Návrh a kryptoanalýza šifier - Zadanie 9

Peter Čuřík

5. decembra 2021

1 Differential Power Analysis - DPA

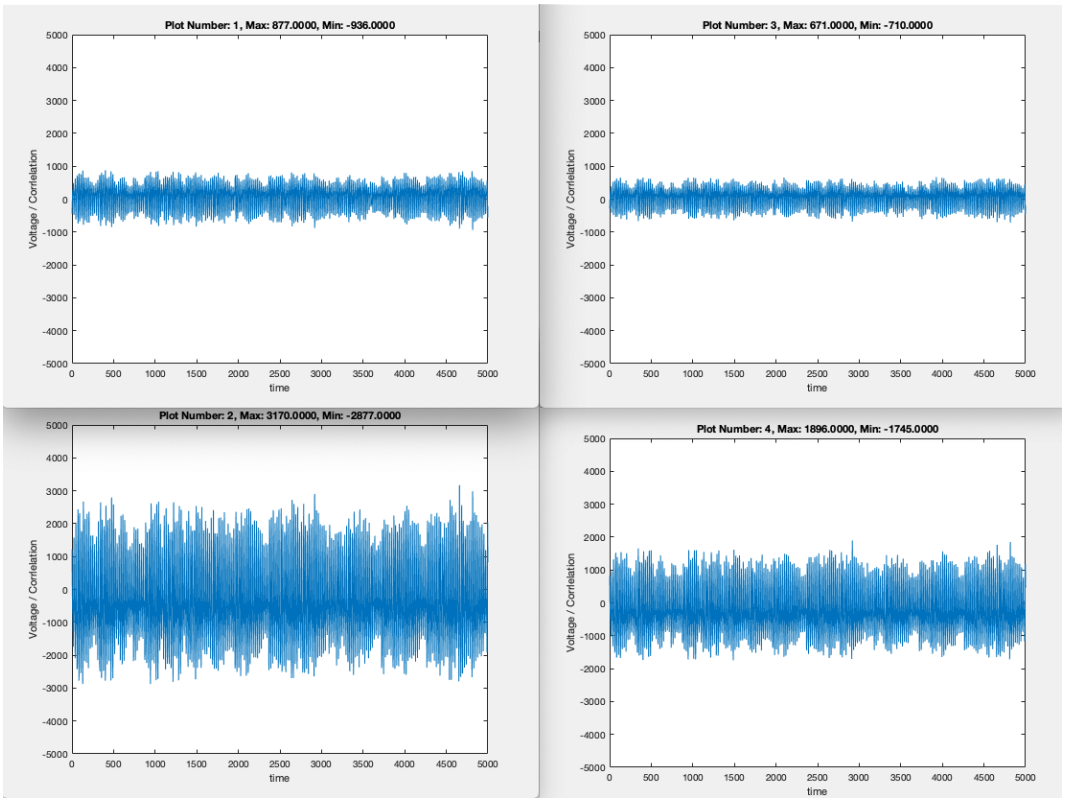
Na základe dokumentu *Guided Analysis of WS1* bol vykonaný DPA útok na odhalenie kľúča šifry AES. Pozorovaný bol výstup z S-boxu inštrukcie SubBytes.

1.1 Úloha 3.1: Attacking Different Bits - Kocher Method

Pomocou Kocherovej metódy bol pozorovaný konkrétny bit výstupu z S-boxu. Druhý vstup funkcie `bitget()` nám dovoľuje konfigurovať sledovaný bit.

