Postup a výzkum týmu VUT v 2022: Analýza kryptografických primitiv na FPGA, bezpečnost, návrh testbedu

Jan Hajný, Lukáš Malina, Petr Jedlička, Tomáš Gerlich

Vysoké učení technické v Brně

Workshop AI-SecTools (PESW) 1. 7. 2022 - Horoměřice

MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

BRNO UNIVERSITY OF TECHNOLOGY

Představení týmu VUT v 2022

Hlavní řešitel: doc. Ing. Jan Hajný, Ph.D
Manažer: doc. Ing. Zdeněk Martinásek, Ph.D.
Činnosti:

- Analýza bezpečnosti implementace vůči SCA
  - doc. Martinásek, Ing. Gerlich
  - Výsledek ”Funkční vzorek systému pro automatické testování bezpečnosti”
- Návrh a realizace opatření proti SCA na FPGA
  - doc. Malina, Ing. Jedlička
  - Výsledek ”Demonstrace best-practice implementace kryptografických algoritmů pro FPGA”

Činnosti týmu VUT v 2022

- 1. oblast: bezpečná implementace kryptografie na FPGA - Etapa 5 (1-12/2022) ”Analýza a volba kryptografických primitiv pro FPGA implementaci ve VHDL, výzkum protiopatření pro HW implementace eliminujících útoky postranními kanály ...”
- 2. oblast: kryptoanalýza a testování pomocí AI, návrh testbedu - Etapa 6 (1-12/2022) ”Výzkum vhodných metod využívající AI pro profilaci kryptografických zařízení...”

Plánované výsledky 2022:

- Stať ve sborníku (RIV-D) - podán a **přijat** článek na konferenci ARES 2022 (workshop SP2I), s názvem ”On Secure and Side-Channel Resistant Hardware Implementations of Post-Quantum Cryptography”

Cíle a zaměření Etapy 5

Cíle:

- Analýza a volba kryptografických primitiv pro FPGA implementaci ve VHDL,
- výzkum protiopatření pro HW implementace eliminujících útoky postranními kanály,
- výzkum požadavků na testbed a jeho specifikace.

Zaměření:

- Orientace na postkvantovou kryptografii (PQC) a na finalisty standardizace NIST.
- Experimentální hardwarové implementace metod protiopatření na PQC schémata.

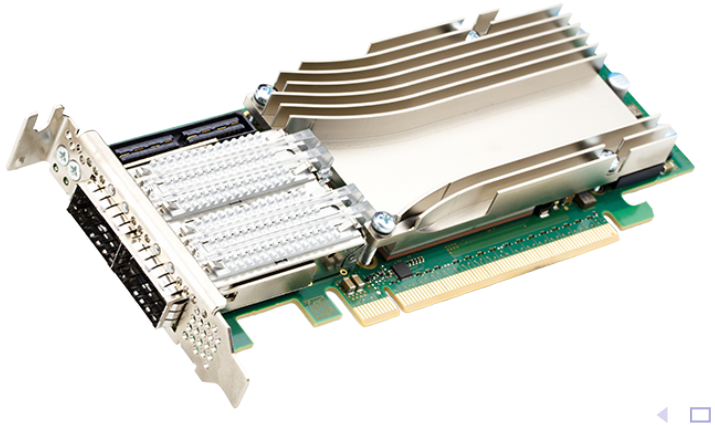


Figure: NFB-200G2QL FPGA Network Card

Analýza útoků

Table: Útoky na hardwarové implementace PQC NIST finalistů.

Scheme	SCA	Fault Injection
Encryption/KEM NIST PQC Finalists		
Kyber	Cold boot attack (2018)	Attack on the Fujisaki-Okamoto transform (2021) Attack on error samplers (2018)
McEliece	Differential power analysis (2016)	✗
NTRU	✗	Attack on error samplers (2018)
SABER	✗	Attack on the Fujisaki-Okamoto transform (2021) Attack on error samplers (2018)
Signature NIST PQC Finalists		
Dilithium	Correlation power analysis (2022)	Attack on error samplers (2018)
FALCON	Correlation power analysis (2021)	Attack on error samplers (2018)
Rainbow	Correlation power analysis (2021)	Attack on the quadratic map (2021)

Note: ✗– no attack could be found.

