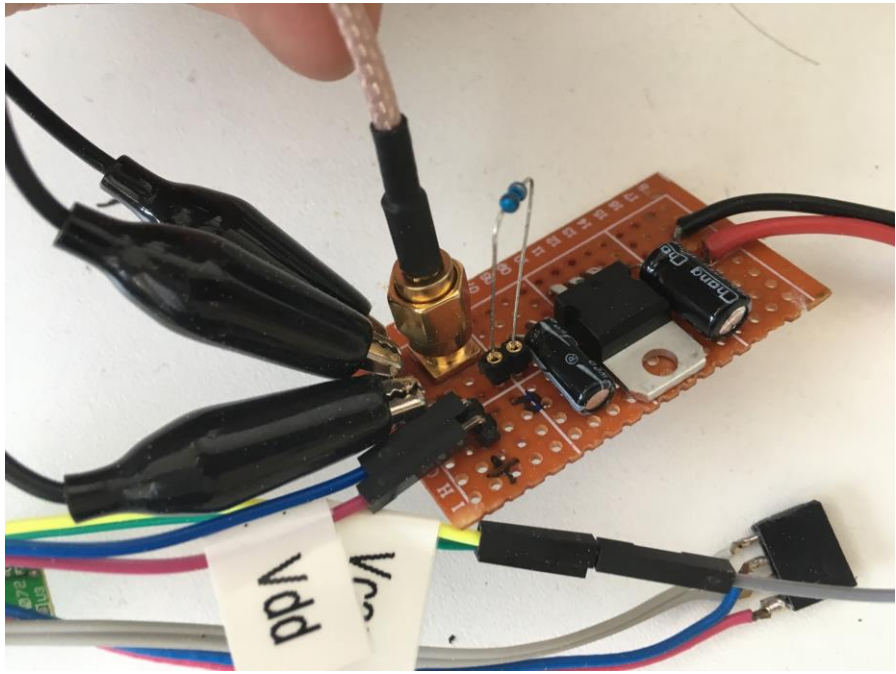
- Tachografický snímač



Měřený přípravek



Měřený + měřicí přípravek



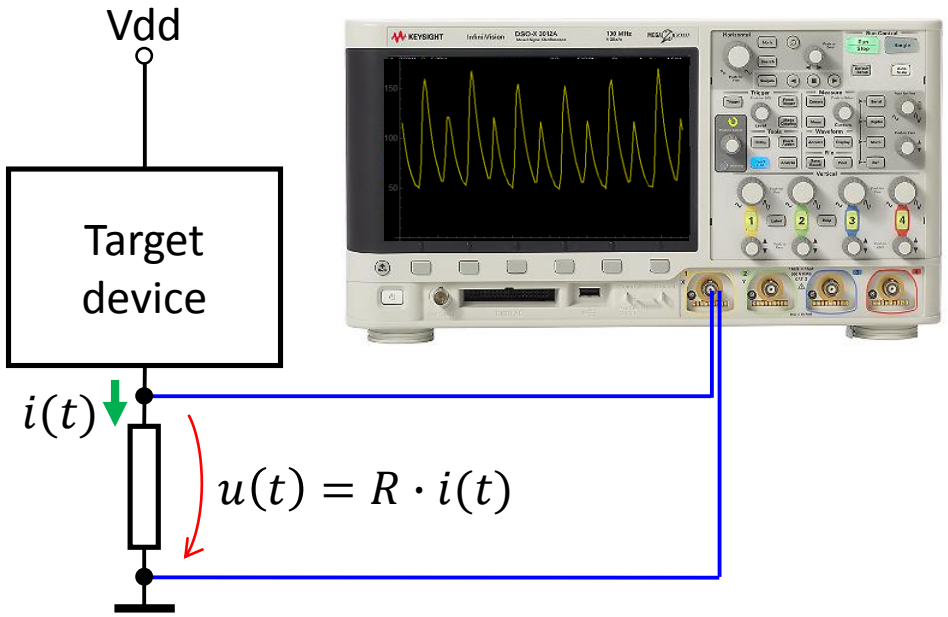
