NEWS

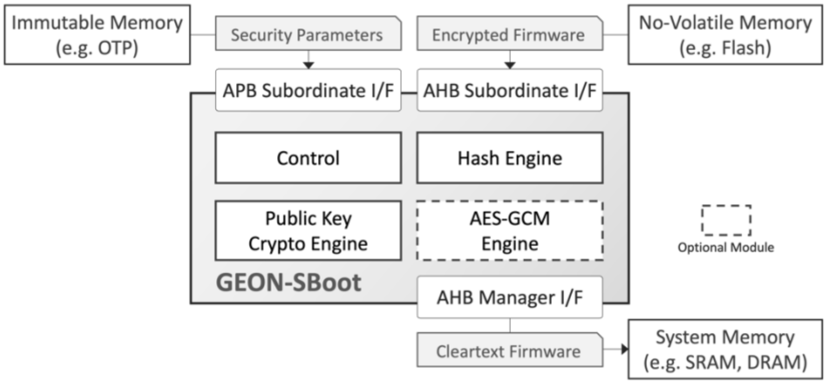
CAST

SoC Secure Boot Hardware Engine IP Core Now Available from CAST

New IP provides fast, area-efficient, processor-agnostic protection against booting a system from malicious or otherwise insecure code

Woodcliff Lake, New Jersey — **March 15, 2024** — Semiconductor intellectual property provider CAST today announced a new security IP product that SoC developers can use to ensure that their system only boots with unmodified firmware from a trusted source.

The new GEON-SBoot GEON™ Secure Boot Hardware Engine employs public-key encryption, namely RSA or optionally NIST-validated Curves, to ensure the integrity and authenticity of a system's boot image firmware. This approach requires no secret to be stored on the chip, resisting physical and side-channel attacks, easing security deployment, and enabling secure firmware updates over the air (OTA). GEON-SBoot can optionally use AES-GCM symmetric authenticated encryption to protect the confidentiality of the firmware and prevent other devices from running firmware clones. Functioning autonomously without any software assistance from the host CPU(s), GEON-SBoot's operation is isolated and, hence, immune to software attacks.



GEON-SBoot is carefully designed to provide its extensive security benefits with minimal impact on silicon area or system performance. A typical base configuration occupies approximately 50,000 gates and requires 8k to 11k bytes of internal memory. Its impact on boot time is typically on the order of a few milliseconds.

The new secure boot engine is compatible with nearly any system and using it is straightforward. GEON-SBoot works with all modern processor architectures—including RISC-V and ARM®—and is independent of memory types. Standard AMBA® AHB and APB interfaces simplify system integration. GEON-SBoot provides great boot control flow flexibility, and designers can optionally use the crypto accelerators within it post-boot elsewhere in their system.

The new GEON-SBoot IP core is production-proven and is shipping now with royalty-free licensing in RTL source code for ASICs or optimized netlists for FPGAs.

The off-the-shelf, ready-to-use GEON-SBoot product complements the **GEON-SoC** SoC Security Platform/Hardware Root of Trust, a semi-custom package of IP cores and capabilities that CAST optimizes for any particular system in collaboration with the system's developers. CAST also offers a variety of AES, SHA, and other Encryption Primitive IP Cores for easily adding a secure hardware crypto engine where required.

GEON-SBoot is sourced from Beyond Semiconductor, who have extensive experience in processor design and system security solutions.

See more GEON-SBoot details on its product web page.

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a silicon IP provider founded in 1993. The company's ASIC and FPGA IP product line includes microcontrollers and processors; compression engines for data, images, and video; interfaces for automotive, aerospace, and other applications; various common peripheral devices; and comprehensive SoC security modules. Learn more by visiting www.cast-inc.com.

CAST is a trademark of Computer Aided Software Technologies Inc.
Other trademarks are the property of their respective owners.
# # #

Media Contact:
Artemis Couroupaki, a.couroupaki@cast-inc.com