Analýza protiopatření

Table: Protiopatření pro hardwarové implementace PQC NIST finalistů.

Scheme	Against SCA	Against Fault Injection
Encryption/KEM NIST PQC Finalists		
Kyber	Attack on error samplers (2017)	Attack on the Fujisaki-Okamoto transform (2021) Attack on error samplers (2019)
McEliece	Differential power analysis (2016)	✗
NTRU	Attack on error samplers (2017)	Attack on error samplers (2019)
SABER	Attack on error samplers (2017)	Attack on the Fujisaki-Okamoto transform (2021) Attack on error samplers (2019)
Signature NIST PQC Finalists		
Dilithium	Attack on error samplers (2018)	Attack on error samplers (2019)
FALCON	Attack on error samplers (2018)	Attack on error samplers (2019)
Rainbow	Correlation power analysis (2021)	Attack on the quadratic map (2021)

Note: ✗– no countermeasure published yet

Experimentální implementace skrývání v časové oblasti

- Proměnná doba vykonávání pomocí náhodně generovaného CE (clock enable) signálu.
- Univerzální způsob implementace.
- 3 způsoby náhodného generování CE signálu:
  - náhodně generovaný CE signál.
  - CE signál s konstantní střídou,
  - CE signál s proměnnou střídou.

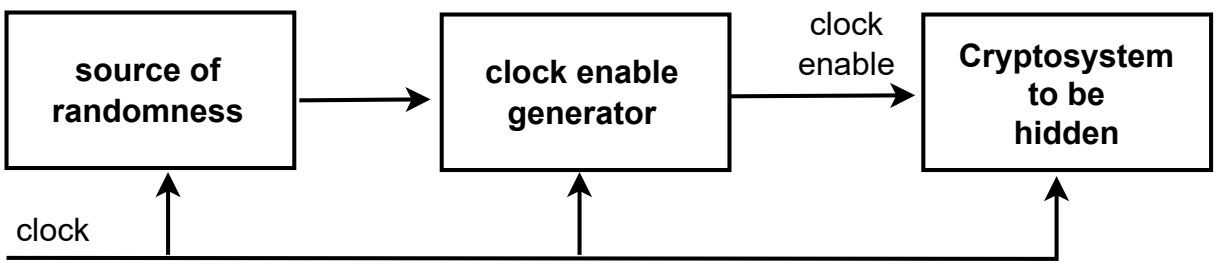


Figure: Blokové schéma implementace.

Experimentální implementace skrývání v časové oblasti

- Proměnná doba vykonávání pomocí náhodně generovaného CE (clock enable) signálu.
- Univerzální způsob implementace.
- 3 způsoby náhodného generování CE signálu:
  - **náhodně generovaný CE signál**,
  - CE signál s konstantní střídou,
  - CE signál s proměnnou střídou.

