Apple Corecrypto v13 Non-Physical Entropy Source

Version 13

SP 800-90B Non-Proprietary Public Use Document

December 2023

Version 0.3

Prepared for:

Apple, One Apple Park Way, Cupertino, CA 95014

Prepared by:

www.lightshipsec.com

Document History

Version	Date	Description
0.1	30 Jul 2023	First draft.
0.2	17 Oct 2023	Added list of processors.
0.3	11 Dec 2023	Addressed ESV submission comments.

Copyright

Trademarks

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Description

1 The Apple Corecrypto v13 non-physical entropy source (ES) is a non-physical entropy source based upon interrupt timings.

2 The entropy source was tested on the processors listed in Table 1 under the assumption that its output is non-IID.

Table 1: List of Processors

Processor	Operating System	Hardware Platform
Intel i5 (Amber Lake)	macOS Ventura v13	MacBook Air (Retina, 13-inch, 2018)
Intel i5 (Coffee Lake)	macOS Ventura v13	MacBook Pro (13-inch, 2019, 2-port)
Intel i7 (Ice Lake)	macOS Ventura v13	MacBook Air (Retina, 13-inch, 2020)
Intel i7 (Coffee Lake)	macOS Ventura v13	MacBook Pro (15-inch, 2018)
Intel i7 (Comet Lake)	macOS Ventura v13	iMac iMac 27-Inch (5K, 2020)
Intel i9 (Coffee Lake)	macOS Ventura v13	MacBook Pro MacBook Pro (16-inch, 2019)
Xeon W (Sky Lake)	macOS Ventura v13	iMac Pro (2017)
Xeon W (Cascade Lake)	macOS Ventura v13	Mac Pro (2019)

1.2 Security Boundary

3 The ES boundary is defined by the blue box in Figure 1.

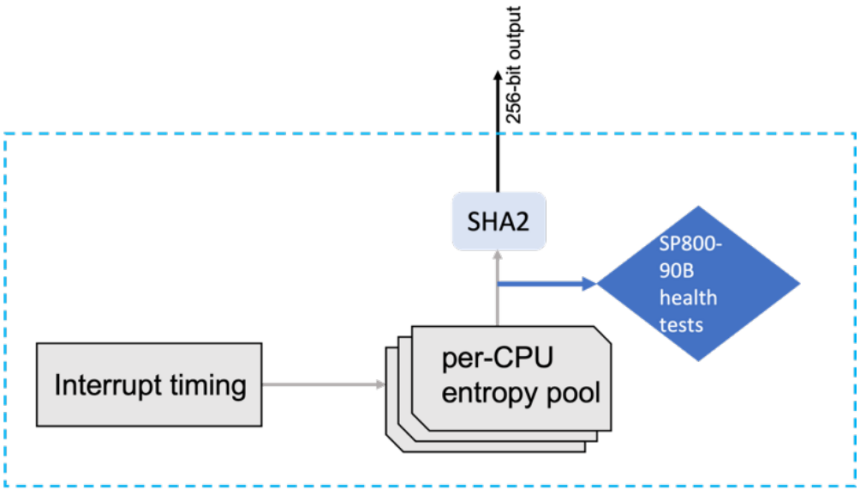

Figure 1: Security Boundary

4 The ES boundary is composed of the following components:

a) **System Interrupts.** This is a non-physical noise source.

b) **Per-CPU entropy pool.** Contains the entropic data.

c) **SHA2-256 vetted conditioning.** SP800-90B compliant.

2 Configuration

2.1 Operating Conditions

5 The ES operates correctly under the inherent operating conditions of the hardware platform:

a) **Temperature Range:** between -25°C and 125°C.

b) **Voltage Range:** between 0.595V and 1.115V.

2.2 Configuration Settings

6 For the ES tested in the OEs listed in Table 1, the customer does not have the ability to modify the ES configuration settings.

2.3 Physical Security Mechanisms

7 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.

2.4 Maintenance

8 There are no maintenance requirements.

3 Entropy Source

3.1 Interfaces

9 There is a proprietary kernel space interface per-CPU entropy pool which is accessible using a special software tooling to provide access to raw data of the noise source.

3.2 Min-Entropy

10 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.

3.3 Health Tests

11 Apple has designed 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 in this product:

a) **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 entropy source before the successful completion of the Start-up Test.

b) **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, 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 ES enters an error state.

c) **On-Demand Test.** The On-Demand health test is performed on the ENT (NP) output by rebooting the hardware platform which results in the immediate execution of the Start-up Test.

3.4 Statistical Testing

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

13 The 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.

14 To test the entropy source one million consecutive raw physical noise samples must be collected using a special build that can access the per-CPU entropy pool that serves as the noise interface from the entropy source. The health tests are the only way a user could ensure their entropy source is properly operating.

15 The results obtained from the NIST SP800-90B tool must be at least as high as the H_submitter.

16 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.