AES-GCM DV Test Report

Author(s) and Contributors: Pascal Nasahl Pirmin Vogel
Reviewers: Pirmin Vogel Pascal Nasahl
Last Update: Mar 25, 2025
Status: Reviewed

This document reports the current AES pass rates and test coverage results. The analysis was conducted using the RTL & DV state of commit f722f21.

The report was generated using Cadence Xcelium 22.09.001 and the following command:

```
./util/dvsim/dvsim.py hw/ip/aes/dv/aes_masked_sim_cfg.hjson -i all \
-t xcelium --cov
```

Test Pass Rate

As shown in the Appendix, the test pass rate is at **97.49%**. In the upstream OpenTitan repository, the latest regression pass rate without the new GCM mode is at **97.63%**.

The 45 failing tests can be categorized as following:

Category	**Tests**	**Number of failures**	**Assessment**
Fault Injection Test	*aes_fi* *aes_control_fi* *aes_cipher_fi* *aes_core_fi*	35	Low risk
Stress Test	*aes_stress_all_with_rand_reset*	10	Low risk

Analysis

Fault Injection Test

All of these errors, except the second one in the *aes_fi* test, are also present in the latest upstream report. As they occur in FI tests, they are of no concern regarding functionality.

2/35 *aes_fi*

- `Assertion tb.dut.u_aes_core.AesSecCmDataRegLocalEscDataOut has failed`
- `UVM_FATAL (aes_fi_vseq.sv:86) virtual_sequencer [aes_fi_vseq] Was Able to finish without clearing reset`
    - This is a new failure signature that is related to an uncritical testbench issue.

14/35 *aes_control_fi*

- `Job timed out after * minutes`

- `UVM_FATAL (aes_control_fi_vseq.sv:62) [aes_control_fi_vseq] wait timeout occurred!`

18/35 *aes_cipher_fi*

- `Job timed out after * minutes`
- `UVM_FATAL (aes_cipher_fi_vseq.sv:62) [aes_cipher_fi_vseq] wait timeout occurred!`

1/35 aes_core_fi

- `UVM_FATAL (aes_core_fi_vseq.sv:70) [aes_core_fi_vseq] wait timeout occurred!`

Stress Test

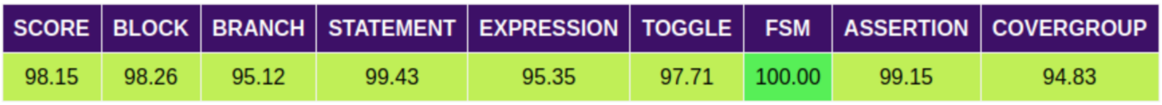
10/10 *aes_stress_all_with_rand_reset* tests are also failing in the upstream report. The reported failures are either identical to the fault injection test failures, not specific to AES but due to a general DV environment issues which are known in the OpenTitan project, or AES-specific DV issues which are not of concern.

- **3/10:** `UVM_ERROR (cip_base_vseq.sv:868) [aes_common_vseq] Check failed (!has_outstanding_access()) Waited * cycles to issue a reset with no outstanding accesses.`
  - The sequence times out waiting for a window without an ongoing TLUL access. A DV environment issue.
- **3/10**: `UVM_ERROR (uvm_sequencer_base.svh:757) sequencer [SEQREQZMB] The task responsible for requesting a wait_for_grant on sequencer 'sequencer' for sequence 'sideload_seq' has been killed, to avoid a deadlock the sequence will be removed from the arbitration queues`
  - This is a general DV issue in the OpenTitan DV environment and the sideload DV agent in particular. Other block-level regressions “solve this” by not enabling sideload in the stress_all_with_rand_reset sequence.
- **3/10**: `UVM_FATAL (aes_base_vseq.sv:75) [aes_alert_reset_vseq] Check failed (aes_ctrl_aux[*] == cfg.do_reseed)`
  - The base sequence erroneously assumes that the aes_init() task is always run when the DUT comes out of reset, meaning when the aes_ctrl_aux CSR isn’t locked. This doesn’t hold for the aes_stress_all_with_rand_reset test.
- **1/10**: `UVM_FATAL (aes_base_vseq.sv:306) virtual_sequencer [aes_reseed_vseq] Expected GCM phase GCM_AAD, got GCM_TEXT`
  - Configuration errors randomly injected during the reseed sequence are not properly handled by the DV environment (during a reseed operation the GCM control register is not writable, meaning the configuration cannot be resolved successfully).

Test Coverage

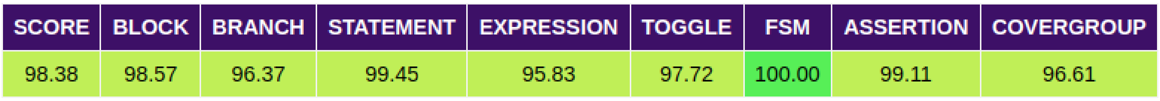
As shown in the picture below, the test coverage slightly dropped in comparison to the upstream report:

This report (with AES-GCM):



SCORE	BLOCK	BRANCH	STATEMENT	EXPRESSION	TOGGLE	FSM	ASSERTION	COVERGROUP
98.15	98.26	95.12	99.43	95.35	97.71	100.00	99.15	94.83

Upstream report (without AES-GCM):

