Reverse engineering MT8173 PCM firmwares and ISA for a fully free bootchain

Embedded Freedom

Paul Kocialkowski
contact@paulk.fr

Thursday October 26th 2017

EUROPEAN COREBOOT CONFERENCE 2017

MediaTek MT8173

MediaTek MT8173

Presentation, Support and Devices

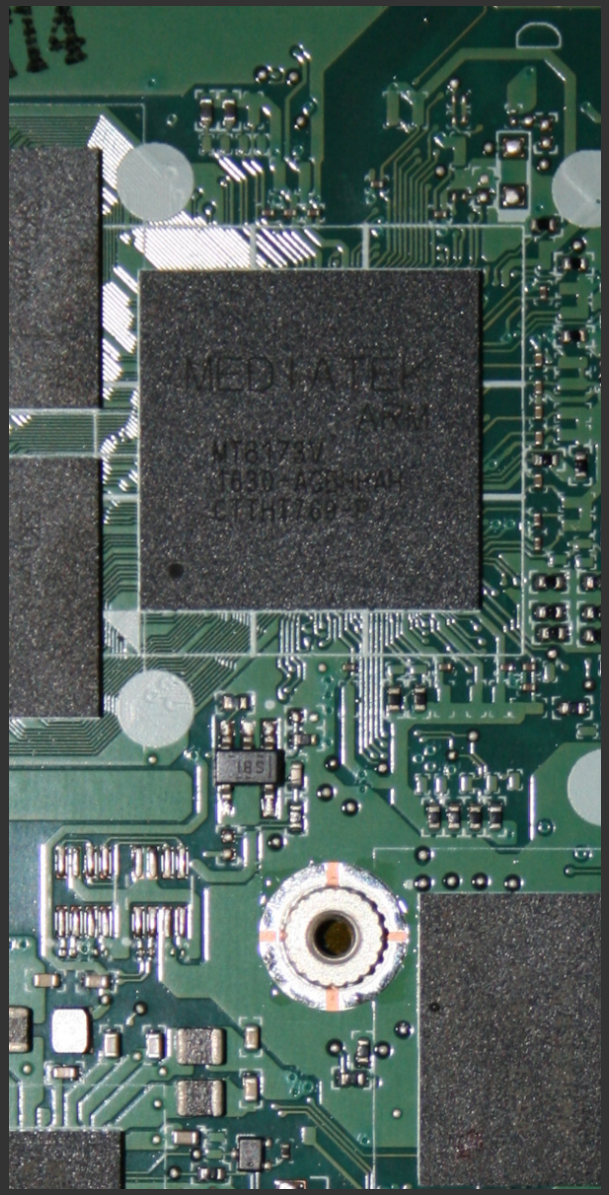
MT8173 SoC Presentation

ARMv8 SoC from MediaTek:

- 2x Cortex-A72 CPU
- 2x Cortex-A53 CPU
- PowerVR GX6250 GPU
- No onboard modem/baseband

Sales:

- Available Q1 2015
- High-end tablets



MT8173 Support from MediaTek

Releases from Mediatek:

- No SDK/BSP available
- No Linux kernel or boot software source code
- No datasheet or technical reference manual

Access to software sources and documentation:

- Available for a fee, under NDA
- MediaTek is known to violate the GPL
- History of horribly broken code

MT8173 Support in Chromium OS

Interest from the Chromium OS (CrOS) project:

- Previous ARM(v7) platforms:
  Exynos, Tegra K1, RK3288
- First selected ARM(v8) platform (2015)
  Followed by RK3399

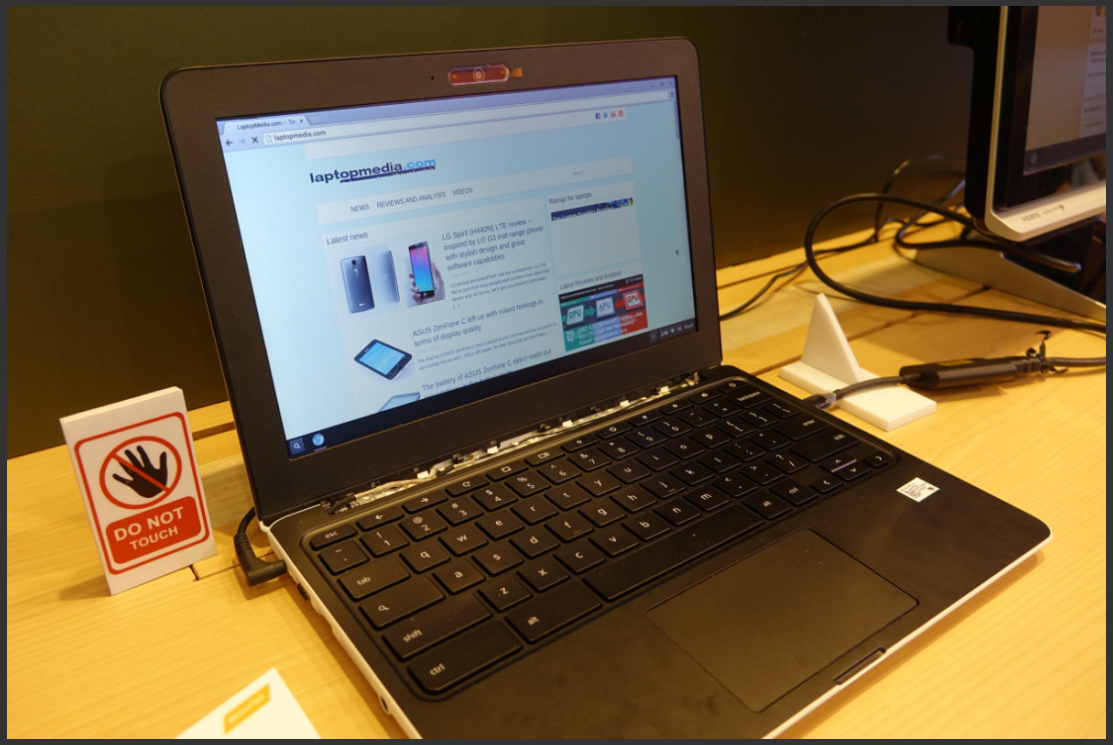
Support in CrOS boot projects:

- coreboot: *boot software*
- Depthcharge: *coreboot payload*
- ARM Trusted Firmware: *TEE*
- CrOS-EC: *EC firmware*
- Linux: *kernel*

