Verification Report

Overview

- Number of blocks: 7
- Number of assertions: 829
- Lines of Code: >13.2k
- Reported Bugs: 9
- Reported Enhancements: 7

Formal Effort

	Version	Block	# of Assertions	AIP LoC	Reported Issues
1	1.0	SHA256	9	533	
2	1.1	SHA256 (LMRS)	31	1032	6
3	1.0	SHA512	11	588	
4	1.0	DOE (ENC + DEC)	110	1660	2
5	1.0	HMAC	11	211	
6	1.5	ECC	589	7182	7
7	1.5	ECC - HMAC_DRBG	54	896	1
8	1.0	ECC- SHA512_masked	14	1151	

Reported Issues DOE

Enhancements:

1. #165
2. #542

Reported Issues ECC

Bugs:

1. #237
2. #223
3. #221(Note: this bug was notified by design team to us and later it was found by our AIP)
4. #184
5. #173

Enhancements:

1. #194
2. Deadcode: in ecc_pm_ctrl:63 the last else if () is always taken. Enhancement for code readability.
3. When the error happens for the first time, the error flag goes high and will remain high until zeroize.We expect that uC issues zeroize if there is an error in ECC.In this scenario, although the second command will be performed, the results should not be used since error flag is kept high. However, this can be considered as another enhancement to stop faulty ECC from continuing before zeroize.

Reported Issues ECC-HMAC_DRBG

Bugs:

1. #832

Reported Issues SHA256 (LMRS)

Bugs:

1. The signal core_ready remained high for one clock cycle after receiving an init/next command which caused the ready register to remain high as well and, therefore, allowed to send in a winternitz computation request causing the fsm to go into winternitz computation mode, although, currently a regular sha operation is performed
2. Combinational computation for the next state (wntz_fsm_next) did not cover all paths so that the state signal may become X
3. LMS module raised the ready signal whenever sha core finishes a computation, although, it is realated to not finished LMS computation

Enhancements:

1. Unreachable default case in switch cases for a single bit signal
2. Not used signal (written but never read)
3. Not used bit in state signal

Formal Proofs

	# Version	≡ Block	≡ Formal Coverage*	≡ Prove Time	≡ I/O Delay (minimum)
1	1.0	SHA256	100%	< 1h	>70 cycles per block
2	1.1	SHA256 (LMRS)	100%	< 1h	>136 cycles per block
3	1.0	SHA512	100%	< 1h	>85 cycles per block
4	1.0	DOE (ENC + DEC)	100%	< 12h	>100 cycles per block
5	1.0	HMAC	100%	< 1h	>380 cycles per block
6	1.5	ECC	100%	< 24h	millions of cycles per command
7	1.5	ECC - HMAC_DRBG	100%	< 3h	>90 cycles per block

8	1.0	ECC - SHA512_masked	100%	< 3h	>400 cycles per block

*) Excluding unreachable and dead code