INTRINSIC ID

BroadKey
Software IP Family

Create. Wrap. Manage. SRAM PUF-based Hardware Root of Trust

SRAM PUF Benefits

- Use standard SRAM
- Unclonable and immutable
- Device-unique high-quality keys
- No secrets when power is off
- No root key programming
- Flexible and scalable

Applications

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

Operating Specifications

- 256- or 128-bit key entropy
- Highly reliable across large range of operating environments and on every fab/technology node
- Lifetime > 25 years
- Proven: 125 million-plus SRAM PUF ICs shipped

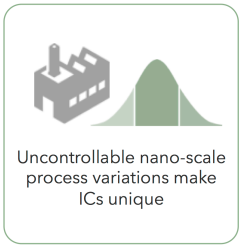
Certifications

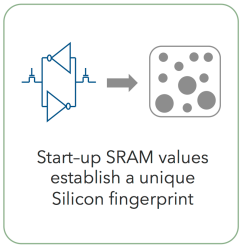
- EMVCo, Visa, CC EAL6+
- U.S. and EU Governments
- BroadKey-Safe compatible w/China's OSCCA standard

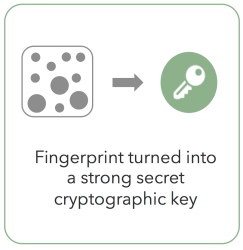
SRAM PUF – Root Key from Silicon "Fingerprint"

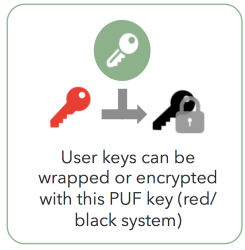
SRAM Physical Unclonable Functions or PUF use the behavior of standard SRAM, available in any digital chip, to differentiate chips from each other. They are virtually impossible to duplicate, clone or predict. This makes them very suitable for applications such as secure key generation and storage, device authentication, flexible key provisioning and chip asset management.

Due to deep submicron process variations in the production process, every transistor in an SRAM cell has slightly random electric properties. This randomness is expressed in the startup values of "uninitialized" SRAM. These values form a unique chip fingerprint, called the SRAM PUF response.


Uncontrollable nano-scale process variations make ICs unique


Start-up SRAM values establish a unique Silicon fingerprint


Fingerprint turned into a strong secret cryptographic key


User keys can be wrapped or encrypted with this PUF key (red/black system)

BroadKey™

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 BroadKey software IP. BroadKey reliably reconstructs the same cryptographic key under all environmental circumstances. It generates an Activation Code which, in combination with the SRAM startup behavior, is used to reconstruct on demand, in real time, an intrinsic PUF key which is never stored. When it is needed later it can be reconstructed. The intrinsic PUF key can be used as a root key to wrap and manage user keys. Reconstruction can be done very quickly starting at 0.7M cycles for 128 bits keys. All of BroadKey's features are accessed by the host software via the BroadKey API.

BroadKey is available in three configurations:

BroadKey-Pro: Device-unique key derivation, random number generation, wrapping and management, including elliptic curve private key generation and storage, importing and exporting of public keys, signature generation and verification, key agreement functionality and public key encryption and decryption.

BroadKey-Plus: Device-unique key derivation, random number generation, application key wrapping and management.

BroadKey-Safe: Low footprint, device-unique key derivation and random number generation.

BroadKey Software IP Family

The intrinsic PUF key is used to wrap and unwrap application keys. A key protected by BroadKey is integrity protected, and can be retrieved only on the same device, while it will be meaningless on other devices. The ECC functionality can be used to generate and protect elliptic curve private and public keys, and to perform elliptic curve crypto operations (sign, verify, key agreement, encrypt and decrypt). The ECC functionality is called only with device-protected keys. This shields the host application from having to handle sensitive key material. The key values themselves are present only internally to BroadKey.

Secure: BroadKey has significant security advantages compared to traditional key storage methods. Each chip has its unique unclonable key. At power-up, SRAM bits settle in the one or zero state in a non-deterministic way that not even the manufacturer can predict or duplicate. Furthermore, because the key is not permanently stored, it is not present when the device is unpowered (no key at rest) and hence cannot be found by an attacker opening up the device.

Low Cost: Keys are extracted from the chip, on demand. Keys do not need to be programmed in NVM or OTP.

Flexible & Scalable: Keys can be provisioned at any suitable stage in the production process. The low footprint and flexible design make BroadKey suitable for most semiconductor platforms, and scalable to billions of devices.

Operating Conditions

Intrinsic ID's SRAM PUF technology operates reliably over a wide range of applications and operating conditions:

- Qualified semiconductor technology nodes ranging from 350nm to 7nm
- Semiconductor processes include low power, high speed and high density
- Temperature range for SRAM PUF reading from -55°C to 150°C [-67°F to 300°F]
- Supply voltage variation +/- 20%
- Lifetime > 25 years

Deliverables

BroadKey Software IP is delivered as a library compiled for a specific target chip, along with interface specifications and user manual.

BroadKey Configurations	Safe	Plus	Pro
Security Strength (bits)	128/256	128/256	128/256
PUF (KB) related to Security Strength	0.7/1	0.7/1	0.7/1
Code Size (KB)	8	10	21
Generate Device Keys and Random Values	Y	Y	Y
Wrap and Unwrap Application Keys		Y	Y
Public Key Management and Crypto Operations			Y

Intrinsic ID Featured Customers

info@intrinsic-id.com
www.intrinsic-id.com
Intrinsic ID Inc., 710 Lakeway Drive, Sunnyvale, CA 94085 U.S.
Intrinsic ID B.V., High Tech Campus 9, 5656 AE Eindhoven, The Netherlands