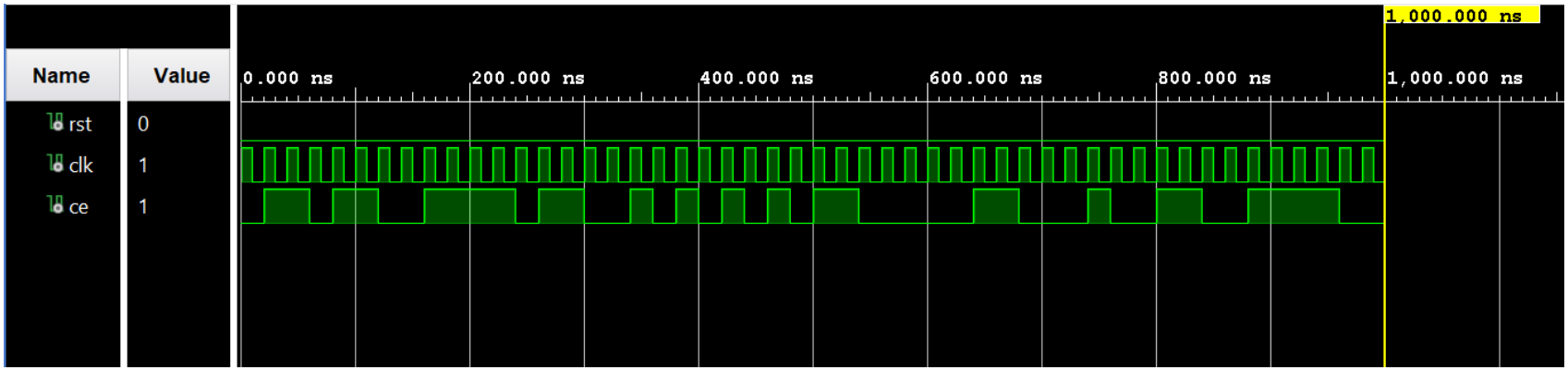


Figure: Náhodně generovaný CE signál.

Experimentální implementace skrývání v časové oblasti

- Proměnná doba vykonávání pomocí náhodně generovaného CE (clock enable) signálu.
- Univerzální způsob implementace.
- 3 způsoby náhodného generování CE signálu:
  - náhodně generovaný CE signál,
  - **CE signál s konstantní střídou**,
  - CE signál s proměnnou střídou.

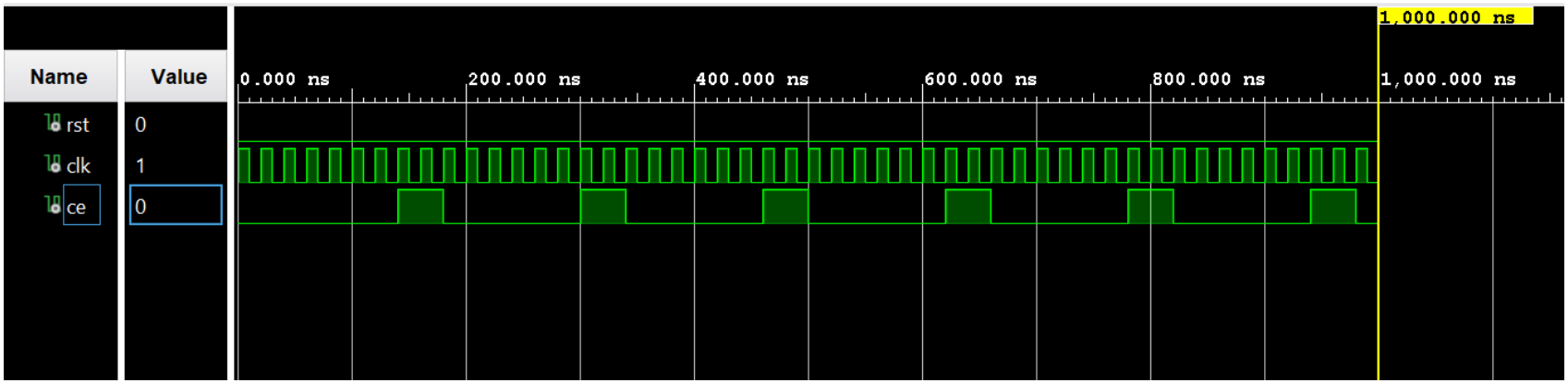


Figure: CE signál s konstantní střídou 1.

Experimentální implementace skrývání v časové oblasti

- Proměnná doba vykonávání pomocí náhodně generovaného CE (clock enable) signálu.
- Univerzální způsob implementace.
- 3 způsoby náhodného generování CE signálu:
  - náhodně generovaný CE signál,
  - **CE signál s konstantní střídou**,
  - CE signál s proměnnou střídou.

