Configurable Cryptographic Controller Die (C3D)

Brandon Eames, PhD
Principal Engineer,
Principal Investigator for C3D

NIST Crypto Agility Workshop
April 17-18, 2025

intel®

Notices and Disclaimers

For notices and disclaimers, visit
www.intel.com/PerformanceIndex or scan the QR code:

What is Security Autonomy?

Control of Security Implementation

(e.g., autonomous attestation, ownership of keys, verified updates)

Choice of Security Features

(e.g., crypto agility, value-added features, such as acceleration)

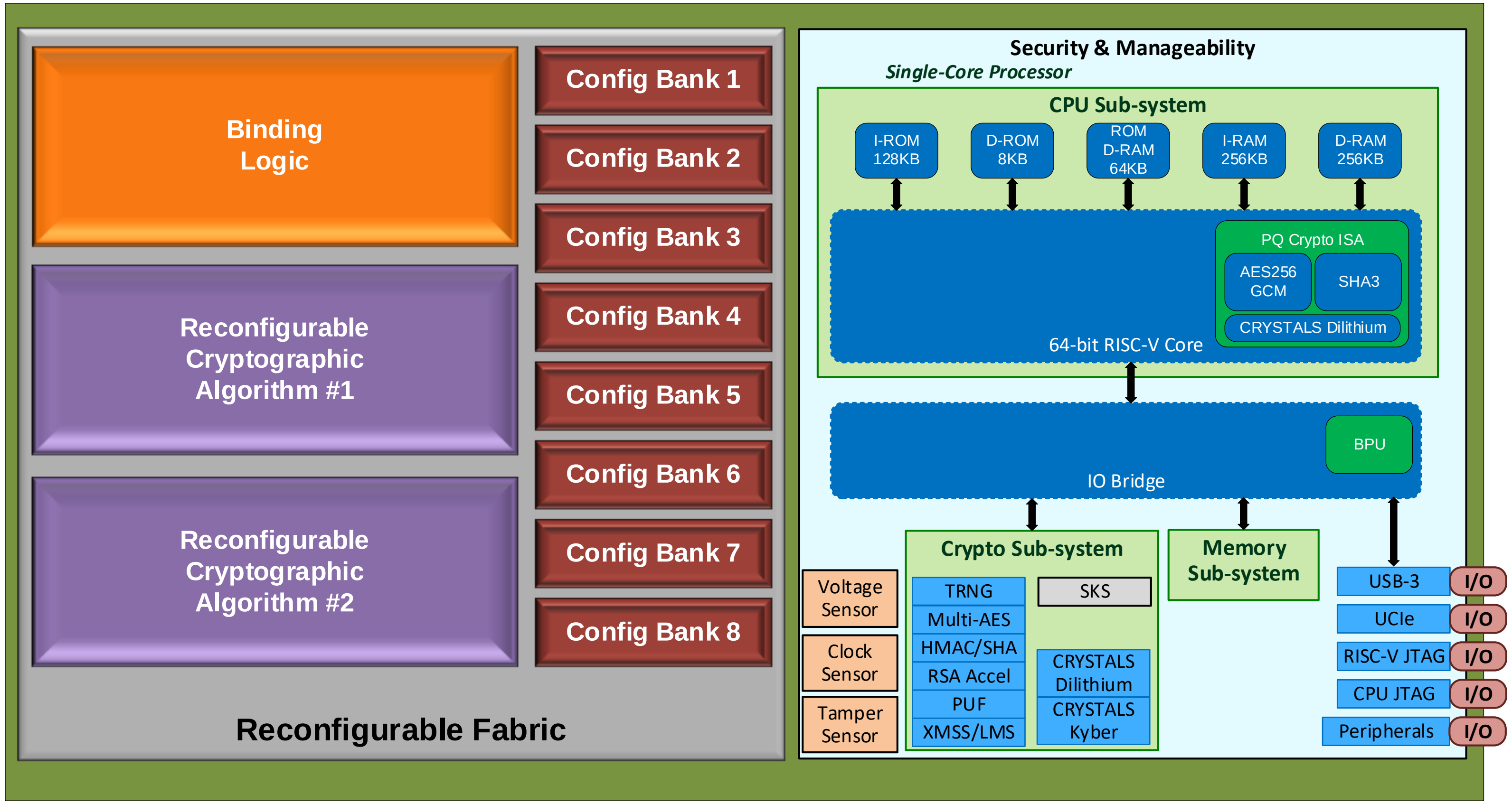
Transparency for Design & Implementation

