Side-channel attacks

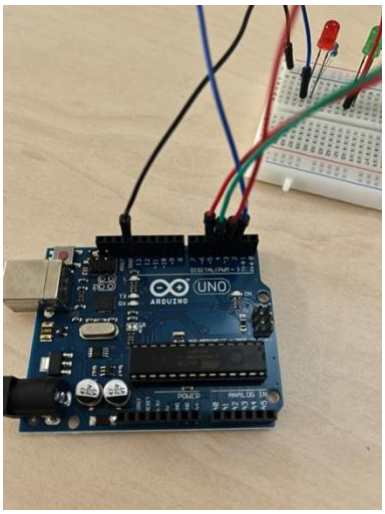
V kryptografii sú *side-channel attacks* útoky, ktoré sa snažia zneužiť informácie, ktoré priamo unikajú z fyzickej implementácie systému, na rozdiel od kryptoanalýzy, ktorá sa snaží nájsť slabiny v matematickej štruktúre algoritmu.

V tomto projekte som sa zaoberal *elektromagnetickými útokmi (EMA)*. Komponenty systému pri zmene prúdu generujú striedavé magnetické pole, ktoré ak je dostatočne silné, môže byť detegované a následne analyzované. Tieto útoky sú zvyčajne neinvazívne, teda môžeme ich uskutočniť pomocou pozorovania daného zariadenia. Zariadenia, ktoré nie sú zabezpečené voči takýmto útokom, môžu byť náchylné na zneužitie citlivých informácií.

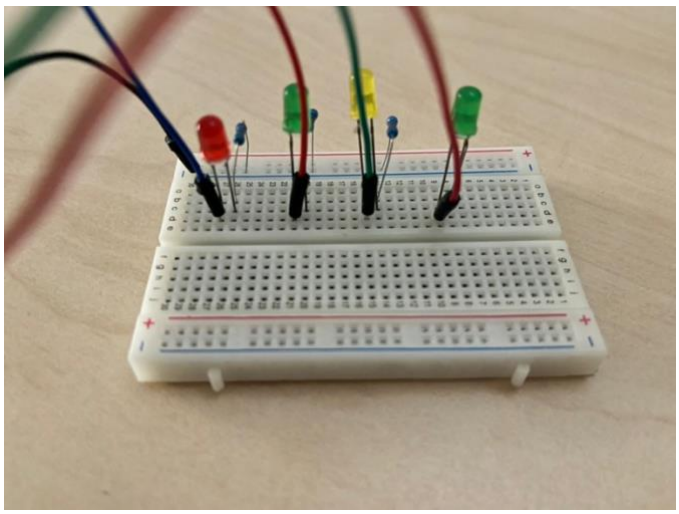
Report – zimný semester

Počas zimného semestra som sa zoznamoval s mikrokontrolérom *Arduino UNO R3* na účely odmerania jeho elektromagnetického vyžarovania pri vykonávaní aritmetických operácií. Cieľom bolo zistiť, či vieme nájsť medzi operáciami a vyžarovaním koreláciu, ktorú by sme vedeli neskôr využiť.

Vytvoril som jednoduché programy, v ktorých sa striedali aritmetické operácie +, -, *, / a pri vykonaní danej operácie sa rozsvietilo jej príslušné LED svetielko, aby sme pri meraní vedeli rozpoznať, ktorá operácia bola vykonaná.



