GEON-SoC

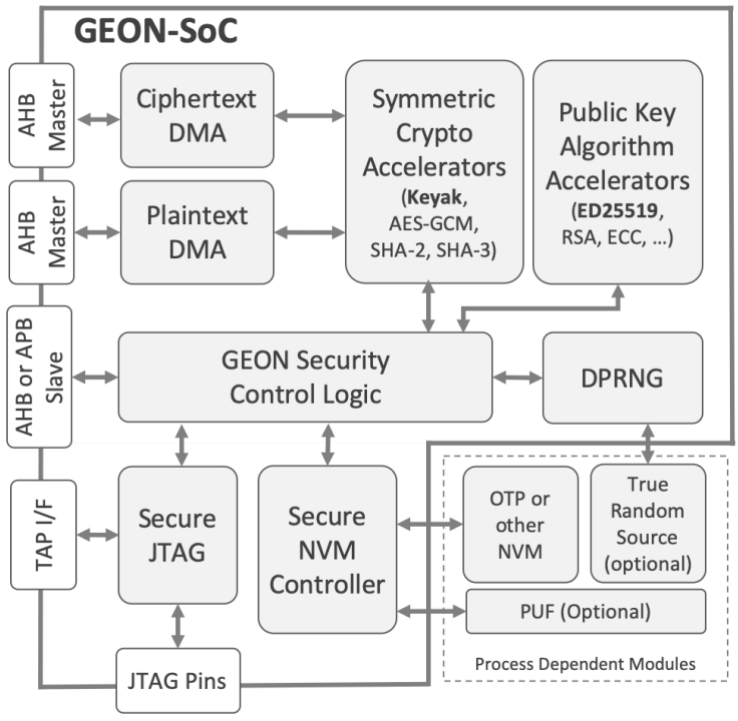
SoC Security Platform

GEON-SoC is an area-efficient, processor-agnostic, hardware root of trust for SoC designs. It implements secure boot and can optionally be enhanced to support firmware decryption and secure debug, or to act as a post-boot hardware security module (HSM).

As a hardware root of trust, the GEON-SoC platform guarantees the authenticity and integrity of the loaded firmware. To this end, GEON uses state-of-the-art cryptographic digital signatures, an approach that requires no “secret” to be stored on-chip (only the vendors’ public key). GEON optionally supports authenticated decryption in case the firmware itself needs to be protected using encryption.

Furthermore, the optional GEON Secure Debug function restricts functional access via the debug interface to trusted users only, and may also provide device authentication. Authentication of trusted users employs a challenge/response scheme based on public-key cryptography. As in the case of firmware authentication, user authentication requires no private key to be stored on chip.

After booting, the SoC Security Platform can be transformed to an HSM, allowing the system to use its cryptographic primitives and functions (random number generation, generation of keys, implementation of encryption algorithms).



Designed for reuse, the GEON SoC Security Platform is processor-agnostic and works with all modern architectures including ARM, MIPS, RISC-V, and the entire BA2x processor family from Beyond Semiconductor. It is also configurable so that only those functions needed to address the threat assessment of the design team need be selected. This allows a team to minimize area requirements while optimizing the performance of the security subsystem being deployed. Under its default configuration, GEON implements EdDSA/Ed25519 digital signatures, and SHA-3/Keyak v2 authenticated decryption, but can be further equipped with other asymmetric and symmetric cryptographic algorithms like RSA, AES-GSM, etc.

FEATURES

Reusable, Reliable, Compact HW Root of Trust Platform

- Processor-Agnostic: Works with ARM, MIPS, RISC-V, Beyond BA2x, or any other microprocessor
- Process-Independent: RTL design with flexible interface to technology-specific modules (e.g. OTP)
- Customizable and tunable boot sequence, security algorithms, features, and interfaces
- Security functions share common hardware modules
- Production-proven

Secure Boot

- Ensures integrity and authenticity of firmware
- Independent of & isolated from the application processor(s)
- Uses ED25519 (default) and requires no secret to be stored on-chip
- Minimal boot-time impact (typically 0-5ms)

Firmware Encryption

- Protects confidentiality of externally or internally stored firmware
- On-the-fly Keyak (default) decryption for zero boot-time overhead.

Secure Debug

- Secure JTAG Debug, with end-to-end cryptographic guarantees
- Uses digital signatures to authenticate users. Optional device authentication
- Requires no secret to be stored on-chip

HSM

- Secure generation and storage of secret key material
- Secure operations using secret key material, such as sign, encrypt, decrypt etc.
- Supports ED25519, RSA, AES-GCM, SHA-2, SHA-3 and others

Deliverables

- Verilog RTL source code or targeted FPGA netlist
- Comprehensive User Documentation

Support

GEON-SoC as delivered is warranted against defects for ninety 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.

CAST

www.cast-inc.com • info@cast-inc.com • tel +1 201.391.8300

Sourced from BEYOND SEMICONDUCTOR