Secure Chip Design

Essential Building Blocks for Securing Your SoC

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

Secure & Security - what does it mean for you and me?

- Immune to attack ?
- Incapable of being tampered with ?

- You can’t protect everything all the time - You need to make choices about possible threats and your assets

Secure data EQUALS secure SoC

- SoCs are associated with data at every stage:
  - Generation
  - Transmission
  - Processing
  - Storage
  - Displaying
  - …
- SoC are everywhere – power plants, meters, cars, phones, …

Security around the SoC

- Trade -offs

- The main goals:
  - Keep the original functionality it was designed with
  - Restrict access to only authorized users
  - Prevent data leak, copy, modification
  - …
  - Application specific objectives

Critical components for buliding Hardware Root of Trust

- Secure Boot is a must-have for every application
- Firmware Encryption
- Debugging
- Hardware Security Model

Cryptography for RoT

- Public key cryptography

$\neq$

- Software Lab:
  - Hash generation
  - Private key $\rightarrow$ Signature (certificate of authority)
- SoC:
  - Public key $\rightarrow$ Signature confirmation $\rightarrow$ Authenticity
  - Hash generation & verification – 'tampered or not'?

Firmware Encryption

- Extra protection for critical run-time code:
  - Crucial algorithms, look-up tables, passwords, etc.
- Symetric keys

- Stored encrypted and decrypted when loaded into chip memory

Debugging

- The safest way – No Debugging Access !

- But, if really needed (medical, automotive, ...)

Challenge-response authentication

  - A new public key on the chip
  - True -random number generator
  - A private key on the JTAG external terminal

Multiple Encryption/Decryption Resources

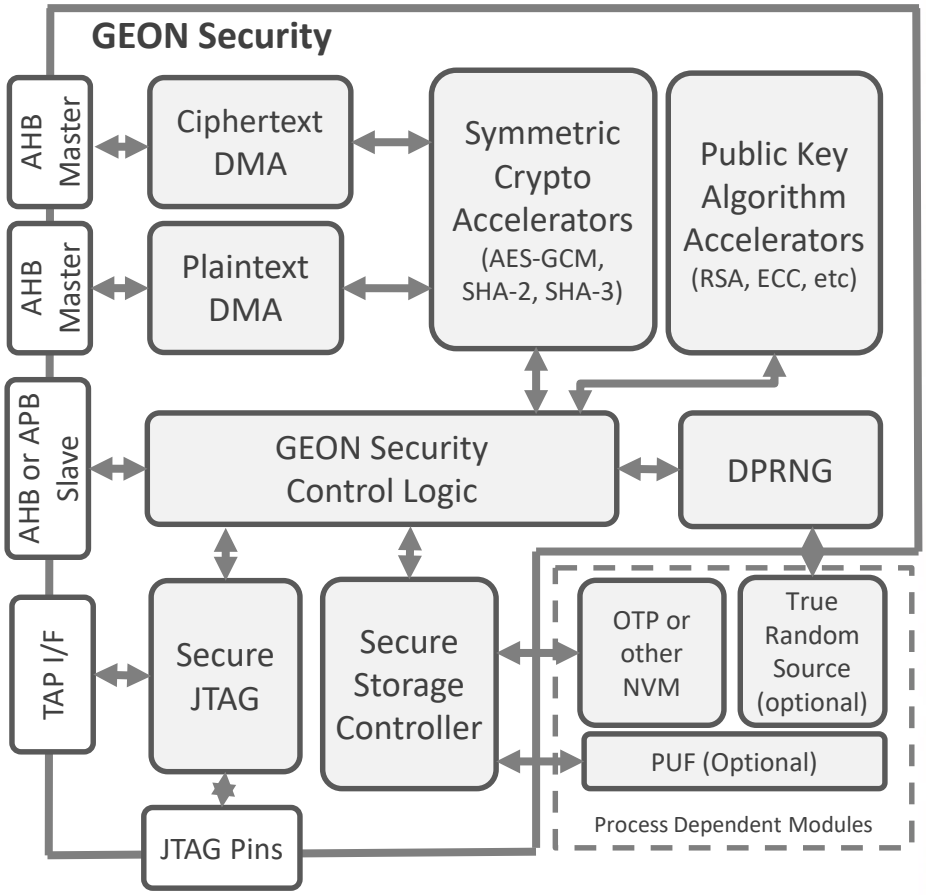
- Hardware Security Model (HSM)
- Re-use by SoC during the run-time
  - Data encryption/decryption
  - Key generation
  - Hashing and many more
- What Next: Design & Use, or ?

CAST Response
The GEON SoC Security Platform

- A scalable collection of essential building blocks each with a specific purpose for designing a customized hardware Root of Trust for a specific secure SoC
  - Processor agnostic
  - Works with RISC-V, ARM, MIPS, BA2x, and any other modern CPU
- GEON consists of the following modules:
  - Secure Boot with Secure OTP
  - Firmware Encryption
  - Secure JTAG
  - HSM
- Everything is designed to work together
  - Saves space
  - Maximizes performance

GEON Flexibility

- The GEON Platform is:
  - Configurable - select only the modules you need to support your security architecture
  - Flexible - reusable components are shared between modules to reduce size and improve performance
  - Arichtecture independent - works with ARM, MIPS, RISC-V, Beyond BA2x or other well known processor architectures
  - Designed to work as HSM and performs stand alone functions during the run-time



Why you should consider GEON Security Platform

- It offers a flexible solution to all the basic problems of building a hardware Root of Trust for a secure SoC
  - It is designed to fit the needs of different kinds of customers with different kinds of SoC designs
  - Customer and silicon proven
- Supported by an experienced team of experts that can help solve even the most difficult security problems
- Come and check us out! → **CAST booth at D&R**

Thank you