Obrázok 1 - Arduino UNO R3



Obrázok 2 - Breadboard so zapojenými LED svetielkami

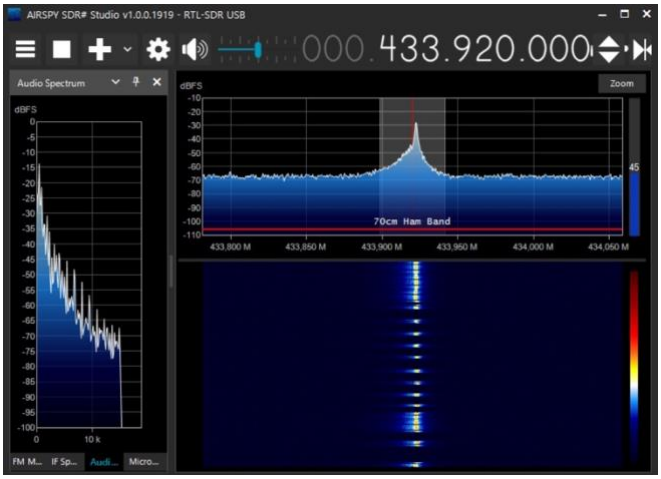
Pri meraní sme so školiteľom použili osciloskop *Tektronix MDO4104C*. Jednu testovaciu sondu sme napojili na kryštál Arduina, ktorý sa nachádza vedľa jeho čipu a druhu sondu na anódu daného LED svetielka, aby sme vedeli, kedy bola operácia vykonaná. Výsledky tohto merania neboli presvedčivé, nakoľko nebola viditeľná korelácia medzi jednotlivými operáciami a zmenami napätia mikrokontroléru.

Následne sme sa snažili odmerať rádiové frekvencie (RF) kryštálu pri daných operáciách pomocou *near-field* sondy, no výsledky boli rovnaké ako pri predošlom meraní.

Po neúspešných meraniach som sa začal venovať odpočúvaniu obrazoviek pomocou *softvérovo definovaných rádií (SDR)*. Cieľom bolo vyčítať, čo je na obrazovke zariadenia bez toho, aby sme na danú obrazovku priamo videli. Pomocou SDR vieme zachytiť elektromagnetický signál, ktorý je posielaný káblom od zariadenia do obrazovky.

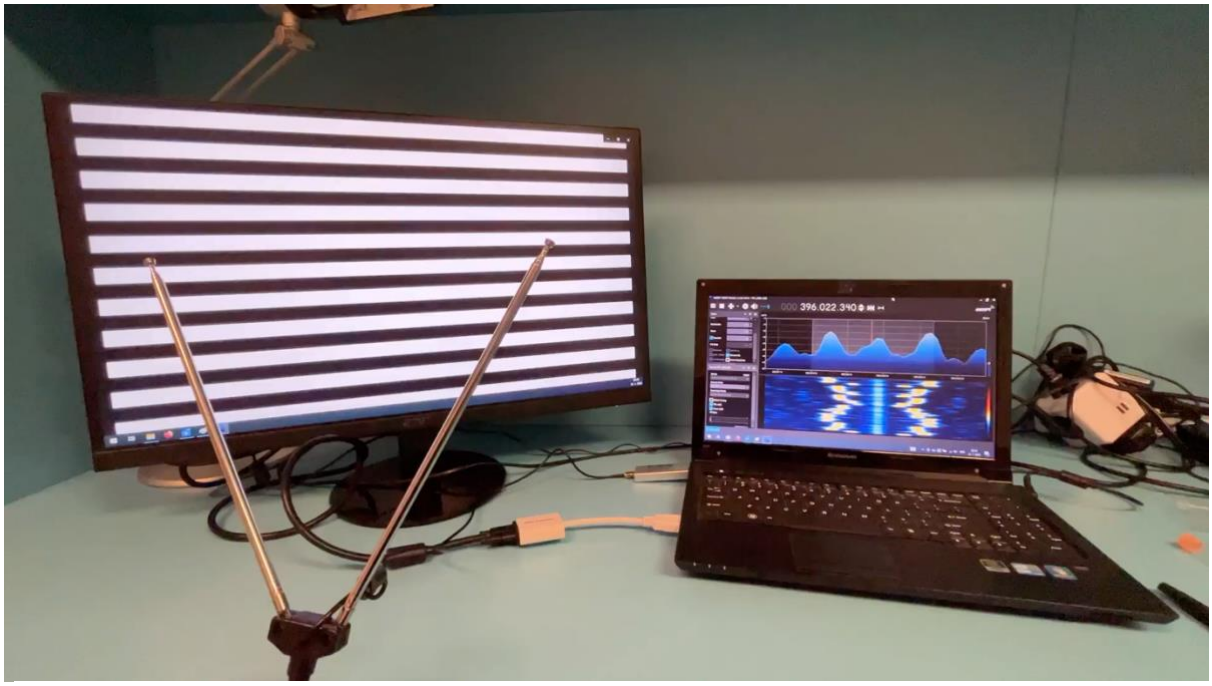
Zoznamoval som sa s *RTL-SDR*, ktoré sa radí medzi lacné SDR. Pri učení, ako sa s SDR pracuje som využíval aplikáciu *SDR#*.