Měřicí/napájecí přípravek

Odběrová analýza

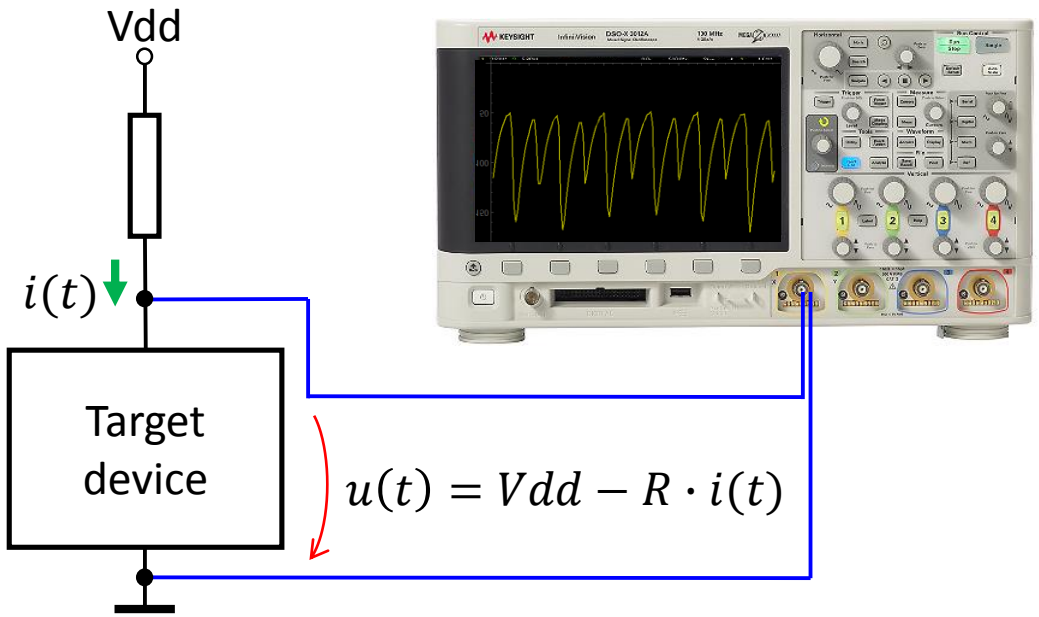
- Platformy
- **Osciloskopy**
- Krypto algoritmy
- Scénáře