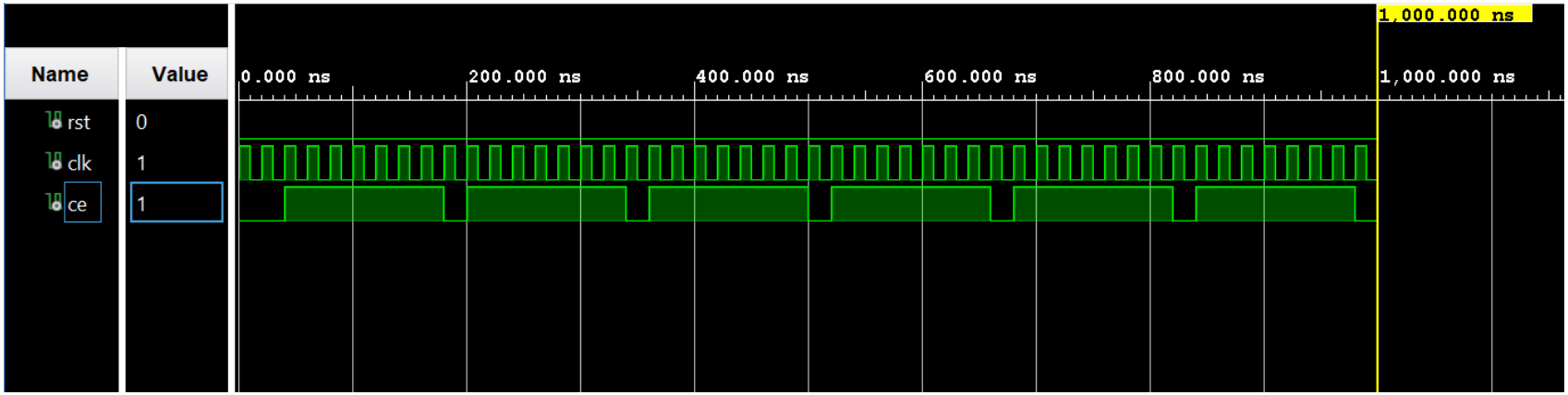


Figure: CE signál s konstantní střídou 2.

Experimentální implementace skrývání v časové oblasti

- Proměnná doba vykonávání pomocí náhodně generovaného CE (clock enable) signálu.
- Univerzální způsob implementace.
- 3 způsoby náhodného generování CE signálu:
  - náhodně generovaný CE signál,
  - CE signál s konstantní střídou,
  - **CE signál s proměnnou střídou**.

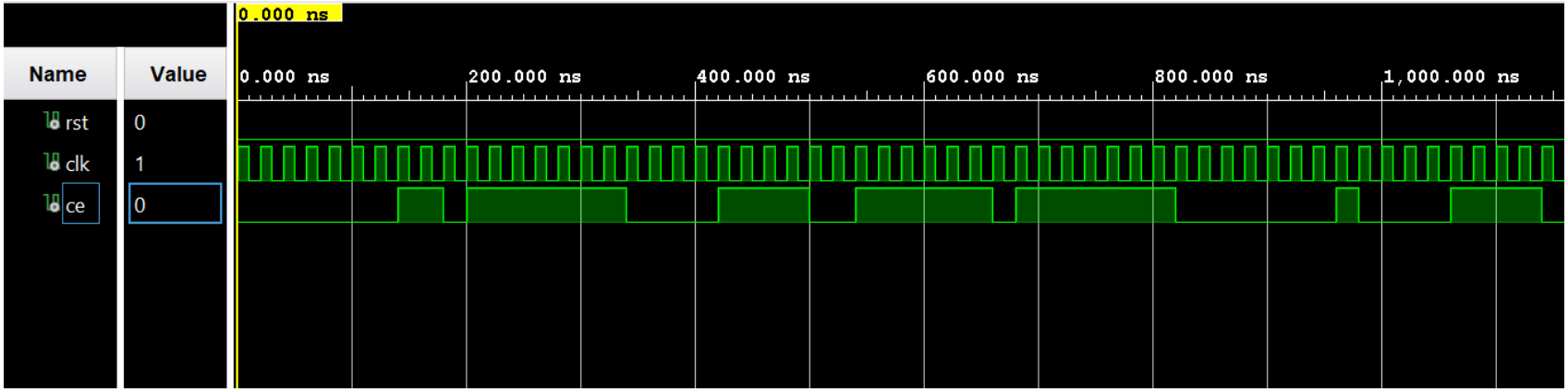


Figure: CE signál s proměnnou střídou.

Další postup

- Validace protiopatření: Generování náhodných čísel jakožto ochraně proti vložení chyby
- Zhodnocení protiopatření z pohledu efektivity (časová, počet HW zdrojů).
- Přiřazení vhodných ochran a postupů v rámci best practice HW implementací kryptografických operací.

