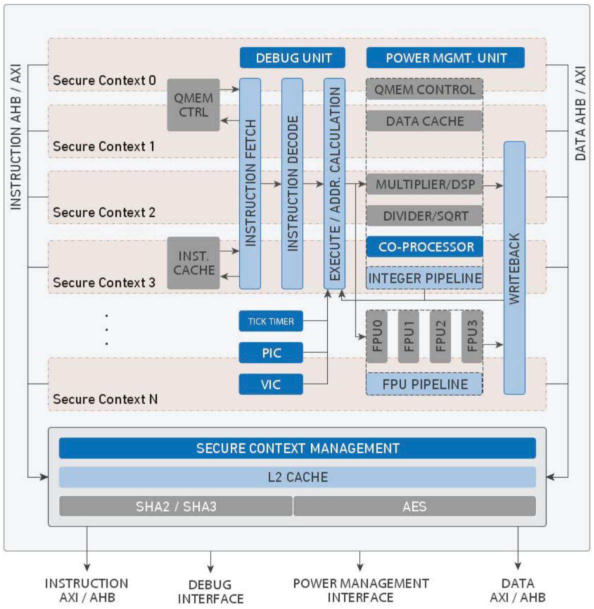
GEON

Secure Execution Processor

The Geon™ Secure Execution Processor is a low-power, 32-bit processor IP core with built-in protection of sensitive code and data. It uses two or more cryptographically separated execution contexts for a high degree of security during code execution and for data storage and transfer to and from the processor.

Geon benefits from the extreme code density of the BA2x^{TM} ISA, and employs advanced power management to further lower CPU and memory subsystem power consumption. It can be licensed without volume-based royalty fees.

Secure Execution with Geon



Geon addresses two fundamental security risks of modern SoC designs. First, it protects against breaches of confidentiality and integrity when firmware is stored outside or transferred to the processor. Geon does this by using authenticated encryption: code and data are only decrypted and checked for integrity at fetch time within the processor, and therefore are protected while they reside on the system memory or while being transferred to the processor.

Second, Geon protects against breaches of sensitive code and data from compromised software threads. For this it assigns address spaces and processor units to just one of the multiple secure execution contexts, and uses a separate set of encryption keys per execution context for the code and data encryption. In this manner, even a complete breach of a software thread in one execution context fails to compromise the data and code of the other contexts.

Processor Description

Geon implements a versatile and efficient 32-bit processor with five pipeline stages. It interfaces to main memory via separate instruction and data caches. It supports tightly coupled memories for fast and deterministic access to code and data, and its Memory Management Unit enables the use of virtual memory.

Geon connects to main memory and peripherals via 32-bit wide AMBA® AHB™ or AXI data and instruction buses. Its default configuration includes up to 32 general purpose registers, a tick-timer, a programmable interrupt controller, and an advanced power management unit. Options include modules for debug, floating point, vectored interrupt control, ROM patching, and hardware multiplication and division. The processor can be extended to execute the rich set of DSP extensions of the BA2x ISA, or to handle custom instructions using its inline coprocessor interface.

Features

Built-in protection of code and data in a 32-bit compact, low-power, royalty-free, processor IP core.

Secure Execution

- Protects sensitive code and data during execution, storage, and transfer to/from the processor
- Uses two or more cryptographically isolated secure execution contexts
- Agnostic to cryptographic primitives:
  - uses lowest-overhead Keccak-based (SHA3) crypto engine by default;
  - can alternatively support any cryptographic hash functions and symmetric cipher

Low-Power Operation

- Extreme Code Density of the BA2x™ ISA minimizes instruction memory area and power consumption
- Advanced Power Management
  - Dynamic clock gating and power shut-off of unused units
  - Software- and hardware-controlled clock frequency
  - Wake-up on tick timer or external interrupt
- Small silicon footprint: just 35K gates on 90nm

Processing Efficiency

- 1.79 DMIPs/MHz
- More than 450 MHz on 90nm

Optional Processor Units

- Programmable Vectored Interrupt Controller Unit
- Timer Unit
- Debug Unit:MDB and Trace port support
- ROM patching Unit
- Floating Point Unit
- Hardware Multiplier/Divider

Easy Software Development

- Non-intrusive JTAG CPU and system debug/trace
  - Complex chained watchpoint and breakpoint conditions
  - BeyondStudio™ complete IDE for Windows or Linux (Eclipse)
  - Ported libraries and operating systems

April 2017

Applications

Designers using Geon get the benefit of robust protection of code and data in a compact, low-power processor core. Geon brings secure execution to embedded and deeply-embedded processors, and is suitable for the design of a wide-range of SoCs, especially wearable electronics and Internet of Things nodes for automotive, industrial, healthcare, and home automation applications.

The BA2 Instruction Set

Geon supports the BA2x instruction set, which provides extreme code density without compromises in performance, ease of use, or scalability. It features:

- A linear, 32-bit address space
- Variable length instructions: 16, 24, 32, or 48 bits
- Simple memory addressing modes
- A configurable number of 12 to 32 general purpose registers
- Efficient flow-control, arithmetic, and load/store instructions
- Floating point and DSP extensions

Deliverables

The core is available for ASICs in synthesizable Verilog source code, and includes everything required for successful implementation. The core is delivered with software development tools Windows and Linux, with an Eclipse IDE interface.

Additional microcontroller peripherals may be ordered for pre-integration and delivery with the core, individually or in a complete platform. IP Integration Services are also available to help integrate the processor with memory controllers, image compression, or other CAST IP cores.

Support and Services

The core as delivered is warranted against defects for 90 days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

IP Integration Services are also available to help minimize time to market for Geon-based systems.

Related Products

The BA2x™ Processor Family includes a set of royalty-free, pre-configured products intended for different applications:

- **BA25** 32-bit Application Processor, for demanding systems running applications on general-purpose operating systems such as Linux and Android.
- **BA22-AP** 32-bit Basic Application Processor, for embedded applications that may need to run a full OS.
- **BA22-CE** 32-bit Cache-Enabled Embedded Processor**,** for deeply embedded systems using off-chip instruction and data memories and possibly running an RTOS; 5-stage pipeline, caches but no MMU.
- **BA22-DE** 32-bit Deeply Embedded Processor, for deeply embedded applications that use on-chip instruction and data memories.
- **BA21** 32-bit Low-Power Deeply Embedded Processor, that delivers better performance than most processors of its size..
- **BA20** PipelineZero 32-bit Embedded Processor, uses an architecture optimized for maximum energy and performance efficiency in wearables and other mobile devices.

A hardware debug key plus complete reference designs and pre-integrated platforms for AMBA bus based systems are also available.

CAST
info@cast-inc.com
www.cast-inc.com

CAST, Inc.   50 Tice Blvd, Suite 340
Woodcliff Lake, NJ 07677 USA
tel 201-391-8300   fax 201-391-8694

BEYOND SEMICONDUCTOR

Geon is sourced from
Technology Partner Beyond Semiconductor