08. Diferenciální analýza spotřeby

Dostali jste sadu měření spotřeby čipové karty, která provádí šifrovací operace AES. Šifrování bylo provedeno 100krát, a pro každé z nich byl zaznamenán průběh spotřeby. Všechny potřebné soubory jsou v archivu dpa_student_v2.zip (../files/dpa_student_v2.zip) .

Soubory jsou:

- `traces.bin` : Binární hodnoty vzorků tvořících změřené průběhy, jeden za druhým, každý vzorek 1 byte
- `traceLength.txt` : textový soubor obsahující délku 1 průběhu
- `plaintext.txt` : datové bloky otevřeného textu, ve formě hex-řetězců, jeden blok na každém řádku, bajty odděleny mezerami
- `ciphertext.txt` : podobně jako plaintext
- `dpa_student.ipynb` : Jupyter notebook obsahující kostru řešení a užitečný kód
- `dpa_bi-hwb_student.nb` (nebo podobný): Mathematica notebook obsahující kostru řešení a užitečný kód (pokud nemáte rádi Python)

Dokončete Jupyter nebo Mathematica notebook:

1. Zobrazte jeden nebo několik málo kompletních průběhů
2. Vyberte část průběhů, která je zajímavá pro DPA, viz přednášku o útocích postranními kanály
3. Změňte program tak, aby nahrával pouze zajímavé části všech průběhů
4. Doplňte program tak, aby prolomil první bajt klíče
5. Zobrazte průběh korelace pro správnou hypotézu klíče, pozorujte špičky korelačního koeficientu
6. Zobrazte průbeh korelace pro špatnou hypotézu, porovnejte
7. Doplňte kód tak, abyste prolomili celý klíč
8. Ověřte klíč pomocí jednoho páru bloků otevřený/šifrový text. (Můžete použít i webovou AES kalkulačku, pak o tom aspoň učiňte zápis, odkaz, screenshot…)

Řešení předveďte a nahrajte na Gitlab. Velký soubor `traces.bin` nahrávat nemusíte.

Pozn. Pro jistotu ještě nechávám kopii archivu i na jiném serveru

```
!wget https://users.fit.cvut.cz/bucekj/dpa_student_v2.zip
!unzip -j dpa_student_v2.zip
```