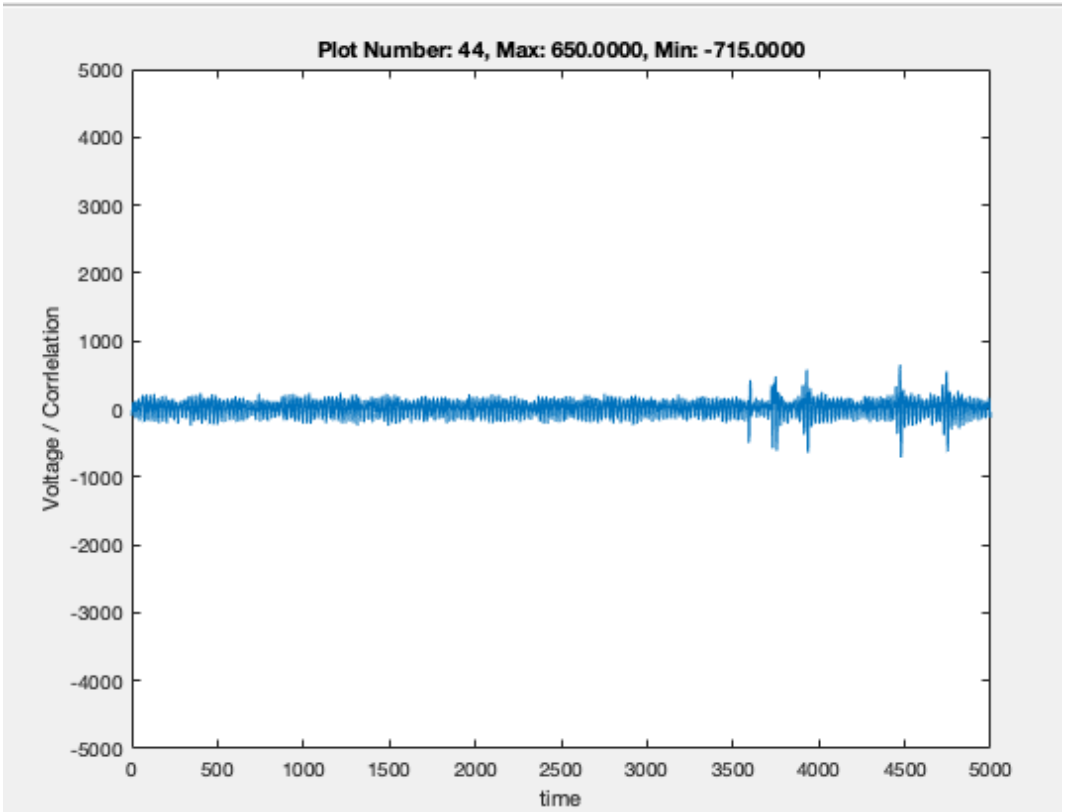
Kocherova metóda pracuje s dvomi vzorkami dát, jedna predikuje výstupný sledovaný bit = 0, druhý očakáva opačnú hodnotu. Z meraní oboch vzoriek sú vypočítané mediány a namerané hodnoty sú vzájomne odčítané. Hľadáme vysoké rozdiely (výchylky v grafe), ktoré indikujú potenciálne správny bajt kľúča.

Niektoré hypotézy na kľúč sú s vysokou pravdepodobnosťou nesprávne. To vieme usúdiť z grafov. Napríklad, v nasledujúcich grafoch nevidíme nijaké výrazné výchylky:



Obr. 1: Niektoré nepravdepodobné kľúče - Kocherova metóda.

Najvýraznejšie výchylky pozorujeme pri kľúči s poradovým číslom 44, teda ide o decimálnu hodnotu 43 (hex: `0x2B`). Viď obrázok:



