DATASHEET

Quiddikey
Secure Key Management with SRAM PUF

Features and benefits

- Key generation and reconstruction using SRAM Physically Unclonable Function (PUF)
- User key encryption (wrapping) for key vault / black key insertion
- Keys extracted from device's unique unclonable hardware fingerprint
- High protection against tampering and invasive attacks
- No need to program or store root keys in non-volatile memory
- Different variants optimized for footprint and functionality

Target Markets and applications

- Chip identification and authentication
- Key vault, hardware root-of-trust
- Black key insertion
- Secure Boot, Content Protection
- Supply chain protection, anti counterfeit
- Government and defense
- Industry, automotive
- Mobile, IoT, wearables, tags

Specifications

- 256-bit key strength (80 bit for optimized Quiddikey-Nano)
- High reliability across temperature (-40°C to +125°C), V_{DD}(+/-20%), EMC, Humidity
- Lifetime 25+ years
- Requires 0.3 - 2 Kbyte uninitialized and dedicated SRAM

Deliverables

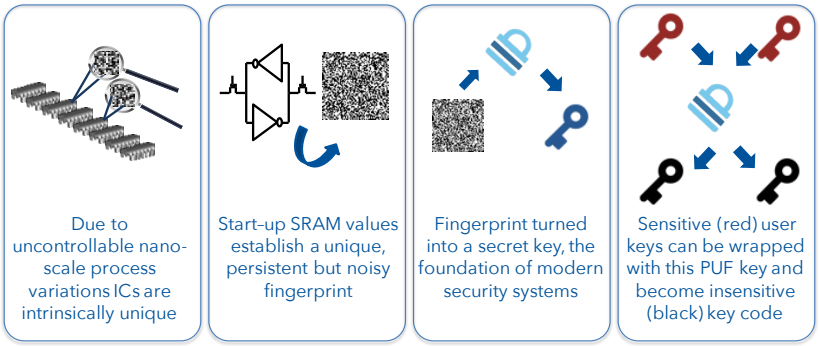
- Delivered as Synthesized IP netlist, Software binary for microprocessor or as an FPGA, ASIC, SoC built-in feature
- Documentation and code samples

Quiddikey - Secure Key Management with SRAM PUF

Quiddikey enables designers to extract a unique device fingerprint from standard embedded SRAM. This fingerprint can be converted to a device-unique cryptographic key that can be used to encrypt or wrap user keys.

SRAM PUF technology

Tiny variations in a semiconductor manufacturing process make each transistor and each piece of silicon unique. These variations are random and uncontrollable making it impossible to construct an exact clone hence Physically Unclonable Function or PUF. These variations are too small to cause chips to malfunction yet they can be measured. Standard SRAM is used for this purpose. The startup behavior of standard SRAM cells results in a unique pattern. This pattern is only available after SRAM power-up and is unique for each chip yet persistent across a wide range of operating conditions.



Due to uncontrollable nano-scale process variations ICs are intrinsically unique

Start-up SRAM values establish a unique, persistent but noisy fingerprint

Fingerprint turned into a secret key, the foundation of modern security systems

Sensitive (red) user keys can be wrapped with this PUF key and become insensitive (black) key code

Quiddikey

Turning this fingerprint into a high-quality and secure key vault requires further processing of the SRAM fingerprint which is done with the Quiddikey logic. Quiddikey extracts the entropy from the SRAM PUF and corrects any errors caused by unstable bits. Quiddikey requires helper data (called Activation Code or AC) to assist in the error correction but this AC is non-sensitive and can be stored off-chip. The resulting PUF key can be used as a root key to encrypt or wrap user keys.

