KB9012 Embedded Controller firmware reverse engineering

Paul Kocialkowski
contact@paulk.fr

Monday June 13rd 2016

coreboot conference
San Francisco 2016

Situation and Motivation

Personal Use Case

Use of technology:

Personal Use Case

Use of technology:

- Freedom-respecting computers

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Laptops situation, targets:

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Laptops situation, targets:

- Previous Intel x86 laptops (Thinkpads)

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Laptops situation, targets:

- Previous Intel x86 laptops (Thinkpads)
- Recent Intel x86 laptops

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Laptops situation, targets:

- Previous Intel x86 laptops (Thinkpads)
- Recent Intel x86 laptops
- CrOS devices (Intel/ARM chromebooks)

Personal Use Case

Use of technology:

- Freedom-respecting computers
  knowledge, power, community, security
- Form factors (desktops, laptops, mobile, HTPC)
- Heavy tasks (kernel, system builds)
- Roadmap: free system, bootup software, firmwares

Laptops situation, targets:

- Previous Intel x86 laptops (Thinkpads)
- Recent Intel x86 laptops
- CrOS devices (Intel/ARM chromebooks)
- AMD x86 laptops

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS
- CPU microcode, updates

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS
- CPU microcode, updates
- Firmwares:

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS
- CPU microcode, updates
- Firmwares:
  - IMC
  - SMU

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS
- CPU microcode, updates
- Firmwares:
  - IMC
  - SMU
  - xHCI (USB 3)

G505s Laptop (Lenovo)

Candidate: G505s Laptop:

- 15" Lenovo laptop from 2013
- AMD Bolton M3 FCH
- AMD A-series APU (Family 15h)

Software freedom status:

- Coreboot support (AGESA)
- Option ROM/VGA BIOS
- CPU microcode, updates
- Firmwares:
  - IMC
  - SMU
  - xHCI (USB 3)
  - Embedded Controller

Embedded Controller

Specific interest:

Embedded Controller

Specific interest:

- User interaction, modification

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!
- Privacy/security

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!
- Privacy/security
- Power sequencing, optimizations

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!
- Privacy/security
- Power sequencing, optimizations
- Fun to learn about!

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!
- Privacy/security
- Power sequencing, optimizations
- Fun to learn about!

Free software support:

Embedded Controller

Specific interest:

- User interaction, modification
  Start up with lid open!
- Privacy/security
- Power sequencing, optimizations
- Fun to learn about!

Free software support:

- CrOS EC

Embedded Controller

Specific interest:

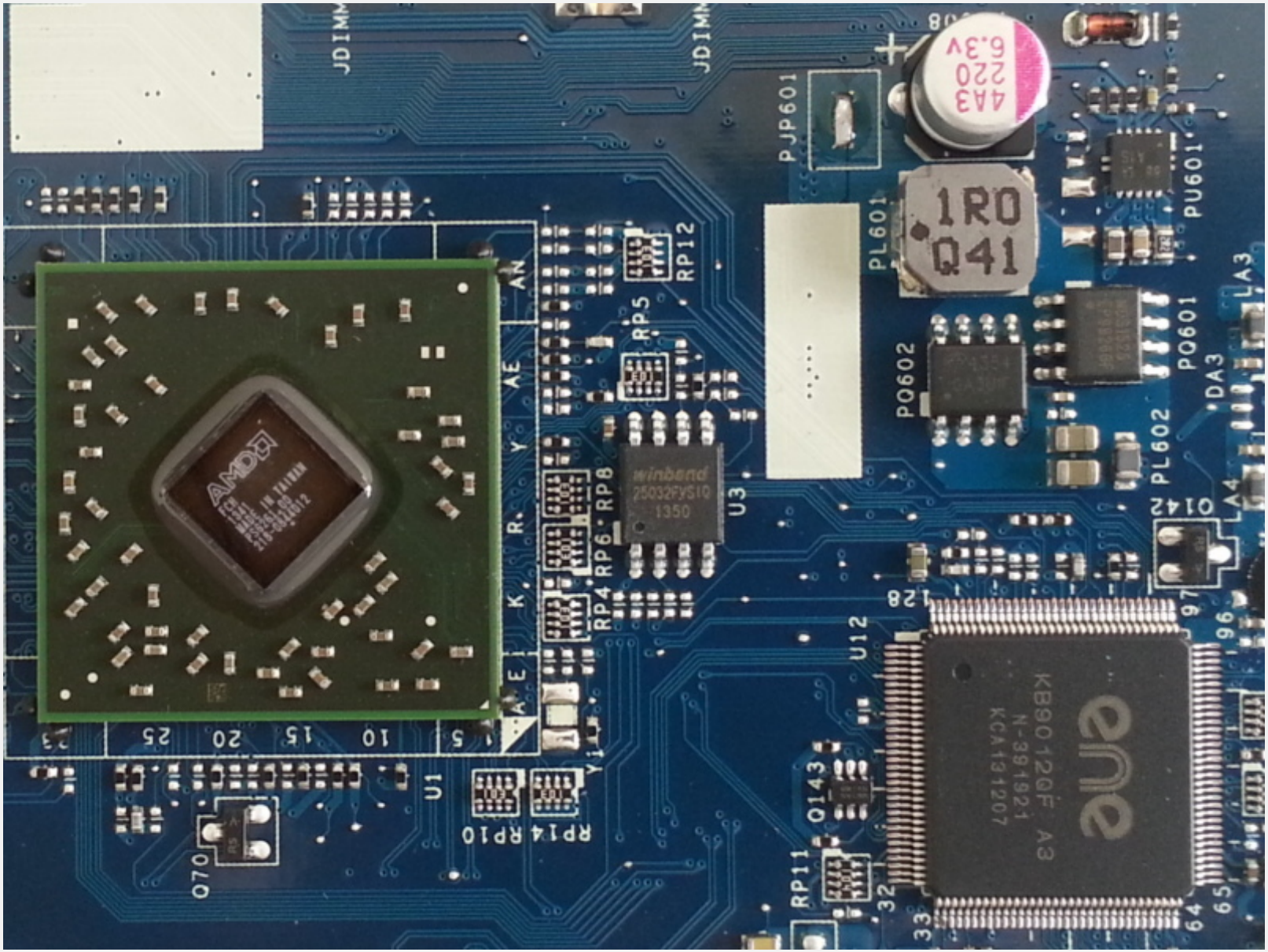
- User interaction, modification
  Start up with lid open!
- Privacy/security
- Power sequencing, optimizations
- Fun to learn about!

Free software support:

- CrOS EC
- Lynxis 2015 GSoC project

Hardware Investigation

Hardware Investigation



Documentation

Laptop (G505s) documentation:

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Power sequencing diagram

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Power sequencing diagram
- No PCB layout, labels

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Power sequencing diagram
- No PCB layout, labels

EC (KB9012) documentation:

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Power sequencing diagram
- No PCB layout, labels

EC (KB9012) documentation:

- Extensive datasheet:
  - Platform description
  - Registers description

Documentation

Laptop (G505s) documentation:

- Full schematics:
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Power sequencing diagram
- No PCB layout, labels

EC (KB9012) documentation:

- Extensive datasheet:
  - Platform description
  - Registers description
- Some application notes

KB9012 Platform Description

KB9012 platform:

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words
  - Memory layout: program, external, internal, SFR

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words
  - Memory layout: program, external, internal, SFR
  - Interrupt controller, timers
  - Specific extensions

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words
  - Memory layout: program, external, internal, SFR
  - Interrupt controller, timers
  - Specific extensions
- Storage memory (128 kiB flash)
- Volatile memory (4 kiB SRAM)

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words
  - Memory layout: program, external, internal, SFR
  - Interrupt controller, timers
  - Specific extensions
- Storage memory (128 kiB flash)
- Volatile memory (4 kiB SRAM)
- Controllers:

KB9012 Platform Description

KB9012 platform:

- 8051-based CPU:
  - 8-32 MHz clock frequency
  - 8-bit words
  - Memory layout: program, external, internal, SFR
  - Interrupt controller, timers
  - Specific extensions
- Storage memory (128 kiB flash)
- Volatile memory (4 kiB SRAM)
- Controllers:
  - LPC, SMBUS (I2C), SPI
  - GPIO, ADC, DAC
  - Keyboard, PS/2
  - IR, FAN, OW
  - Some more

Development Setup

Development Setup

Hardware

Serial and Debug Output

Serial port:

Serial and Debug Output

Serial port:

- UART from the 8051 CPU

Serial and Debug Output

Serial port:

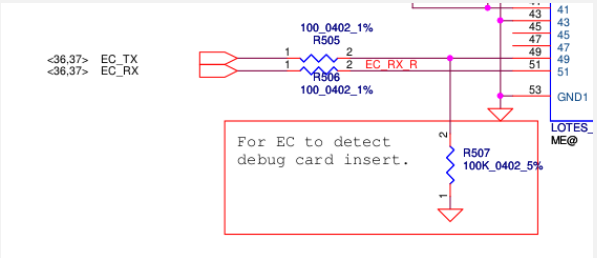
- UART from the 8051 CPU
- Exported to:
  - PCI-e
  - Pads (*JP3*)

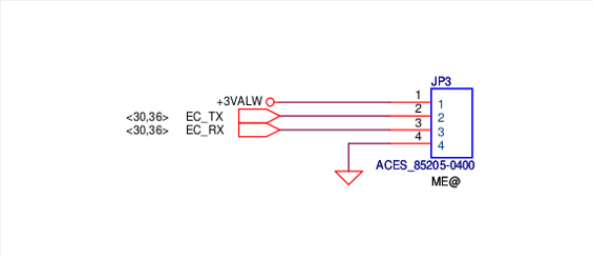
Serial and Debug Output

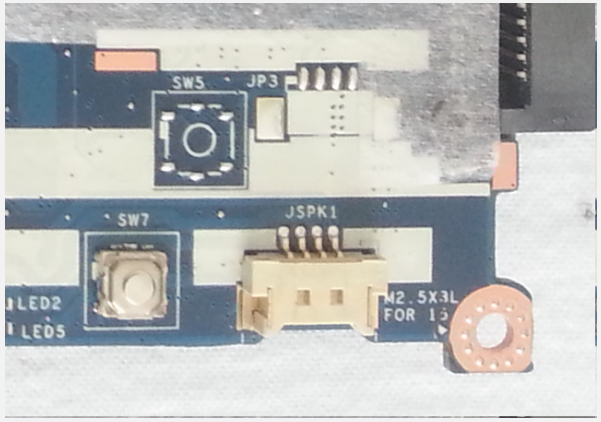
Serial port:

- UART from the 8051 CPU
- Exported to:
  - PCI-e
  - Pads (*JP3*)

```
KSTART!R
EF-01,E7,E0,ON01,NON1N2N3N3N4N5N6EXN7
EF-01,E0,F0,N8NANANANANANANBNBNBNBNBNBNB
I52,KC52,DA4,KDA4,OOO,NBO,
e59,Kc59,dE9,KdE9,
KxFF,NB
I52,KC52,DA4,KDA4,OOO,O,
e59,Kc59,NBdE9,KdE9,NBNBNBNB
MC4E,MDED,
EF-01,EO,ED,MrFF,
MC4E,MDEC,
EF-01,EO,EC,Mr06,NBVFF,NBC,RFA,OFA,RAA,K20
MC42,MDOO,
MC4E,MDEB,
EF-01,EO,EB,Mr55,O,NB
```







Flashing the Firmware

Internal memory access:

Flashing the Firmware

Internal memory access:

- X-Bus interface, commands

Flashing the Firmware

Internal memory access:

- X-Bus interface, commands
- LPC Index-I/O:

Flashing the Firmware

Internal memory access:

- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)

Flashing the Firmware

Internal memory access:

- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)
  - Firmware-disabled

Flashing the Firmware

Internal memory access:

- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)
  - Firmware-disabled
- ENE Debug Interface (EDI):

Flashing the Firmware

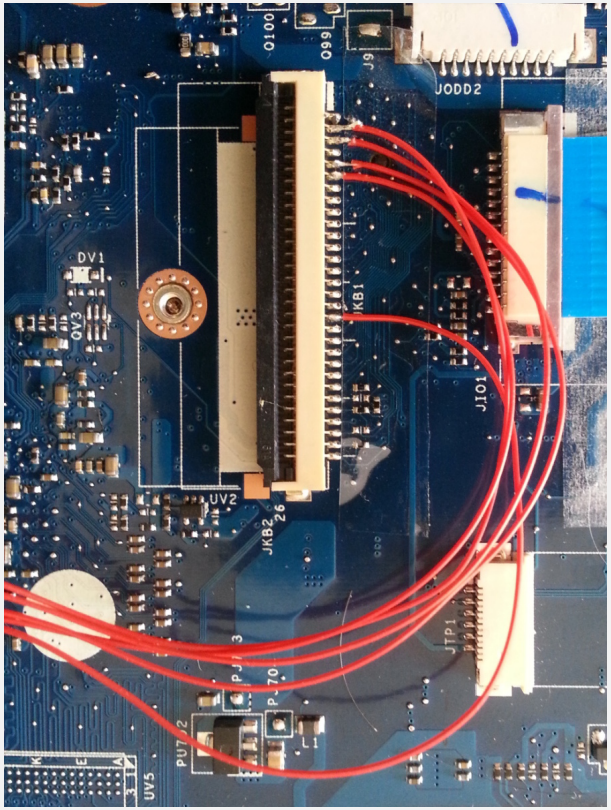
Internal memory access:

- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)
  - Firmware-disabled
- ENE Debug Interface (EDI):
  - SPI protocol
  - Application note (commands)
  - Keyboard pins

Flashing the Firmware

Internal memory access:

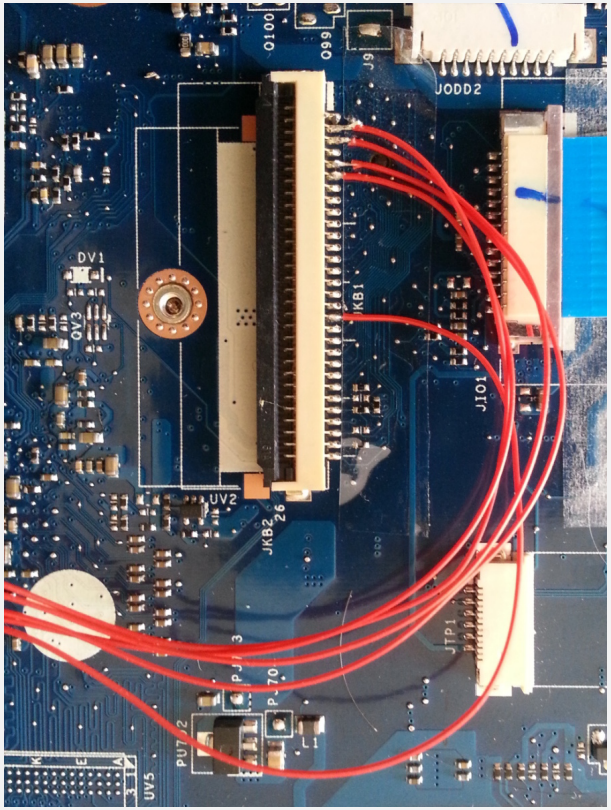
- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)
  - Firmware-disabled
- ENE Debug Interface (EDI):
  - SPI protocol
  - Application note (commands)
  - Keyboard pins



Flashing the Firmware

Internal memory access:

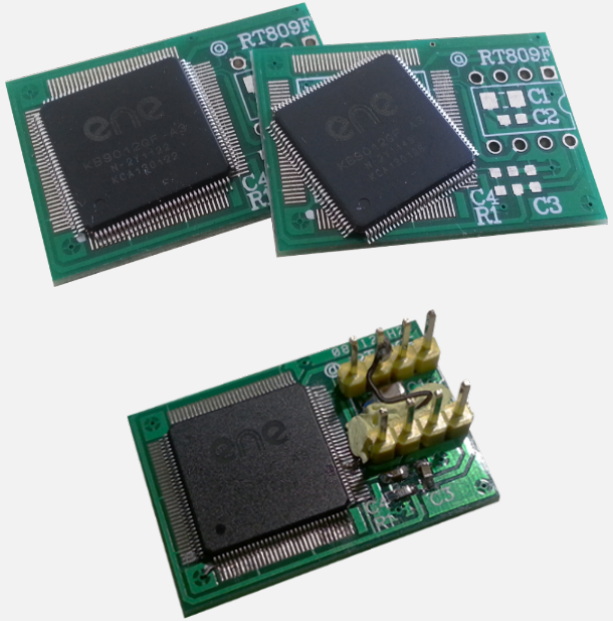
- X-Bus interface, commands
- LPC Index-I/O:
  - CrOS Flashrom support (KB9xx)
  - Firmware-disabled
- ENE Debug Interface (EDI):
  - SPI protocol
  - Application note (commands)
  - Keyboard pins



Flashrom support (under review)!