MediaTek MT8173

CrOS Devices

MediaTek Chromebook



- Codename: oak
- Reference development Chromebook (supposed)
- Not for sale

Acer Chromebook R13 CB5-312T

- Codename: elm
- Convertible Chromeboook
- Released September 2016

Lenovo N23 Yoga/Flex 11 Chromebook

- Codename: hana
- Convertible Chromeboook
- Released March 2017

MediaTek MT8173

Boot Software and Freedom

ARMv8 CrOS Boot Process

Normal boot process:

1. BootROM (Silicon → SRAM)
2. coreboot bootblock (RO SPI flash → SRAM)
3. coreboot verstage (RO SPI flash → SRAM)
4. coreboot romstage (RW SPI flash → SRAM)
5. coreboot ramstage (RW SPI flash → DRAM)
6. ARM Trusted Firmware (RW SPI flash → Secure DRAM)
7. Depthcharge (RW SPI flash → DRAM)
8. Linux (Storage → DRAM)

Handlers :

- ARM Trusted Firmware PECI handlers (SMC)

Free Boot Software

Support in upstream projects:

- coreboot: **complete** upstream support
- Depthcharge: **upstream** (ToT) support
- ARM Trusted Firmware: **complete** upstream support
- CrOS-EC: **upstream** (branch) support
- Linux: **early** upstream support

Blobs in the boot process:

```
arm-trusted-firmware:
plat/mediatek/mt8173/drivers/spm/spm_hotplug.c
plat/mediatek/mt8173/drivers/spm/spm_mcdi.c
plat/mediatek/mt8173/drivers/spm/spm_suspend.c
```

MT8173 Proprietary Blobs

Proprietary software in the boot process:

- SPM firmwares in ARM Trusted Firmware

All other aspects of boot supported by free software!

Non-free software in firmwares/kernel drivers/userspace:

- VPU decoding/encoding firmwares
- GPU support libraries (PowerVR)

Dealing with non-free software:

- VPU can be **avoided** with CPU decoding/encoding
- GPU can be **avoided** with CPU rendering
- SPM firmwares are **critical** for power management

MT8173 System Power Manager

MT8173 System Power Manager

Introduction

SPM Introduction

Description from ARM Trusted Firmware:

```
plat/mediatek/mt8173/drivers/spm/spm.c:
System Power Manager (SPM) is a hardware module, which controls cpu or
system power for different power scenarios using different firmware, i.e.,
- spm_hotplug.c for cpu power control in cpu hotplug flow.
- spm_mcdi.c for cpu power control in cpu idle power saving state.
- spm_suspend.c for system power control in system suspend scenario.
```

Situation in ARM Trusted Firmware:

- 3 distinct firmwares
- 3 dedicated files
- large arrays of numbers
- `SPDX-License-Identifier: BSD-3-Clause`

Let's liberate PCM firmwares!
(on spare time)

SPM PCM Execution

ARM Trusted Firmware source code details:

- Firmware address written to `SPM_PCM_IM_PTR`
- Firmware length written to `SPM_PCM_IM_LEN`
- PCM registers configuration
- PCM kick

```
/* kick IM to fetch (only toggle PCM_KICK) */
con0 = mmio_read_32(SPM_PCM_CON0) & ~(CON0_IM_KICK | CON0_PCM_KICK);
mmio_write_32(SPM_PCM_CON0, con0 | CON0_CFG_KEY | CON0_PCM_KICK);
mmio_write_32(SPM_PCM_CON0, con0 | CON0_CFG_KEY);
```

The System Power Manager contains a dedicated processor!

MT8173 System Power Manager

Research, Documentation, Requests

Research on the MT8173 PCM

Gathering information about the SPM and PCM:

- Still **no documentation**
- US patent 20140189400A1:

  > *During idle of the processing unit, system and associated method achieving improved power saving by [...] a system power manager (SPM) capable of allocating system resources during idle of processing unit.*

- Linux kernel SCPSYS driver:

  > *The System Power Manager (SPM) inside the SCPSYS is for the MTCMOS power domain control.*

- **No substantial** information

Tracking PCM Firmwares

MediaTek PCM firmwares and logic:

- Found in: MT6797 (Helio X20), MT6795 (Helio X10), MT6752, MT6589, MT6582, MT6572, ...
- Integrated in the kernel
- Probably widely used
- Size is usually 0x200-0x400 words
- Recent firmwares are **the biggest**
- No additional information

Needed answers:

- PCM ISA: custom/public?
- Precise role of the PCM firmwares?

Requesting Help

Asking the right people:

- MediaTek engineers (ATF commits):

  However, for this PCM specifically, we consider the negative impact of leaking MTK's confidential info is more significant to the positive benefit of open sourcing it.

- Google engineers (CrOS commits):

  Sorry, I really don't know anything about the SPM. IIRC they just gave the code to us as is and we didn't have enough spare time at that moment to ask for details.

MT8173 System Power Manager

Next Steps and Legal Matters

Development Steps and Plan

The road to liberating PCM firmwares:

1. Understand the ISA
2. Implement a disassembler
3. Understand the firmwares
4. Implement an assembler
5. Implement free firmwares

Sounds like a challenge... a real hard one!

Legal Evaluation

Disassembling firmwares:

- Article 6 of the EU Computer Programs Directive:

  The provisions [...] shall not permit the information obtained through its application [...] to be used for the development, production or marketing of a computer program substantially similar in its expression [...].

Wait a minute :

- `SPDX-License-Identifier: BSD-3-Clause`
- Reverse engineering is permitted!
- Only source code is missing!

MediaTek's PCM firmwares can be liberated!

Final Development Steps and Plan

The road to liberating PCM firmwares:

1. Understand the ISA
2. Implement a disassembler
3. Understand the firmwares
4. Implement an assembler
5. ~~Implement free firmwares~~

Looks better, but how to go about this?

