SP 800-90B Non-Proprietary Public Use Document
CPU Jitter (JENT)
Firmware v3.4.1

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Document Version 1.5
December 7, 2023

Revision History

Version	Change
0.1	Initial draft
0.2	Modified configuration settings table
0.3	Modified Operating Conditions table.
0.4	Updated NIST 90B test tool results in “Required Testing” to show results for latest sequential and restart entropy samples.
0.5	Final clean up
0.6	CCOM1 updates.
1.1	First set of additional OEs added
1.2	Added more OEs
1.3	Responded to lab comments
1.4	Deleted duplicate processor (D-1548)
1.5	Added bit about OSR

Table of Contents

1 Description

CPU Jitter Entropy (JENT) is a non-physical entropy source. It makes no IID claim and thus meets all the requirements for non-IID compliance. The report is for JENT version 3.4.1.

2 Security Boundary

The boundary of the JENT implementation is shown in Figure 1. JENT gets its entropy from the time deltas between repeated hash/memory collection operations. The JENT output is used seed an SP 800-90A compliant DRBG (which is outside of the boundary of the entropy source). The security boundary of the JENT implementation contains the source code files provided as part of the software delivery. The source code contains API calls which are used by modules requesting entropy from JENT.

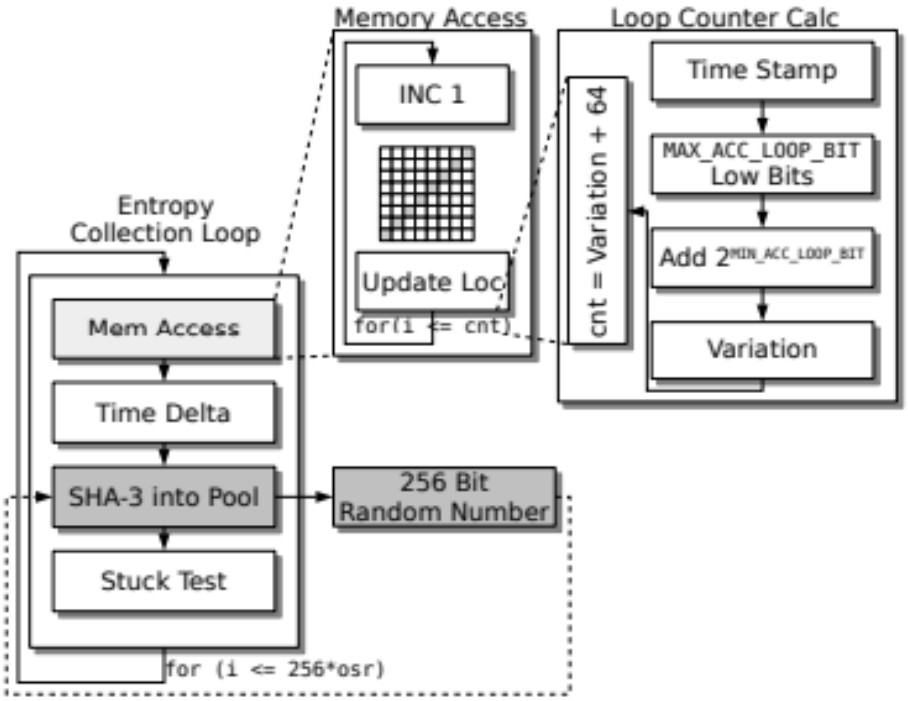

Figure 1: Entropy Source Diagram

3 Operating Conditions

Table 2 summarizes the operating conditions for each of the tested platforms.

