Verification Report

Overview

- Number of blocks: 31
- Number of assertions: 1716
- Lines of Code: >98 k
- Reported Bugs/Enhancements: 22

Formal Effort

The effort table contains the information for each individual block which has been verified using the commercial formal tools and the bugs/enhancements observed in the due period with their respective github issue ID's.

	Version	Block	# Assertions	AIP LoC	# Bugs/Enhancements	Issue ID
1	1.0	sha3/keccak Round	10	722	0	
2	1.0	sha3/keccak	45	2262	3	#127,#126,#128
3	1.0	adamsbridge_ctrl	872	46178	6	#85, #78, #64, #55,#43,#46
4	1.0	sample_in_ball_ctrl	21	2056	1	#62
5	1.0	exp_mask_ctrl	1	166	0	
6	1.0	rej_bounded_ctrl	12	1744	0	
7	1.0	rej_sampler_ctrl	12	1280	0	
8	1.0	abr_piso	13	682		
9	1.0	sib_mem	4	156	0	
10	1.0	ntt_shuffle_buffer	3	656	1	#93
11	1.0	ntt_ctrl	170	11414	3	#89, #86,#90
12	1.0	ntt_butterfly	6	378	0	
13	1.0	ntt_hybrid_butterfly_2x2	10	660	0	
14	1.0	ntt_masked_BFU_add_sub	6	175	0	

15	1.0	ntt_masked_BFU_mult	12	228	0	
16	1.0	ntt_masked_butterfly1x2	2	185	0	
17	1.0	ntt_masked_gs_butterfly	2	115	0	
18	1.0	ntt_masked_pwm	3	129	0	
19	1.0	power2round_top	34	2124	0	
20	1.0	decompose	37	3420	2	#87, #41
21	1.0	skencode	34	3194	0	
22	1.0	skdecode_top	124	6942	0	
23	1.0	makehint	47	2806	1	#95
24	1.0	norm_check_top	17	1382	1	#96
25	1.0	sigencode_z_top	16	1030	0	
26	1.0	pkdecode	16	844	0	
27	1.0	sigdecode_z_top	16	1018	0	
28	1.0	sigdecode_h	32	1752	3	#131, #130,#132
29	1.0	sampler_top	54	784	0	
30	1.0	ntt_top	50	1616	0	
31	2.0	adamsbridge_ctrl (stream_msg)	35	1924	1	#145(found in simulation and then in FPV)

Formal Proof

	Version	Block	Formal Coverage*	Prove time minimum ^
1	1.0	sha3/keccak Round	100%	< 1h
2	1.0	sha3/keccak	100%	< 1h
3	1.0	adamsbridge_ctrl	100%	< 24h
4	1.0	sample_in_ball_ctrl	100%	<1h

5	1.0	exp_mask_ctrl	100%	<1h
6	1.0	rej_bounded_ctrl	100%	<1h
7	1.0	rej_sampler_ctrl	100%	<1h
8	1.0	abr_piso	100%	<1h
9	1.0	sib_mem	100%	<1h
10	1.0	ntt_shuffle_buffer	100%	<1h
11	1.0	ntt_ctrl	100%	< 24h
12	1.0	ntt_butterfly		< 24h
13	1.0	ntt_hybrid_butterfly_2x2		< 24h
14	1.0	ntt_masked_BFU_add_sub		< 24h
15	1.0	ntt_masked_BFU_mult		< 24h
16	1.0	ntt_masked_butterfly1x2		< 24h
17	1.0	ntt_masked_gs_butterfly		< 24h
18	1.0	ntt_masked_pwm		< 24h
19	1.0	power2round_top	100%	< 4h
20	1.0	decompose	100%	< 3h
21	1.0	skencode	100%	< 1h
22	1.0	skdecode_top	100%	< 3h
23	1.0	makehint	100%	< 1h
24	1.0	norm_check_top	100%	< 1h
25	1.0	sigencode_z_top	100%	< 1h
26	1.0	pkdecode	100%	< 1h
27	1.0	sigdecode_z_top	100%	< 1h
28	1.0	sigdecode_h	100%	< 4h
29	1.0	sampler_top	100%	< 2h
30	1.0	ntt_top	100%	< 2h
31	2.0	adamsbridge_ctrl(stream_msg)	100%	< 24h

*) excluding unreachable and deadcode.

^) Proof time with 24h have some non-converging proofs

And the ntt compute modules like butterfly formal coverage is subjective since it involves arithmetic operations like multiplication, modulo which are tough to solve in formal environment.