



SP 800-90B Non-Proprietary Public Use Document

Apple SEP TRNG entropy source

Prepared for:

*Apple Inc.
One Apple Park Way
Cupertino, CA 95014*

Prepared by:

*atsec information security corporation,
4516 Seton Center Parkway, Suite 250
Austin, TX 78759*

*Document Version 1.2
Date: February 2025*

Trademarks

Apple's trademarks applicable to this document are listed in <https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html>. Other company, product, and service names may be trademarks or service marks of others.

Table of Contents

1. DESCRIPTION.....4

2. SECURITY BOUNDARY5

3. OPERATING CONDITIONS.....5

4. CONFIGURATION SETTINGS.....6

5. PHYSICAL SECURITY MECHANISMS.....6

6. CONCEPTUAL INTERFACES.....6

7. MIN-ENTROPY RATE.....6

8. HEALTH TESTS..... 6

9. MAINTENANCE.....7

10. REQUIRED TESTING..... 7

11. VENDOR PERMISSIONS AND RELATIONSHIP.....7

1. Description

The Apple SEP TRNG entropy source (also called "Apple ES" in this document) is a physical (P) entropy source validated as conformant to SP 800-90B by the Entropy Source Validation Program. The physical entropy source is built upon Free Running Oscillators (FROs). The entropy source was tested on the processors listed in Table 1.

Processor
Apple A Series A9
Apple A Series A9X
Apple A Series A10 Fusion
Apple A Series A10X Fusion
Apple A Series A11 Bionic
Apple A Series A12 Bionic
Apple A Series A12X Bionic
Apple A Series A12Z Bionic
Apple A Series A13 Bionic
Apple A Series A14 Bionic
Apple A Series A15 Bionic
Apple A Series A16 Bionic
Apple A Series A17 Pro
Apple S Series S3
Apple S Series S4
Apple S Series S5
Apple S Series S6
Apple S Series S7
Apple S Series S8
Apple S Series S9
Apple S Series S10
Apple T Series T2
Apple M Series M1

Apple M Series M1 Pro
Apple M Series M1 Max
Apple M Series M1 Ultra
Apple M Series M2
Apple M Series M2 Pro
Apple M Series M2 Max
Apple M Series M2 Ultra
Apple M Series M3
Apple M Series M3 Pro
Apple M Series M3 Max
Apple M Series M4
Apple M Series M4 Pro
Apple M Series M4 Max

Table 1 Tested Operational Environments

2. Security Boundary

The Apple ES boundary is defined by the blue box in Figure 1. The Apple ES boundary contains the following components: physical noise source (twenty-four FROs and shift registers), SP 800-90B health tests, and a SHA-256 vetted conditioning component.

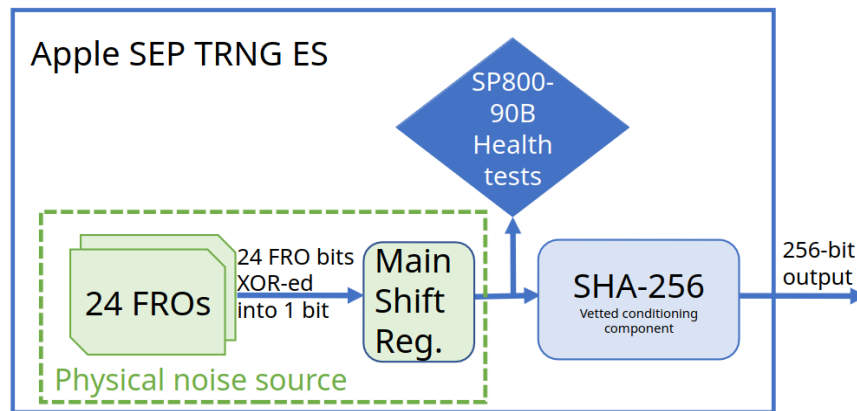


Figure 1: Block Diagram of the Apple ES with the FRO physical noise source

3. Operating Conditions

The entropy source is claimed to operate correctly under the inherent operating conditions of the System-on-Chip (SoC):

- temperature range [-25°C; 125°C]
- voltage range [0.595 V, 1.115 V]

4. Configuration Settings

For the Apple ES tested in the OEs listed in Table 1 there are no configurable settings.

5. Physical Security Mechanisms

The Apple ES is embedded in the system on chip (SoC)s / processors-listed in Table 1. The SoCs are single-chip embodiments of production-grade components that include standard passivation. The SoCs are covered with either an opaque lid or compartment or black-coated material or metal coating. They are soldered in the logic board from the ball grid array (BGA) or embedded in hardened resin in a system-in-package (SiP). The components above are opaque within the visible spectrum.

6. Conceptual Interfaces

The entropy source provides the following interfaces:

- Apple is able to access the raw data of the noise source from interfaces embedded in the entropy source. The data collection does not impact the frequencies of FROs and their jitters.

7. Min-Entropy Rate

The $H_{\text{submitter}}$ is 0.125 bits / bit. 4096 bits from the FROs are input to the SHA-256 vetted conditioning component. The min-entropy rate at the output of the ES (h_{out} for the output of the conditioning component per Section 3.1.5 of SP 800-90B) is 256 bits per 256-bit output.

8. Health Tests

Apple has designed the health tests to detect failures of the noise source, or to detect a deviation from the expected entropy rate during the correct operation of the noise source before the raw data is conditioned. Following the NIST SP 800-90B requirements, the vendor has implemented three types of health tests:

- Start-up Tests. The start-up tests run over a minimum of 1024 consecutive 8 concatenated 1-bit (noise) samples cumulated into sixteen 512-bit noise blocks. The start-up tests comprise the Repetitive Count Test (RCT) and Adaptive Proportion Test (APT). If any of these tests fail, the sampled bits will be discarded, and the start-up tests are performed on the next 1024 consecutive 8 concatenated 1-bit (noise) samples. There is no output available from the Apple ES before the successful completion of the start-up test.
- Continuous Tests. The approved health tests Repetition Count Test (RCT), and the Adaptive Proportion Test (APT) are implemented. When any of the health tests fail, the

Apple ES discards the raw entropy data and moves on to the next set of raw entropy data subject to the health tests. If the failure persists, then the Apple ES enters an error state.

- On-Demand Tests. The On-Demand health tests are performed on the physical noise source output by rebooting the hardware platform which results in the immediate execution of the start-up tests.

9. Maintenance

There are no maintenance requirements.

10. Required Testing

To test the Apple ES, noise samples must be collected using a test harness that can access the shift register that serves as the output interface of the noise source.

One million consecutive samples must be collected from the operational environment at its normal operating conditions and processed using the SP 800-90B entropy tool that is provided by NIST. The results must be at least as high as the H_submitter.

Restart data must be collected at normal operating conditions following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The sanity test must pass, and the minimum of the row-wise and column-wise entropy rate must not be less than half of the H_submitter.

The Apple ES continuously runs the SP 800-90B health tests and will produce an error upon failure.

11. Vendor Permissions and Relationship

The Apple ES status is indicated as "Open for Reuse".