AMD and coreboot

History and Future

What this talk is not...

ARM cores

Zen cores

AMD-approved

factual? 😉

What this talk is...

- How to speak AMD
- Old and legacy
- AGESA and CIMx
- binaryPI
- Going forward
- Resources

How to speak AMD - CPUs and APUs

- Family: microarchitecture generation
  - Models: microarchitectural improvements, and other features
  - ex. Family 15h, Models 70h-7Fh
  - May iterate concurrently
- Codenames
  - For microarchitectures, dies, variants, platforms
    - ex. name: Bulldozer/Orochi/Valencia/Adelaide
  - Some codenames seemed to stick, while others didn’t
    - ex. Ontario/Desna/Zacate -> Brazos
- Embedded
  - G-Series and R-Series
  - Bird codenames
  - Unique graphics Device IDs

How to speak AMD, continued

- Accelerated Processing Unit (APU)
  - Re-monikered Fusion device
  - CPU and graphics on same die
- Infrastructure
  - Socket, Package
- AMD64: Integrated northbridge
  - northbridge/amd/cimx/rd890 ?
- IO hubs
  - For APUs - Fusion Controller Hub (FCH)
    - Many variants
    - Codenames Hudson, Bolton
  - 3-chip - SBxx0
  - Newest APUs use integrated FCH
    - e.g. Kern

The old

- Native coreboot ports
  - AMD64
    - Family 0Fh
    - Family 10h
      - Still active?
    - Family 15h
      - Still active for certain models
  - Geode
    - Geode GX2: branded as Geode GX (IIRC)
    - Geode LX
    - No Geode NX
    - No SCxx00

AGESA and CIMx

- AMD Generic Encapsulated Software Architecture
  - Current version “Arch2008”, v5
  - Spec at http://developer.amd.com/resources/developer-guides-manuals/
- BIOS enablement source code
  - Various coreboot ports beginning at Family 10h
  - Firmware calls specific Entry Point functions
    - May populate structures for system configuration
  - Firmware implements callback functions
  - Firmware provides cache-as-RAM setup/teardown (from reference)
  - Proprietary debug interface
- CIMx
  - Older initialization reference code
  - May be overly named in coreboot?

AGESA Entry Points

- romstage
  - AmdInitReset() - minimal system setup
  - AmdInitEarly() - release and wait for APs
  - AmdInitPost() - bring DRAM online
  - AmdInitEnv() - close down pre-DRAM operations
- ramstage
  - AmdInitMid() - set up UMA and graphics
  - AmdInitLate() - fill ACPI and DMI info
  - AmdInitRtb() - ready to boot, S3 save
- S3 resume only
  - AmdInitRsm() - device and memory reinitialization
  - AmdS3LateRestore() - restoration after PCI

AGESA and CIMx - continued

- AGESA
  - See vendorcode/amd/agesa/f<xx>/Proc
  - Significant duplication of source
  - Various settings established at build
    - Not possible to override with structures at Entry Points
  - Cache-as-RAM teardown known issue in some ports
    - Some use wbinvd to preserve stack info into DRAM backing
    - Kyosti Malkki refactored boot flow for teardown with empty stack - WIP?
- CIMx
  - Term may be overused in coreboot?
    - AMD releases Platform Initialization (PI) package

binaryPI

- Precompiled AGESA blob
  - Identical Entry Point functions and callbacks
  - Wrapper locates module, calls offset it finds in blob header
    - Entry Point indicated with a token
- Developed to enable coreboot at first silicon availability
  - Alleviated “IP scrub”
  - Eased resource constraints at AMD
- Bad!
  - It’s a blob
    - Not auditable
    - Ownership
  - Sync two separate builds for default values
  - No S3?

Going forward

- Stoney Ridge - Family 15h Models 70h-7Fh
  - APU similar to Carrizo
  - Initially went into coreboot as typical cpu/northbridge/southbridge
- Change to soc/
  - More intuitive supporting soc_ function calls
  - Clean break
    - No backward-compatibility with other AMD support
    - No bringing older AMD forward
  - Improve source and function
    - Meet coreboot standards
    - NB is carried from Family 15h native port?
      - Multi-node, multi-chip module
    - Modernize SMM

Going forward - continued

- Change to soc/ ...
  - Support across additional coreboot stages
  - Boot flow via soc code, not mainboard
  - Enable C_ENVIRONMENT_BOOTBLOCK
    - Move CAR setup to bootblock
    - Move AmdInitReset() and AmdInitEarly() to bootblock
    - Use lib/bootblock.c
  - Implement postcar stage
    - Remove CAR global migration issue
- Improve binaryPI-coreboot interaction
  - Address plaguing architectural issues
    - Move control to coreboot where possible
      - APs, MTRRs, etc.
    - Port from AmdLib functions
    - S3

Going forward - AGESA

- Some Platform Security Processor (PSP) support
  - Required for proper graphics operation
  - Required for proper power and temperature management
  - Required for S3
  - PSP restores DRAM and Memory controllers: t.b.d.
- binaryPI
  - Push to open the source
    - Separate location, probably
  - Relocatable
- AGESA v9
  - Newest architecture
  - Encompasses PSP functionality
  - Hope to use binaryPI experience to influence changes to v9
    - Currently developed for UEFI
  - Push to open-source the code

Resources - Specs

- BIOS and Kernel Developer’s Guide (BKDG), mixed public and NDA
- AMD64 Architecture Programmer’s Manual (APM) vols. 1-5, public
  - 2: System Programming
  - 3-5 Instruction set
- Discrete core logic
  - Register Reference Guide (RRG), mixed
  - Register Programming Requirements (RPR), mixed
- AMD Platform Security Processor BIOS Architecture Design Guide, NDA

Resources - Specs, continued

- Revision Guide / Specification Update, mixed
- Less interesting
  - Software Optimization Guide, family-specific is NDA
  - Power and Thermal Datasheet (PTDS), NDA
    - Detailed definition of each SKU
  - Infrastructure Roadmap (IRM), NDA
    - List of features by family, by package
  - Functional Datasheet (FDS), NDA
    - Pinout and physical attributes of a package
  - Electrical Datasheet (EDS), NDA
    - AC, DC characteristics, sequencing

Resources - Other

- nda.amd.com
- Platform Initialization (PI) package
- Hardware Development Tool (HDT)
  - Probes: Wombat, Purple Possum, … special request/purchase from AMD
  - Processor Debug Mode (PDM) block accessed over JTAG
- BIOS TestSuite
  - Confirms proper system configuration according to BKDG
  - Run local or over HDT
- AMD Specialized Tool Suite
  - Windows: one big installer
  - Linux: N/A but individual tools for download
- Honorable Mention: Sage SmartProbe
  - JTAG probe
  - No general availability, no updates for new APUs, no support, no licenses

Thanks. Questions?