

Záver letného semestra:

Použili sme vytvorenú knižnicu z minulého semestra na analyzovanie signálov z áut: Kia, Oktavia, Karoq 2018, Karoq 2023. Signáli sme nahráli pomocou GQRX a RTL-SDR. Pre Karoqi sme nahráli zatváranie, otváranie a kufor. Pre Oktaviu otváranie a zatváranie a pre Kiu len zatváranie.

Knižnicu sme rozšírili o ďalšie potrebné funkcie pre analýzu.

Pri porovnaní Karoqov sme zistili, že počas rokov, zmenili len inicializačnú/synchronizačnú sekvenciu, ktorá bola pridaná na začiatok ak sa dlho nevysielal signál z ovládania pre rok 2023. Identifikačné číslo je uložené na 0 - 461 kde id sú:

Karoq 2018:

```
0x2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaab4cd55355
```

Karoq 2023:

```
0x2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaab2b55534a
```

Button bity sú pri Karoqoch na 463 - 466 pričom pre nadobúdajú hodnotu:

otváranie: 0110

zatváranie: 1001

kufor: 1010

Separátor sa môže nachádzať na bitoch 477 - 478.

Celková dĺžka jednej sekvencie je 622.

Pri Oktavii bol signál kľúču štruktúrovo rozdielny. Na oddelenie vysielanie sekvencií pri jednom stlačení ovládania bolo použité striedanie 1 a 0 namiesto 0. Je tiež možné že niektoré striedanie bolo súčasťou identifikátora, keďže ten sa nachádza na 0 - 29 avšak toto striedanie malo rôznu dĺžku medzi jednotlivými sekvenciami. Preto sme každé striedanie odstránili. Identifikátor pre Oktaviu je 0x36da9556.

Button bit sa pravdepodobne nachádza na 30 - 31, keďže je nepravdepodobné že by sa nachádzal niekde v strede sekvencie (bitov pre button bolo, viac a preto sme sa rozhodli predpokladať, že button bit bude nasledov hneď po identifikátore).

Je tiež možné že checksum sa nachádza na 156 - 159, keďže to bolo 2. najdlhšia sekvencia po identifikátore, ktorá sa opakovala.

Celková dĺžka jednej sekvencie je 170.

[illegible]

Tiež bola nájdená len jedna subsekvencia ktorá mala 2. najdlhšiu dĺžku, 468 - 537, čo predpokladáme, že bude checksum. Zvyšné nájdené nezmenené bity sme označili ako separátori, ale je možné, že sú rovnaké len z dôvodu malej vzorky kľúčov.