MT8173 System Power Manager

Firmwares Analysis

First Look at the Firmwares

Power down firmware:

- Pattern of a specific value: 0x17c07c1f

```
pcm_power_down_mt8173_V37:
[0x0036] 0x10006404 0x1950001f 0x10006404 0xa1568405 0xe1000005 0xf0000000
[0x003c] 0x17c07c1f 0x1900001f 0x10006404 0x1950001f 0x10006404 0x89400005
[0x0042] 0x0000dfff 0xe1000005 0xe2e00036 0xe2e0003e 0x1910001f 0x1000660c
[0x0048] 0x81079001 0x1950001f 0x10006610 0x81479401 0x81001404 0xd82008c4
[0x004e] 0x17c07c1f 0xe2e0002e 0x1a00001f 0x100062b8 0x1910001f 0x100062b8
[0x0054] 0x89000004 0x0000fffe 0xe2000004 0x1910001f 0x100062b8 0x81142804
[0x005a] 0xd8000ae4 0x17c07c1f 0xe2e0006e 0xe2e0004e 0xe2e0004c 0xe2e0004d
[0x0060] 0x1900001f 0x10001220 0x1950001f 0x10001220 0x89400005 0xbfffffff
[0x0066] 0xe1000005 0x1900001f 0x10001228 0x1950001f 0x10001228 0x810f1401
[0x006c] 0xd8000ce4 0x17c07c1f 0x1900001f 0x1020020c 0x1950001f 0x1020020c
[0x0072] 0x89400005 0xfffffffe 0xe1000005 0xf0000000 0x17c07c1f 0x1212841f
[0x0078] 0xe2e00036 0xe2e0003e 0x1380201f 0xe2e0003c 0xe2a00000 0x1b80001f
[0x007e] 0x20000080 0xe2e0007c 0x1b80001f 0x20000003 0xe2e0005c 0xe2e0004c
[0x0084] 0xe2e0004d 0xf0000000 0x17c07c1f 0xe2e0004f 0xe2e0006f 0xe2e0002f
[0x008a] 0xe2a00001 0x1b80001f 0x20000080 0xe2e0002e 0xe2e0003e 0xe2e00032
[0x0090] 0xf0000000 0x17c07c1f 0x1212841f 0xe2e00026 0xe2e0002e 0x1380201f
[0x0096] 0x1a00001f 0x100062b4 0x1910001f 0x100062b4 0x81322804 0xe2000004
[0x009c] 0x81202804 0xe2000004 0x1b80001f 0x20000034 0x1910001f 0x100062b4
[0x00a2] 0x81142804 0xd8001404 0x17c07c1f 0xe2e0000e 0xe2e0000c 0xe2e0000d
[0x00a8] 0xf0000000 0x17c07c1f 0xe2e0002d 0x1a00001f 0x100062b4 0x1910001f
[0x00ae] 0x100062b4 0xa1002804 0xe2000004 0xa1122804 0xe2000004 0x1b80001f
[0x00b4] 0x20000080 0x1910001f 0x100062b4 0x81142804 0xd82016a4 0x17c07c1f
[0x00ba] 0xe2e0002f 0xe2e0002b 0xe2e00023 0x1380201f 0xe2e00022 0xf0000000
[0x00c0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[......]
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0x1840001f 0x00000001
[0x0204] 0x1840001f 0x00000001 0xa1d48407 0x1b00001f 0x2f7be75f 0xe8208000
[0x020a] 0x10006354 0xfffe7b47 0xa1d10407 0x1b80001f 0x20000020 0x17c07c1f
[0x0210] 0x1910001f 0x10006b00 0x81461001 0xb14690a1 0xd82044e5 0x17c07c1f
[0x0216] 0x1910001f 0x10006610 0x81079001 0xd80044e4 0x17c07c1f 0x1990001f
[0x021c] 0x10006b00 0x81421801 0x82429801 0x81402405 0xd80044e5 0x17c07c1f
[0x0222] 0x1a40001f 0x100062b0 0x1280041f 0xc24007a0 0x17c07c1f 0x1910001f
[0x0228] 0x10006b00 0x81449001 0xd8204be5 0x17c07c1f 0x1910001f 0x10006b00
```

```
pcm_power_down_mt8173_V37:
[0x0036] 0x10006404 0x1950001f 0x10006404 0xa1568405 0xe1000005 0xf0000000
[0x003c] 0x17c07c1f 0x1900001f 0x10006404 0x1950001f 0x10006404 0x89400005
[0x0042] 0x0000dfff 0xe1000005 0xe2e00036 0xe2e0003e 0x1910001f 0x1000660c
[0x0048] 0x81079001 0x1950001f 0x10006610 0x81479401 0x81001404 0xd82008c4
[0x004e] 0x17c07c1f 0xe2e0002e 0x1a00001f 0x100062b8 0x1910001f 0x100062b8
[0x0054] 0x89000004 0x0000fffe 0xe2000004 0x1910001f 0x100062b8 0x81142804
[0x005a] 0xd8000ae4 0x17c07c1f 0xe2e0006e 0xe2e0004e 0xe2e0004c 0xe2e0004d
[0x0060] 0x1900001f 0x10001220 0x1950001f 0x10001220 0x89400005 0xbfffffff
[0x0066] 0xe1000005 0x1900001f 0x10001228 0x1950001f 0x10001228 0x810f1401
[0x006c] 0xd8000ce4 0x17c07c1f 0x1900001f 0x1020020c 0x1950001f 0x1020020c
[0x0072] 0x89400005 0xfffffffe 0xe1000005 0xf0000000 0x17c07c1f 0x1212841f
[0x0078] 0xe2e00036 0xe2e0003e 0x1380201f 0xe2e0003c 0xe2a00000 0x1b80001f
[0x007e] 0x20000080 0xe2e0007c 0x1b80001f 0x20000003 0xe2e0005c 0xe2e0004c
[0x0084] 0xe2e0004d 0xf0000000 0x17c07c1f 0xe2e0004f 0xe2e0006f 0xe2e0002f
[0x008a] 0xe2a00001 0x1b80001f 0x20000080 0xe2e0002e 0xe2e0003e 0xe2e00032