Typická konfigurace

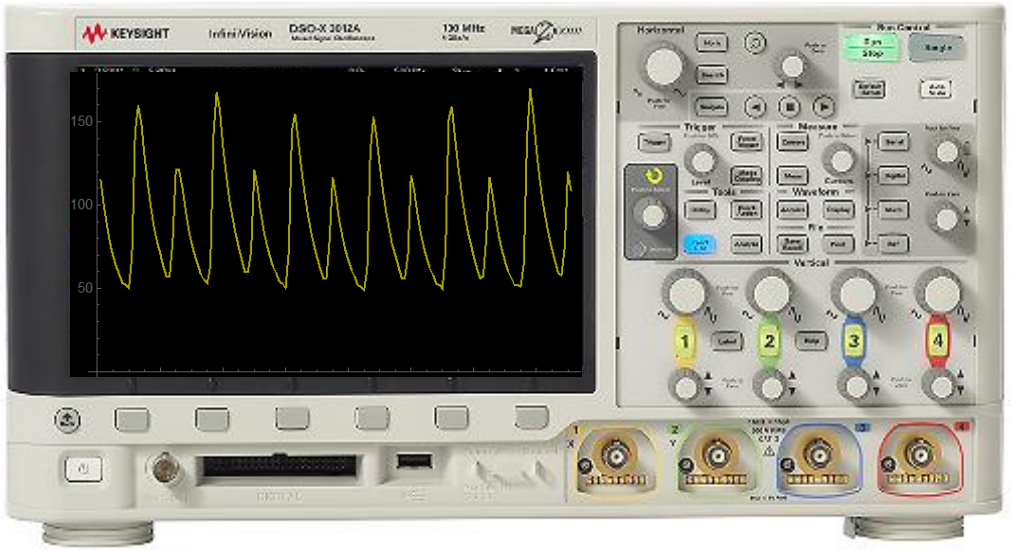
DC coupling

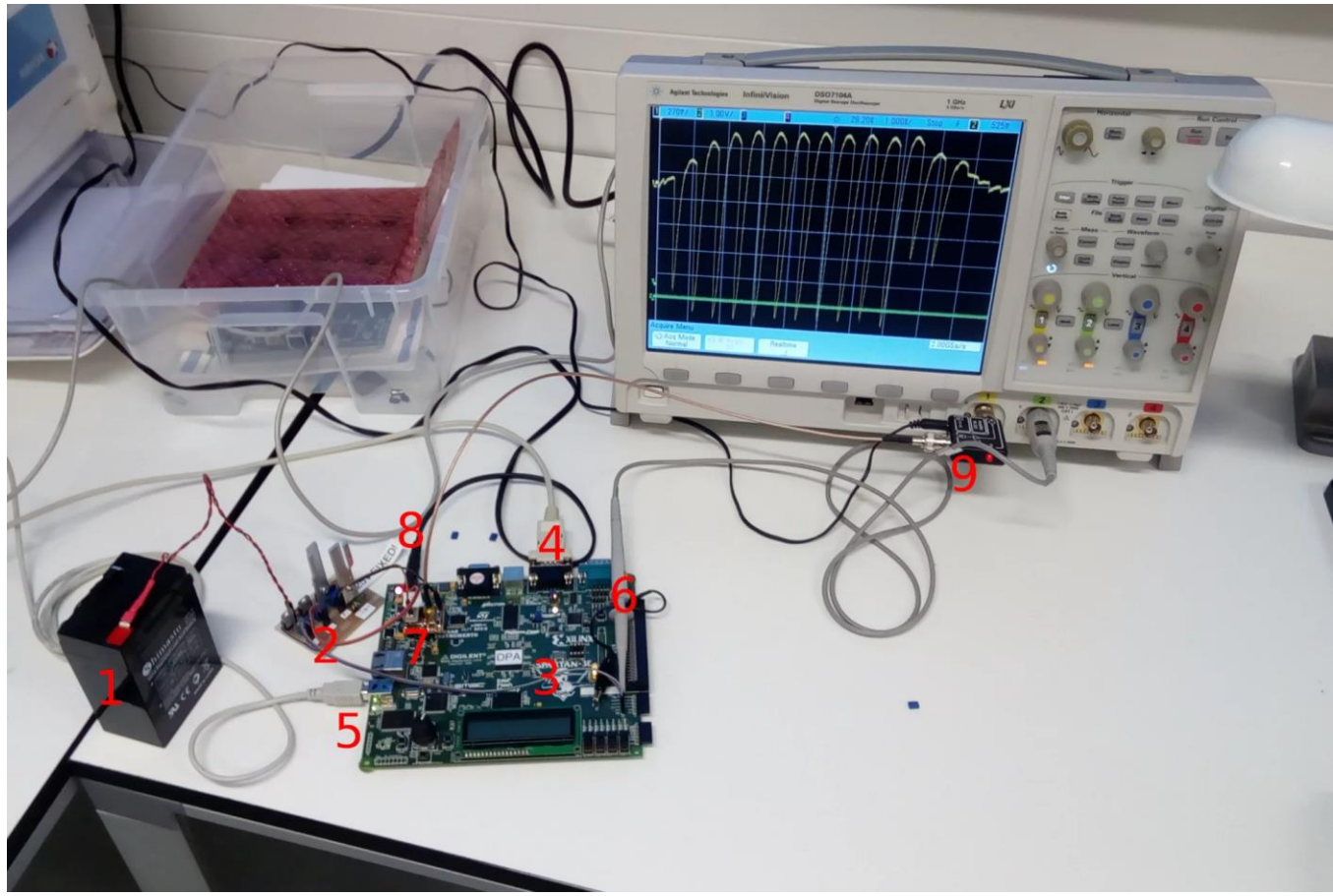


AC coupling



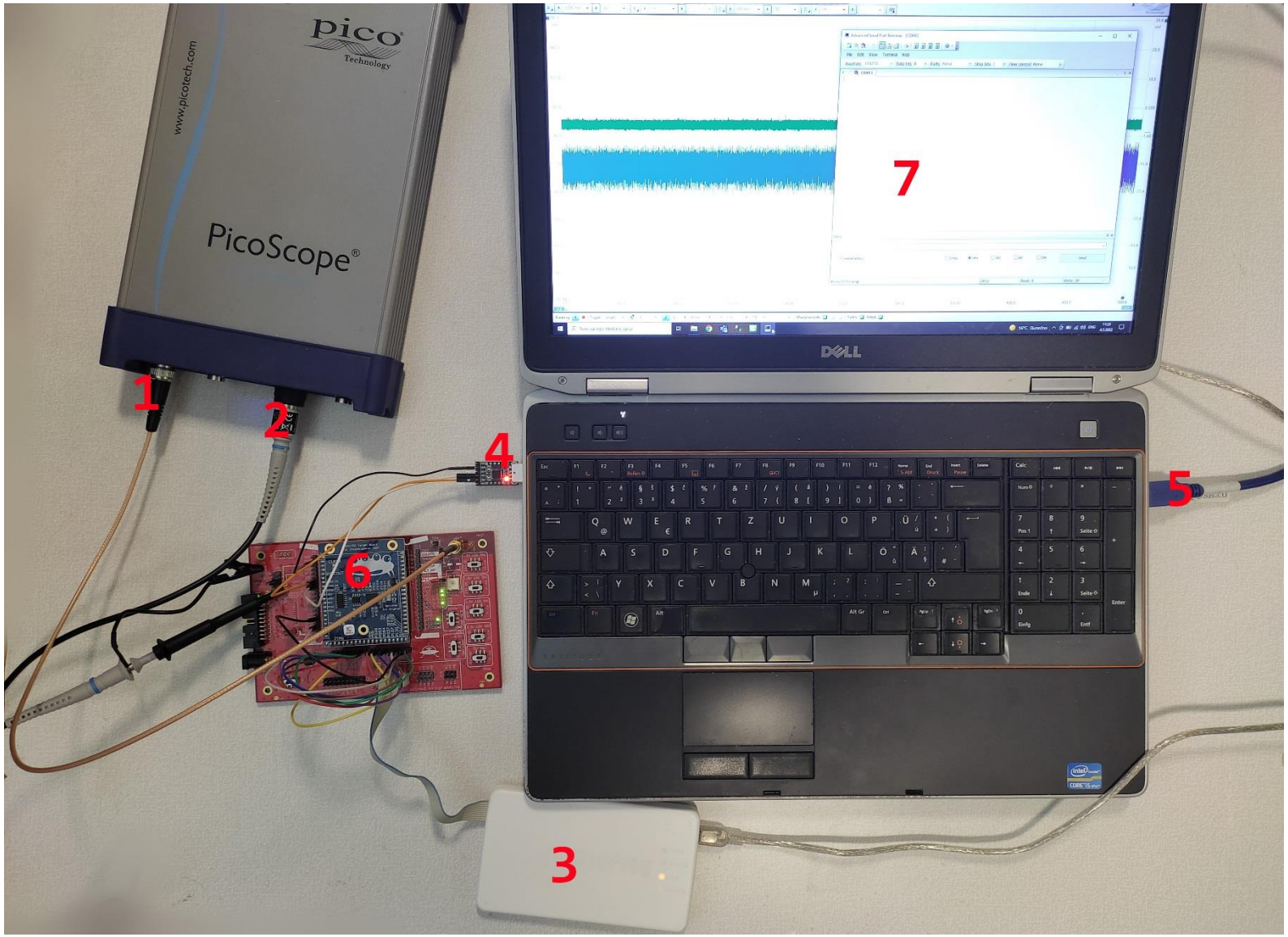
Agilent/Keysight



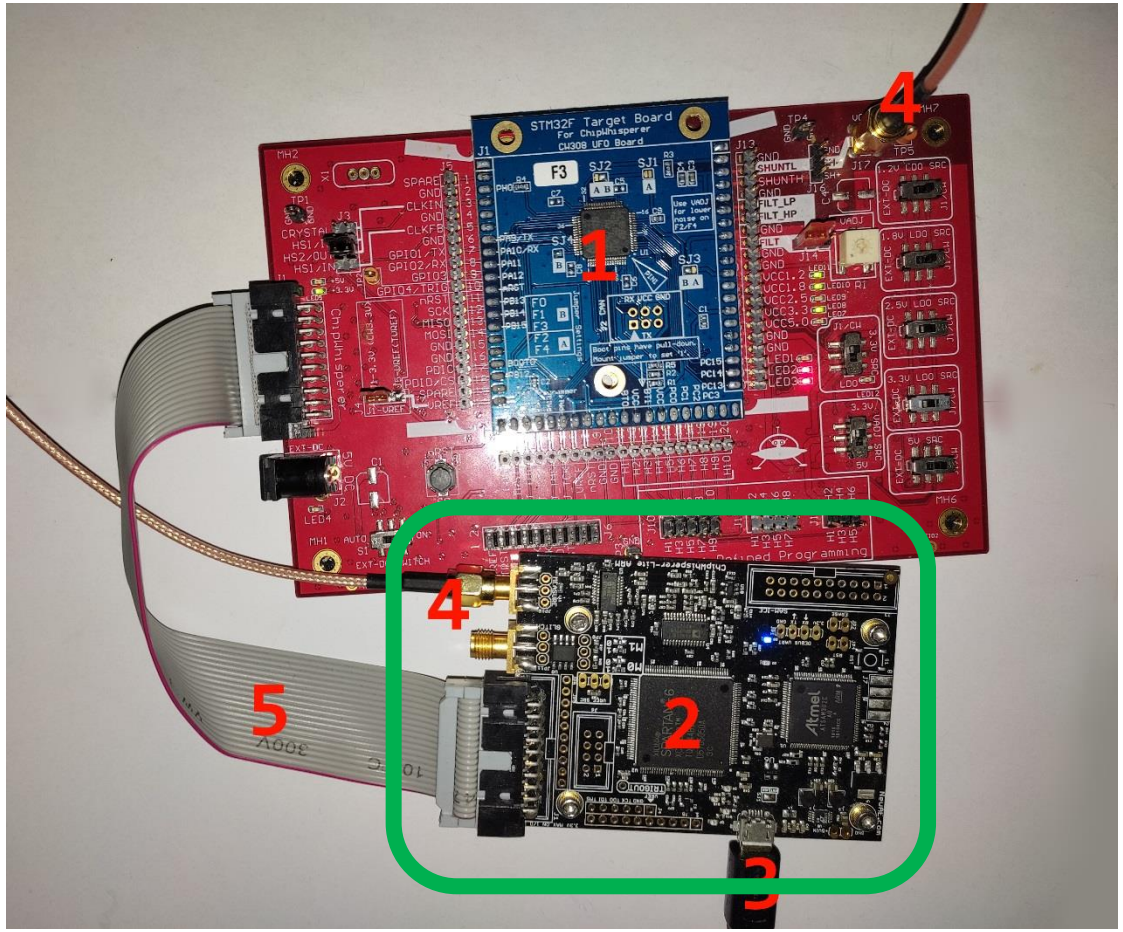


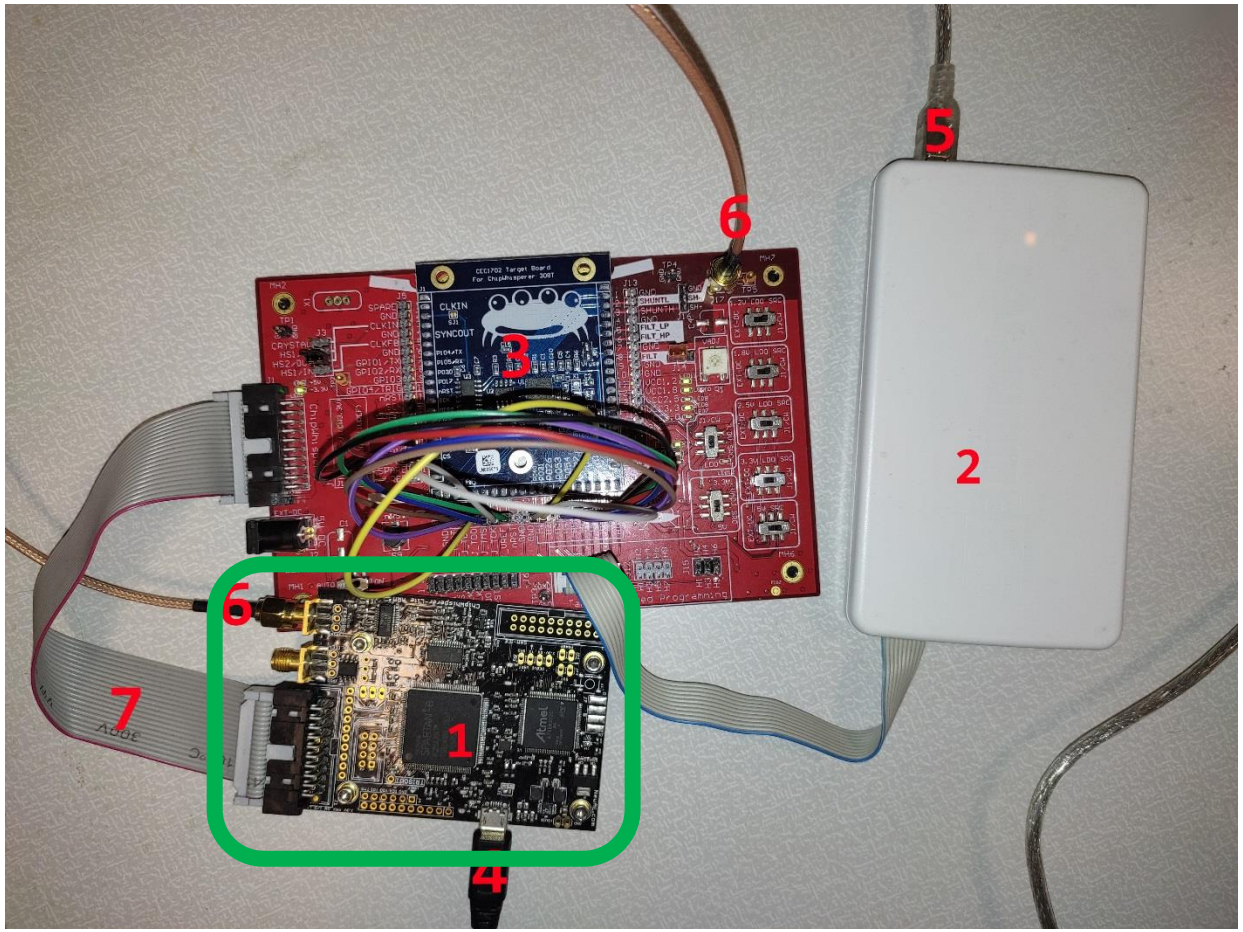