Quiddikey is available in 3 optimized variants:

- ***Quiddikey-Flex***: 256-bit full-entropy key generation, reconstruction and programming. It is the most complete product.
- ***Quiddikey-Light***: 256-bit full-entropy key generation and reconstruction
- ***Quiddikey-Nano***: generation and reconstruction of 256 bit keys with 80 bits of entropy

Quiddikey server products

- **Quiddicard**: enables remote key programming or key wrapping in combination with Quiddikey-Flex
- **Fuzzy-ID**: enables remote identification of a chip based on a fuzzy SRAM fingerprint, often used to retrieve the AC for devices with no local storage option.
- **Trusted-Endpoint**: enables authentication and the set-up of a secure connection with remote devices that have no Non Volatile Memory and limited resources. Uses Fuzzy-ID and Quiddikey.

Note that the Quiddikey product family is closely related to Intrinsic-ID's Confidentio security processing products.

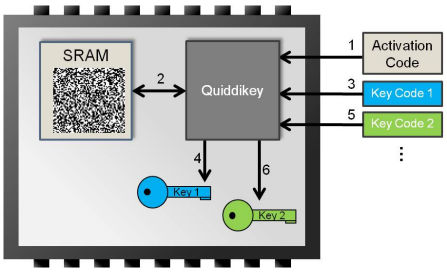
Features and benefits

- Security: Instead of storing keys in non-volatile memory (typically secure FLASH, OTP or E-fuses), Quiddikey allows for secure key extraction from the unique physical properties of the underlying hardware. This "biometrics for electronic devices" provides a high level of resistance against invasive attacks and tampering. Unlike keys stored in NVM, nothing is permanently programmed and no secrets are present at power-off.
- Cost-effectiveness: Quiddikey uses available SRAM as a PUF source, adds minimal overhead with an optimized hardware or software design and eliminates the need for (secure) NVM.
- Flexible and scalable: the low footprint and flexible design make Quiddikey suitable for most semiconductor platforms. Requires no centralized key management and programming.

Detailed operation

During the key reconstruction phase, Quiddikey reads the SRAM startup pattern and receives the Activation Code (AC) as well as a Key Code (KC). AC includes helper data for error correction and KC is effectively an encrypted or wrapped user key. AC and KC are non-sensitive and can be stored off-chip or remotely.

Quiddikey then reconstructs the user key and provides this key to the host system.



The AC code and the PUF key are established during the enrolment phase. This takes place only once, usually during device manufacturing, device testing or at first use.

The KC is established during a key programming phase where Quiddikey-Flex converts the plaintext user key into a wrapped key code. Programming can also be done remotely e.g., in an HSM using Intrinsic-ID's Quiddicard key management software.

Quiddikey-Light and Quiddikey-Nano do not feature user key programming and return a single PUF key.

Operating conditions

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

- Semiconductor process nodes: 180nm, 150nm, 130nm, 90nm, 65nm, 45nm, 40nm, 28nm,16/14nm
- Applications include low power, high speed, and high density
- Temperature range for PUF reading from -40°C to 125°C and beyond
- Voltage supply variation +/- 20%
- Lifetime aging tested up to 25 years

The technology is already used in state of the art security chips for financial, identity and government markets. It was included in chips that achieved EMVCO certification.

Deliverables

Quiddikey can be easily integrated in any semiconductor design or firmware. Standard deliverables can include:

- Synthesized IP netlist
- Software Binary running as executable code on a secure embedded microprocessor or in a Trusted Execution Environment.
- Documentation and code samples

In addition, Intrinsic-ID partners like NXP, Altera, Microsemi, Synopsys and Mentor Graphics provide FPGA, ASIC and SoC platforms that pre-integrate Quiddikey. For a full list of alternatives, see our website.

Intrinsic-ID can provide the following related services:

- Security consulting and architecture
- Product support and maintenance
- Design integration
- Server-side code and integration

Specifications

Quiddikey variants are optimized for footprint and functionality. The table below show the most important specifications for Nano, Light and Flex.

	NO	LT	FX
Key generation	Y	Y	Y
Key Programing	N	N	Y
Entropy (bits)	80	256	256
Key Length (bits)	256	256	256
SRAM (Kb)	0.3	1	2
Size HW (kgates)	15	20	44
Size SW (Kbyte)	15	30	50

The size of the Quiddikey implementation can be reduced by leveraging available HW or SW crypto capabilities.