(e.g., certifiability, open source where relevant)

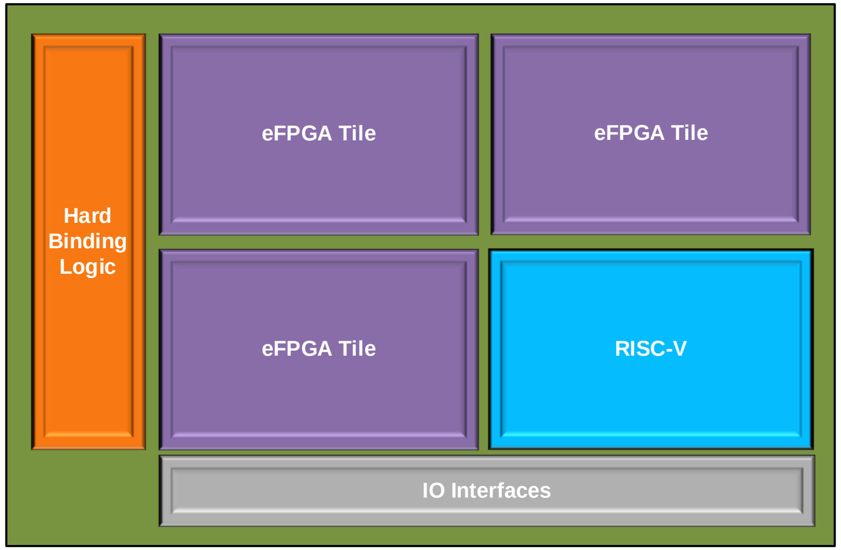
Technical Strategy for Crypto Agility

- Develop a security chiplet solution capable of addressing four pillars of *security autonomy*
- Resulting solution should be capable of being integrated into existing and future products
- Solution should serve as primary security interface into Intel products for external root-of-trust solutions
- Final implementation under complete control of end-customer, though based on initial Intel solution.

Configurable Cryptographic Controller Die (C3D)

