SP 800-90B Non-Proprietary Public Use Document
Aruba CPU Jitter Entropy Source v1.0

CPU Jitter RNG 3.3.1/RNGD 1.2.6

Document Version 1.4

Aruba, a Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

November 2022

Revision History

Version	Change
1.0	First draft Release.
1.1	Updates to operating environments.
1.2	Updates based on QA.
1.3	Removed Krait and NXP OEs.
1.4	Updates for CCOM1 comments.

Table of Contents

Description

The Aruba CPU Jitter Entropy Source v1.0 implements the library from CPU Jitter RNG to obtain entropy for key generation in the module. The source is a non-physical (ENT (NP)) entropy source. The CPU Jitter RNG library v3.3.1 source was tested on ArubaOS running on Intel Atom, Intel Xeon, Qualcomm IPQ, and Broadcom BCM, and Broadcom XLP processors.

Identifier	**Version**
Aruba Product	ArubaOS
Release Version	8.10
Entropy Version	Aruba CPU Jitter Entropy Implementation 3.3.1/RNGD 1.2.6

Table 1 - Evaluated Version

Processor	Speed	L1 Cache/Core
Broadcom XLP (MIPS64)	1.5 GHz	32 KB
Intel Atom C3508 (Denverton)	1.6 GHz	32 KB
Intel Xeon (Cascade Lake) with/without AES-NI	2.1 GHz	32 KB
Intel Xeon E5 (Broadwell) with AES-NI	3.2 GHz	32 KB
Qualcomm IPQ (64-bit ARM A7)	0.8 GHz	8 KB
Broadcom BCM (64-bit ARMv8)	3.0 GHz	32 KB
Qualcomm IPQ (64-bit ARM Cortex A53)	2.3 GHz	8 KB

Table 2 - Tested Processors

Security Boundary

The basic operation of the CPU Jitter RNG entropy source is shown in Figure 1. Timing jitter from memory access and hashing operations is collected and injected into the entropy pool for access by the module.

The entropy source is internal to the module as identified by the red dashed box showing the logical cryptographic boundary in the block diagram below (Figure 2). Output from the entropy source is used to seed a deterministic random bit generator (DRBG). The module implements a NIST SP800-90Arev1 Counter DRBG for the generation of random bits.

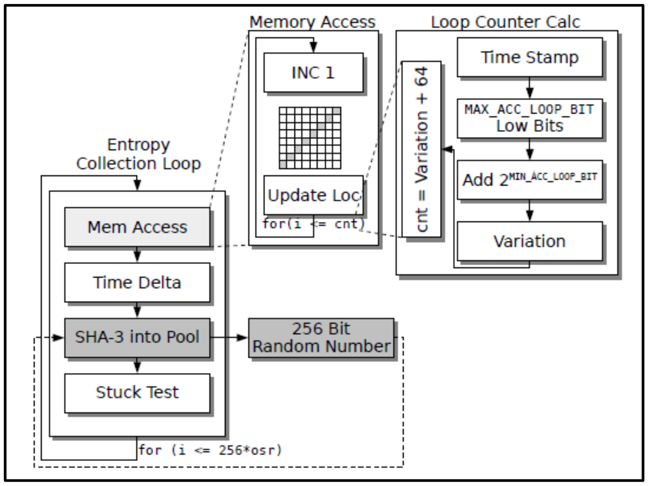

Figure 1 - Entropy source diagram

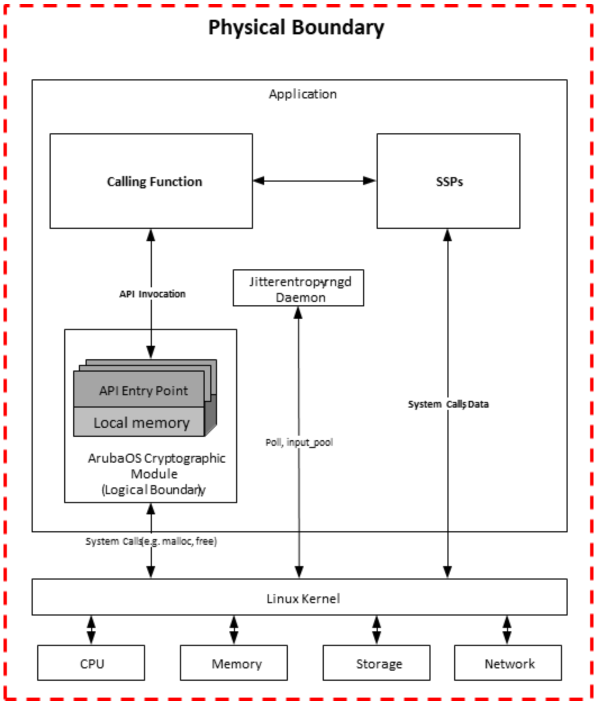

Figure 2 - Module Block Diagram

Operating Conditions and Configuration Settings

The following table summarizes operating conditions and compilation configuration settings.

Parameter	Value	Description
Temperature	0 °C – 40°C	Operating temperature range of the implementation.
Voltage	0.75V- 1.35V	Processor (s) voltage range. VID (Voltage Identification)
Clock speed	0.8 GHz - 3.20 GHz	Processor clocking speed with impact on high-resolution timing required for the CPU Jitter RNG.
Compilation Options (JENT v3.3.1)		
JENT_MEMORY_BLOCKS	512	Number of memory blocks
JENT_MEMORY_BLOCKSIZE	128	Memory block size
JENT_MEMORY_ACCESSLOOPS	128	Memory access loops
JENT_CONF_DISABLE_LOOP_SHUFFLE	True	Disables pseudo-random looping

Table 3 – Operating Conditions and Configuration Parameters

The CPU Jitter RNG library was tested on ArubaOS 8.10 running on Intel Atom, Intel Xeon, Qualcomm IPQ, and Broadcom BCM, and Broadcom XLP processors. All processors provide a high-resolution timer and default compilation options for CPU Jitter RNG v3.3.1 were used.

Physical Security Mechanisms

Aruba CPU Jitter Entropy Source v1.0 implements is a Security Level 1 firmware module within a Multiple-chip standalone embodiment. The cryptographic module consists of production-grade components that include standard passivation techniques and is entirely contained within a metal production-grade enclosure that includes removable covers.

Conceptual Interfaces

The GetEntropy interface is called during the instantiation function of the DRBG to provide the seed.

Min-Entropy Rate

The Aruba CPU Jitter Entropy Source v1.0 entropy source provides 256 bits of assessed min-entropy per 256-bit output sample, or full entropy.

Health Tests

The module continuously performs the Health Tests in SP 800-90B section 4.4 using the repetition count test (RCT) and adaptive proportion test (APT) as part of the module's conditional self-tests.

Maintenance

There are no specific maintenance requirements for the entropy source.

Required Testing

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

In addition, raw sequential and restart data samples can be obtained from the entropy source for statistical testing using SP 800-90B test tools with the following requirements:

1. Raw noise data through the raw noise source interface and processed by the SP800-90B tool to obtain an entropy rate must be near equal to or the defined min-entropy rate.
2. Obtain the restart noise data through the raw noise source interface and processed by the SP800-90B tool.
   a. the sanity test to apply to the noise restart data must pass, and
   b. the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.