[0x0090] 0xf0000000 0x17c07c1f 0x1212841f 0xe2e00026 0xe2e0002e 0x1380201f
[0x0096] 0x1a00001f 0x100062b4 0x1910001f 0x100062b4 0x81322804 0xe2000004
[0x009c] 0x81202804 0xe2000004 0x1b80001f 0x20000034 0x1910001f 0x100062b4
[0x00a2] 0x81142804 0xd8001404 0x17c07c1f 0xe2e0000e 0xe2e0000c 0xe2e0000d
[0x00a8] 0xf0000000 0x17c07c1f 0xe2e0002d 0x1a00001f 0x100062b4 0x1910001f
[0x00ae] 0x100062b4 0xa1002804 0xe2000004 0xa1122804 0xe2000004 0x1b80001f
[0x00b4] 0x20000080 0x1910001f 0x100062b4 0x81142804 0xd82016a4 0x17c07c1f
[0x00ba] 0xe2e0002f 0xe2e0002b 0xe2e00023 0x1380201f 0xe2e00022 0xf0000000
[0x00c0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[......]
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0x1840001f 0x00000001
[0x0204] 0x1840001f 0x00000001 0xa1d48407 0x1b00001f 0x2f7be75f 0xe8208000
[0x020a] 0x10006354 0xfffe7b47 0xa1d10407 0x1b80001f 0x20000020 0x17c07c1f
[0x0210] 0x1910001f 0x10006b00 0x81461001 0xb14690a1 0xd82044e5 0x17c07c1f
[0x0216] 0x1910001f 0x10006610 0x81079001 0xd80044e4 0x17c07c1f 0x1990001f
[0x021c] 0x10006b00 0x81421801 0x82429801 0x81402405 0xd80044e5 0x17c07c1f
[0x0222] 0x1a40001f 0x100062b0 0x1280041f 0xc24007a0 0x17c07c1f 0x1910001f
[0x0228] 0x10006b00 0x81449001 0xd8204be5 0x17c07c1f 0x1910001f 0x10006b00
```

```
pcm_power_down_mt8173_V37:
[0x0036] 0x10006404 0x1950001f 0x10006404 0xa1568405 0xe1000005 0xf0000000
[0x003c] 0x17c07c1f 0x1900001f 0x10006404 0x1950001f 0x10006404 0x89400005
[0x0042] 0x0000dfff 0xe1000005 0xe2e00036 0xe2e0003e 0x1910001f 0x1000660c
[0x0048] 0x81079001 0x1950001f 0x10006610 0x81479401 0x81001404 0xd82008c4
[0x004e] 0x17c07c1f 0xe2e0002e 0x1a00001f 0x100062b8 0x1910001f 0x100062b8
[0x0054] 0x89000004 0x0000fffe 0xe2000004 0x1910001f 0x100062b8 0x81142804
[0x005a] 0xd8000ae4 0x17c07c1f 0xe2e0006e 0xe2e0004e 0xe2e0004c 0xe2e0004d
[0x0060] 0x1900001f 0x10001220 0x1950001f 0x10001220 0x89400005 0xbfffffff
[0x0066] 0xe1000005 0x1900001f 0x10001228 0x1950001f 0x10001228 0x810f1401
[0x006c] 0xd8000ce4 0x17c07c1f 0x1900001f 0x1020020c 0x1950001f 0x1020020c
[0x0072] 0x89400005 0xfffffffe 0xe1000005 0xf0000000 0x17c07c1f 0x1212841f
[0x0078] 0xe2e00036 0xe2e0003e 0x1380201f 0xe2e0003c 0xe2a00000 0x1b80001f
[0x007e] 0x20000080 0xe2e0007c 0x1b80001f 0x20000003 0xe2e0005c 0xe2e0004c
[0x0084] 0xe2e0004d 0xf0000000 0x17c07c1f 0xe2e0004f 0xe2e0006f 0xe2e0002f
[0x008a] 0xe2a00001 0x1b80001f 0x20000080 0xe2e0002e 0xe2e0003e 0xe2e00032
[0x0090] 0xf0000000 0x17c07c1f 0x1212841f 0xe2e00026 0xe2e0002e 0x1380201f
[0x0096] 0x1a00001f 0x100062b4 0x1910001f 0x100062b4 0x81322804 0xe2000004
[0x009c] 0x81202804 0xe2000004 0x1b80001f 0x20000034 0x1910001f 0x100062b4
[0x00a2] 0x81142804 0xd8001404 0x17c07c1f 0xe2e0000e 0xe2e0000c 0xe2e0000d
[0x00a8] 0xf0000000 0x17c07c1f 0xe2e0002d 0x1a00001f 0x100062b4 0x1910001f
[0x00ae] 0x100062b4 0xa1002804 0xe2000004 0xa1122804 0xe2000004 0x1b80001f
[0x00b4] 0x20000080 0x1910001f 0x100062b4 0x81142804 0xd82016a4 0x17c07c1f
[0x00ba] 0xe2e0002f 0xe2e0002b 0xe2e00023 0x1380201f 0xe2e00022 0xf0000000
[0x00c0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[......]
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0x1840001f 0x00000001
[0x0204] 0x1840001f 0x00000001 0xa1d48407 0x1b00001f 0x2f7be75f 0xe8208000
[0x020a] 0x10006354 0xfffe7b47 0xa1d10407 0x1b80001f 0x20000020 0x17c07c1f
[0x0210] 0x1910001f 0x10006b00 0x81461001 0xb14690a1 0xd82044e5 0x17c07c1f
[0x0216] 0x1910001f 0x10006610 0x81079001 0xd80044e4 0x17c07c1f 0x1990001f
[0x021c] 0x10006b00 0x81421801 0x82429801 0x81402405 0xd80044e5 0x17c07c1f
[0x0222] 0x1a40001f 0x100062b0 0x1280041f 0xc24007a0 0x17c07c1f 0x1910001f
[0x0228] 0x10006b00 0x81449001 0xd8204be5 0x17c07c1f 0x1910001f 0x10006b00
```