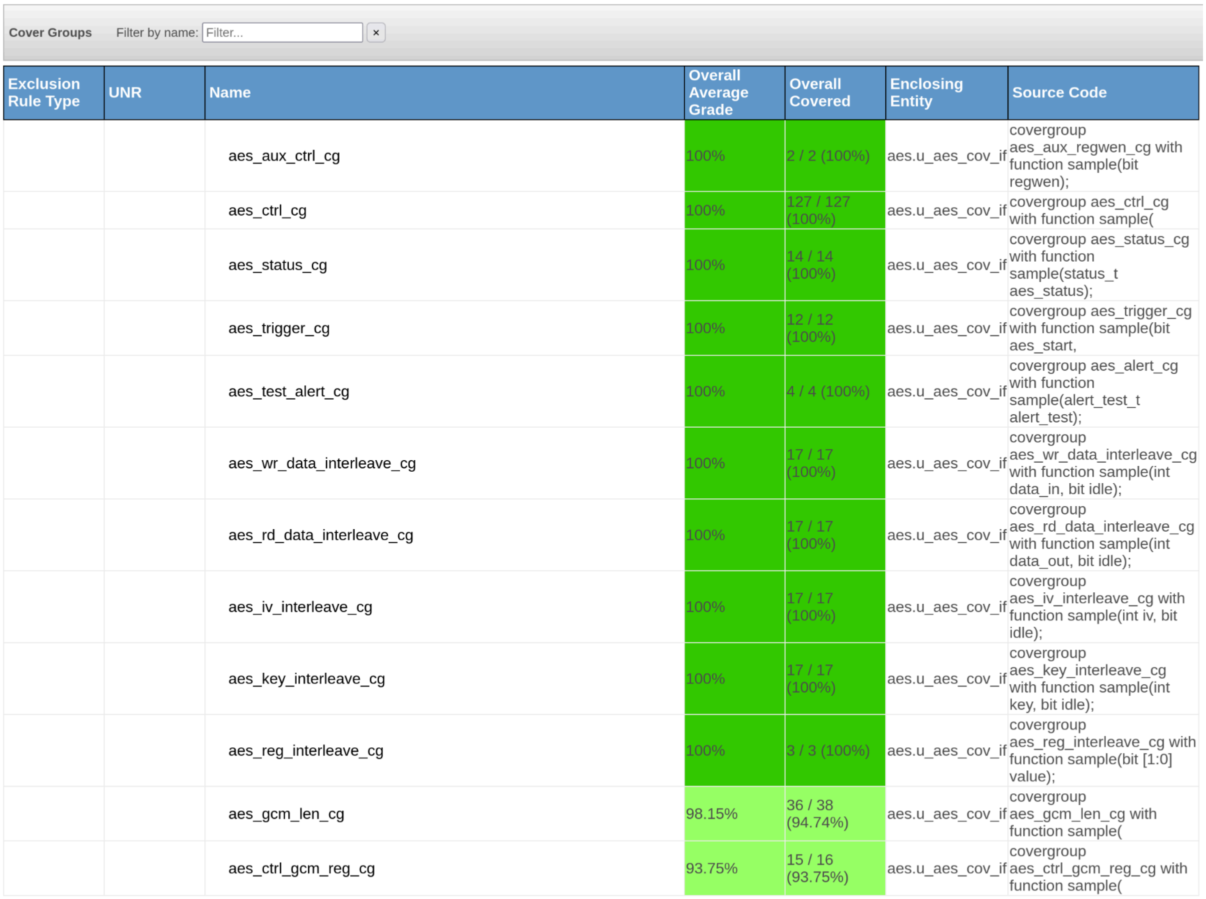


SCORE	BLOCK	BRANCH	STATEMENT	EXPRESSION	TOGGLE	FSM	ASSERTION	COVERGROUP
98.38	98.57	96.37	99.45	95.83	97.72	100.00	99.11	96.61

In the next subsections, we focus on analyzing the coverage gaps for COVERGROUP, FSM, and BRANCH as the other cover class results are similar.

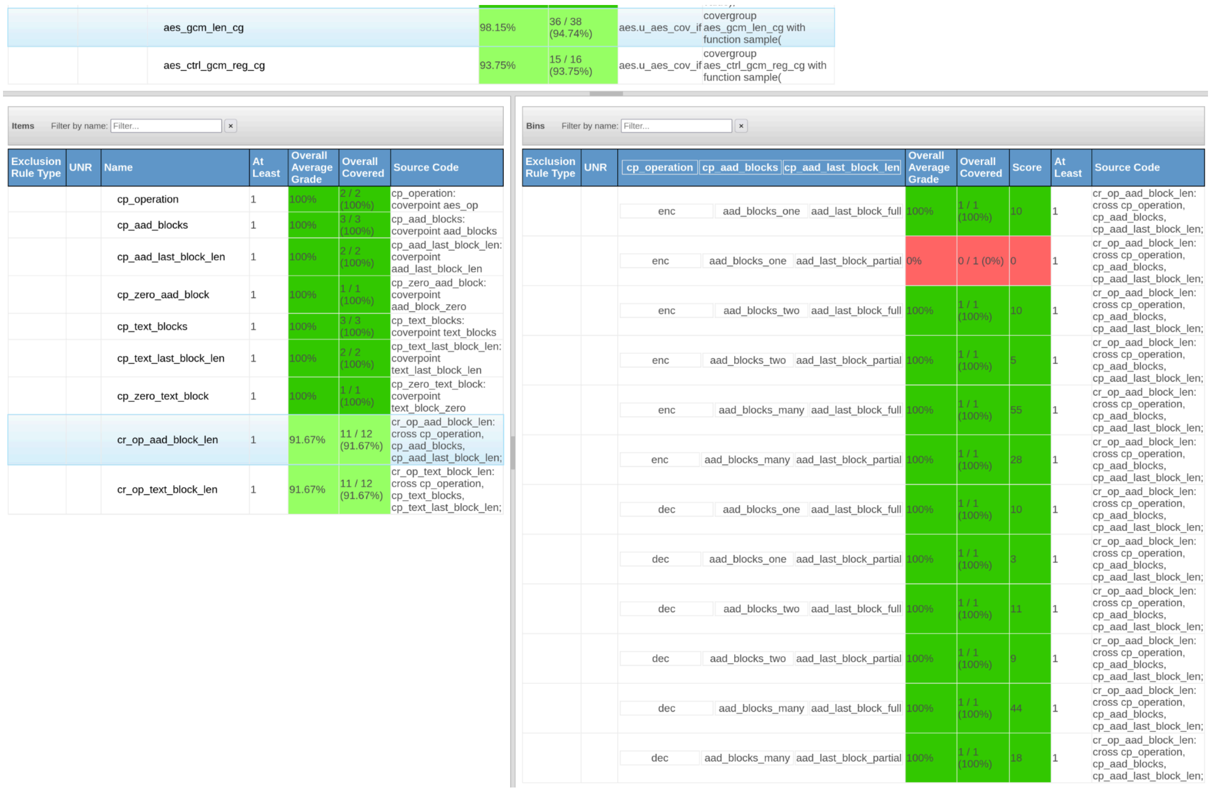
Covergroup

The cover group coverage dropped as new AES-GCM specific cover groups were added.



