SP 800-90B Non-Proprietary Public Use Document

AS578 Entropy Source

Document Version: 1.1

Hardware Version: 3.4.0
Firmware Version: 1.4.0

Shenzhen IBestChain Technology Co., Ltd.
2C-208A, 2nd Floor, Building 213,
Tairan Science and Technology Park, Tairan 6th Road,
Tianan Community, Shatou Street,
Futian District, Shenzhen

Date： January 9, 2023

Revision History

Version	Change
1.0	Initial release
1.1	Added Cert. # with link in Security Boundary section

Table of Contents

Description 4

Security Boundary 4

Operating Conditions and Configuration Settings 5

Physical Security Mechanisms 5

Conceptual Interfaces 5

Min-Entropy Rate 5

Health tests 5

Maintenance 6

Required Testing 6

Description

The AS578 entropy source is a physical entropy source whose hardware Version is 3.4.0 and Firmware Version is 1.4.0. Data produced by the entropy source is expected to be non-IID. The entropy source was tested on ThinkBook 15 G3 ITL.

Security Boundary

The security boundary of the AS578 entropy source is formed by a noise source, digitizer, 128 bits shift register, health tests, and a conditioner. See Figure 1 below. The AS578 entropy source is within the security boundary of the cryptographic module which utilizes physical security mechanisms as described below.

The physical random noise source contains 1 ring oscillator consisting of 53 inverters. The raw data register is a 128-bit shift register. The raw data is shifted into the register bit by bit until the 128-bit shift register is filled. The digitizer is a D flip-flop providing a sampling frequency of 2Mhz. The health tests are divided into start-up health tests, on-demand health tests and continuous health tests, all of which use the methods in SP 800-90B: APT and RCT. The conditioner is a Vetted Conditioning Component, which is a SHA2-256, a CAVP approved hash algorithm, Cert# A2750.

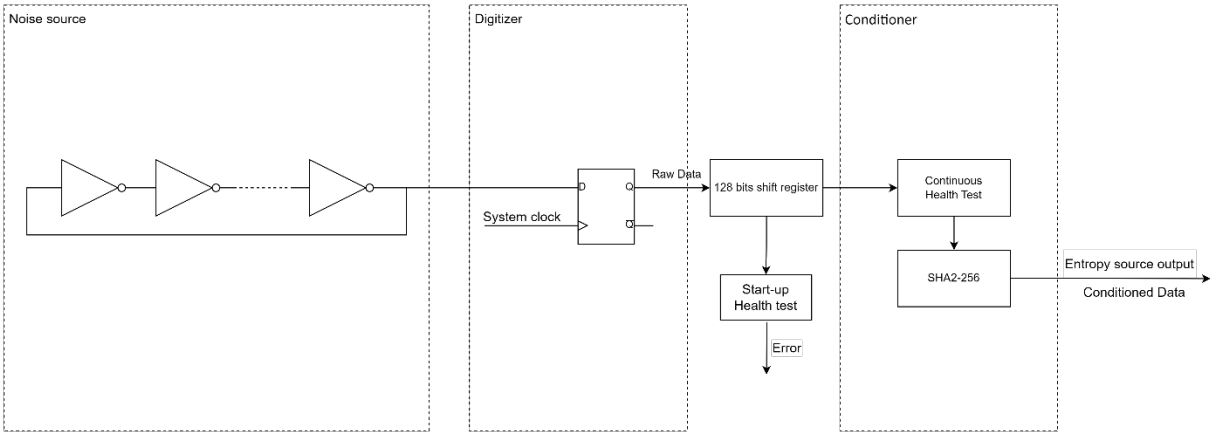

Figure 1. Security Boundary of the Entropy Source

Operating Conditions and Configuration Settings

Table 1. Entropy-Relevant Parameters

Parameter	Value	Description
Temperature	0℃ - 40℃	The temperature range in which the entropy source works normally.
Voltage	3V - 5V	The voltage range in which the entropy source works normally.
Clock speed	2Mhz	The clock frequency at which the noise source is sampled.
The APT's cutoff	687	The test fails if 687 of 1024 consecutive samples have the same value as the first sample.
The RCT's cutoff	49	The test fails if the values of 49 consecutive samples tested are the same value.
ring oscillator frequency	200Mhz	Central frequency of ring oscillation.
start-up delay	100ms	After the chip is powered on and initialized for 100ms, the entropy source can be output.

Physical Security Mechanisms

The AS578 entropy source has physical security mechanisms of opacity, tamper response and temperature protection.

Conceptual Interfaces

The get_entropy_conditioned_data() interface is called during the instantiation function and reseed function of the DRBG to provide entropic data for the seed. The DRBG specifies how much entropy it needs from the AS578 entropy source, and the entropy source returns the requested amount.

Min-Entropy Rate

The AS578 entropy source provides 256 bits of min-entropy per 256-bit output sample, or full entropy.

Health tests

When the chip is powered on, start-up health tests are performed on raw data from the noise source.

The AS578 performs the start-up tests for on-demand health tests. On-demand tests can be called upon by reset. The on-demand health tests and start-up health tests both use continuous health test methods: APT and RCT, but do not pass any data on to the conditioner.

When the DRBG algorithm is seeded, the continuous health tests are performed on raw data from the noise source. If both APT and RCT tests do not detect any failures, the tested data is provided to the conditioner and conditioned bits are provided to the calling function for use by the DRBG hash reseed function.

The failure mode is Error state. When the health test fails, the entropy source chip will enter the error state, close the external interface of the chip, and the entropy source will stop outputting data.

Maintenance

There are no specific maintenance requirements for the entropy source.

Required Testing

The AS578 entropy source was tested by collecting data from the device operating in its designated operational range and then processed with the SP 800-90B tool. Test data was collected following the requirements of Section 3 of SP 800-90B.

No further testing is required.