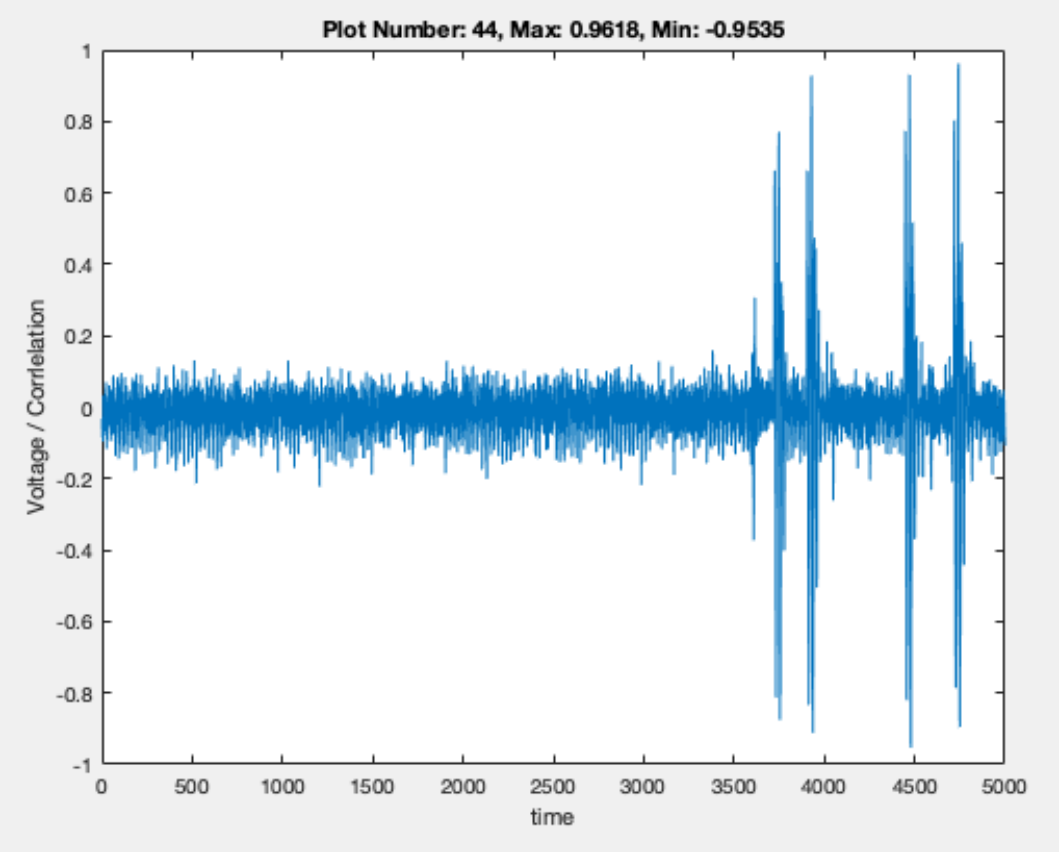
Obr. 2: Najpravdepodobnejší kľúč - Kocherova metóda.

Všetky výsledky a analýza ukázaná vyššie vyplynuli z pozorovanie most signifficant bitu. Medzi ďalšími pozorovanými bitmi bolo možné vidieť uspokojivé výsledky pri bitoch číslo 3 a 4.

1.2 Úloha 3.2: Attacking Multiple Bits - Correlation Method

Korelačná metóda narozdiel od Kocherovej počíta korelačné koeficienty. Je to matematicky komplexnejší výpočet ako rozdiel dvoch vzoriek (Kocher), preto aj DPA trval časovo dlhšie. Výsledky sú avšak omnoho presnejšie. Hodnoty osi y majú väčšiu výpovednú hodnotu. Hodnota 1 (resp. -1) definuje silnú previazanosť dvoch javov. Na druhej strane, Kocherova metóda vykonáva operáciu rozdielu dvoch vzoriek. Tam záleží od situácie, aká hodnota je rozhodujúca. Avšak z korelačného koeficientu vieme odčítať pravdepodobnosť udalosti vždy rovnako, nezávisle od konkrétneho prípadu.

Týmto úvahám odpovedajú výsledky. V porovnaní s Obr. 2 je korelačná metóda oveľa viac výpovednejšia a jasne ukazuje kandidáta na kľúč - viď obrázok nižšie. Hodnota korelácie je skoro rovná jednej, teda máme vysokú pravdepodobnosť, že práve tento kandidát je ten správny.



Obr. 3: Najpravdepodobnejší kľúč - Korelačná metóda.