Exclusion Rule Type	UNR	Name	Overall Average Grade	Overall Covered	Enclosing Entity	Source Code
		aes_aux_ctrl_cg	100%	2 / 2 (100%)	aes.u_aes_cov_if	covergroup aes_aux_regwen_cg with function sample(bit regwen);
		aes_ctrl_cg	100%	127 / 127 (100%)	aes.u_aes_cov_if	covergroup aes_ctrl_cg with function sample(
		aes_status_cg	100%	14 / 14 (100%)	aes.u_aes_cov_if	covergroup aes_status_cg with function sample(status_t aes_status);
		aes_trigger_cg	100%	12 / 12 (100%)	aes.u_aes_cov_if	covergroup aes_trigger_cg with function sample(bit aes_start,
		aes_test_alert_cg	100%	4 / 4 (100%)	aes.u_aes_cov_if	covergroup aes_alert_cg with function sample(alert_test_t alert_test);
		aes_wr_data_interleave_cg	100%	17 / 17 (100%)	aes.u_aes_cov_if	covergroup aes_wr_data_interleave_cg with function sample(int data_in, bit idle);
		aes_rd_data_interleave_cg	100%	17 / 17 (100%)	aes.u_aes_cov_if	covergroup aes_rd_data_interleave_cg with function sample(int data_out, bit idle);
		aes_iv_interleave_cg	100%	17 / 17 (100%)	aes.u_aes_cov_if	covergroup aes_iv_interleave_cg with function sample(int iv, bit idle);
		aes_key_interleave_cg	100%	17 / 17 (100%)	aes.u_aes_cov_if	covergroup aes_key_interleave_cg with function sample(int key, bit idle);
		aes_reg_interleave_cg	100%	3 / 3 (100%)	aes.u_aes_cov_if	covergroup aes_reg_interleave_cg with function sample(bit [1:0] value);
		aes_gcm_len_cg	98.15%	36 / 38 (94.74%)	aes.u_aes_cov_if	covergroup aes_gcm_len_cg with function sample(
		aes_ctrl_gcm_reg_cg	93.75%	15 / 16 (93.75%)	aes.u_aes_cov_if	covergroup aes_ctrl_gcm_reg_cg with function sample(

Cover group *aes_gcm_len_cg* tests, whether different numbers of AAD/TEXT blocks (1,2,>2) have been seen with different sized final AAD/TEXT blocks (partial, full). All the cover points were seen but the cross coverage does not reach 100%. These coverage gaps are not systematic and the crosses could be fully covered by slightly tuning the randomization to generate more partial final blocks. Refer to the following figures for the details.



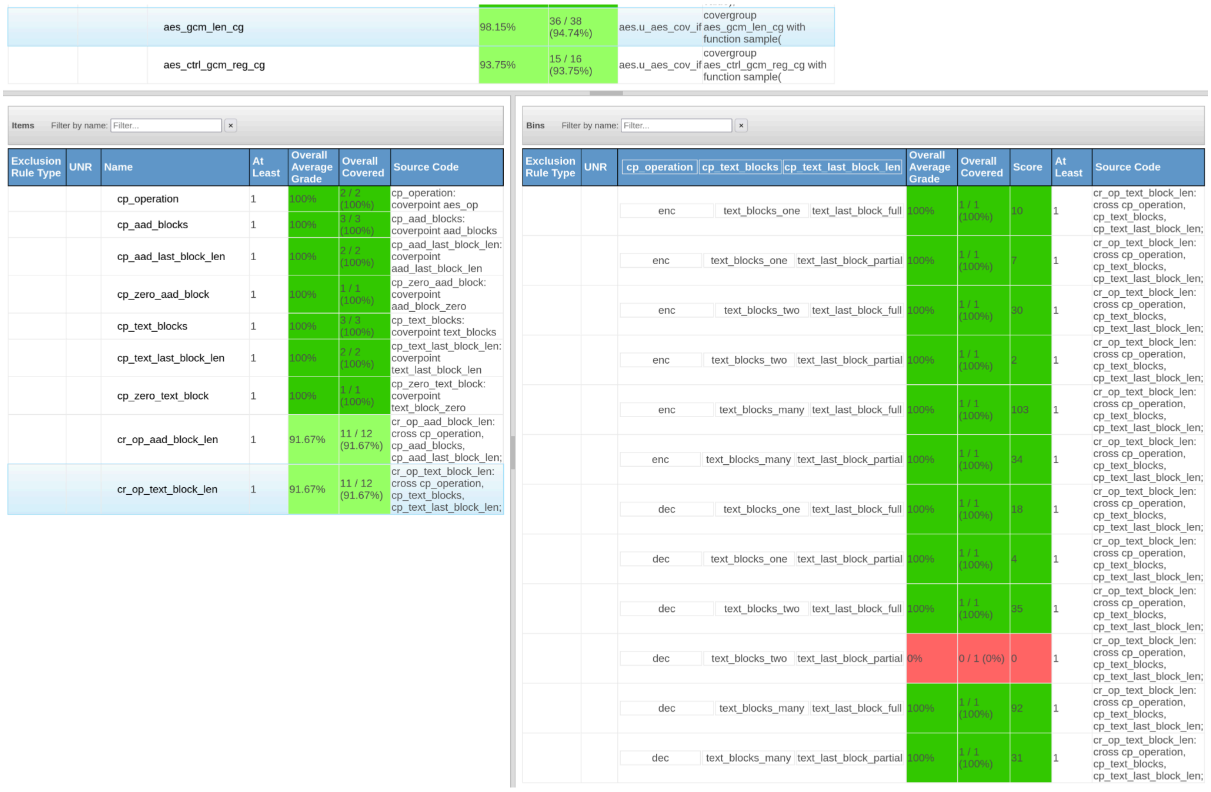
		aes_gcm_len_cg	98.15%	36 / 38 (94.74%)	aes.u_aes_cov_if	covergroup aes_gcm_len_cg with function sample(
		aes_ctrl_gcm_reg_cg	93.75%	15 / 16 (93.75%)	aes.u_aes_cov_if	covergroup aes_ctrl_gcm_reg_cg with function sample(

Items Filter by name: Filter... ×

Exclusion Rule Type	UNR	Name	At Least	Overall Average Grade	Overall Covered	Source Code
		cp_operation	1	100%	2 / 2 (100%)	cp_operation: coverpoint aes_op
		cp_aad_blocks	1	100%	3 / 3 (100%)	cp_aad_blocks: coverpoint aad_blocks
		cp_aad_last_block_len	1	100%	2 / 2 (100%)	cp_aad_last_block_len: coverpoint aad_last_block_len
		cp_zero_aad_block	1	100%	1 / 1 (100%)	cp_zero_aad_block: coverpoint aad_block_zero
		cp_text_blocks	1	100%	3 / 3 (100%)	cp_text_blocks: coverpoint text_blocks
		cp_text_last_block_len	1	100%	2 / 2 (100%)	cp_text_last_block_len: coverpoint text_last_block_len
		cp_zero_text_block	1	100%	1 / 1 (100%)	cp_zero_text_block: coverpoint text_block_zero
		cr_op_aad_block_len	1	91.67%	11 / 12 (91.67%)	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		cr_op_text_block_len	1	91.67%	11 / 12 (91.67%)	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;