First Look at the Firmwares

Power down firmware:

- Pattern of a specific value: 0x17c07c1f
- Looks like padding, probably nop
- Padding up to 0x200, maybe entry point

Suspend firmware:

```
pcm_suspend_20150917_V4:
[0x0174] 0xa0180400 0x803d8400 0xa01e0400 0xa0160400 0xa0170400 0xa0168400
[0x017a] 0x1b80001f 0x20000104 0x81011801 0xd80030c4 0x17c07c1f 0x18c0001f
[0x0180] 0x10006240 0xc0c034a0 0x17c07c1f 0xe8208000 0x1000f600 0xd2000001
[0x0186] 0xd8000848 0x17c07c1f 0xc2803800 0x1291841f 0x1b00001f 0x7ffff7ff
[0x018c] 0xf0000000 0x17c07c1f 0x1900001f 0x10006830 0xe1000003 0x18c0001f
[0x0192] 0x10006834 0xe0e00000 0xe0e00001 0xf0000000 0x17c07c1f 0xe0f07f16
[0x0198] 0x1380201f 0xe0f07f1e 0x1380201f 0xe0f07f0e 0x1b80001f 0x20000104
[0x019e] 0xe0f07f0c 0xe0f07f0d 0xe0f07e0d 0xe0f07c0d 0xe0f0780d 0xf0000000
[0x01a4] 0xe0f0700d 0xe0f07f0d 0xe0f07f0f 0xe0f07f1e 0xf0000000 0xe0f07f12
[0x01aa] 0x11407c1f 0x81f08407 0x81f18407 0x1b80001f 0x20000001 0xa1d08407
[0x01b0] 0xa1d18407 0x1392841f 0x812ab401 0x80ebb401 0xa0c00c04 0xd8203743
[0x01b6] 0x17c07c1f 0x80c01403 0xd8203563 0x01400405 0xf0000000 0xa1d00407
[0x01bc] 0x1b80001f 0x20000208 0x80ea3401 0xf0000000 0x18c0001f 0x10006b6c
[0x01c2] 0x1910001f 0x10006b6c 0xa1002804 0xf0000000 0xe0c00004 0x17c07c1f
[0x01c8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ce] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01d4] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01da] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e6] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0xa1d48407 0x1990001f
[0x0204] 0x10006b08 0x1a50001f 0x10006610 0x8246a401 0xe8208000 0x10006b6c
[0x020a] 0x00000000 0x1b00001f 0x2f7be75f 0x81469801 0xd8004305 0x17c07c1f
[0x0210] 0x1b80001f 0xd00f0000 0x8880000c 0x2f7be75f 0xd8005fa2 0x17c07c1f
[0x0216] 0xd0004340 0x17c07c1f 0x1b80001f 0x500f0000 0xe8208000 0x10006354
[0x021c] 0xfffe7b47 0xc0c06c00 0x81401801 0xd80048e5 0x17c07c1f 0x81f60407
[0x0222] 0x18c0001f 0x10006200 0xc0c06060 0x12807c1f 0xe8208000 0x1000625c
[0x0228] 0x00000001 0x1b80001f 0x20000080 0xc0c06060 0x1280041f 0x18c0001f
[0x022e] 0x10006204 0xc0c06400 0x1280041f 0x18c0001f 0x10006208 0xc0c06060
[0x0234] 0x12807c1f 0xe8208000 0x10006244 0x00000001 0x1b80001f 0x20000080
[0x023a] 0xc0c06060 0x1280041f 0x18d0001f 0x10200200 0x18c0001f 0x10006290
[0x0240] 0xc0c06060 0x1280041f 0xe8208000 0x10006404 0x00003101 0xc2803800
[0x0246] 0x1292041f 0x81469801 0xd8204a45 0x17c07c1f 0x1b00001f 0x2f7be75f
```

```
pcm_suspend_20150917_V4:
[0x0174] 0xa0180400 0x803d8400 0xa01e0400 0xa0160400 0xa0170400 0xa0168400
[0x017a] 0x1b80001f 0x20000104 0x81011801 0xd80030c4 0x17c07c1f 0x18c0001f
[0x0180] 0x10006240 0xc0c034a0 0x17c07c1f 0xe8208000 0x1000f600 0xd2000001
[0x0186] 0xd8000848 0x17c07c1f 0xc2803800 0x1291841f 0x1b00001f 0x7ffff7ff
[0x018c] 0xf0000000 0x17c07c1f 0x1900001f 0x10006830 0xe1000003 0x18c0001f
[0x0192] 0x10006834 0xe0e00000 0xe0e00001 0xf0000000 0x17c07c1f 0xe0f07f16
[0x0198] 0x1380201f 0xe0f07f1e 0x1380201f 0xe0f07f0e 0x1b80001f 0x20000104
[0x019e] 0xe0f07f0c 0xe0f07f0d 0xe0f07e0d 0xe0f07c0d 0xe0f0780d 0xf0000000
[0x01a4] 0xe0f0700d 0xe0f07f0d 0xe0f07f0f 0xe0f07f1e 0xf0000000 0xe0f07f12
[0x01aa] 0x11407c1f 0x81f08407 0x81f18407 0x1b80001f 0x20000001 0xa1d08407
[0x01b0] 0xa1d18407 0x1392841f 0x812ab401 0x80ebb401 0xa0c00c04 0xd8203743
[0x01b6] 0x17c07c1f 0x80c01403 0xd8203563 0x01400405 0xf0000000 0xa1d00407
[0x01bc] 0x1b80001f 0x20000208 0x80ea3401 0xf0000000 0x18c0001f 0x10006b6c
[0x01c2] 0x1910001f 0x10006b6c 0xa1002804 0xf0000000 0xe0c00004 0x17c07c1f