Early Investigation

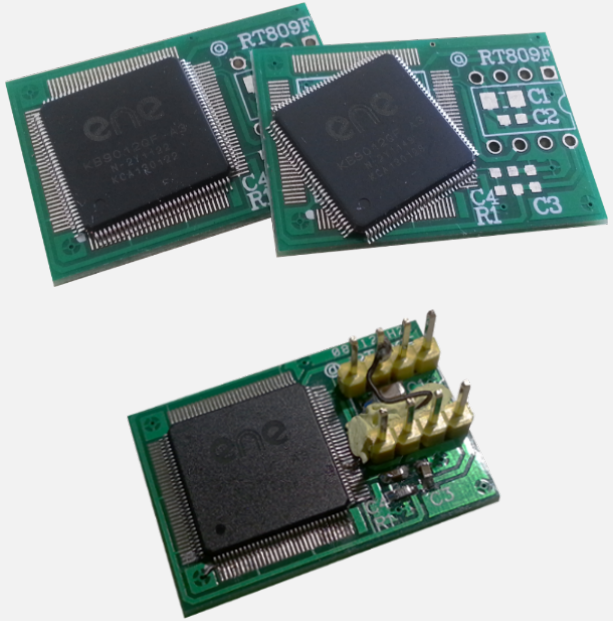
Development board:



Early Investigation

Development board:

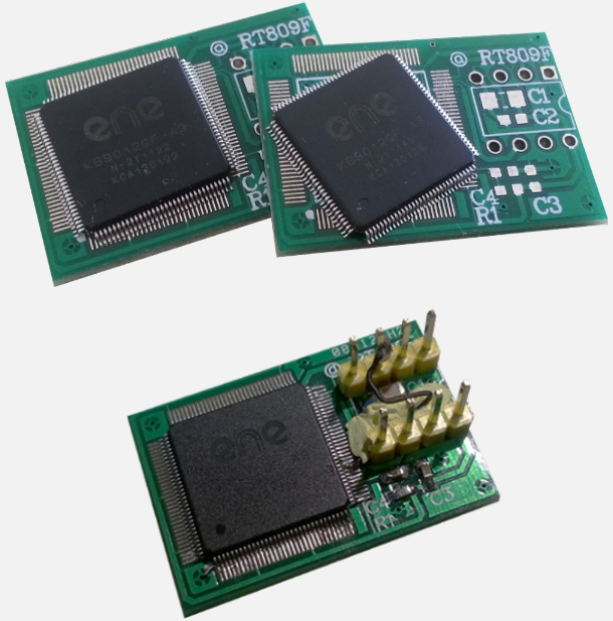
- Spare board and chips
- LQFP128 soldering



Early Investigation

Development board:

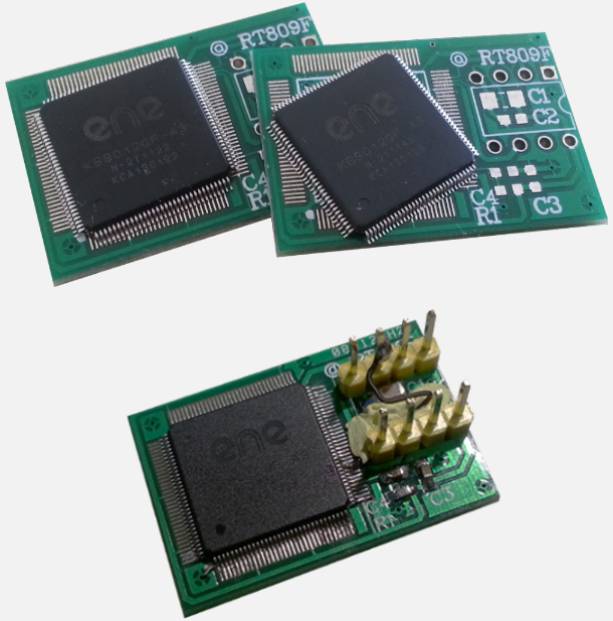
- Spare board and chips
- LQFP128 soldering
- Exposed pins
- Used for memory flash



Early Investigation

Development board:

- Spare board and chips
- LQFP128 soldering
- Exposed pins
- Used for memory flash
- Low interest otherwise



Development Setup

Software

Software Investigation

Early software bringup:

Software Investigation

Early software bringup:

- 8051 ISA

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

- C compiler: SDCC, extensions

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

- C compiler: SDCC, extensions
- Memory models, stack

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

- C compiler: SDCC, extensions
- Memory models, stack
- Reverse engineering tools:

Software Investigation

Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

- C compiler: SDCC, extensions
- Memory models, stack
- Reverse engineering tools:
  - Static: radare2, 8051 support