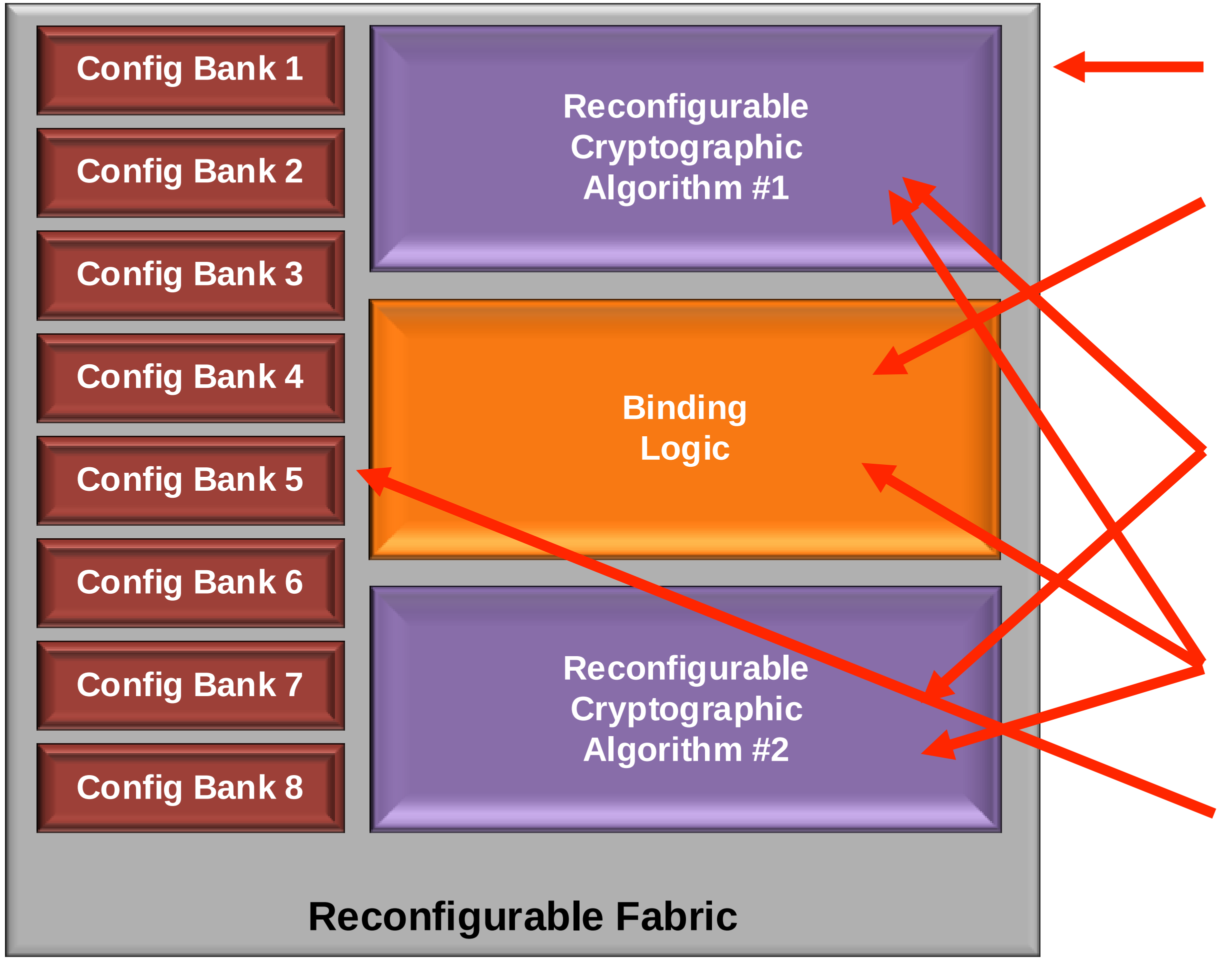


Logical architecture of C3D



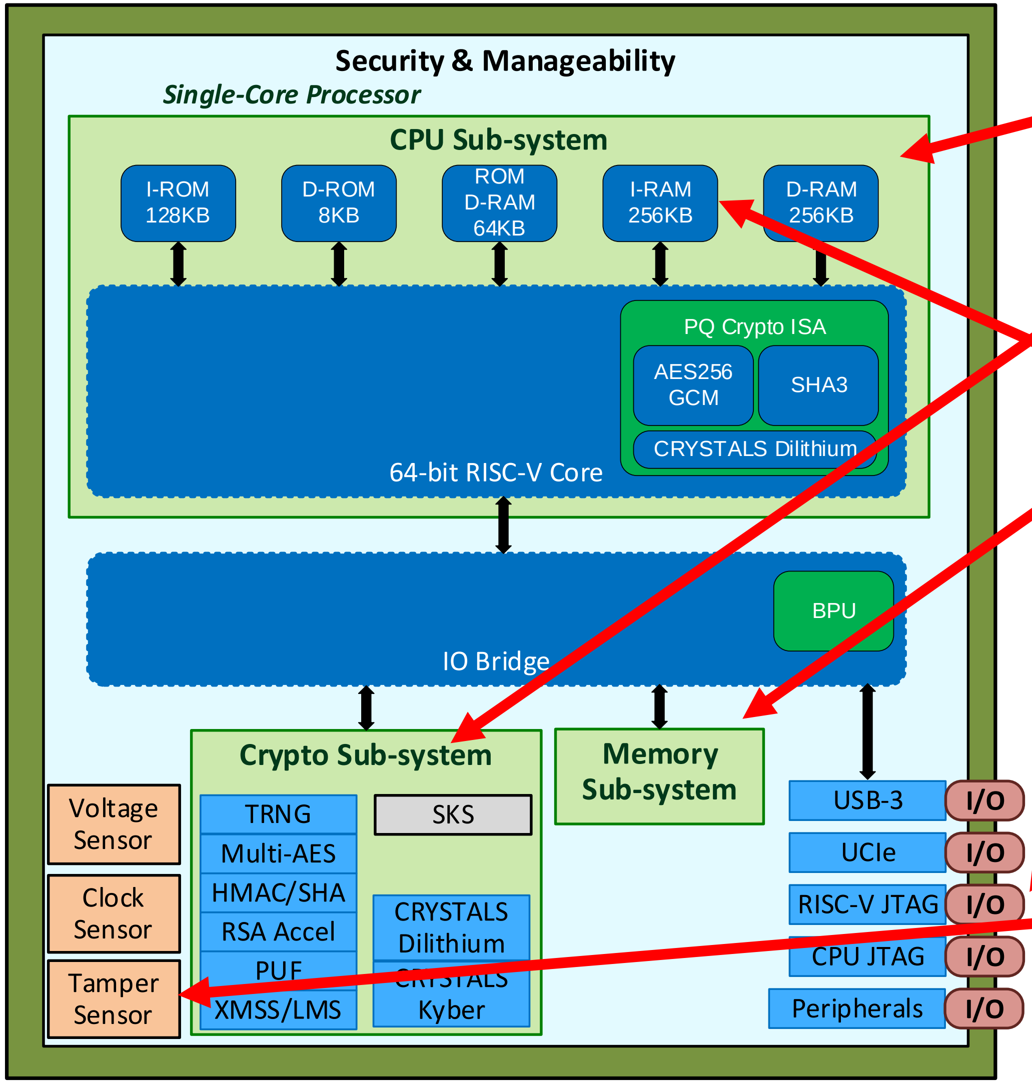
Physical architecture of C3D

C3D – Reconfigurable Logic



- Implemented in embedded FPGA fabric
- Hard binding logic provisioned during manufacturing
  - Can be offered with commercial, government, or custom logic
- Two slots for reconfigurable cryptographic support
  - Provides in-field updateable logic to support new algorithms and updated parameters
- Binding logic implements cryptographic challenge/response binding between itself, the die, and Cryptographic Algorithm implementations
- Binding data used to maintain and protect device key and identification material for downstream devices