[0x01c8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ce] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01d4] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01da] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e6] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0xa1d48407 0x1990001f
[0x0204] 0x10006b08 0x1a50001f 0x10006610 0x8246a401 0xe8208000 0x10006b6c
[0x020a] 0x00000000 0x1b00001f 0x2f7be75f 0x81469801 0xd8004305 0x17c07c1f
[0x0210] 0x1b80001f 0xd00f0000 0x8880000c 0x2f7be75f 0xd8005fa2 0x17c07c1f
[0x0216] 0xd0004340 0x17c07c1f 0x1b80001f 0x500f0000 0xe8208000 0x10006354
[0x021c] 0xfffe7b47 0xc0c06c00 0x81401801 0xd80048e5 0x17c07c1f 0x81f60407
[0x0222] 0x18c0001f 0x10006200 0xc0c06060 0x12807c1f 0xe8208000 0x1000625c
[0x0228] 0x00000001 0x1b80001f 0x20000080 0xc0c06060 0x1280041f 0x18c0001f
[0x022e] 0x10006204 0xc0c06400 0x1280041f 0x18c0001f 0x10006208 0xc0c06060
[0x0234] 0x12807c1f 0xe8208000 0x10006244 0x00000001 0x1b80001f 0x20000080
[0x023a] 0xc0c06060 0x1280041f 0x18d0001f 0x10200200 0x18c0001f 0x10006290
[0x0240] 0xc0c06060 0x1280041f 0xe8208000 0x10006404 0x00003101 0xc2803800
[0x0246] 0x1292041f 0x81469801 0xd8204a45 0x17c07c1f 0x1b00001f 0x2f7be75f
```

```
pcm_suspend_20150917_V4:
[0x0174] 0xa0180400 0x803d8400 0xa01e0400 0xa0160400 0xa0170400 0xa0168400
[0x017a] 0x1b80001f 0x20000104 0x81011801 0xd80030c4 0x17c07c1f 0x18c0001f
[0x0180] 0x10006240 0xc0c034a0 0x17c07c1f 0xe8208000 0x1000f600 0xd2000001
[0x0186] 0xd8000848 0x17c07c1f 0xc2803800 0x1291841f 0x1b00001f 0x7ffff7ff
[0x018c] 0xf0000000 0x17c07c1f 0x1900001f 0x10006830 0xe1000003 0x18c0001f
[0x0192] 0x10006834 0xe0e00000 0xe0e00001 0xf0000000 0x17c07c1f 0xe0f07f16
[0x0198] 0x1380201f 0xe0f07f1e 0x1380201f 0xe0f07f0e 0x1b80001f 0x20000104
[0x019e] 0xe0f07f0c 0xe0f07f0d 0xe0f07e0d 0xe0f07c0d 0xe0f0780d 0xf0000000
[0x01a4] 0xe0f0700d 0xe0f07f0d 0xe0f07f0f 0xe0f07f1e 0xf0000000 0xe0f07f12
[0x01aa] 0x11407c1f 0x81f08407 0x81f18407 0x1b80001f 0x20000001 0xa1d08407
[0x01b0] 0xa1d18407 0x1392841f 0x812ab401 0x80ebb401 0xa0c00c04 0xd8203743
[0x01b6] 0x17c07c1f 0x80c01403 0xd8203563 0x01400405 0xf0000000 0xa1d00407
[0x01bc] 0x1b80001f 0x20000208 0x80ea3401 0xf0000000 0x18c0001f 0x10006b6c
[0x01c2] 0x1910001f 0x10006b6c 0xa1002804 0xf0000000 0xe0c00004 0x17c07c1f
[0x01c8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ce] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01d4] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01da] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e0] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01e6] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01ec] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f2] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01f8] 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f 0x17c07c1f
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0xa1d48407 0x1990001f
[0x0204] 0x10006b08 0x1a50001f 0x10006610 0x8246a401 0xe8208000 0x10006b6c
[0x020a] 0x00000000 0x1b00001f 0x2f7be75f 0x81469801 0xd8004305 0x17c07c1f
[0x0210] 0x1b80001f 0xd00f0000 0x8880000c 0x2f7be75f 0xd8005fa2 0x17c07c1f
[0x0216] 0xd0004340 0x17c07c1f 0x1b80001f 0x500f0000 0xe8208000 0x10006354
[0x021c] 0xfffe7b47 0xc0c06c00 0x81401801 0xd80048e5 0x17c07c1f 0x81f60407
[0x0222] 0x18c0001f 0x10006200 0xc0c06060 0x12807c1f 0xe8208000 0x1000625c
[0x0228] 0x00000001 0x1b80001f 0x20000080 0xc0c06060 0x1280041f 0x18c0001f
[0x022e] 0x10006204 0xc0c06400 0x1280041f 0x18c0001f 0x10006208 0xc0c06060
[0x0234] 0x12807c1f 0xe8208000 0x10006244 0x00000001 0x1b80001f 0x20000080
[0x023a] 0xc0c06060 0x1280041f 0x18d0001f 0x10200200 0x18c0001f 0x10006290
[0x0240] 0xc0c06060 0x1280041f 0xe8208000 0x10006404 0x00003101 0xc2803800
[0x0246] 0x1292041f 0x81469801 0xd8204a45 0x17c07c1f 0x1b00001f 0x2f7be75f
```