Požadavky na testbed

- Výzkum **požadavků na testbed** a jeho specifikace.
- Analýza vlastností dostupných řešení (výhody x nevýhody),
- desky SAKURA (G, GIII, W), ChipWhisperer, vlastní DPA board a jiné.

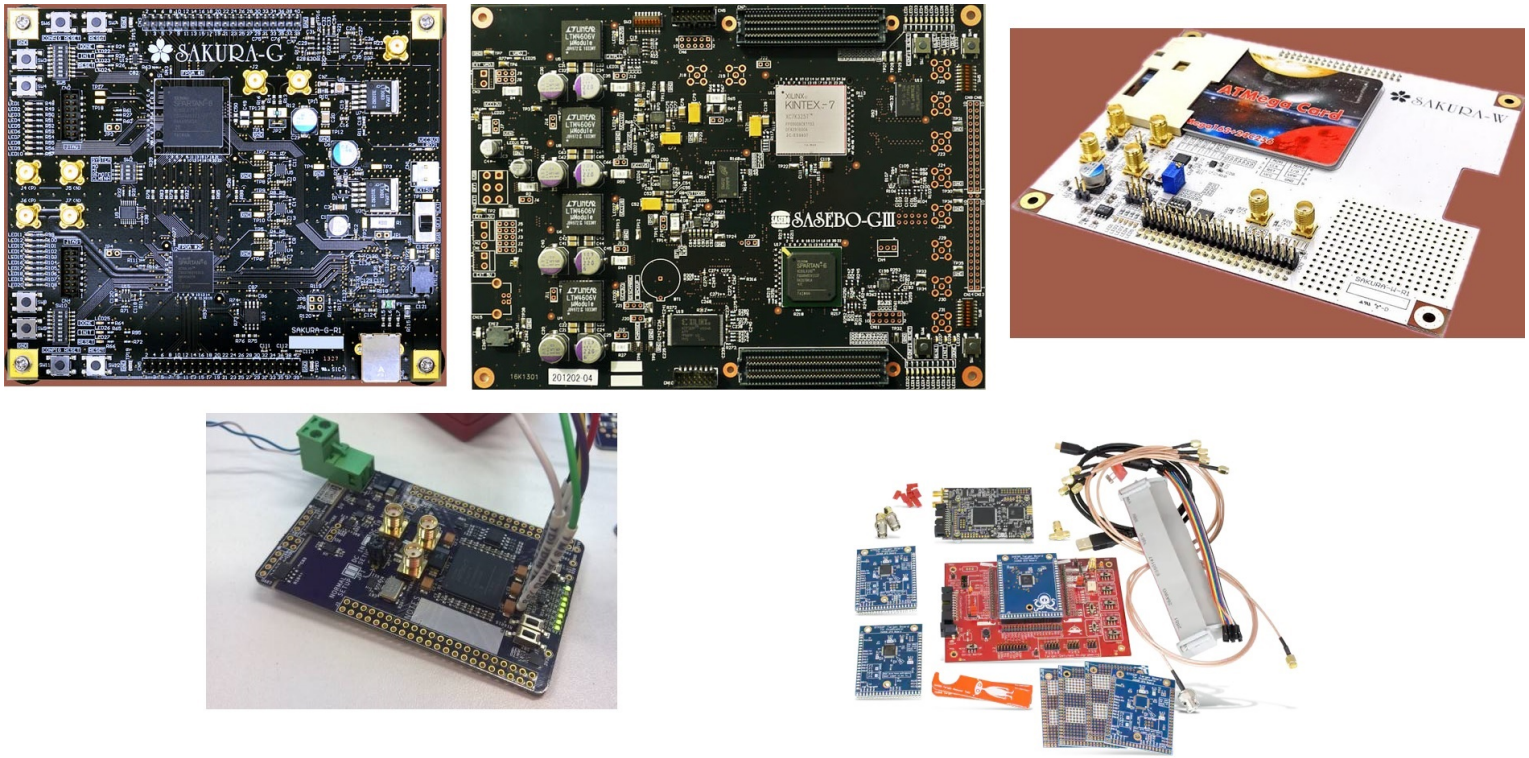
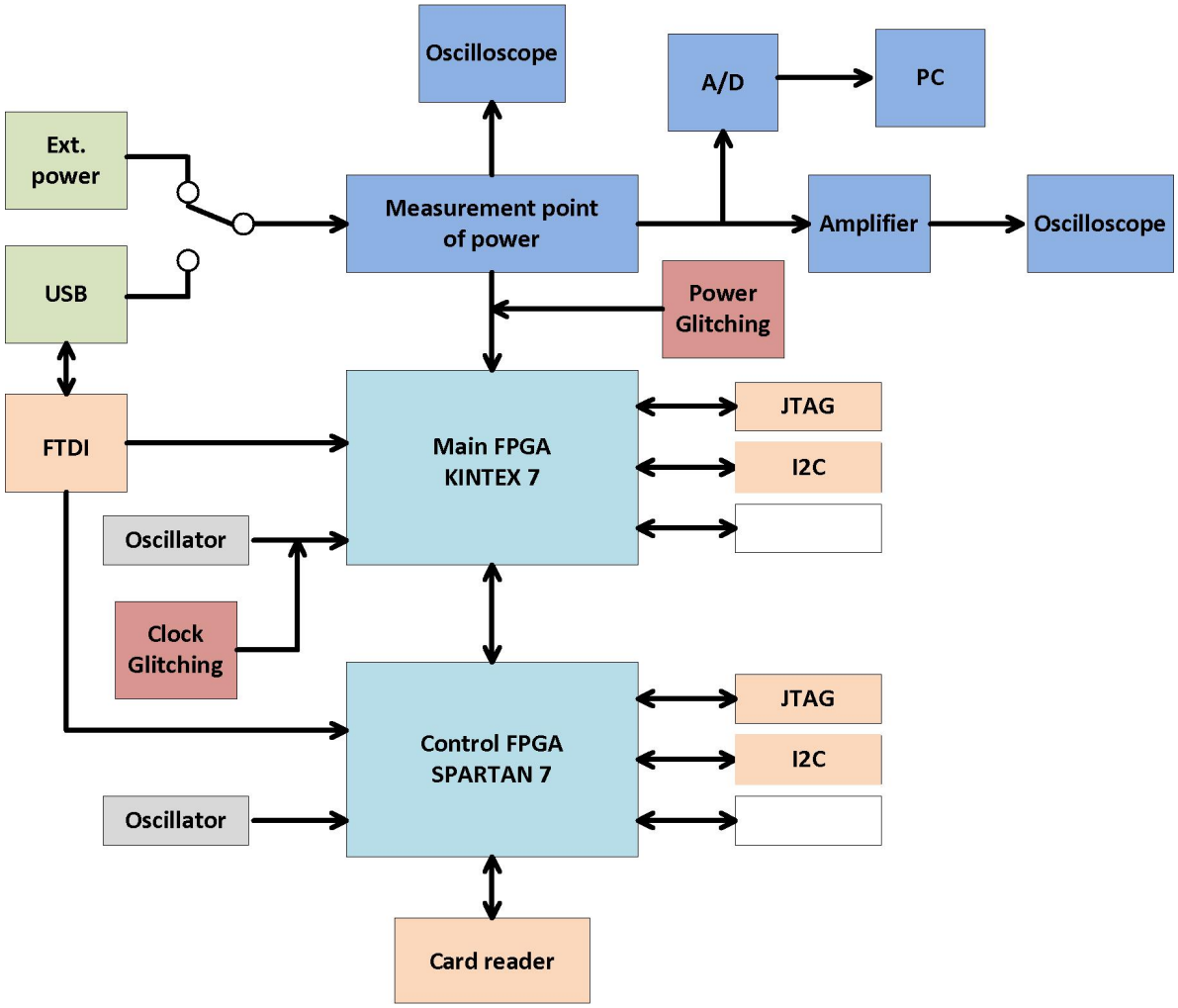