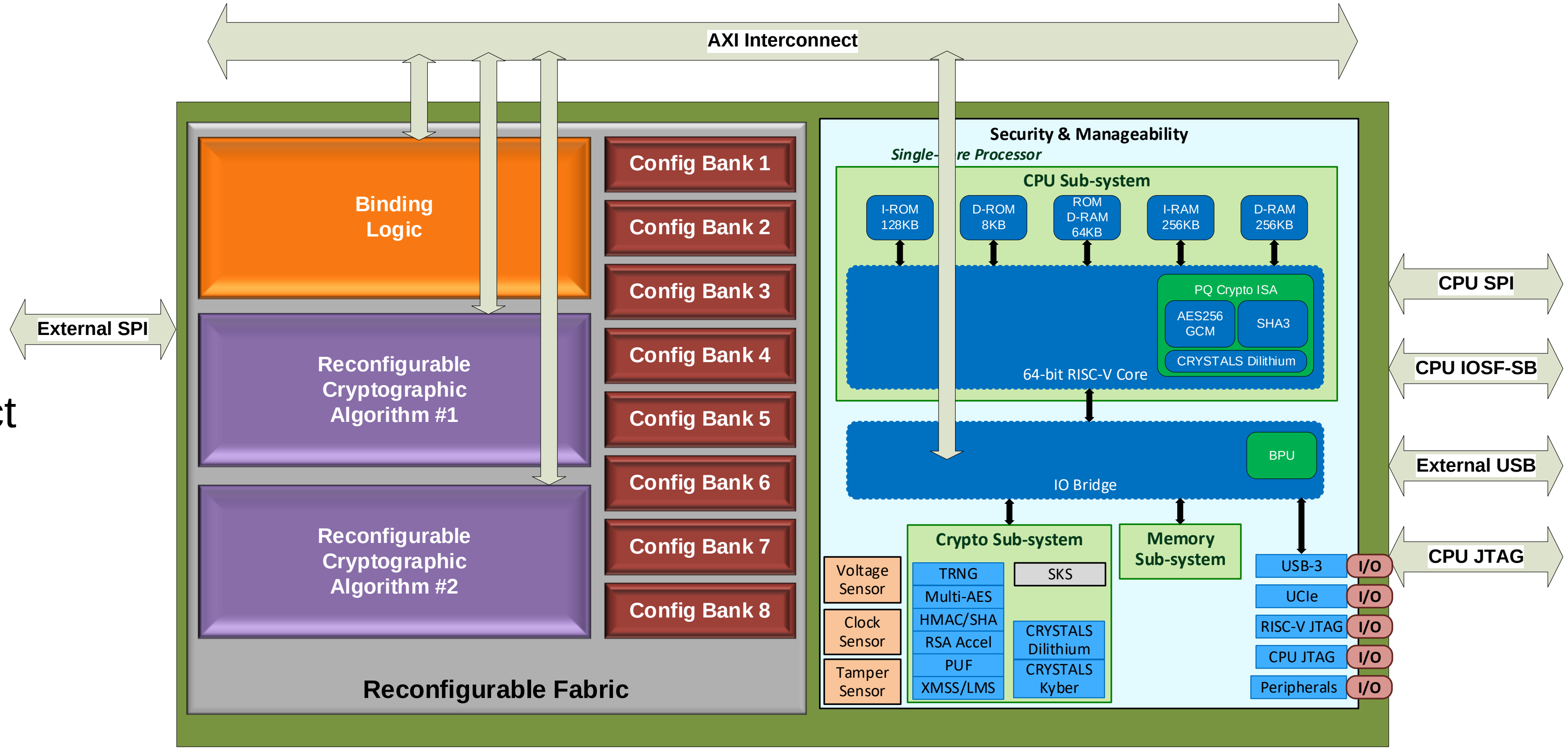
C3D – Security Controller



- Modified Intel Outlook Peak: secure single-core RISC-V processor
- Full crypto suite, including PUF and PQ-resistant algorithms
- Boot code loaded by C3D Reconfigurable Logic into 256 KB I-RAM
  - No code in NVM of RISC-V
  - Full boot control via External RoT
- No open JTAG
  - Managed via External RoT
  - Requires encrypted comms
  - Removable for deployment builds
- Inputs for various tamper sensors