First Look at the Firmwares

Power down firmware:

- Pattern of a specific value: 0x17c07c1f
- Looks like padding, probably nop
- Padding up to 0x200, maybe entry point

Suspend firmware:

- Same pattern, also found up to 0x200

General observations:

- Words seem to be 32-bit long
- Doesn't match any known ISA
- Value of 0xf0000000 often before padding

First Look at the Firmwares

MCDI (Multi-Core Deep Idle) firmware:

- Same pattern, also found up to 0x200
- Constants used in ATF code:

```
#define PCM_MCDI_HANDSHAKE_SYNC 0xbeefbeef
#define PCM_MCDI_HANDSHAKE_ACK  0xdeaddead
#define PCM_MCDI_UPDATE_INFORM  0xabcdabcd
#define PCM_MCDI_CKECK_DONE     0x12345678
#define PCM_MCDI_ALL_CORE_AWAKE 0x0
#define PCM_MCDI_OFFLOADED      0xaa55aa55

mmio_write_32(SPM_PCM_REG_DATA_INI, PCM_MCDI_HANDSHAKE_SYNC);
mmio_write_32(SPM_PCM_PWR_IO_EN, PCM_RF_SYNC_R6);
mmio_write_32(SPM_PCM_PWR_IO_EN, 0);

while (mmio_read_32(SPM_PCM_REG6_DATA) != PCM_MCDI_HANDSHAKE_ACK)
```

```
pcm_mcdi_mt8173_20160401_v1:
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0x11407c1f 0xe8208000
[0x0204] 0x10006310 0x0b160008 0x1900001f 0x000f7bde 0x1a00001f 0x10200268
[0x020a] 0xe2000004 0xe8208000 0x10006600 0x00000000 0x69200006 0xbeefbeef
[0x0210] 0xd8204584 0x17c07c1f 0x1910001f 0x10006358 0x810b1001 0xd8004244
[0x0216] 0x17c07c1f 0x1980001f 0xdeaddead 0x69200006 0xabcdabcd 0xd8204324
[0x021c] 0x17c07c1f 0x88900001 0x10006814 0x1910001f 0x10006400 0x81271002
[0x0222] 0x1880001f 0x10006600 0xe0800004 0x1910001f 0x10006358 0x810b1001
[0x0228] 0xd80044a4 0x17c07c1f 0x1980001f 0x12345678 0x60a07c05 0x89100002
[0x022e] 0x10006600 0x80801001 0xd8007bc2 0x17c07c1f 0x1890001f 0x10006b00
[0x0234] 0x82090801 0xc8800008 0x17c07c1f 0x1b00001f 0x3fffe7ff 0x8a00000c
[0x023a] 0x3fffe7ff 0xd82041c8 0x17c07c1f 0x1b80001f 0xd0010000 0x1a10001f
[0x0240] 0x10006720 0x82002001 0x82201408 0xd8204988 0x17c07c1f 0x1a40001f
[0x0246] 0x10006200 0x1a80001f 0x1000625c 0xc24028e0 0x17c07c1f 0xa1400405
[0x024c] 0x1a10001f 0x10006720 0x8200a001 0x82209408 0xd8204b28 0x17c07c1f
[0x0252] 0x1a40001f 0x10006218 0x1a80001f 0x10006264 0xc24028e0 0x17c07c1f
[0x0258] 0xa1508405 0x1a10001f 0x10006720 0x82012001 0x82211408 0xd8204cc8
[0x025e] 0x17c07c1f 0x1a40001f 0x1000621c 0x1a80001f 0x1000626c 0xc24028e0
[0x0264] 0x17c07c1f 0xa1510405 0x1a10001f 0x10006720 0x8201a001 0x82219408
[0x026a] 0xd8204e68 0x17c07c1f 0x1a40001f 0x10006220 0x1a80001f 0x10006274
[0x0270] 0xc24028e0 0x17c07c1f 0xa1518405 0x1a10001f 0x10006720 0x82022001
[0x0276] 0x82221408 0xd8204fe8 0x17c07c1f 0x1a40001f 0x100062a0 0x1280041f
[0x027c] 0xc2402cc0 0x17c07c1f 0xa1520405 0x1a10001f 0x10006720 0x8202a001
[0x0282] 0x82229408 0xd8205168 0x17c07c1f 0x1a40001f 0x100062a4 0x1290841f
[0x0288] 0xc2402cc0 0x17c07c1f 0xa1528405 0x1a10001f 0x10006720 0x82032001
[0x028e] 0x82231408 0xd8205248 0x17c07c1f 0xa1530405 0x1a10001f 0x10006720
[0x0294] 0x8203a001 0x82239408 0xd8205328 0x17c07c1f 0xa1538405 0x1a10001f
[0x029a] 0x10006b00 0x8108a001 0xd8205e84 0x17c07c1f 0x1910001f 0x1000660c
[0x02a0] 0x1a10001f 0x10006610 0xa2002004 0x89000008 0x00001e00 0xd8005944
[0x02a6] 0x17c07c1f 0x82042001 0xd8205948 0x17c07c1f 0x1900001f 0x1020002c
[0x02ac] 0x1a10001f 0x1020002c 0xaa000008 0x00000010 0xe1000008 0x1910001f
[0x02b2] 0x10006720 0x820c1001 0xd8205628 0x17c07c1f 0x1900001f 0x10001250
[0x02b8] 0x1a10001f 0x10001250 0xa2110408 0xe1000008 0x1b80001f 0x20000080
[0x02be] 0x1900001f 0x10001220 0x1a10001f 0x10001220 0xa21e8408 0xe1000008
[0x02c4] 0x1b80001f 0x20000080 0x1a40001f 0x10006208 0xc24024e0 0x17c07c1f
[0x02ca] 0x1a10001f 0x10006610 0x82042001 0xd8005e88 0x17c07c1f 0x1a10001f
[0x02d0] 0x10006918 0x8a000008 0x00000f0f 0xba00010c 0x1fffe7ff 0xd8205e88
```

```
pcm_mcdi_mt8173_20160401_v1:
[0x01fe] 0x17c07c1f 0x17c07c1f 0x1840001f 0x00000001 0x11407c1f 0xe8208000
[0x0204] 0x10006310 0x0b160008 0x1900001f 0x000f7bde 0x1a00001f 0x10200268
[0x020a] 0xe2000004 0xe8208000 0x10006600 0x00000000 0x69200006 0xbeefbeef
[0x0210] 0xd8204584 0x17c07c1f 0x1910001f 0x10006358 0x810b1001 0xd8004244
[0x0216] 0x17c07c1f 0x1980001f 0xdeaddead 0x69200006 0xabcdabcd 0xd8204324
[0x021c] 0x17c07c1f 0x88900001 0x10006814 0x1910001f 0x10006400 0x81271002
[0x0222] 0x1880001f 0x10006600 0xe0800004 0x1910001f 0x10006358 0x810b1001
[0x0228] 0xd80044a4 0x17c07c1f 0x1980001f 0x12345678 0x60a07c05 0x89100002
[0x022e] 0x10006600 0x80801001 0xd8007bc2 0x17c07c1f 0x1890001f 0x10006b00
[0x0234] 0x82090801 0xc8800008 0x17c07c1f 0x1b00001f 0x3fffe7ff 0x8a00000c
[0x023a] 0x3fffe7ff 0xd82041c8 0x17c07c1f 0x1b80001f 0xd0010000 0x1a10001f
[0x0240] 0x10006720 0x82002001 0x82201408 0xd8204988 0x17c07c1f 0x1a40001f
[0x0246] 0x10006200 0x1a80001f 0x1000625c 0xc24028e0 0x17c07c1f 0xa1400405
[0x024c] 0x1a10001f 0x10006720 0x8200a001 0x82209408 0xd8204b28 0x17c07c1f
[0x0252] 0x1a40001f 0x10006218 0x1a80001f 0x10006264 0xc24028e0 0x17c07c1f
[0x0258] 0xa1508405 0x1a10001f 0x10006720 0x82012001 0x82211408 0xd8204cc8
[0x025e] 0x17c07c1f 0x1a40001f 0x1000621c 0x1a80001f 0x1000626c 0xc24028e0
[0x0264] 0x17c07c1f 0xa1510405 0x1a10001f 0x10006720 0x8201a001 0x82219408
[0x026a] 0xd8204e68 0x17c07c1f 0x1a40001f 0x10006220 0x1a80001f 0x10006274
[0x0270] 0xc24028e0 0x17c07c1f 0xa1518405 0x1a10001f 0x10006720 0x82022001
[0x0276] 0x82221408 0xd8204fe8 0x17c07c1f 0x1a40001f 0x100062a0 0x1280041f
[0x027c] 0xc2402cc0 0x17c07c1f 0xa1520405 0x1a10001f 0x10006720 0x8202a001
[0x0282] 0x82229408 0xd8205168 0x17c07c1f 0x1a40001f 0x100062a4 0x1290841f
[0x0288] 0xc2402cc0 0x17c07c1f 0xa1528405 0x1a10001f 0x10006720 0x82032001
[0x028e] 0x82231408 0xd8205248 0x17c07c1f 0xa1530405 0x1a10001f 0x10006720
[0x0294] 0x8203a001 0x82239408 0xd8205328 0x17c07c1f 0xa1538405 0x1a10001f
[0x029a] 0x10006b00 0x8108a001 0xd8205e84 0x17c07c1f 0x1910001f 0x1000660c
[0x02a0] 0x1a10001f 0x10006610 0xa2002004 0x89000008 0x00001e00 0xd8005944
[0x02a6] 0x17c07c1f 0x82042001 0xd8205948 0x17c07c1f 0x1900001f 0x1020002c
[0x02ac] 0x1a10001f 0x1020002c 0xaa000008 0x00000010 0xe1000008 0x1910001f
[0x02b2] 0x10006720 0x820c1001 0xd8205628 0x17c07c1f 0x1900001f 0x10001250
[0x02b8] 0x1a10001f 0x10001250 0xa2110408 0xe1000008 0x1b80001f 0x20000080
[0x02be] 0x1900001f 0x10001220 0x1a10001f 0x10001220 0xa21e8408 0xe1000008
[0x02c4] 0x1b80001f 0x20000080 0x1a40001f 0x10006208 0xc24024e0 0x17c07c1f
[0x02ca] 0x1a10001f 0x10006610 0x82042001 0xd8005e88 0x17c07c1f 0x1a10001f
[0x02d0] 0x10006918 0x8a000008 0x00000f0f 0xba00010c 0x1fffe7ff 0xd8205e88
```

