

**Sunday, January 13, 2019**

Since acquiring target control via **Spy-Bi-Wire** and **LaunchPad** I am able to inspect and dump flash, disassemble and program back the flash to original stage

## Dumping Flash

In .hex intell format that is usable to programming it back:

In .raw binary format

## Reprogramming back to original

Use .hex Intel format

## Disassembling flash

## Things learned from the disassembly:

- Operating mode is low power state LM3 and waking on interrupt from key press (connected to P2.7). However, LM1 is also entered after key press, perhaps to await for another key press before going LM3. Does this save energy?
- Apparently, the randomization of remote's ID is done via...an ADC reads which ends up as middle 4 bytes of the message (each ADC read uses only lowest bit). That likely saves mfg time instead of individually programming each remote with ID - this is smart!
- The SPI communication with CC2500 is bit-banged (not using build-in MSP's SPI engine). This is likely due to messed up hw design - the MOSI/MISO lines are switched from their default pins:

Posted by **Unknown** at 3:59 PM

## Post a Comment

Newer Post

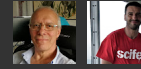
Home

Older Post

Subscribe to: [Post Comments \(Atom\)](#)

## Followers

## Mga sumusubaybay (2)



Sundin

## About Me

 Unknown

## Blog Archive

▼ 2019 (5)

▶ March (3)

▼ January (2)

▶ 2018 (5)

▶ 2015 (1)

▶ 2014 (3)

▶ 2011 (1)

▶ 2010 (2)

▶ 2009 (4)

Simple theme. Powered by [Blogger](#).