Table 2: Operating ConditionsPlatform	Processor	Processor Family	Processor Clock Speed	Cache Sizes			Platform Temperature	Platform Voltage (AC)
				L1 (L1-D/L1-I if different)	L2	L3		
C9800-40, FPR 2130	Intel Xeon D-1548	Broadwell	2.00GHz	512 KB	2MB	12 MB	0°C – 40°C	90V – 264V
C9800-80	Intel Xeon Silver 4116T	Skylake	2.10GHz	768 KB	12 MB	16.5 MB	0°C – 40°C	90V – 264V
C9800-L	Intel Xeon D-1563N	Broadwell	2.00GHz	1.5 MB per core	1.5 MB per core	1.5 MB per core	0°C – 40°C	90V – 264V
FPR 2110	Intel Xeon D-1526	Broadwell	1800 MHz	32 KB	256 KB	6 MB	0°C – 40°C	100V – 240V
FPR 2110	Cavium CN 7235	Octeon III	1200 MHz	32 KB	78 KB	2 MB	0°C – 40°C	100V – 240V
FPR 2120	Intel Xeon D-1528	Broadwell	1900 MHz	32 KB	256 KB	9 MB	0°C – 40°C	100V – 240V
FPR 2120	Cavium CN 7340	Octeon III	1200 MHz	32 KB	78 KB	4 MB	0°C – 40°C	100V – 240V
FPR 2130	Cavium CN 7350	Octeon III	1200 MHz	32 KB	78 KB	4 MB	0°C – 40°C	100V – 240V
FPR 2140	Intel Xeon D-1577	Broadwell	1300 MHz	32 KB	256 KB	24 MB	0°C – 40°C	100V – 240V
FPR 2140	Cavium CN 7360	Octeon III	1800 MHz	32 KB	78 KB	4 MB	0°C – 40°C	100V – 240V
FPR 1010	Intel Atom C3558	Goldmont	1500 MHz	24 KB/ 32 KB	2MB	N/A	0°C – 40°C	100V – 240V
FPR 1120	Intel Atom C3858	Goldmont	2000 MHz	24 KB/ 32 KB	2MB	N/A	0°C – 40°C	100V – 240V
FPR 1140, FPR 1150	Intel Atom C3958	Goldmont	2000 MHz	24 KB/ 32 KB	2 MB	N/A	0°C – 40°C	100V – 240V
FPR 3105, FPR 3110	AMD EPYC 7272	Zen 2	2900 MHz	32 KB	256 KB	64 MB	0°C – 40°C	100V – 240V
FPR 3120	AMD EPYC 7282	Zen 2	2800 MHz	32 KB	512 KB	64 MB	0°C – 40°C	100V – 240V
FPR 3130	AMD EPYC 7352	Zen 2	2300 MHz	32 KB	512 KB	128 MB	0°C – 40°C	100V – 240V
FPR 3140	AMD EPYC 7452	Zen 2	2350 MHz	32 KB	512 KB	128 MB	0°C – 40°C	100V – 240V
FPR 4215	AMD EPYC 7543	Zen 2	2800 MHz	32 KB	512 KB	256 MB	0°C – 40°C	100V – 240V
FPR 4225	AMD EPYC 7763	Zen 2	2450 MHz	32 KB	512 KB	256 MB	0°C – 40°C	100V – 240V
FPR MIO 9K	Intel Xeon E3-1105C v2 **OSR=4**	Ivy Bridge	1.8 GHz	32 KB	512 KB	16 MB	0°C – 40°C	100V – 240V
FPR 4125	Intel Xeon Gold 6130T	Skylake	2100 MHz	32 KB	1 MB	22 MB	0°C – 40°C	100V – 240V

FPR 9300 SM-40	Intel Xeon Gold 6138T	Skylake	2100 MHz/ 2700 MHz	32 KB	1 MB	27.5 MB	0°C – 40°C	100V – 240V
FPR 4145	Intel Xeon Gold 6152	Skylake	2100 MHz	32 KB	1 MB	30.25 MB	0°C – 40°C	100V – 240V
FPR 9300 SM-48	Intel Xeon Platinum 8160	Skylake	2100 HMz/ 2800 MHz	32 KB	1 MB	33 MB	0°C – 40°C	100V – 240V
FPR 9300 SM-56	Intel Xeon Platinum 8176	Skylake	2100 HMz/ 2800 MHz	32 KB	1 MB	38.5 MB	0°C – 40°C	100V – 240V
QP MIO	Intel Xeon i3-3115C **OSR=4**	Ivy Bridge	2.5 GHz	32 KB	256 KB	4096 KB	0°C – 40°C	100V – 240V
FPR 4112, FPR 4115	Intel Xeon Silver 4116	Skylake	2100 MHz	32 KB	1 MB	16.5 MB	0°C – 40°C	100V – 240V
FMC 1700	AMD EPYC 7232P	Zen 2	3173.03 MHz	32 KB	512 KB	32 MB	0°C – 40°C	100V – 240V
ASA 5506	Intel Atom C2508	Silvermont	1250 MHz	32 KB	256 KB	2 MB	0°C – 40°C	100V – 240V
ASA 5508	Intel Atom C2718	Silvermont	2000 MHz	32 KB	512 KB	4 MB	0°C – 40°C	100V – 240V
ASA 5516	Intel Atom C2758	Silvermont	2416 MHz	32 KB	512 KB	4 MB	0°C – 40°C	100V – 240V
FPR 4110, FPR 4120, FPR 9300 SM-24	Intel Xeon E5-2658 v3	Haswell - EP	2200 MHz	32 KB	256 KB	30 MB	0°C – 40°C	100V – 240V
FPR 4140, FPR 9300 SM-36	Intel Xeon E5-2699 v3	Haswell - EP	2300 MHz	32 KB	256 KB	45 MB	0°C – 40°C	100V – 240V
FPR 4150, FPR 9300 SM-44	Intel Xeon E5-2699 v4	Broadwell	2300 MHz	32 KB	256 KB	55 MB	0°C – 40°C	100V – 240V
AIR-AP2802, AIR-AP3802, AIR-AP4800, AIR-AP1562, IW6300, ESW6300	Marvell 88F6920	ARM V7 Cortex-A9	1.8 GHz	32 KB	1 MB	N/A	0°C – 50°C (AIR-AP2802, AIR-AP3802, AIR-AP4), -40°C – 65°C (AIR-AP1562), -40°C – 65°C (IW6300), -40°C – 85°C (ESW6300)	100V – 240V
CW9162	Qualcomm IPQ6010	ARM Cortex A53	1.8 GHz	32 KB	512 KB	N/A	0°C – 50°C	100V – 240V
C9124, CW9164, CW9166, IW9167	Qualcomm IPQ8076	ARM Cortex A53	2.2 GHz	32 KB	512 KB	N/A	-40°C – 65°C (C9124, IW9167), 0°C – 50°C (CW9164, CW9166),	100V – 240V (C9124, CW9164, CW9166) 90V – 264V (IW9167)