First Look at the Firmwares

MCDI (Multi-Core Deep Idle) firmware:

- Same pattern, also found up to 0x200
- Constants used in ATF code:

```
#define PCM_MCDI_HANDSHAKE_SYNC 0xbeefbeef
#define PCM_MCDI_HANDSHAKE_ACK  0xdeaddead
#define PCM_MCDI_UPDATE_INFORM  0xabcdabcd
#define PCM_MCDI_CKECK_DONE     0x12345678
#define PCM_MCDI_ALL_CORE_AWAKE 0x0
#define PCM_MCDI_OFFLOADED      0xaa55aa55

mmio_write_32(SPM_PCM_REG_DATA_INI, PCM_MCDI_HANDSHAKE_SYNC);
mmio_write_32(SPM_PCM_PWR_IO_EN, PCM_RF_SYNC_R6);
mmio_write_32(SPM_PCM_PWR_IO_EN, 0);

while (mmio_read_32(SPM_PCM_REG6_DATA) != PCM_MCDI_HANDSHAKE_ACK)
```

- Access to PCM registers (MMIO) r0-r15
- Sets or waits for constants in registers
- Constants found as-is in the firmware
- Close to 0x200: init code at entry point?

Discovering the First Instructions

Constants, associated registers and context:

constant	register	direction	previous word
`0xbeefbeef`	r6	CPU → PCM	`0x69200006`
`0xdeaddead`	r6	PCM → CPU	`0x1980001f`
`0xabcdabcd`	r6	CPU → PCM	`0x69200006`
`0x12345678`	r6	PCM → CPU	`0x1980001f`
`0xaa55aa55`	r5	PCM → CPU	`0x1940001f`

- Consistent previous word (probably opcode)
- Probably contains source/destination register

Discovering the First Instructions

hexadecimal	r	binary
0x69200006	6	0110 1001 0010 0000 0000 0000 0000 0110
0x1980001f	6	0001 1001 1000 0000 0000 0000 0001 1111
0x1940001f	5	0001 1001 0100 0000 0000 0000 0001 1111

First opcode (followed by immediate):

0001 10xx xx00 0000 0000 0000 0001 1111, loadi rx

More information needed for 0x69200006.

Verifying Instructions

It's time to execute code!

Plan:

- Craft a test program (hex editor)
- Single opcode and immediate 0xcafecafe
- Load it to the PCM in ATF
- Dump registers from ATF

Required setup:

- Flashing coreboot (includes ATF) to SPI flash
- Accessing CPU UART (ATF serial)

Code Execution

No luck with it...

Hints:

- Wrong entry point?
- Try adding 0x17c07c1f padding up to 0x200
- Follow with loadi r6 0xcafecafe instruction

Result:

```
r6 = 0xcafecafe
```

Teachings:

- Entry point is 0x200
- r15 looks like it's PC

Development Tools

Dedicated tools to ease development:

- `pcm-asm`: Assemble instructions from arguments
- `pcm-disasm`: Disassemble instructions from arguments
- `pcm-analysis`: Disassemble full binaries
- `pcm-assembler`: Assemble full sources
- `pcm-header`: Format binaries for ATF

Public and available:

- Personal git: `https://git.code.paulk.fr` (temporary)
- GPLv3+ license

Moving Forward, Finding More Instructions

Discovering APB read:

- ATF commit: `mt8173: update spm suspend pcm codes`:
  `git show 0ad1a9b32939b3ecaffb2ee626326e39b8230d0e --word-diff`
- Added instruction:
  `add dummy apb read before mcusys power down`

`0x18d0001f 0x10200200`

- **0x10200200** is a valid APB address: MCUCFG
- PCM can access APB registers
  security, anyone? (DRAM too...)

Moving Forward, Finding More Instructions

Discovering jump/call:

- ATF commit: `mt8173: update spm suspend pcm codes`:
  `git show 0ad1a9b32939b3ecaffb2ee626326e39b8230d0e --word-diff`
- Updates some instructions after adding code
  Consistent increase: offset

`0xd8005103` → `0xd8005143`
`0xd8005183` → `0xd80051c3`

More instructions discovered with similar tricks!
ALU operations are easy...

Current Status

Instructions support:

- 10 base instructions:
  and, call, eq, jump, load, mask, nop, or, ret, store
- 16 extended instructions:
  and, andi, andn, call, eqi, jump, jumpn, jumpz, loada, loadi, nop, or, ori, ret, store, storeai

firmware	decoded	total	progress
`pcm_mcdi_mt8173_20160401_v1`	912	1001	91 %
`pcm_power_down_mt8173_V37`	837	888	94 %
`pcm_suspend_20150917_V4`	748	869	86 %

Project started **February 2017**

Upcoming Work

Remaining tasks:

- Figure out remaining instructions
  probably the hardest, maybe stack-related?
- Obtain a fully disassembled binary
- Comment what's going on, name functions
  APB registers are (more or less) documented
- Release source code

Lessons Learned and Advice

- Working without any documentation or reference is fun!
  or is it?
- Some background (CPU architecture) required
- Deduction is key and *might* just be enough!
- Short binaries are easier
- Take a good look at the binary
  (patterns, repetitions, similarities)
- Don't give up hope!

Thank-You!

Questions?