Software Investigation

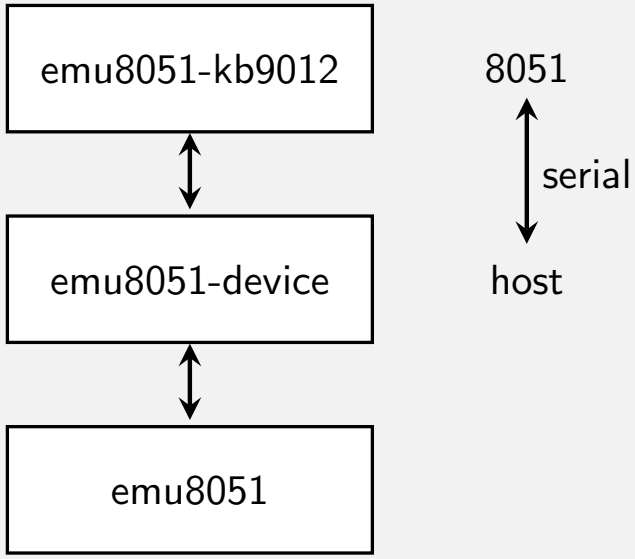
Early software bringup:

- 8051 ISA
- Bare opcodes (*hexedit*)
- Serial Hello World!, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Proper development base:

- C compiler: SDCC, extensions
- Memory models, stack
- Reverse engineering tools:
  - Static: radare2, 8051 support
  - Dynamic: emu8051, emu8051-device



Free Software EC Implementation

Functional Free EC Firmware

Associated constraints, requirements:

Functional Free EC Firmware

Associated constraints, requirements:

- Written in C

Functional Free EC Firmware

Associated constraints, requirements:

- Written in C
- Memory size (program, RAM, stack)

Functional Free EC Firmware

Associated constraints, requirements:

- Written in C
- Memory size (program, RAM, stack)
- Flexible implementation for 8051 ECs

Functional Free EC Firmware

Associated constraints, requirements:

- Written in C
- Memory size (program, RAM, stack)
- Flexible implementation for 8051 ECs
- GPLv3-licensed

Functional Free EC Firmware

Associated constraints, requirements:

- Written in C
- Memory size (program, RAM, stack)
- Flexible implementation for 8051 ECs
- GPLv3-licensed

Origami Embedded Controller firmware (Origami-EC)

A flexible free software embedded controller firmware implementation for 8051-based platforms.

Origami-EC

Architecture:

Origami-EC

Architecture:

- Event-driven, no task and context switch

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Current status:

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Current status:

- Console, commands

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Current status:

- Console, commands
- LEDs
- Buttons, switches

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Current status:

- Console, commands
- LEDs
- Buttons, switches
- Close to power on!

Origami-EC

Architecture:

- Event-driven, no task and context switch
- Generic APIs, common code
- Platform/device-specific implementations

Current status:

- Console, commands
- LEDs
- Buttons, switches
- Close to power on!
- Not public yet

Roadmap and Discussion

Roadmap:

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)
- Keyboard support
- Peripherals support

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)
- Keyboard support
- Peripherals support
- Advanced power management (*suspend/resume*)
- EC power saving

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)
- Keyboard support
- Peripherals support
- Advanced power management (*suspend/resume*)
- EC power saving

Discussion:

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)
- Keyboard support
- Peripherals support
- Advanced power management (*suspend/resume*)
- EC power saving

Discussion:

- EC-host protocol

Roadmap and Discussion

Roadmap:

- Turn the damn thing on!
- Host communication (LPC)
- Keyboard support
- Peripherals support
- Advanced power management (*suspend/resume*)
- EC power saving

Discussion:

- EC-host protocol
- Installation process

About the project:

About the project:

- Origami-EC public release

About the project:

- Origami-EC public release
- Associated infrastructure:

About the project:

- Origami-EC public release
- Associated infrastructure:
    - Development repository
    - Documentation
    - Mailing list

About the project:

- Origami-EC public release
- Associated infrastructure:
  - Development repository
  - Documentation
  - Mailing list
- emu8051, emu8051-device public release

About the project:

- Origami-EC public release
- Associated infrastructure:
  - Development repository
  - Documentation
  - Mailing list
- emu8051, emu8051-device public release
- Contributions (technical or not) are welcome!

About the project:

- Origami-EC public release
- Associated infrastructure:
  - Development repository
  - Documentation
  - Mailing list
- emu8051, emu8051-device public release
- Contributions (technical or not) are welcome!

Thank-you!