Bins Filter by name: Filter... ×

Exclusion Rule Type	UNR	cp_operation	cp_aad_blocks	cp_aad_last_block_len	Overall Average Grade	Overall Covered	Score	At Least	Source Code
		enc	aad_blocks_one	aad_last_block_full	100%	1 / 1 (100%)	10	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		enc	aad_blocks_one	aad_last_block_partial	0%	0 / 1 (0%)	0	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		enc	aad_blocks_two	aad_last_block_full	100%	1 / 1 (100%)	10	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		enc	aad_blocks_two	aad_last_block_partial	100%	1 / 1 (100%)	5	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		enc	aad_blocks_many	aad_last_block_full	100%	1 / 1 (100%)	55	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		enc	aad_blocks_many	aad_last_block_partial	100%	1 / 1 (100%)	28	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_one	aad_last_block_full	100%	1 / 1 (100%)	10	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_one	aad_last_block_partial	100%	1 / 1 (100%)	3	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_two	aad_last_block_full	100%	1 / 1 (100%)	11	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_two	aad_last_block_partial	100%	1 / 1 (100%)	9	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_many	aad_last_block_full	100%	1 / 1 (100%)	44	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		dec	aad_blocks_many	aad_last_block_partial	100%	1 / 1 (100%)	18	1	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;



		aes_gcm_len_cg	98.15%	36 / 38 (94.74%)	aes.u_aes_cov_if	covergroup aes_gcm_len_cg with function sample(
		aes_ctrl_gcm_reg_cg	93.75%	15 / 16 (93.75%)	aes.u_aes_cov_if	covergroup aes_ctrl_gcm_reg_cg with function sample(

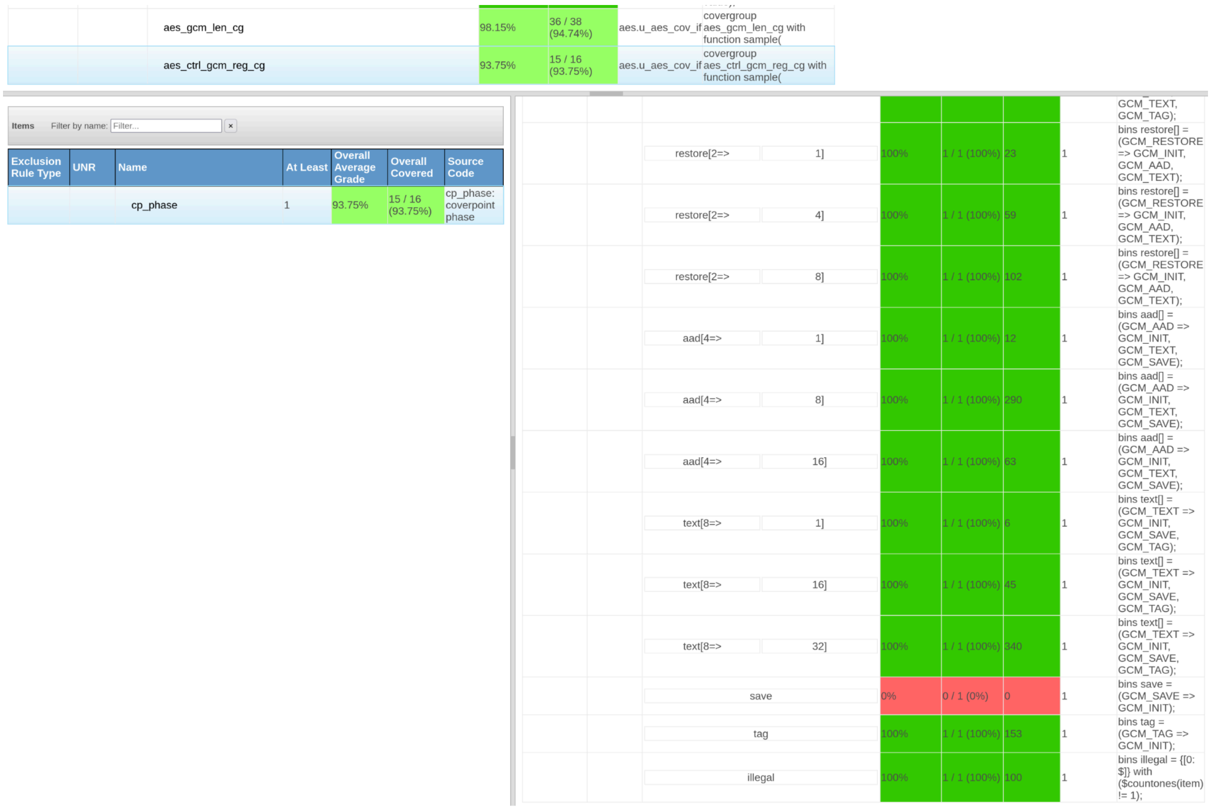
Items Filter by name: Filter... ×

Exclusion Rule Type	UNR	Name	At Least	Overall Average Grade	Overall Covered	Source Code
		cp_operation	1	100%	2 / 2 (100%)	cp_operation: coverpoint aes_op
		cp_aad_blocks	1	100%	3 / 3 (100%)	cp_aad_blocks: coverpoint aad_blocks
		cp_aad_last_block_len	1	100%	2 / 2 (100%)	cp_aad_last_block_len: coverpoint aad_last_block_len
		cp_zero_aad_block	1	100%	1 / 1 (100%)	cp_zero_aad_block: coverpoint aad_block_zero
		cp_text_blocks	1	100%	3 / 3 (100%)	cp_text_blocks: coverpoint text_blocks
		cp_text_last_block_len	1	100%	2 / 2 (100%)	cp_text_last_block_len: coverpoint text_last_block_len
		cp_zero_text_block	1	100%	1 / 1 (100%)	cp_zero_text_block: coverpoint text_block_zero
		cr_op_aad_block_len	1	91.67%	11 / 12 (91.67%)	cr_op_aad_block_len: cross cp_operation, cp_aad_blocks, cp_aad_last_block_len;
		cr_op_text_block_len	1	91.67%	11 / 12 (91.67%)	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;

Bins Filter by name: Filter... ×

Exclusion Rule Type	UNR	cp_operation	cp_text_blocks	cp_text_last_block_len	Overall Average Grade	Overall Covered	Score	At Least	Source Code
		enc	text_blocks_one	text_last_block_full	100%	1 / 1 (100%)	10	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		enc	text_blocks_one	text_last_block_partial	100%	1 / 1 (100%)	7	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		enc	text_blocks_two	text_last_block_full	100%	1 / 1 (100%)	30	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		enc	text_blocks_two	text_last_block_partial	100%	1 / 1 (100%)	2	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		enc	text_blocks_many	text_last_block_full	100%	1 / 1 (100%)	103	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		enc	text_blocks_many	text_last_block_partial	100%	1 / 1 (100%)	34	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_one	text_last_block_full	100%	1 / 1 (100%)	18	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_one	text_last_block_partial	100%	1 / 1 (100%)	4	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_two	text_last_block_full	100%	1 / 1 (100%)	35	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_two	text_last_block_partial	0%	0 / 1 (0%)	0	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_many	text_last_block_full	100%	1 / 1 (100%)	92	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;
		dec	text_blocks_many	text_last_block_partial	100%	1 / 1 (100%)	31	1	cr_op_text_block_len: cross cp_operation, cp_text_blocks, cp_text_last_block_len;