C9124, C9130, C9136	Qualcomm IPQ8078	ARM Cortex A53	2.2 GHz	32 KB	512 KB	N/A	-40°C – 65°C (C9124), 0°C – 50°C (C9130 and C9136)	100V – 240V
C9105	Broadcom BCM47622	ARM Cortex A7	1.5 GHz	32 KB	512 KB	N/A	0°C – 50°C	100V – 240V
C9115, C9120	Broadcom BCM49408	ARM v8 Cortex B53	1.8 GHz	32 KB	1 MB	N/A	-20°C – 50°C	100V – 240V

4 Configuration Settings

Table 3 summarizes the configuration settings used by the Cisco implementation of JENT. These settings must be preserved to comply with the JENT ESV certificate.

Table 3: Configuration Settings

JENT_RANDOM_MEMACCESS	Enabled	Determines the method of memory access
JENT_CONF_ENABLE_INTERNAL_TIMER	Disabled	Disables the use of internal timers
JENT_CONF_DISABLE_LOOP_SHUFFLE	Enabled	Disables the random number of hash loops performed for each call (only one hash operation is performed with this setting)
JENT_MIN_OSR	3 or 4	Oversampling rate

5 Physical Security Mechanisms

The JENT implementation is a software module. As such, it does not include physical security mechanisms. The JENT module may be used on a variety of devices with differing security levels. Physical security requirements are, therefore, dependent on the modules that use JENT. Conceptual Interfaces

GetEntropy:

The call to jent_read_entropy serves as a GetEntropy interfaces, according to the SP 800-90B definition. The jent_read_entropy function generates a random number in a way that is compliant with all SP 800-90B requirements. The caller specifies the size of the random value that it wants. The function returns an error code to indicate whether or not the request was fulfilled successfully. The error code also reports failures of the health tests.

GetNoise:

The JENT library doesn't have a GetNoise interface, but JENT comes with scripts that collect the raw noise data (jitterentropy-rng). The scripts collect 1,000,000 samples of raw data.

HealthTest:

The JENT library doesn't have a HealthTest interface, but health tests can be run by allocating a new JENT handle. This is in compliance with SP 800-90B.

6 Min-Entropy Rate

The Cisco JENT implementation generates an output that is considered to have full entropy. A request for 256 bits of entropy results in 256 bits of entropy per output sample, or full entropy.

7 Health Tests

Per the SP 800-90B requirements, health tests are run when JENT starts, and are then run continuously while it is operating. All tests check for persistent failures base on their respective "cutoff" values, which represent expected error thresholds.

JENT implements four types of health tests:

- Stuck Test
- Repetition Count Test (RCT)
- Adaptive Proportion Test (APT)
- Lag Predictor Test

The stuck test calculates the first, second and third discrete derivative of the time to be processed by the hash. Only if all three values are non-zero, the received time delta is considered to be non-stuck.

