INTRINSIC ID®

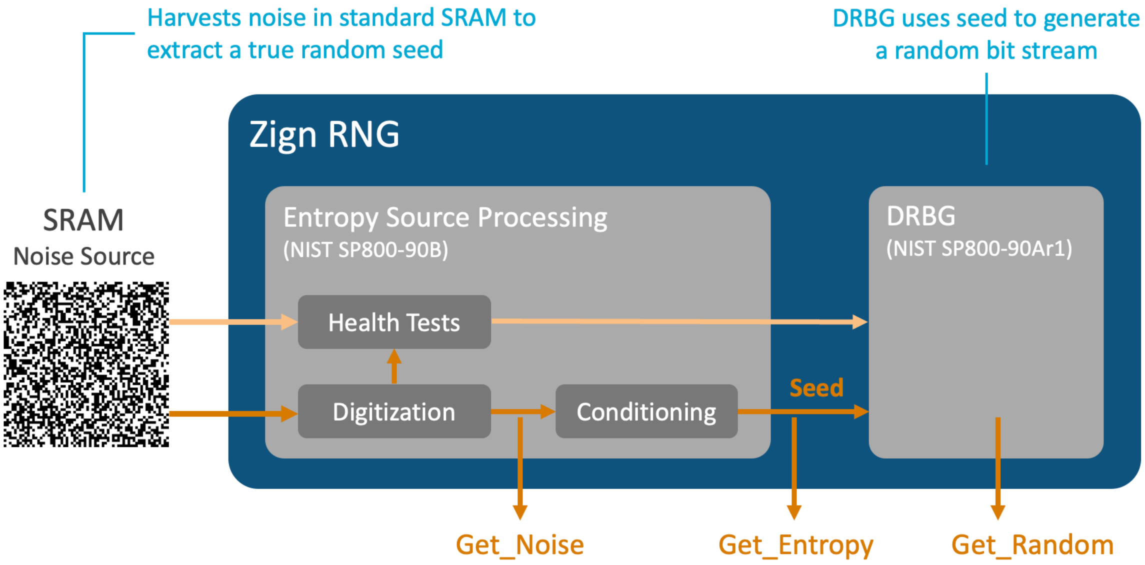
Product Brief: Zign RNG Software IP

Zign RNG enables device manufacturers and designers to add a NIST-certified RNG to their products without the need for hardware modifications.

Zign RNG

Intrinsic ID Zign® RNG is an embedded software IP solution that enables device manufacturers and designers to add a random number generator to their products without the need for hardware modifications. Random number generators are essential in many cryptographic operations, for example, to secure connections in settings such as IoT, automotive or datacenter. The Zign RNG product is compliant with the NIST SP 800-90 standard. It implements a deterministic random bit generator (DRBG) as specified in NIST SP 800-90A. The DRBG is seeded by a true random seed that is harvested from the noise in the SRAM physical unclonable function (PUF). This construction follows the NIST SP 800-90B specification.

Zign RNG is an embedded software implementation that leverages existing SRAM as a PUF, so it is the only hardware entropy source that does not need to be loaded at silicon fabrication. Zign RNG can be installed later in the supply chain, and even retrofitted on already-deployed devices. This enables a never-before-possible “brownfield” deployment of a cryptographically secure, NIST-certified RNG.


Harvests noise in standard SRAM to extract a true random seed
DRBG uses seed to generate a random bit stream
Zign RNG
SRAM
Noise Source
Entropy Source Processing
(NIST SP800-90B)
Health Tests
Digitization
Conditioning
Seed
DRBG
(NIST SP800-90Ar1)
Get_Noise
Get_Entropy
Get_Random

Applications

- Content protection
- Authentication
- Secure communications
- Platform security

Certifications

- NIST CAVP for DRBG, AES
- NIST SP 800-90 compliant
- Supports FIPS140-3 certification

Features

- Uses standard SRAM start-up values as a true random source
- Passes NIST SP 800-22 statistical test suite for randomness
- Direct access to digitized noise and NIST-compliant entropy via API
- NIST CAVP certified for DRGB and AES
- Compliant with NIST SP 800-90
- Compliant with BSI AIS 20/31
- Supports FIPS 140-3 certification

Benefits

- No need for additional or modified silicon
- Can be added at any point in the supply chain
- Can be used as a NIST-compliant entropy source – i.e. for users who want to use their own DRBG
- Fits in resource-constrained embedded devices
- Portable across different technologies
- The Intrinsic ID SRAM PUF-based random number generators are post-quantum secure

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

Zign RNG deliverables include:

- Library compiled for a specific target chip
- Reference manual
- Code examples, e.g. integration with mbed TLS, WolfSSL, and OpenSSL

		Zign RNG v1.3-0	Zign RNG v1.3-1
Code Size*		4.3 kB	4.3 kB
SRAM required for PUF		2.2 kB	3.0 kB
Performance on Arm Cortex-M4		(clock cycles)	(clock cycles)
• Initialize#		1.5M	2.4M
• Get random bytes:	64	24k	36k
	128	37k	55k
	512	116k	161k
Security strength		128 bits	256 bits
Compliant with NIST SP 800-90 • Health checks • Test interface		✓	✓
NIST CAVP certified for DRBG (SP 800-90A) and AES		✓	✓

* On Arm Cortex M4 (STM32L476RG-NUCLEO)

# To be run once after power-up