PicoScope


PicoScope


pico
Technology
www.picotech.com
PicoScope®
DELL
1
2
3
4
5
6
7

ChipWhisperer-Lite





Odběrová analýza

- Platformy
- Osciloskopy
- **Krypto algoritmy**
- Scénáře

Krypto algoritmy

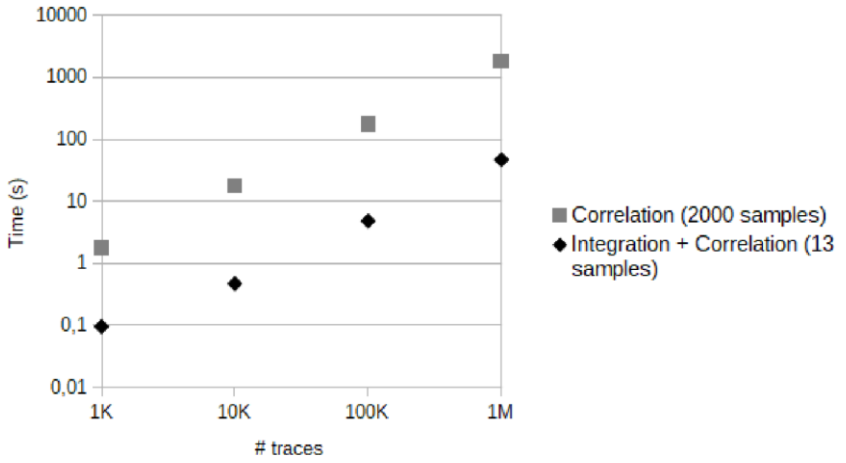