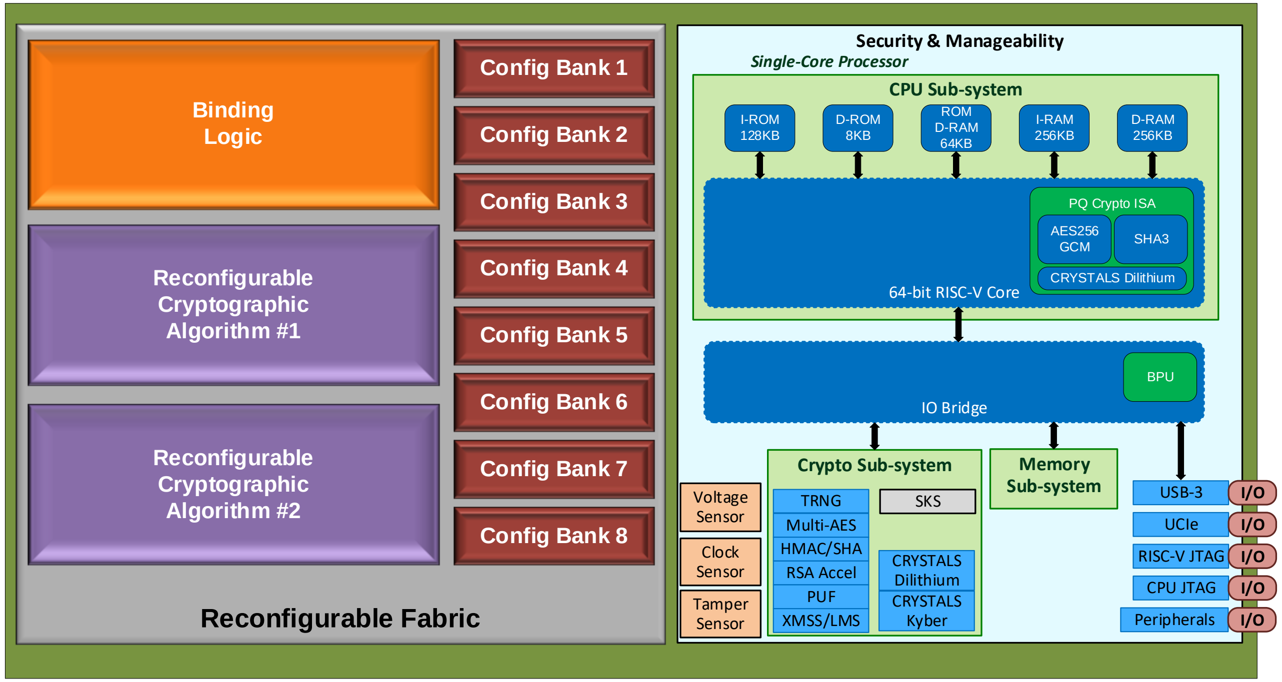
C3D with Interfaces

- Internal interface for C3D is currently based upon AXI
- External interfaces are generic, but can be customized based upon implementation
- Likely to provide UCI interconnect for high-speed data transactions
- AXI interconnect allows Binding Logic controller to directly write processor boot code into CPU subsystem I-RAM



C3D – Reconfigurable Logic Protections

- Individual elements protected using 3rd-party or custom IP blocks, such as:
  - Physically unclonable function (PUF)
  - Interface integrity sensors
  - Physical volume protection (PVP)
  - Temperature, voltage, clock sensors
- Initial die developed by Intel and provided with open access to HW design and open-source control over SW



- C3D expected to be enabled within Intel Foundry Services (IFS), allowing adopters to fully control the hardware design as well
- Adopter may also create a separate instance of C3D and have it integrated into an existing Intel product
  - Dimensional and interface specification will be provided to enable such development

Current State

C3D – TRL 2

- Components
    - Unmodified Intel Outlook Peak (TRL 6) test chip completed, currently working on version 2.0
        - Includes PQC implementations
        - C3D-specific modifications to Intel Outlook Peak have not yet been developed
    - Binding logic implementation is under development, leveraging external IP
- Implementation
    - Estimated size at 4mm x 2mm, much smaller than traditional chiplet
    - Two potential options –
        - Leave as standalone chiplet that integrates with external RoT (co-packaged or separate)
        - Integrate 3rd-party RoT element onto C3D chiplet, using a full 16mm x 16mm offering
- Interconnects
    - Currently assessing best interconnects for ease of integration with all possible components
    - Planning support for USB-3, PCIe/UCIe, and ethernet (likely only for commercial) to external RoT or depot provisioning element

Acknowledgements

- Matt Areno, CTO of Rickert-Areno Engineering, LLC is partnering with Intel and has contributed significantly to the development and evolution of C3D

intel®