The Lag Predictor Test is a vendor-defined conditional test that is designed to detect a known failure mode where the result becomes mostly deterministic. It is based on the Lag Prediction Test described in SP 800-90B, section 6.3.8.

The RCT and APT tests are as described in SP 800-90B.

When any health test fails, the API call to generate random numbers jent_read_entropy(3) informs the caller about the failure with error codes. When a health test failure occurs, the Jitter RNG block causing the failure is not returned to the caller.

All health test failures are considered permanent failures. If one is triggered, the current instance of the Jitter RNG will always remain in error state. The documentation of the API call jent_read_entropy(3) explains that the caller can only clear this error state by deallocating the Jitter RNG instance followed by an allocation of a new Jitter RNG instance to reset the noise source.

8 Maintenance

There are no maintenance requirements for the JENT library.

9 Required Testing

The entropy report contains the results of the testing done on the raw and restart data. Raw data was collected by running the invoke_testing.sh script included in the JENT package. This script gathers 1,000,000 samples of raw data. It also gathers 1000 samples of raw data after restarting JENT each time, thus eventually gathering 1,000,000 samples of data for the restart tests.

JENT allows two modes of operation. In one mode, the number of hashing operations performed each time a time stamp is to be added to the entropy pool varies between 1 and 8. In the other mode, the number of hashing operations is always one. For best compliance to SP 800-90B, the second mode is preferred (and is the default setting for JENT 3.4.1).

Raw Data Analysis

The CPU Jitter RNG does not have a stochastic model, but an $H_{submitter}$ estimate of 2 was determined using analysis as described in SP 800-90B Section 3.2.2, Requirement 3. The Jitter RNG implementation uses an oversampling rate of 3, except for the two MIO platforms, which use an oversampling rate of 4 because of their very low system load. For that reason, $H_{submitter}$ is set to 0.667 (2/3) (or 0.5000 (2/4) for the MIOs) for the purpose of running the NIST restart tests. The oversampling rate is set in the JENT code.

Each raw data sample consists of one time stamp, which is 64 bits long. It is assumed that only the least significant 4 bits of each time stamp contain any true entropy. The JENT design states that the Jitter RNG can deliver full entropy if and only if the min-entropy is at least 2/osr bit of entropy per time stamp. The Jitter RNG implementation uses an oversampling rate of 3 for most platforms, but uses an oversampling rate of 4 for the FPR MIO 9K and the QP MIO platforms[1], which operate under very low load and thus need to collect more entropy.

The min-entropy for the raw data samples collected on all the platforms covered by this report ranges from 1.576943 to 3.629426 bits of entropy per 4-bit sample, thus greatly exceeding the requirement of 2/3 of a bit of entropy per 4-bit sample to claim full entropy.

Restart Data Analysis

The CPU Jitter RNG does not have a stochastic model, but an Hsubmitter estimate of 2 was determined using analysis as described in SP 800-90B Section 3.2.2, Requirement 3. The Jitter RNG implementation uses an oversampling rate of 3, except for the two MIO platforms, which use an oversampling rate of 4 because of their very low system load. For that reason, Hsubmitter is set to 0.667 (2/3) (or 0.5000 for the MIOs) for the purpose of running the NIST restart tests.

[1] OSR was set to 4 for the FPR MIO 9K platform (which uses Intel Xeon E3-1105C v2) and the QP MIO platform (which uses Intel Xeon i3-3115C). All other platforms use OSR of 3.

For the restart tests, the raw entropy data is collected for 1,000 Jitter RNG instances allocated sequentially. That means, for one collection of raw entropy, one Jitter RNG instance is allocated. After the conclusion of the data gathering it is deallocated and a new Jitter RNG instance is allocated for the next restart test round.

The min-entropy for the restart data samples collected on all the platforms covered by this report ranges from 1.844298 to 3.895149 bits of entropy per 4-bit sample, thus greatly exceeding the requirement of 2/3 of a bit of entropy per 4-bit sample (or, for the two MIO platforms, 2/4 bits of entropy per 4-bit sample) to claim full entropy.