- Symetrické šifry
  - AES
  - PRESENT
  - Serpent
- Hash
  - SipHash
- Post-kvantová schémata
  - Rainbow

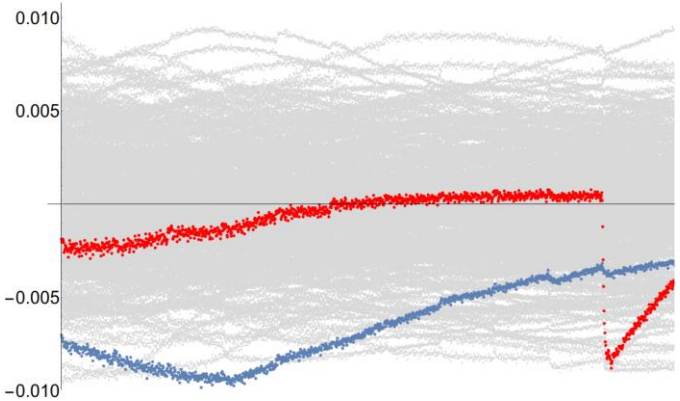
Odběrová analýza

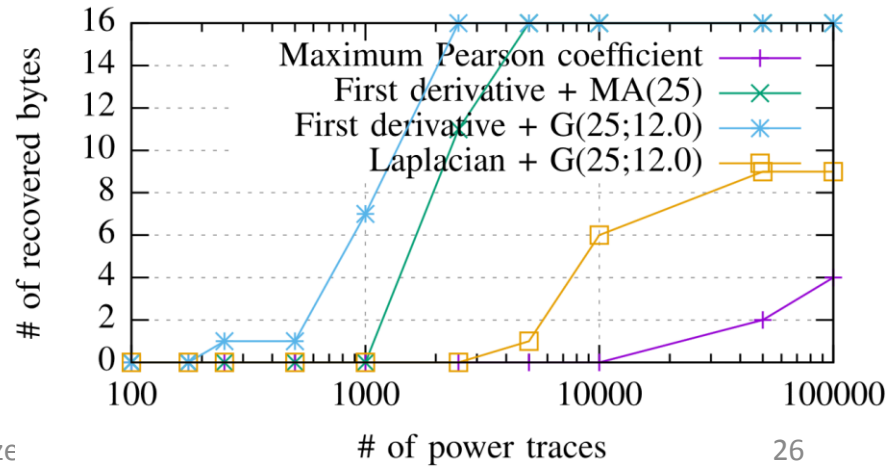
- Platformy
- Osciloskopy
- Krypto algoritmy
- **Scénáře**

Scénáře – CPA

- Útok na: 1. rundu / poslední rundu
- Preprocessing: nic /
  agregace vzorků (po hodinových cyklech)
- Postprocessing – korelační koeficient:
  |maximum| / |max. derivace|







Scénáře – TVLA

- Welch’s t-test
- χ^2 test
- Neuronové sítě

Odběrová analýza

- Platformy
- Osciloskopy
- Krypto algoritmy
- Scénáře
- **Další rozměry v Kartézském součinu?**

Odběrová analýza

- Platformy
- Osciloskopy
- Krypto algoritmy
- Scénáře
- Další rozměry v Kartézském součinu?

Další souřadnice v každém rozměru?