Apollo

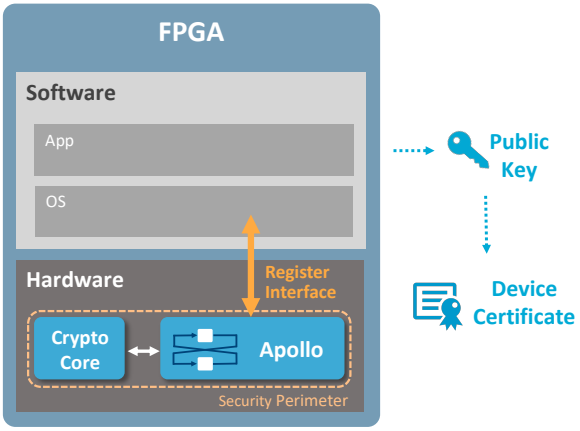
Apollo uses circuits present inside the FPGA to create a key vault which allows designers to secure data in transit and on chip.

FPGAs are widely used in mission-critical environments with specific processing needs. Motivations for copying or altering sensitive data or valuable IP are abundant. Especially in aerospace and defense, attacks can result in loss of IP, leakage of top-secret information and compromised national security. A way for designers to secure their FPGAs, its sensitive data and communications, is the use of cryptography. Authenticity, integrity and confidentiality can be guaranteed by using strong cryptographic keys, rooted in the hardware of the FPGA.

Apollo combines a butterfly Physical Unclonable Function (PUF) with Intrinsic ID's helper data algorithms. Butterfly shaped circuits are configured on the fabric of the FPGA to intrinsically generate the entropy needed for a strong hardware root of trust. Keys derived from Apollo are volatile and derived only when required providing a significant high security assurance. Since Apollo is part of the FPGA configuration file it is a "soft PUF" implementation and security functionality can be retrofitted on deployed devices, enabling remote "brownfield" installation of a hardware root of trust.

The FPGA "Intrinsic Fingerprint"

The biggest challenge when solving security problems is getting credentials, such as cryptographic keys, into the device and keeping them secure. For FPGA architectures in which standard uninitialized SRAM is not available, a butterfly PUF* enables designers to extract a unique device fingerprint from standard FPGA fabric. This fingerprint is converted to a high-quality device-unique PUF key using Intrinsic ID's helper data algorithms (or fuzzy extractor). Apollo FPGA IP reliably reconstructs the same cryptographic key under all environmental circumstances.



Upon first use, called the enrollment, Apollo generates an activation code which, in

Applications

- Secure Key Storage
- Authentication
- Flexible Key Provisioning
- Anti-Counterfeiting
- IP Binding
- Supply Chain Protection

Benefits

- Compatible with standard FPGA products
- No sensitive key material present on device
- High protection against tampering and invasive attacks

combination with the butterfly PUF fingerprint, is used to reconstruct on demand, in real time, an intrinsic PUF key inside a secure perimeter. The intrinsic PUF key can be used as a root key for key derivation and key wrapping. A key protected by Apollo is integrity protected and can be retrieved only on the same device, while it will be meaningless on other devices.

When used in combination with a crypto core, Apollo allows designers to provision their FPGAs with an unclonable identity, which consists of a private key, a public key and a device certificate. Once provisioned, the FPGA can prove its identity and establish a secure channel with another device, a server or a cloud. The private key is never stored in NVM or OTP, but regenerated on the fly when needed, making the solution very effective against counterfeiting.

	Apollo v1.3
Security Strength (bits)	256
Maximum Key Length (bits)	4096
Size: #LUTS	14.7k - 16.6k
Activation Code Size (bytes)	740
Generate Device Keys and Random Values	✓
Wrap and Unwrap Keys	(✓)
Attack Countermeasures	✓
Anti-aging Measures	✓
PUF Monitoring	✓
Logic BIST	(✓)
Register interface with APB or AXI protocol (optional to remove)	(✓)

(✓) Features are optional

Use Cases

- **Anti-counterfeiting:** binding of proprietary mission-critical IP to the device.
- **Secure communication:** Authentication and encryption of data between heterogeneous devices that are part of a homogenous defense electronics system.
- **Secure supply chain:** enabled by generation of end-user keys which can be wrapped or protected using device-unique cryptographic keys.

Specifications

- Verified on Xilinx platforms Artix-7, Virtex-7, Kintex-7, and Zynq 7000, Kintex UltraScale+, Zynq UltraScale+ and Virtex UltraScale+ (✳)
- Temperature range from -40°C to +125°C
- Voltage supply variation +/- 20%
- Accelerated lifetime > 25 years

Deliverables

Apollo FPGA IP is easily integrated in any FPGA design. Standard deliverables include:

- VHDL top-level design for specific platform
- FPGA module with routing scripts
- Simulation and test bench
- Driver for easy integration
- Documentation

** A butterfly PUF consists of an array of circuits, each consisting of two cross-coupled memory elements, to obtain a bi-stable output behavior. During operation each circuit is brought temporarily into a "conflicting state," and once released the circuit will settle into one of the two allowed states in a non-deterministic way that not even the manufacturer can predict or duplicate.*

✳ For details of specific Xilinx FPGA/SoC platforms, please contact us at MAGsales@intrinsic-id.com