INTRINSIC ID™

Product Brief: QuiddiKey for Intel FPGAs

QuiddiKey – SRAM PUF Based Secure Key Vault

As the threat level from adversaries increases, security countermeasures must be deployed to protect devices used in mission-critical environments. Motivations for copying or altering sensitive data, cloning devices and stealing valuable IP are abundant. In aerospace and defense, nation-state attacks can result in loss of IP, leakage of classified information and compromised national security.

QuiddiKey® for Intel FPGAs is a secure key generation and key vault solution that enables users of Intel Stratix™ and Agilex™ FPGA devices to augment security with intrinsically generated, device-unique cryptographic keys. Keys derived with QuiddiKey are never stored but are reliably reconstructed when required, providing a significantly higher security assurance.

QuiddiKey uses SRAM as a physical unclonable function or PUF source. Based on the randomness inside uninitialized SRAM the IP generates the entropy needed for a strong hardware root of trust. The Intel Secure Device Manager (SDM), of which QuiddiKey is the hardware root of trust, is NIST-compliant security IP.

QuiddiKey uses SRAM PUF technology to generate multiple strong and independent device-unique cryptographic keys that can be used to secure an FPGA device

Proven Security Technology

Intrinsic ID SRAM PUF hardware root of trust technology, QuiddiKey, has been deployed by aerospace and defense electronics end-customers for over a decade. It has been operational in challenging mission-critical environments – both terrestrial and space-based – without breach or failure. The IP is agnostic to foundry and process node technology, and is actively deployed in over 350 million devices.

Use Cases

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

Applications

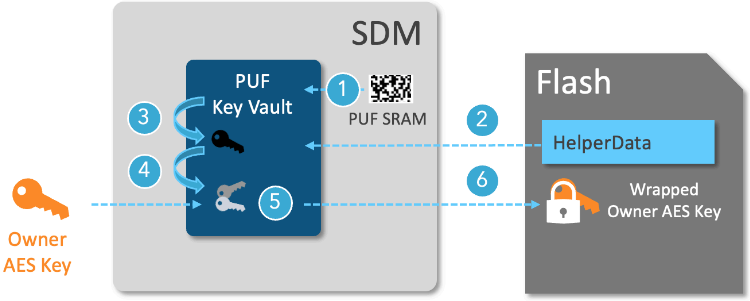
- Secure Key Storage
- Device Authentication
- Supply Chain Protection
- Flexible Key Provisioning
- Anti-Cloning
- IP Binding
- Protection of Bitstream Encryption Key

Certifications

- NIST-compliant crypto
- DoD and EU government approved

Benefits

- No sensitive key material present on device
- High protection against invasive attacks including tampering



Secure Supply Chain

An unlimited number of device-unique keys can be generated by each respective user/owner of the Intel FPGA device in the supply chain. None of these keys are ever stored on the device even when powered off.

This enables users to derive their own device-unique keys and import and protect other secrets. QuiddiKey's wrapping functionality enables the applications and IP of each respective user/owner to be securely and reliably protected – for the lifetime of the device – prior to being deployed in the field.

Secure Based on SRAM PUF

At power up, SRAM bits settle in the one or zero state in a non-deterministic way that not even the fabricator or designer can predict or duplicate. That is what makes a PUF that can be used as a unique "silicon fingerprint."

An SRAM PUF response is a noisy fingerprint, and turning it into a high-quality and secure key vault requires further processing. This is done with the Quiddikey IP. QuiddiKey reliably reconstructs the same cryptographic key under all environmental circumstances. This (PUF) key is never stored in NVM or OTP. When it is needed, it can be reliably reconstructed.

Operational Range

QuiddiKey IP has been embedded on SoC/ASICs in most foundry/process node combinations and proven in diverse operating environments.

- All major fabs from 0.35 µm to 5 nm
- Operating temperatures of -55°C to 150°C
- Voltage supply variation +/- 20%
- Lifetime > 25 years

Deliverables

QuiddiKey IP is integrated into the Secure Device Manager of Intel Stratix™ and Agilex™ FPGA devices.

It is enabled after completion of a license agreement with Intrinsic ID

Standard deliverables include:

- QuiddiKey pre-integrated on Intel FPGA hardware
- Datasheet and training documentation

Stratix and Agilex are registered trademarks of Intel Corporation

For further information about this product please contact us at MAGsales@intrinsic-id.com

INTRINSIC ID

www.Intrinsic-ID.com | info@Intrinsic-ID.com