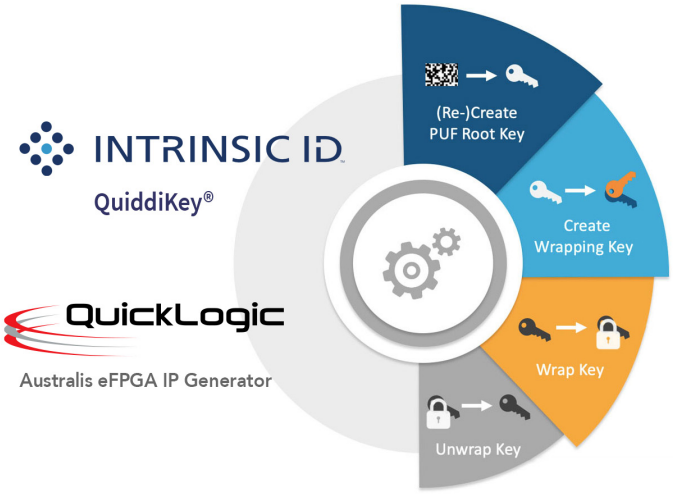
Security Solutions for SoCs with Embedded FPGA Technology



QuickLogic's Australis-generated eFPGA IP is now available with bitstream protection by using Intrinsic ID's QuiddiKey® to provide security options for devices incorporating embedded FPGA (eFPGA) technology. Some of the security options include secure key generation based on SRAM Physical Unclonable Function (PUF) to full security solutions including bitstream encryption, key wrapping, authentication tags, key verification, and data encryption/decryption for storage within the device or for board- or system-level communications. As a result, QuickLogic's eFPGA customers can secure the designs that they implement on the eFPGA or authenticate the design being loaded in the eFPGA.

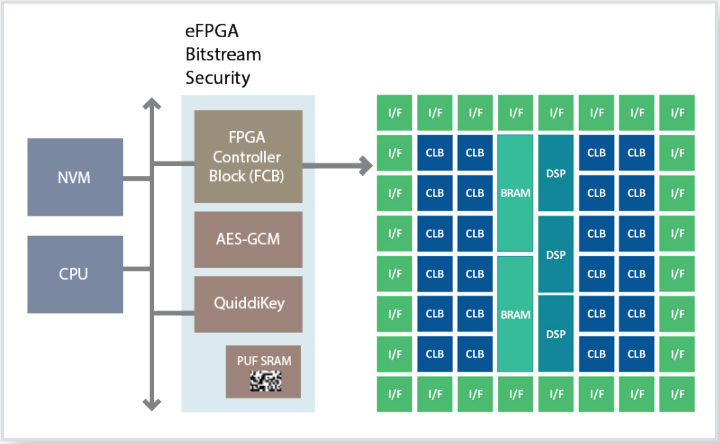
The combined solution provides multiple security options for a wide range of applications ranging from industrial IoT to aerospace and defense. Specific applications include secure key storage, authentication, flexible key provisioning, anti-counterfeiting, IP binding, and supply chain protection.

FEATURES

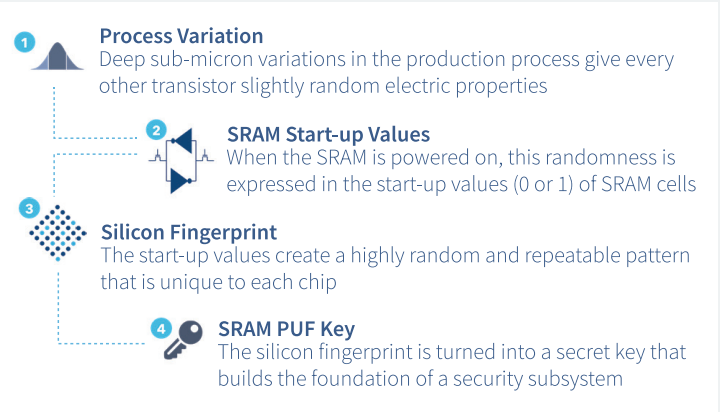
- Uses standard SRAM start-up values as a PUF to create a hardware root of trust
- Root key and other cryptographics keys are reconstructed with QuiddiKey when needed
- The eFPGA bitstream can be securely encrypted and authenticated with AES in GCM mode, protecting its contents and blocking any copying onto unauthorized devices
- The eFPGA bitstream encryption key is protected within a QuiddiKey key code, which encrypts and authenticates keys for the physical device it was created on. The key code can be safely stored in any NVM

BENEFITS

- Secure your eFPGA design and keep your devices from being cloned
- No keys at rest: no sensitive data is present when the device is powered off
- Keys are bound to the device and can only be recreated and accessed on the device they have been created on
- Minimizes overhead through optimized hardware design
- Highly reliable secure key storage solution in the most advanced technology nodes



HOW IT WORKS



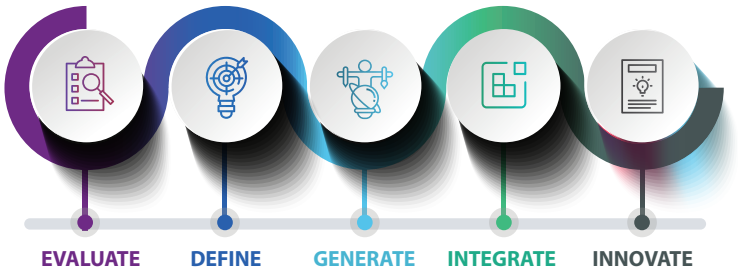
For more information, visit intrinsic-id.com/sram-puf

australis

eFPGA IP Generator

Enables rapid prototyping of customizable FPGA architectures

Australis is QuickLogic's eFPGA IP Generator, blending our three decades of deep domain expertise in designing and shipping programmable logic architectures that are silicon-efficient, reliable, high quality, and manufacturable at scale with the silicon design automation capabilities of the OpenFPGA project.



Features

- eFPGA IP can be generated / customized to any foundry / process technology within days for a process we already support and within a quarter for new process technologies
- eFPGA optimizations for performance, power or area are available
- Multiple eFPGA architectures from LUT4 toLUT6, variable routing density, and more
- Variety of eFPGA array sizes with option to include Block RAM and/or DSPs blocks

Benefits

- Fast-time to market – Customized eFPGA IP cores that meet your development window
- Flexibility to meet your SoC design requirements – Optimized for your power, performance and area requirements
- Cost effective – Our automated approach means cores are customized to your requirements with substantially less cost and time, meeting your cost target

Learn more on the web

QuickLogic

CORPORATE HEADQUARTERS:
2220 Lundy Drive, San Jose, CA 95131 USA
1-408-990-4000 I info@quicklogic.com

SALES OFFICES: https://www.quicklogic.com/company/sales-locations/
NORTH AMERICA: america-sales@quicklogic.com I CHINA: asia-sales@quicklogic.com I JAPAN: japan-sales@quicklogic.com
KOREA: korea-sales@quicklogic.com I TAIWAN: asia-sales@quicklogic.com I UNITED KINGDOM: europe-sales@quicklogic.com