Obrázok 3 - RTL-SDR kit



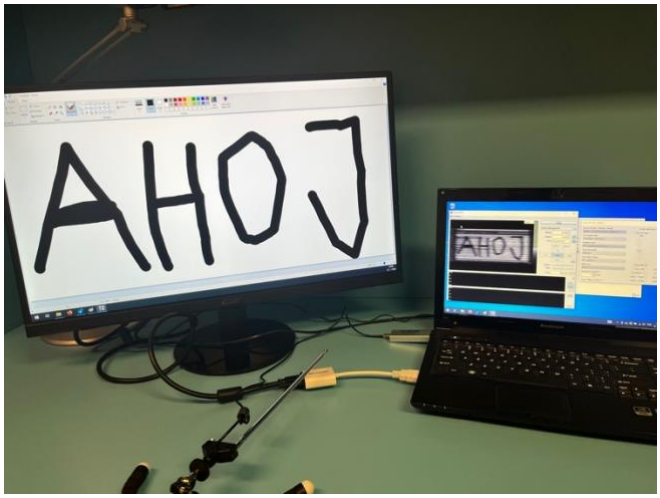
Obrázok 4 - Posielanie signálov pomocou tlačítka s frekvenciou 433,920 MHz

Následne som na monitore, ktorý bol napojený k PC pomocou redukcie z HDMI na VGA a VGA káblu, začal zobrazovať čierno-biele pásiky, pomocou ktorých som dokázal nájsť frekvenciu, pri ktorej z káblu uniká elektromagnetické vyžarovanie. Pri nájdení správnej frekvencie začne hrať melódia z rádia (video). Našiel som, že pri mojom set-upe uniká najviac signálov pri frekvencii ~396 MHz.



Video 1 - Zachytenie unikajúceho signálu z káblu

Po nájdení správnej frekvencie som využil software toolkit *TempestSDR*, ktorý dokáže z nájdených elektromagnetických vĺn vyhotoviť čierno-biely obraz v reálnom čase pomocou mapovania sily elektromagnetickej vlny k jej príslušnému odtieňu čiernej.



Obrázok 5 - Využitie TempestSDR k vyhotoveniu obrazu

Pri meraní som narazil na viacero skutočností. Prvé merania som vykonával bez redukcie z HDMI na VGA. Elektromagnetické vlny boli pri týchto meraniach veľmi slabé – môj VGA kábel je pravdepodobne ošetrený voči únikom elektromagnetických vĺn. Pochopiteľne, aj vyhotovený obraz cez TempestSDR bol veľmi zlý a nepoužiteľný.

Po zapojení redukcie sa sila elektromagnetických vĺn drasticky zväčšila. Možno usúdiť, že pri konverzii je únik elektromagnetických vĺn zväčšený a pri použití redukcie sa môžeme vystaviť nebezpečenstvu pri práci s citlivými informáciami na obrazovke.

Následne som testoval, aký dobrý obraz dokážeme vyhotoviť s rastúcou vzdialenosťou medzi anténou a káblom. Obraz bol prakticky rovnaký pri vzdialenostiach do 30 cm. Pri väčších vzdialenostiach sa obraz pochopiteľne zhoršoval až kým úplne nezanikol.

Študent: Filip Tuch
Školiteľ: RNDr. Richard Ostertág PhD.