SP 800-90B Non-Proprietary Public Use Document

Apple corecrypto 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 1.0
Date: January 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.

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Table of Contents

1. DESCRIPTION 4
2. SECURITY BOUNDARY 7
3. OPERATING CONDITIONS 7
4. CONFIGURATION SETTINGS 8
5. PHYSICAL SECURITY MECHANISMS 8
6. CONCEPTUAL INTERFACES 8
7. MIN-ENTROPY RATE 8
8. HEALTH TESTS 8
9. MAINTENANCE 9
10. REQUIRED TESTING 9
11. VENDOR PERMISSIONS AND RELATIONSHIP 9

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

1. Description

The Apple corecrypto physical entropy source (also called "Apple ES" in this document) is a physical (P) entropy source validated as conformant to SP800-90B by the Entropy Source Validation Program (ESVP) with certificate number #E14. The Physical entropy source is built upon Free Running Oscillators (FROs). The entropy source was tested on the processors listed in Table 1.

Operating Environment (OE)		
Processor	Operating System	Hardware Platform
Apple A Series A9	iPadOS 16	iPad (5th generation)
Apple A Series A9X	iPadOS 16	iPad Pro 9.7-inch
Apple A Series A10 Fusion	iPadOS 16	iPad (7th generation)
Apple A Series A10X Fusion	iPadOS 16	iPad Pro 10.5-inch
	tvOS 16	Apple TV 4K
Apple A Series A11 Bionic	iOS 16	iPhone X
Apple A Series A12 Bionic	iPadOS 16	iPad mini (5th generation)
	iOS 16	iPhone XS Max
	tvOS 16	Apple TV 4K (2nd generation)
Apple A Series A12X Bionic	iPadOS 16	iPad Pro 11-inch (1st generation)
Apple A Series A12Z Bionic	iPadOS 16	iPad Pro 11-inch (2nd generation)
Apple A Series A13 Bionic	iPadOS 16	iPad (9th generation)
	iOS 16	iPhone 11 Pro
Apple A Series A14 Bionic	iPadOS 16	iPad Air (4th generation)
	iOS 16	iPhone 12
Apple A Series A15 Bionic	iPadOS 16	iPad mini (6th generation)
	iOS 16	iPhone 13 Pro Max
	tvOS 16	Apple TV 4K (3rd generation)
Apple A Series A16 Bionic	iOS 16	iPhone 14 Pro Max
Apple S Series S4	watchOS 9	Apple Watch Series S4
Apple S Series S5	watchOS 9	Apple Watch Series S5

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Apple S Series S6	watchOS 9	Apple Watch Series S6
Apple S Series S7	watchOS 9	Apple Watch Series S7
Apple S Series S8	watchOS 9	Apple Watch Series S8
Apple T Series T2	T2OS 13	Apple Security Chip T2
Apple M Series M1	iPadOS 16	iPad Pro 11-inch (3rd generation)
	macOS Ventura 13	MacBook Air
Apple M Series M1 Pro	macOS Ventura 13	MacBook Pro 14-inch
Apple M Series M1 Max	macOS Ventura 13	MacBook Pro 14-inch
Apple M Series M1 Ultra	macOS Ventura 13	Mac Studio
Apple M Series M2	iPadOS 16	iPad Pro 11-inch (4th generation)
	macOS Ventura 13	MacBook Pro 13-inch
Apple M Series M2 Pro	macOS Ventura 13	MacBook Pro 14-inch
Apple M Series M2 Max	macOS Ventura 13	MacBook Pro 14-inch
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 11-inch (2nd generation)
Apple A Series A13 Bionic	iOS 15	iPhone 11 Pro
	iPadOS 15	iPad (9th generation)

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Apple A Series A14 Bionic	iPadOS 15	iPad Air (4th generation)
	iOS 15	iPhone 12
Apple A Series A15 Bionic	iOS 15	iPhone 13 Pro Max
	iPadOS 15	iPad mini (6th generation)
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	T2OS 12	Apple Security Chip T2
Apple M Series M1	macOS Monterey 12	MacBook Air
	iPadOS 15	iPad Pro 11in (3rd generation)
Apple M Series M1 Pro	macOS Monterey 12	MacBook Pro 14-inch
Apple M Series M1 Max	macOS Monterey 12	MacBook Pro 14-inch
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 11-inch (2nd generation)
Apple A Series A13 Bionic	iOS 14	iPhone 11 Pro
Apple A Series A14 Bionic	iPadOS 14	iPad Air (4th generation)

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

	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

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: physical noise source (twenty-four FROs and shift register), SP800-90B health tests, a SHA2-256 vetted conditioning function and a CTR_DRBG bijective function.

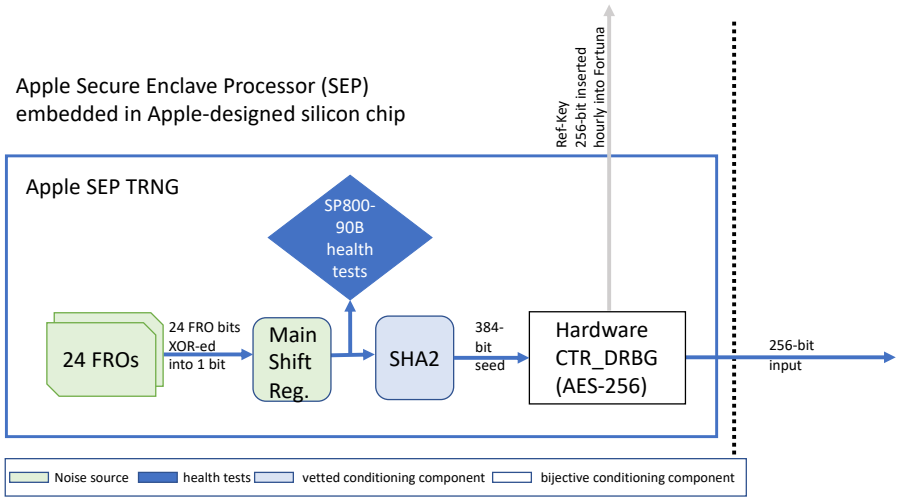

Figure 1: Block Diagram of the Apple ES with the FRO physical entropy source

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]

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

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_submitter is 0.125 bit / bit.
The bits per request sample is 4096-bits at the input of the SHA-256 vetted conditioning function. For the second conditioning function i.e. the CTR_DRBG based on AES 256, the input is 384 bits.
The min-entropy rate at the output of source (H_out for the output of the conditioning chain 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 8 concatenated 1-bit samples cumulated into sixteen 512-bit noise blocks. 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 8 concatenated 1–bit 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 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.

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

- On-Demand Test. The On-Demand health test is performed on the 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 Apple ES continuously runs the SP 800-90B health tests and will produce an error upon failure.

- The Apple ES is configured in the SoCs listed in Table 1 to comply with SP800-90B at the first start of the SoC. There is no required testing.
- To test the Apple ES one million consecutive raw physical noise samples must be collected using a test harness that can access the output of the shift register 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".

© 2024 Apple Inc., All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.