Cover group *aes_ctrl_gcm_reg_cg* tests, whether we have seen all valid and invalid GCM_PHASES and all valid phase transactions. The group coverage here is at 93.75%. There is one uncovered valid transition from GCM_SAVE to GCM_INIT. This coverage gap is not systematic and can be fixed by increasing the probability for injecting this transition instead of transitioning to an invalid phase in the aes_gcm_save_restore test. Refer to the following figure for details.



		aes_gcm_len_cg	98.15%	36 / 38 (94.74%)	aes.u_aes_cov_if	covergroup aes_gcm_len_cg with function sample(
		aes_ctrl_gcm_reg_cg	93.75%	15 / 16 (93.75%)	aes.u_aes_cov_if	covergroup aes_ctrl_gcm_reg_cg with function sample(

Exclusion Rule Type	UNR	Name	At Least	Overall Average Grade	Overall Covered	Source Code
		cp_phase	1	93.75%	15 / 16 (93.75%)	cp_phase: coverpoint phase

								GCM_TEXT, GCM_TAG);
		restore[2=> 1]	100%	1 / 1 (100%)	23	1		bins restore[] = (GCM_RESTORE => GCM_INIT, GCM_AAD, GCM_TEXT);
		restore[2=> 4]	100%	1 / 1 (100%)	59	1		bins restore[] = (GCM_RESTORE => GCM_INIT, GCM_AAD, GCM_TEXT);
		restore[2=> 8]	100%	1 / 1 (100%)	102	1		bins restore[] = (GCM_RESTORE => GCM_INIT, GCM_AAD, GCM_TEXT);
		aad[4=> 1]	100%	1 / 1 (100%)	12	1		bins aad[] = (GCM_AAD => GCM_INIT, GCM_TEXT, GCM_SAVE);
		aad[4=> 8]	100%	1 / 1 (100%)	290	1		bins aad[] = (GCM_AAD => GCM_INIT, GCM_TEXT, GCM_SAVE);
		aad[4=> 16]	100%	1 / 1 (100%)	63	1		bins aad[] = (GCM_AAD => GCM_INIT, GCM_TEXT, GCM_SAVE);
		text[8=> 1]	100%	1 / 1 (100%)	6	1		bins text[] = (GCM_TEXT => GCM_INIT, GCM_SAVE, GCM_TAG);
		text[8=> 16]	100%	1 / 1 (100%)	45	1		bins text[] = (GCM_TEXT => GCM_INIT, GCM_SAVE, GCM_TAG);
		text[8=> 32]	100%	1 / 1 (100%)	340	1		bins text[] = (GCM_TEXT => GCM_INIT, GCM_SAVE, GCM_TAG);
		save	0%	0 / 1 (0%)	0	1		bins save = (GCM_SAVE => GCM_INIT);
		tag	100%	1 / 1 (100%)	153	1		bins tag = (GCM_TAG => GCM_INIT);
		illegal	100%	1 / 1 (100%)	100	1		bins illegal = {[0:$]} with ($countones(item) != 1);

FSM

The FSM coverage is 100% but we needed to update the coverage exclusions as the GHASH FSM implementation for the unmasked and the masked implementation partially shares some states.

- *GHASH_ADD_S*: This state is only used when masking is disabled.
- *GHASH_MULT* to *GHASH_OUT/GHASH_IDLE,*
  GHASH_OUT to *GHASH_IDLE,*
  GHASH_IDLE to *GHASH_OUT,*
  GHASH_OUT to *GHASH_IDLE*: These transitions only occur when masking is disabled.

Branch

The branch coverage mainly dropped because of the *aes_ghash* module. Here, branches that only get evaluated when using the non-masked version are not evaluated.

Appendix

Test Report

AES/MASKED Simulation Results

Monday March 24 2025 22:01:38 UTC

GitHub Revision: f722f217a9

Branch: aes-gcm-review

Testplan

Simulator: XCELIUM

Test Results

Stage	Name	Tests	Max Job Runtime	Simulated Time	Passing	Total	Pass Rate
V1	wake_up	aes_wake_up	9.000s	97.130us	1	1	100.00
V1	smoke	aes_smoke	15.000s	591.563us	50	50	100.00
V1	csr_hw_reset	aes_csr_hw_reset	4.000s	71.478us	5	5	100.00
V1	csr_rw	aes_csr_rw	4.000s	51.391us	20	20	100.00
V1	csr_bit_bash	aes_csr_bit_bash	9.000s	511.101us	5	5	100.00

V1	csr_aliasing	aes_csr_aliasing	5.000s	117.747us	5	5	100.00
V1	csr_mem_rw_with_rand_reset	aes_csr_mem_rw_with_rand_reset	4.000s	190.367us	20	20	100.00
V1	regwen_csr_and_corresponding_lockable_csr	aes_csr_rw	4.000s	51.391us	20	20	100.00
		aes_csr_aliasing	5.000s	117.747us	5	5	100.00
V1		**TOTAL**			106	106	100.00
V2	algorithm	aes_smoke	15.000s	591.563us	50	50	100.00
		aes_config_error	41.000s	3.298ms	50	50	100.00
		aes_stress	24.000s	1.519ms	50	50	100.00
V2	key_length	aes_smoke	15.000s	591.563us	50	50	100.00
		aes_config_error	41.000s	3.298ms	50	50	100.00

		aes_stress	24.000s	1.519ms	50	50	100.00
V2	back2back	aes_stress	24.000s	1.519ms	50	50	100.00
		aes_b2b	50.000s	688.350us	50	50	100.00
V2	backpressure	aes_stress	24.000s	1.519ms	50	50	100.00
V2	multi_message	aes_smoke	15.000s	591.563us	50	50	100.00
		aes_config_error	41.000s	3.298ms	50	50	100.00
		aes_stress	24.000s	1.519ms	50	50	100.00
		aes_alert_reset	21.000s	757.606us	50	50	100.00
V2	failure_test	aes_man_cfg_err	9.000s	67.001us	50	50	100.00
		aes_config_error	41.000s	3.298ms	50	50	100.00
		aes_alert_reset	21.000s	757.606us	50	50	100.00

