# Nintendo Switch Modchip Research

## General Q&A

- What is the BCT?
  - switchbrew documentation
  - Boot configuration table
  - Tells hardware where to find the bootloader

## Documentation

- Exploits
  - hardware / kernel software
  - userland
- Chips
  - FPGA
    - Model: ICE40LP1K-CM49TR
    - Manufacturer: Lattice
    - Resources:
      - Datasheet
      - iCE40™ LP/HX/LM Family Handbook
      - Tools for exploiting warm/cold boot in iCE40 FPGAs
  - MCU
    - Model: GD32F350CBT6
    - Manufacturer: GigaDevice Semicon Beijing
    - Resources:
      - Datasheet
      - Manual
      - Firmware guide

## Current Efforts

- MCU firmware
  - Spacecraft-NX
- FPGA firmware
  - Unknown but could be potentially dumped from original SX modchip
  - Maybe loaded via a bitstream on boot or from factory programming

# Community Resources

- YouTube video going over Nintendo Switch's hardware security
    - Timestamp #1: Boot sequence (23:26)
- Reddit discussion on SciresM's effort to bypass firmware for Gateway modchip
    - Think early prototype of Spacecraft-NX
    - Comment #1: Modchip glitches BCT to point to custom payload

    *"It works via hardware glitching like the Xbox 360's rgh mod chips. Specifically (this is second hand knowledge from someone I know who was reverse engineering it) it overwrites the BCT to point to a custom boot loader, when the Switch check the BCT it glitches the signature check and then it does it again once the bootloader is in iram. Bare in mind that he told me this ages ago and I haven't personally reversed it (not that I have the skills to anyway) so I may have got one or two things wrong but that's roughly how it works."*

    - Comment #2: Modchip glitches BCT hash check

    *"The modchip itself is an exceptional piece of work, and stealing keys has nothing to do with its actual operation. TX were just being mean/protecting their 'trade secrets' by intentionally disabling the Switch unless you use SXOS.*

    *The modchip also has nothing to do with RCM -- It glitches the BCT hash check, and allows you to run whatever you want as boot0. For all the Switch knows, it's running fully signed, fully stock firmware; it doesn't have any strange flags set, it's not in an alternate mode, your payload runs with exactly the same hardware configuration as N's code."*

- Paper on Injecting Software Vulnerabilities with Voltage Glitching by Yifan Lu
- Reddit discussion about developing an open source modchip
    - Several comments discussing the legality of such a project
    - Since the modchip is breaching the trustzone on the Switch, this could lead to any software / hardware aiding in the process being taken down by DMCA
        - Needs source (saw this in another thread)
- Article discussing Mariko hacking via SX modchip
- sthetix's tweet about a blank HWFLY modchip he received
    - Had to flash using GD programmer instead of normal DFU method
- Chinese forum post on HWFLY chips
    - Discussion about pricing and firmware