QuiddiKey RNG is a PUF-based, NIST compliant, and technology independent random number generator that can be added easily to almost any chip.

QuiddiKey RNG Hardware IP

Random number generators (RNGs) are essential in many cryptographic operations. For example, RNGs are used to secure connections on the internet of things (IoT), or in automotive or datacenter settings. Intrinsic ID QuiddiKey® RNG is a hardware IP solution compliant with the NIST SP 800-90 standard that implements a chained RBG construction with deterministic random bit generators (DRBG) as specified in NIST SP 800-90A. The RBG is seeded by a true-random seed that is harvested from the noise in an SRAM physical unclonable function (PUF). This construction follows the NIST SP 800-90B specification.

SRAM PUFs use the behavior of standard SRAM, available in any digital chip, to extract entropy. They are virtually impossible to duplicate, clone or predict. This makes them very suitable for applications that require high-quality random numbers to be used as strong key material, initialization vectors (IVs), nonces, etc. QuiddiKey RNG is technology-independent and can be added easily to almost any chip – from tiny microcontrollers (MCUs) to high-performance systems-on-chip (SoCs).

Features

- Supplies 256-bit random entropy
- Uses standard SRAM power-up values as a true random source
- Includes built-in self test
- Eases integration with a custom driver API
- Complies with NIST SP 800-90A/B

Benefits

- Can be added easily to almost any chip – from tiny MCUs to high-performance SoCs
- Foundry- and technology node independent
- Supports FIPS 140-3 certification
- Includes attack countermeasures
- Remains secure post quantum computing

QuiddiKey RNG

Applications

- Content protection
- Authentication
- Secure communications
- Platform security

Certifications

- NIST CAVP for DRBG, HMAC, SHA – pending
- NIST SP 800-90A/B compliant
- Supports FIPS140-3 certification

Operational Range

The Intrinsic ID PUF-based solutions have been deployed on MCUs/SoCs/ASICs in a diverse set of foundry/process node combinations. SRAM PUF responses across this diverse array have been qualified for use in a wide range of operational environments, over years of field operation.

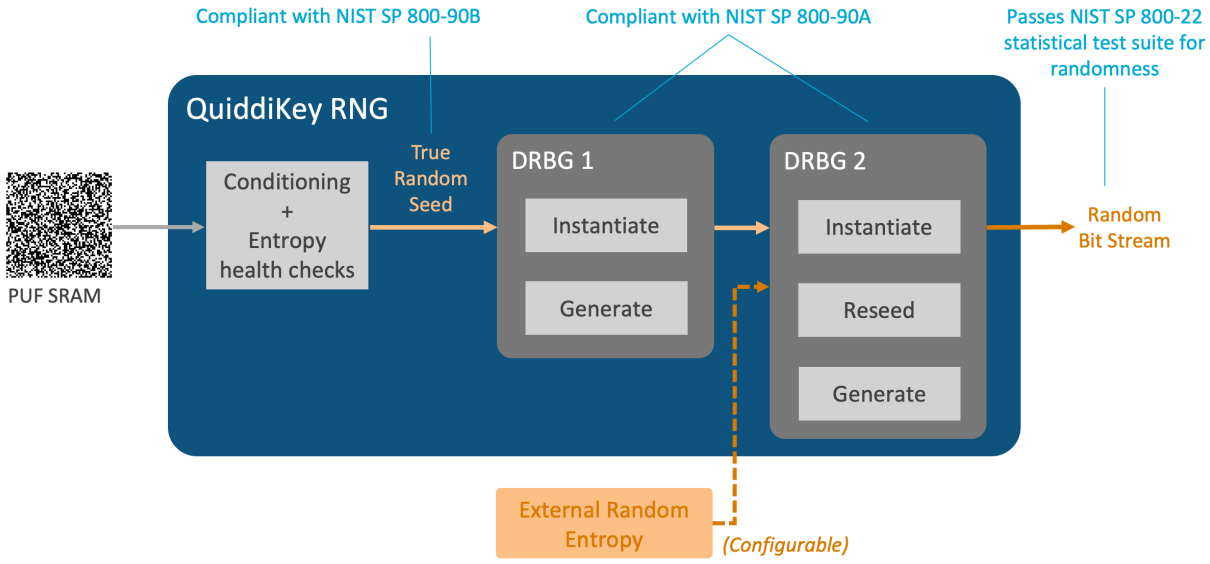
- All major fabs from 0.35 µm to 5 nm
- Temperature range from -55°C to 150°C
- Voltage supply variation +/- 20%
- Lifetime > 25 years

Deliverables

QuiddiKey RNG 100 deliverables include:

- RTL netlist (VHDL, Verilog)
- APB interface
- Testbench (UVM + VHDL)
- Synopsys Design Compiler® synthesis constraints (tcl)
- Register description (IP-XACT)
- Driver (C sources, headers)
- Documentation
- C Model

QuiddiKey RNG	100
Security strength (bits)	256
Logic (gates)	45k
SRAM required (bytes)	4k
Time-to-output (cycles)	25k
Interface	APB
Logic BIST	✓
Attack countermeasures	✓
NIST SP 800-90A compliant DRBG • Health checks • Reseed counter • Test interface	✓
NIST SP 800-90B compliant entropy source • Entropy model and proof	✓
External DRBG instantiate	(✓)
Reseed required after	2^{48} requests



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