V2	trigger_clear_test	aes_clear	1.950m	3.959ms	50	50	100.00
V2	nist_test_vectors	aes_nist_vectors	34.000s	1.119ms	1	1	100.00
V2	nist_test_vectors_gcm	aes_nist_vectors_gcm	17.000s	994.288us	1	1	100.00
V2	reset_recovery	aes_alert_reset	21.000s	757.606us	50	50	100.00
V2	stress	aes_stress	24.000s	1.519ms	50	50	100.00
V2	sideload	aes_stress	24.000s	1.519ms	50	50	100.00
		aes_sideload	1.083m	1.928ms	50	50	100.00
V2	deinitialization	aes_deinit	12.000s	373.516us	50	50	100.00
V2	stress_all	aes_stress_all	1.683m	1.164ms	10	10	100.00
V2	gcm_save_and_restore	aes_gcm_save_restore	17.000s	2.680ms	100	100	100.00
V2	alert_test	aes_alert_test	5.000s	56.490us	50	50	100.00

V2	tl_d_oob_addr_access	aes_tl_errors	5.000s	71.251us	20	20	100.00
V2	tl_d_illegal_access	aes_tl_errors	5.000s	71.251us	20	20	100.00
V2	tl_d_outstanding_access	aes_csr_hw_reset	4.000s	71.478us	5	5	100.00
		aes_csr_rw	4.000s	51.391us	20	20	100.00
		aes_csr_aliasing	5.000s	117.747us	5	5	100.00
		aes_same_csr_outstanding	5.000s	509.910us	20	20	100.00
V2	tl_d_partial_access	aes_csr_hw_reset	4.000s	71.478us	5	5	100.00
		aes_csr_rw	4.000s	51.391us	20	20	100.00
		aes_csr_aliasing	5.000s	117.747us	5	5	100.00
		aes_same_csr_outstanding	5.000s	509.910us	20	20	100.00

V2		**TOTAL**			602	602	100.00
V2S	reseeding	aes_reseed	13.000s	407.502us	50	50	100.00
V2S	fault_inject	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
V2S	shadow_reg_update_error	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	shadow_reg_read_clear_staged_value	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	shadow_reg_storage_error	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	shadowed_reset_glitch	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	shadow_reg_update_error_with_csr_rw	aes_shadow_reg_errors_with_csr_rw	6.000s	1.629ms	20	20	100.00

V2S	tl_intg_err	aes_sec_cm	17.000s	1.539ms	5	5	100.00
		aes_tl_intg_err	5.000s	183.009us	20	20	100.00
V2S	sec_cm_bus_integrity	aes_tl_intg_err	5.000s	183.009us	20	20	100.00
V2S	sec_cm_lc_escalate_en_intersig_mubi	aes_alert_reset	21.000s	757.606us	50	50	100.00
V2S	sec_cm_main_config_shadow	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	sec_cm_gcm_config_shadow	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	sec_cm_main_config_sparse	aes_smoke	15.000s	591.563us	50	50	100.00
		aes_stress	24.000s	1.519ms	50	50	100.00
		aes_alert_reset	21.000s	757.606us	50	50	100.00
		aes_core_fi	30.000s	10.020ms	69	70	98.57

V2S	sec_cm_gcm_config_sparse	aes_gcm_save_restore	17.000s	2.680ms	100	100	100.00
		aes_config_error	41.000s	3.298ms	50	50	100.00
		aes_stress	24.000s	1.519ms	50	50	100.00
		aes_core_fi	30.000s	10.020ms	69	70	98.57
V2S	sec_cm_aux_config_shadow	aes_shadow_reg_errors	5.000s	133.197us	20	20	100.00
V2S	sec_cm_aux_config_regwen	aes_readability	9.000s	121.797us	50	50	100.00
		aes_stress	24.000s	1.519ms	50	50	100.00
V2S	sec_cm_key_sideload	aes_stress	24.000s	1.519ms	50	50	100.00
		aes_sideload	1.083m	1.928ms	50	50	100.00
V2S	sec_cm_key_sw_unreadable	aes_readability	9.000s	121.797us	50	50	100.00

V2S	sec_cm_data_reg_sw_unreadable	aes_readability	9.000s	121.797us	50	50	100.00
V2S	sec_cm_key_sec_wipe	aes_readability	9.000s	121.797us	50	50	100.00
V2S	sec_cm_iv_config_sec_wipe	aes_readability	9.000s	121.797us	50	50	100.00
V2S	sec_cm_data_reg_sec_wipe	aes_readability	9.000s	121.797us	50	50	100.00
V2S	sec_cm_data_reg_key_sca	aes_stress	24.000s	1.519ms	50	50	100.00
V2S	sec_cm_key_masking	aes_stress	24.000s	1.519ms	50	50	100.00
V2S	sec_cm_main_fsm_sparse	aes_fi	17.000s	1.154ms	48	50	96.00
V2S	sec_cm_main_fsm_redun	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86

		aes_ctr_fi	11.000s	487.898us	50	50	100.00
V2S	sec_cm_cipher_fsm_sparse	aes_fi	17.000s	1.154ms	48	50	96.00
V2S	sec_cm_cipher_fsm_redun	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
V2S	sec_cm_cipher_ctr_redun	aes_cipher_fi	29.000s	10.021ms	332	350	94.86
V2S	sec_cm_ctr_fsm_sparse	aes_fi	17.000s	1.154ms	48	50	96.00
V2S	sec_cm_ctr_fsm_redun	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_ctr_fi	11.000s	487.898us	50	50	100.00

V2S	sec_cm_ghash_fsm_sparse	aes_fi	17.000s	1.154ms	48	50	96.00
V2S	sec_cm_ctrl_sparse	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
		aes_ctr_fi	11.000s	487.898us	50	50	100.00
V2S	sec_cm_main_fsm_global_esc	aes_alert_reset	21.000s	757.606us	50	50	100.00
V2S	sec_cm_main_fsm_local_esc	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
		aes_ctr_fi	11.000s	487.898us	50	50	100.00

V2S	sec_cm_cipher_fsm_local_esc	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
		aes_ctr_fi	11.000s	487.898us	50	50	100.00
V2S	sec_cm_ctr_fsm_local_esc	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_ctr_fi	11.000s	487.898us	50	50	100.00
V2S	sec_cm_ghash_fsm_local_esc	aes_fi	17.000s	1.154ms	48	50	96.00
		aes_ghash_fi	26.000s	1.126ms	90	90	100.00
V2S	sec_cm_data_reg_local_esc	aes_fi	17.000s	1.154ms	48	50	96.00

		aes_control_fi	28.000s	10.118ms	286	300	95.33
		aes_cipher_fi	29.000s	10.021ms	332	350	94.86
V2S		**TOTAL**			1040	1075	96.74
V3	stress_all_with_rand_reset	aes_stress_all_with_rand_reset	1.200m	1.052ms	0	10	0.00
V3		**TOTAL**			0	10	0.00
		TOTAL			1748	1793	97.49

Coverage Results

Coverage Dashboard

Score	Block	Branch	Statement	Expression	Toggle	Fsm	Assertion	CoverGroup
98.15	98.26	95.12	99.43	95.35	97.71	100.00	99.15	94.83