Figure: Analyzované desky na VUT a ČVUT.

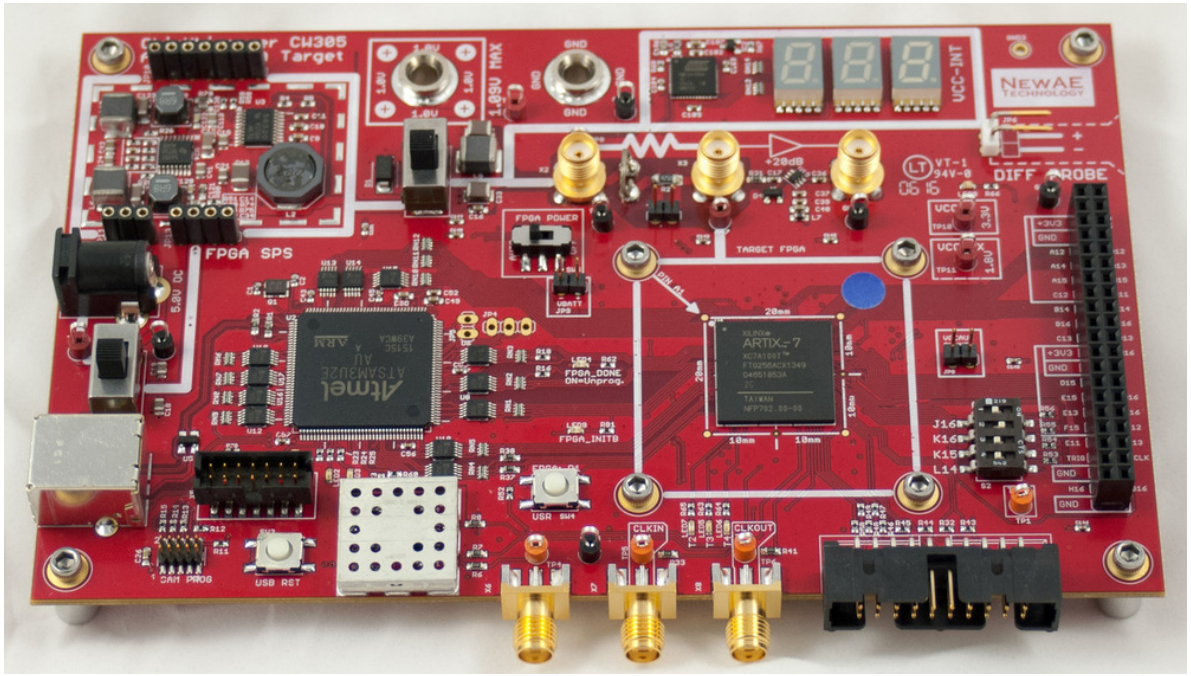
Specifikace požadavků a blokové schéma

- Specifikace požadavků **pomocí blokového diagramu**.
- Nutný zesilovač, FPGA k akceleraci měření, čtečka čipových karet . . .



Výběr desky a rozšíření

- Na základě podrobných analýz a schůzek VUT v Brně, ČVUT a MU rozhodnuto pro řešení využívající **NAE-CW305-04-7A100-0.10-X**.
- **Dostupnost podpory**, cenově dostupné a splnění většiny požadavků.
- Realizace vlastního firmware a čtečky čipových karet.



Další postup ve specifikaci a návrhu testbedu

- **Vlastnosti**: Analýza odolnosti pro HW a SW implementace (FPGA a čipová karta), FPGA pro akceleraci měření, napájení USB/ext., clock a power glitches, programátor FPGA, zesilovač na desce a možnost využití A/D bez OCS.
- **Jaké jsou požadavky NÚKIB** ?
- Například jiné případy užití pouzdro pro ASIC čip ?
- Požadavky na funkcionalitu měření (např. masky úpravy firmware FPGA a SW na PC).

Výzkum vhodných metod AI pro profilace

- Spolupráce s **Xiaolu Hou** a Jakubem Brierem,
- Ze současného stavu zvolena síť **XCM** (An Explainable Convolutional Neural Network for Multivariate Time Series Classification).
- Pro výzkum jsou nyní využity veřejné datasety: **ASCAD**, AES RD (náhodné zpoždění) a AES HD.
- Sestaven testbed (GIGABYTE RTX 3080 TURBO 10G LHR) včetně softwarových nástrojů Keras, TensorFlow a pytorch.

This work is supported by
Ministry of the Interior of Czech Republic
under grant VJ02010010

MANY THANKS

THANKS