SP 800-90B Non-Proprietary Public Use Document

Apple corecrypto non-physical 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 1.1
Date: September 2024

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 BOUNDARY....5

3. OPERATING CONDITIONS....5

4. CONFIGURATION SETTINGS....5

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 corecrypto non-physical entropy source (also called "Apple ES" in this document) is a non-physical (NP) entropy source validated as conformant to SP 800-90B by the Entropy Source Validation Program. The non-physical entropy source is based upon interrupt timings. The entropy source was tested on the hardware platforms listed in Table 1.

Operating Environment (OE)		
Processor	Operating System	Hardware Platform
Apple A Series A10 Fusion	iPadOS 17	iPad (7th generation)
Apple A Series A10X Fusion	iPadOS 17	iPad Pro 10.5-inch
Apple A Series A12 Bionic	iPadOS 17	iPad mini (5th generation)
	tvOS 17	Apple TV 4K (2nd generation)
Apple A Series A12X Bionic	iPadOS 17	iPad Pro 11-inch (1st generation)
Apple A Series A12Z Bionic	iPadOS 17	iPad Pro 11-inch (2nd generation)
Apple A Series A13 Bionic	iPadOS 17	iPad (9th generation)
	iOS 17	iPhone 11 Pro
Apple A Series A14 Bionic	iPadOS 17	iPad Air (4th generation)
	iOS 17	iPhone 12
Apple A Series A15 Bionic	iPadOS 17	iPad mini (6th generation)
	iOS 17	IPhone 13 Pro Max
	tvOS 17	Apple TV 4K (3rd generation)
Apple A Series A16 Bionic	iOS 17	iPhone 14 Pro Max
Apple A Series A17 Pro	iOS 17	iPhone 15 Pro
Apple S Series S6	watchOS 10	Apple Watch Series S6
Apple S Series S7	watchOS 10	Apple Watch Series S7
Apple S Series S8	watchOS 10	Apple Watch Series S8
Apple S Series S9	watchOS 10	Apple Watch Series S9
Apple T Series T2	T2OS 14	Apple Security Chip T2
Apple M Series M1	iPadOS 17	iPad Pro 11-inch (3rd generation)
	macOS Sonoma 14	MacBook Air
Apple M Series M1 Pro	macOS Sonoma 14	MacBook Pro 14-inch
Apple M Series M1 Max	macOS Sonoma 14	MacBook Pro 14-inch
Apple M Series M1 Ultra	macOS Sonoma 14	Mac Studio
Apple M Series M2	iPadOS 17	iPad Pro 11-inch (4th generation)
	macOS Sonoma 14	MacBook Pro 13-inch
	visionOS 1	Apple Vision Pro
Apple M Series M2 Pro	macOS Sonoma 14	MacBook Pro 14-inch
Apple M Series M2 Max	macOS Sonoma 14	MacBook Pro 14-inch

Apple M Series M2 Ultra	macOS Sonoma 14	Mac Studio
Apple M Series M3	macOS Sonoma 14	MacBook Air (13-inch)
Apple M Series M3 Pro	macOS Sonoma 14	MacBook Pro (14-inch, 2024)
Apple M Series M3 Max	macOS Sonoma 14	MacBook Pro (14-inch, fall 2023)
Intel Core i5 Amber Lake	macOS Sonoma 14	MacBook Air 13-inch
Intel Core i5 Coffee Lake	macOS Sonoma 14	MacBook Pro 13-inch
Intel Core i5 Comet Lake	macOS Sonoma 14	iMac
Intel Core i7 Coffee Lake	macOS Sonoma 14	MacBook Pro 16-inch
Intel Core i7 Ice Lake	macOS Sonoma 14	MacBook Pro 13-inch
Intel Core i7 Comet Lake	macOS Sonoma 14	iMac
Intel Core i9 Coffee Lake	macOS Sonoma 14	MacBook Pro 16-inch
Intel Core i9 Comet Lake	macOS Sonoma 14	iMac
Intel Xeon W Cascade Lake	macOS Sonoma 14	Mac Pro

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: non-physical noise source (interrupts and per-CPU entropy pool), SP 800-90B health tests, and two SHA-512 vetted conditioning components.

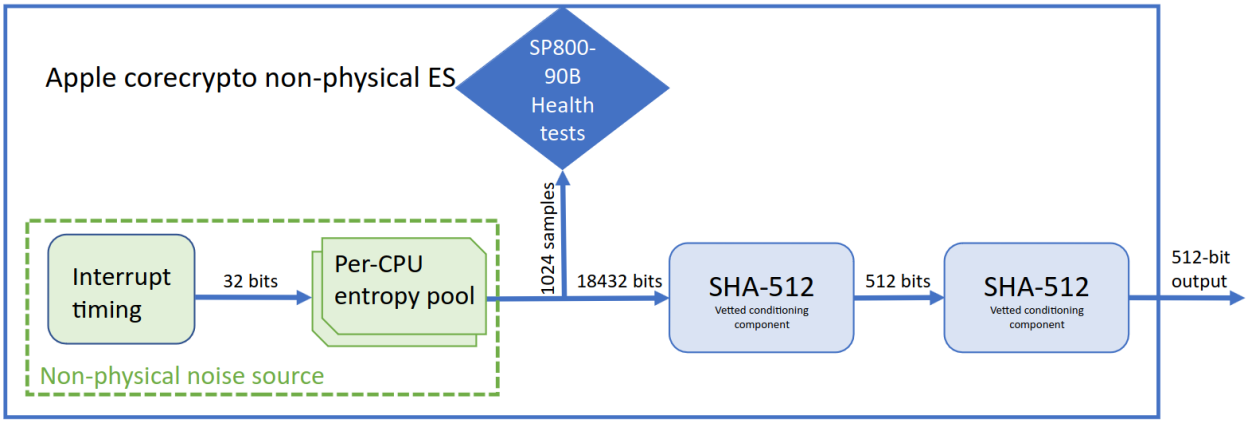

Figure 1: Block Diagram of the Apple ES with the interrupt non-physical noise source

3. Operating Conditions

The entropy source is claimed to operate correctly under the inherent operating conditions of the hardware platform:

- 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 noise source is non-physical. The physical security mechanisms only apply to the hardware component of the operational environment in which the entropy source is installed, and thus the entropy source inherits those mechanisms.

6. Conceptual Interfaces

The entropy source provides the following interfaces:

- The output of the entropy source is directly provided for seeding to the kernel space DRBG. This corresponds to the GetEntropy() interface from SP 800-90B.
- Apple is able to access the raw data of the noise source from each per-CPU entropy pool using a kernel space interface. This corresponds to the GetNoise() interface from SP 800-90B.

7. Min-Entropy Rate

The H_submitter is 1.0 bits per 32-bit sample. During normal operation, 576 32-bit samples from the entropy pools are input to the first SHA-512 vetted conditioning component. Then, 512 bits from the output of this conditioning component are input to the second SHA-512 vetted conditioning component. The min-entropy rate at the output of this second conditioning component is 512 bits per 512-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 Test. The Start-up test runs over a minimum of 1024 consecutive samples. The Start-up test comprises 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 test is performed on the next 1024 samples. There is no output available from the Apple ES before the successful completion of the Start-up Test.
- Continuous Test. 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 the system is rebooted as a means to recover from the health test failure.
- On-Demand Test. The On-Demand health test is performed on the non-physical ES output by rebooting the hardware platform which results in the immediate execution of the Start-up Test.

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 per-CPU entropy pools that serve 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".