Failure Buckets

- Job timed out after * minutes has 16 failures:
  - Test aes_control_fi has 10 failures.
    - 31.aes_control_fi.39762228083301378763231800254642558975800440947684832059202652052124727593999 0
      Log

        /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/31.aes_control_fi/latest/run.log

        Job timed out after 1 minutes

        - 93.aes_control_fi.36200435676179212390397060478829084311207517324260029912163105480276334804687
          Log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/93.aes_control_fi/latest/run.log

          Job timed out after 1 minutes

        - ... and 8 more failures.
    - Test aes_cipher_fi has 6 failures.
        - 128.aes_cipher_fi.24066533726422333578056135198557611620313233650932456999139645770160768375458
          Log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/128.aes_cipher_fi/latest/run.log

          Job timed out after 1 minutes

        - 162.aes_cipher_fi.114648616240477798536067560990876722899773401776673669758368675749613276046609
          Log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/162.aes_cipher_fi/latest/run.log

          Job timed out after 1 minutes

        - ... and 4 more failures.
- UVM_FATAL (aes_cipher_fi_vseq.sv:62) [aes_cipher_fi_vseq] wait timeout occurred! has 12 failures:
    - Test aes_cipher_fi has 12 failures.
        - 12.aes_cipher_fi.75587699867365223712514059445286231267229140064266055455267651752210605723475
          Line 141, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/12.aes_cipher_fi/latest/run.log

          UVM_FATAL @ 10046455036 ps: (aes_cipher_fi_vseq.sv:62)
          [uvm_test_top.env.virtual_sequencer.aes_cipher_fi_vseq] wait timeout occurred!
          UVM_INFO @ 10046455036 ps: (uvm_report_catcher.svh:705)
          [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —

        - 32.aes_cipher_fi.58794345190959110408447932763189643045065574847013004918347345351164932045452
          Line 143, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/32.aes_cip

        her_fi/latest/run.log

        ```
        UVM_FATAL @ 10031949415 ps: (aes_cipher_fi_vseq.sv:62) [uvm_test_top.env.virtual_sequencer.aes_cipher_fi_vseq] wait timeout occurred!
        UVM_INFO @ 10031949415 ps: (uvm_report_catcher.svh:705) [UVM/REPORT/CATCHER]
        --- UVM Report catcher Summary —
        ```

    - ... and 10 more failures.

- UVM_FATAL (aes_control_fi_vseq.sv:62) [aes_control_fi_vseq] wait timeout occurred! has 4 failures:
    - Test aes_control_fi has 4 failures.
        - 5.aes_control_fi.80836928355734599632684880594392109904004823243012311188111517857389762812717
          Line 141, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/5.aes_control_fi/latest/run.log

          ```
          UVM_FATAL @ 10050169973 ps: (aes_control_fi_vseq.sv:62) [uvm_test_top.env.virtual_sequencer.aes_control_fi_vseq] wait timeout occurred!
          UVM_INFO @ 10050169973 ps: (uvm_report_catcher.svh:705) [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary
          ```

        - 156.aes_control_fi.14974503802615213956953483699307443944316189390200052092449445913338539277721
          Line 156, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/156.aes_control_fi/latest/run.log

          ```
          UVM_FATAL @ 10025865160 ps: (aes_control_fi_vseq.sv:62) [uvm_test_top.env.virtual_sequencer.aes_control_fi_vseq] wait timeout occurred!
          UVM_INFO @ 10025865160 ps: (uvm_report_catcher.svh:705) [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —
          ```

        - ... and 2 more failures.
- UVM_ERROR (cip_base_vseq.sv:868) [aes_common_vseq] Check failed (!has_outstanding_access()) Waited * cycles to issue a reset with no outstanding accesses. has 3 failures:
    - Test aes_stress_all_with_rand_reset has 3 failures.
        - 0.aes_stress_all_with_rand_reset.112042677547759686157246073952382333590874423705436052328890072930313317305053
          Line 632, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/0.aes_stress_all_with_rand_reset/latest/run.log

          ```
          UVM_ERROR @ 1052037409 ps: (cip_base_vseq.sv:868) [uvm_test_top.env.virtual_sequencer.aes_common_vseq] Check failed (!has_outstanding_access()) Waited 10000 cycles to issue a reset with no
          ```

outstanding accesses.
UVM_INFO @ 1052037409 ps: (uvm_report_catcher.svh:705)
[UVM/REPORT/CATCHER]
--- UVM Report catcher Summary —

    - 1.aes_stress_all_with_rand_reset.60731543104263988301383790934778935147274371733455313903600959940263701979729
      Line 148, in log
      /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/1.aes_stress_all_with_rand_reset/latest/run.log
      UVM_ERROR @ 166173512 ps: (cip_base_vseq.sv:868)
      [uvm_test_top.env.virtual_sequencer.aes_common_vseq] Check failed
      (!has_outstanding_access()) Waited 10000 cycles to issue a reset with no
      outstanding accesses.
      UVM_INFO @ 166173512 ps: (uvm_report_catcher.svh:705)
      [UVM/REPORT/CATCHER]
      --- UVM Report catcher Summary —

    - ... and 1 more failures.
- UVM_ERROR (uvm_sequencer_base.svh:757) sequencer [SEQREQZMB] The task responsible for requesting a wait_for_grant on sequencer 'sequencer' for sequence 'sideload_seq' has been killed, to avoid a deadlock the sequence will be removed from the arbitration queues has 3 failures:
  - Test aes_stress_all_with_rand_reset has 3 failures.
    - 3.aes_stress_all_with_rand_reset.32024022195977319338801093918507501165026108405700267537869998111241584332688
      Line 1275, in log
      /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/3.aes_stress_all_with_rand_reset/latest/run.log
      UVM_ERROR @ 1575352140 ps: (uvm_sequencer_base.svh:757)
      uvm_test_top.env.keymgr_sideload_agent.sequencer [SEQREQZMB] The
      task responsible for requesting a wait_for_grant on sequencer
      'uvm_test_top.env.keymgr_sideload_agent.sequencer' for sequence
      'uvm_test_top.env.virtual_sequencer.aes_reseed_vseq.sideload_seq' has
      been killed, to avoid a deadlock the sequence will be removed from the
      arbitration queues
      UVM_INFO @ 1575352140 ps: (uvm_report_catcher.svh:705)
      [UVM/REPORT/CATCHER]
      --- UVM Report catcher Summary —