Platform	Processor	H_r	H_c	H_I	Result
C9800-40	Intel Xeon D-1548	3.883929	3.880771	0.666667	Validation Test Passed
C9800-80	Intel Xeon Silver 4116	3.687754	3.658234	0.666667	Validation Test Passed
C9800-L	Intel Xeon D-1563N	3.648910	3.866812	0.666667	Validation Test Passed
FPR 2110	Intel Xeon D-1526	3.687754	3.865286	0.666667	Validation Test Passed
FPR 2110	Cavium CN 7235	3.677642	3.773078	0.666667	Validation Test Passed
FPR 2120	Intel Xeon D-1528	3.667807	3.87451	0.666667	Validation Test Passed
FPR 2120	Cavium CN 7340	3.687754	3.888706	0.666667	Validation Test Passed
FPR 2130	Intel Xeon D-1548	3.687754	3.872578	0.666667	Validation Test Passed
FPR 2130	Cavium CN 7350	3.677642	3.880771	0.666667	Validation Test Passed
FPR 2140	Intel Xeon D-1577	3.872966	3.872578	0.666667	Validation Test Passed
FPR 2140	Cavium CN 7360	3.301738	3.879200	0.666667	Validation Test Passed
FPR 1010	Intel Atom C3558	3.677642	3.883929	0.666667	Validation Test Passed
FPR 1120	Intel Atom C3858	3.890309	3.667807	0.666667	Validation Test Passed
FPR 1140, FPR 1150	Intel Atom C3958	3.872578	3.687754	0.666667	Validation Test Passed
FPR 3105, FPR 3110	AMD EPYC 7272	3.146094	3.089854	0.670000	Validation Test Passed
FPR 3120	AMD EPYC 7282	3.148807	3.118123	0.670000	Validation Test Passed
FPR 3130	AMD EPYC 7352	3.162803	3.124481	0.670000	Validation Test Passed
FPR 3140	AMD EPYC 7452	3.088148	3.058949	0.670000	Validation Test Passed
FPR 4215	AMD EPYC 7543	3.639821	3.677642	0.670000	Validation Test Passed
FPR 4225	AMD EPYC 7763	3.687754	3.677642	0.670000	Validation Test Passed
FPR MIO 9K	Intel Xeon E3-1105C v2 **OSR=4**2	1.907032	1.902660	0.500000	Validation Test Passed
FPR 4125	Intel Xeon Gold 6130T	3.895149	3.890309	0.670000	Validation Test Passed
FPR 9300 SM-40	Intel Xeon Gold 6138T	3.874517	3.677642	0.670000	Validation Test Passed
FPR 4145	Intel Xeon Gold 6152	3.677642	3.687754	0.670000	Validation Test Passed
FPR 9300 SM-48	Intel Xeon Platinum 8160	3.876073	3.773078	0.670000	Validation Test Passed
FPR 9300 SM-56	Intel Xeon Platinum 8176	3.876073	3.773078	0.670000	Validation Test Passed
QP MIO	Intel Xeon i3-3115C **OSR=4**3	1.844298	1.900508	0.500000	Validation Test Passed
FPR 4112, FPR 4115	Intel Xeon Silver 4116	3.677642	3.872578	0.670000	Validation Test Passed
FMC 1700	AMD EPYC 7232P	3.035112	2.950809	0.670000	Validation Test Passed
ASA 5506	Intel Atom C2508	3.667807	3.868343	0.670000	Validation Test Passed
ASA 5508	Intel Atom C2718	3.390956	3.418952	0.670000	Validation Test Passed
ASA 5516	Intel Atom C2758	3.348659	3.433812	0.670000	Validation Test Passed

FPR 4110, FPR 4120, FPR 9300 SM-24	Intel Xeon E5-2658 v3	3.882348	3.885516	0.670000	Validation Test Passed
FPR 4140, FPR 9300 SM-36	Intel Xeon E5-2699 v3	3.773078	3.880771	0.670000	Validation Test Passed
FPR 4150, FPR 9300 SM-44	Intel Xeon E5-2699 v4	3.687754	3.687754	0.670000	Validation Test Passed
AIR-AP2802, AIR-AP3802, AIR-AP4800, AIR-AP1562, IW6300, ESW6300	Marvell 88F6920	3.559714	3.566967	0.670000	Validation Test Passed
CW9162	Qualcomm IPQ6010	3.872578	3.648910	0.670000	Validation Test Passed
C9124, CW9164, CW9166, IW9167	Qualcomm IPQ8076	1.844298	2.158733	0.670000	Validation Test Passed
C9124, C9130, C9136	Qualcomm IPQ8078	2.080408	2.618997	0.670000	Validation Test Passed
C9105	Broadcom BCM47622	3.454634	3.532084	0.670000	Validation Test Passed
C9115, C9120	Broadcom BCM49408	3.318077	3.222160	0.670000	Validation Test Passed

[2] OSR was increased due to very low system load
[3] OSR was increased due to very low system load