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
9130 Jollyville Road, Suite 260
Austin, TX 78759

Document Version 1.0
Date: July 2023

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

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 SP800-90B by the Entropy Source Validation Program (ESVP) with certificate number #E15. The non-physical entropy source is based upon interrupt timings. The Apple ES was tested on the processors listed in Table 1.

Operating Environment (OE)		
Processor	Operating System	Hardware Platform
Apple A Series A9	iPadOS 15	iPad (5th generation)
	iOS 15	iPhone 6S
Apple A Series A9X	iPadOS 15	iPad Pro 9.7-inch
Apple A Series A10 Fusion	iPadOS 15	iPad (7th generation)
	iOS 15	iPhone 7 Plus
Apple A Series A10X Fusion	iPadOS 15	iPad Pro 10.5 inch
	tvOS 15	Apple TV 4K
Apple A Series A11 Bionic	iOS 15	iPhone X
Apple A Series A12 Bionic	iPadOS 15	iPad mini (5th generation)
	iOS 15	iPhone XS Max
	tvOS 15	Apple TV 4K (2nd generation)
Apple A Series A12X Bionic	iPadOS 15	iPad Pro 11-inch (1st generation)
Apple A Series A12Z Bionic	iPadOS 15	iPad Pro 11in (2nd generation)
Apple A Series A13 Bionic	iPadOS 15	iPad (9th generation)
	iOS 15	iPhone 11 Pro
Apple A Series A14 Bionic	iPadOS 15	iPad Air (4th generation)
	iOS 15	iPhone 12
Apple A Series A15 Bionic	iPadOS 15	iPad mini (6th generation)
	iOS 15	iPhone 13 Pro Max
Apple S Series S3	watchOS 8	Apple Watch Series S3

Apple S Series S4	watchOS 8	Apple Watch Series S4
Apple S Series S5	watchOS 8	Apple Watch Series S5
Apple S Series S6	watchOS 8	Apple Watch Series S6
Apple S Series S7	watchOS 8	Apple Watch Series S7
Apple T Series T2	T2OS12	Apple Security Chip T2
Apple M Series M1	iPadOS 15	iPad Pro 11in (3rd generation)
	macOS Monterey 12	MacBook Air
Apple M Series M1 Pro	macOS Monterey 12	MacBook Pro 14 inches
Apple M Series M1 Max	macOS Monterey 12	MacBook Pro 14 inches
Apple A Series A9	iPadOS 14	iPad (5th generation)
	iOS 14	iPhone 6S
Apple A Series A9X	iPadOS 14	iPad Pro 9.7-inch
Apple A Series A10 Fusion	iPadOS 14	iPad (7th generation)
	iOS 14	iPhone 7 Plus
Apple A Series A10X Fusion	iPadOS 14	iPad Pro 10.5 inch
	tvOS 14	Apple TV 4K
Apple A Series A11 Bionic	iOS 14	iPhone X
Apple A Series A12 Bionic	iPadOS 14	iPad mini (5th generation)
	iOS 14	iPhone XS Max
Apple A Series A12X Bionic	iPadOS 14	iPad Pro 11-inch (1st generation)
Apple A Series A12Z Bionic	iPadOS 14	iPad Pro 11in (2nd generation)
Apple A Series A13 Bionic	iOS 14	iPhone 11 Pro
Apple A Series A14 Bionic	iPadOS 14	iPad Air (4th generation)
	iOS 14	iPhone 12
Apple S Series S3	watchOS 7	Apple Watch Series S3
Apple S Series S4	watchOS 7	Apple Watch Series S4
Apple S Series S5	watchOS 7	Apple Watch Series S5
Apple S Series S6	watchOS 7	Apple Watch Series S6

Apple T Series T2	TxFW 11	Apple Security Chip T2
Apple M Series M1	macOS Big Sur 11	MacBook Air
Intel i5-8210Y (Amber Lake)	macOS Big Sur 11	MacBook Air
Intel i7-1060NG7 (Ice Lake)	macOS Big Sur 11	MacBook Air
Intel i7-8850H (Coffee Lake)	macOS Big Sur 11	MacBook Pro
Intel i9-9880H (Coffee Lake)	macOS Big Sur 11	MacBook Pro
Xeon W-2140B (Sky Lake)	macOS Big Sur 11	iMac Pro
Xeon W-3223 (Cascade Lake)	macOS Big Sur 11	Mac Pro

Table 1 Tested Operational Environment

2. Security Boundary

The Apple ES boundary is defined by the blue box in the Figure 1. The Apple ES boundary contains the following components: non-physical noise source interrupt, per-CPU entropy pool and a SHA2-256 vetted conditioning function.

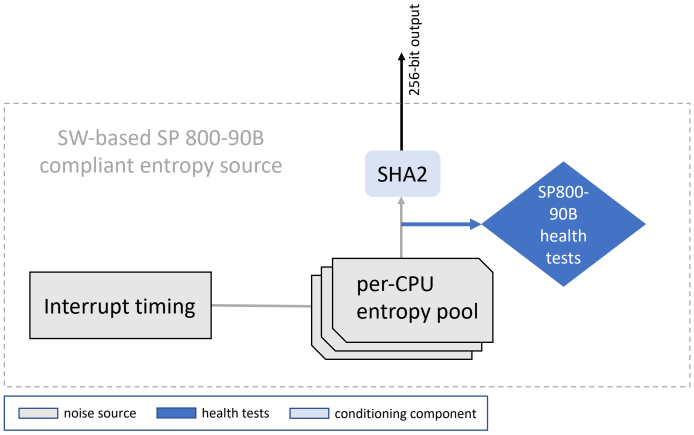

Figure 1: Block Diagram of the Apple ES with the interrupt based non-physical entropy source

3. Operating Conditions

The Apple ES is claimed to operate correctly under the inherent operating conditions of the hardware platform:

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

4. Configuration Settings

There are no configurable settings for the Apple ES tested in the OEs listed in Table 1.

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:

- A kernel-space interface to each CPU entropy pool is used by Apple developers to access the raw data of the noise source.

7. Min-Entropy Rate

The H_submitter is 0.125 bit /bit.
The 65536-bits are input to the SHA-256 vetted conditioning function.
The min-entropy rate at the output of source (H_out for the output of the conditioning function per section 3.1.5 of 90B) is 256-bits per 256-bit output sample.

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 time stamps. 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-time stamps. 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 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 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

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

- The Apple ES is configured in the platforms listed in Table 1 to comply with SP800-90B at the first start of the respective device. There is no testing required.
- To test the Apple ES one million consecutive raw physical noise samples must be collected using a test harness that can access the per-CPU entropy pool that serves as the noise interface from the entropy source.
- The results obtained from the NIST SP800-90B tool must be at least as high as the H_submitter.
- 1000 raw physical noise samples after 1000 restarts for assessment that (1) the sanity test passes and (2) the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.

11. Vendor Permissions and Relationship

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