    - 6.aes_stress_all_with_rand_reset.16668571065127604894682112823795957351385760358700317468316330337089624520924
      Line 318, in log
      /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/6.aes_stress_all_with_rand_reset/latest/run.log
      UVM_ERROR @ 111228300 ps: (uvm_sequencer_base.svh:757)
      uvm_test_top.env.keymgr_sideload_agent.sequencer [SEQREQZMB] The
      task responsible for requesting a wait_for_grant on sequencer
      'uvm_test_top.env.keymgr_sideload_agent.sequencer' for sequence
      'uvm_test_top.env.virtual_sequencer.aes_stress_vseq.sideload_seq' has
      been killed, to avoid a deadlock the sequence will be removed from the
      arbitration queues

```
        UVM_INFO @ 111228300 ps: (uvm_report_catcher.svh:705)
        [UVM/REPORT/CATCHER]
        --- UVM Report catcher Summary —
        ```

        - ... and 1 more failures.
- UVM_FATAL (aes_base_vseq.sv:75) [aes_alert_reset_vseq] Check failed (aes_ctrl_aux[*] == cfg.do_reseed) has 2 failures:
    - Test aes_stress_all_with_rand_reset has 2 failures.
        - 4.aes_stress_all_with_rand_reset.94290855146182943071141257150312169263168513744479042444511894736208554671890
          Line 221, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/4.aes_stress_all_with_rand_reset/latest/run.log
          ```
          UVM_FATAL @86346459 ps: (aes_base_vseq.sv:75)
          [uvm_test_top.env.virtual_sequencer.aes_alert_reset_vseq] Check failed
          (aes_ctrl_aux[0] == cfg.do_reseed)
          UVM_INFO @86346459 ps: (uvm_report_catcher.svh:705)
          [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —
          ```
        - 9.aes_stress_all_with_rand_reset.13147046635261742911820189324408327819772727400659300616246710119518899577573
          Line 364, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/9.aes_stress_all_with_rand_reset/latest/run.log
          ```
          UVM_FATAL @ 934971286 ps: (aes_base_vseq.sv:75)
          [uvm_test_top.env.virtual_sequencer.aes_alert_reset_vseq] Check failed
          (aes_ctrl_aux[0] == cfg.do_reseed)
          UVM_INFO @ 934971286 ps: (uvm_report_catcher.svh:705)
          [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —
          ```
- UVM_FATAL (aes_base_vseq.sv:75) [aes_stress_vseq] Check failed (aes_ctrl_aux[*] == cfg.do_reseed) has 1 failures:
    - Test aes_stress_all_with_rand_reset has 1 failures.
        - 2.aes_stress_all_with_rand_reset.83585366063829575839054222098397024365654275013104902186207328090945741777978
          Line 159, in log
          /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/2.aes_stress_all_with_rand_reset/latest/run.log
          ```
          UVM_FATAL @42056533 ps: (aes_base_vseq.sv:75)
          [uvm_test_top.env.virtual_sequencer.aes_stress_vseq] Check failed
          (aes_ctrl_aux[0] == cfg.do_reseed)
          UVM_INFO @42056533 ps: (uvm_report_catcher.svh:705)
          [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —
          ```
- UVM_FATAL (aes_core_fi_vseq.sv:70) [aes_core_fi_vseq] wait timeout occurred! has 1 failures:
    - Test aes_core_fi has 1 failures.
        - 7.aes_core_fi.99999228629565061850959879040952319720024317284416738633904791756165348311544

        Line 151, in log /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/7.aes_core_fi/latest/run.log
        UVM_FATAL @ 10019539895 ps: (aes_core_fi_vseq.sv:70) [uvm_test_top.env.virtual_sequencer.aes_core_fi_vseq] wait timeout occurred!
        UVM_INFO @ 10019539895 ps: (uvm_report_catcher.svh:705) [UVM/REPORT/CATCHER]
        --- UVM Report catcher Summary —

- UVM_FATAL (aes_base_vseq.sv:306) virtual_sequencer [aes_reseed_vseq] Expected GCM phase GCM_AAD, got GCM_TEXT has 1 failures:
    - Test aes_stress_all_with_rand_reset has 1 failures.
        - 8.aes_stress_all_with_rand_reset.62594070565899760813223446268194914654020338226920008604277069345647102193136
          Line 1400, in log /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/8.aes_stress_all_with_rand_reset/latest/run.log
          UVM_FATAL @ 3095618100 ps: (aes_base_vseq.sv:306) uvm_test_top.env.virtual_sequencer [uvm_test_top.env.virtual_sequencer.aes_reseed_vseq] Expected GCM phase GCM_AAD, got GCM_TEXT
          UVM_INFO @ 3095618100 ps: (uvm_report_catcher.svh:705) [UVM/REPORT/CATCHER]
          --- UVM Report catcher Summary —

- xmsim: *E,ASRTST (/home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/default/src/lowrisc_ip_aes_*/rtl/aes_core.sv,1136): Assertion AesSecCmDataRegLocalEscDataOut has failed (* cycles, starting * PS) has 1 failures:
    - Test aes_fi has 1 failures.
        - 17.aes_fi.106077025152805191433527326664910440832716825705803306564146147709417365689521
          Line 3101, in log /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/17.aes_fi/latest/run.log
          xmsim: *E,ASRTST (/home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/default/src/lowrisc_ip_aes_1.0/rtl/aes_core.sv,1136): (time 17291759 PS) Assertion tb.dut.u_aes_core.AesSecCmDataRegLocalEscDataOut has failed (2 cycles, starting 17270926 PS)
          ($past(iv_q) != $past(state_done_transposed, 2) ^ $past(data_in_prev_q, 2)))
          xmsim: *E,ASRTST (/home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/default/src/lowrisc_ip_aes_1.0/rtl/aes_core.sv,1142): (time 17291759 PS) Assertion tb.dut.u_aes_core.AesSecCmDataRegLocalEscIv has failed (2 cycles, starting 17270926 PS)
          UVM_ERROR @17291759 ps: (aes_core.sv:1136) [ASSERT FAILED] AesSecCmDataRegLocalEscDataOut

- UVM_FATAL (aes_fi_vseq.sv:86) virtual_sequencer [aes_fi_vseq] Was Able to finish without clearing reset has 1 failures:

- Test aes_fi has 1 failures.
    - 27.aes_fi.74159570828820637805593377318611138256706268591106308906422127955529801080042
      Line 25578, in log /home/dev/src/scratch/aes-gcm-review/aes_masked-sim-xcelium/27.aes_fi/latest/run.log

      ```
      UVM_FATAL @57149448 ps: (aes_fi_vseq.sv:86)
      uvm_test_top.env.virtual_sequencer
      [uvm_test_top.env.virtual_sequencer.aes_fi_vseq] Was Able to finish without clearing reset
      UVM_INFO @57149448 ps: (uvm_report_catcher.svh:705)
      [UVM/REPORT/CATCHER]
      --- UVM Report catcher Summary ---
      ```