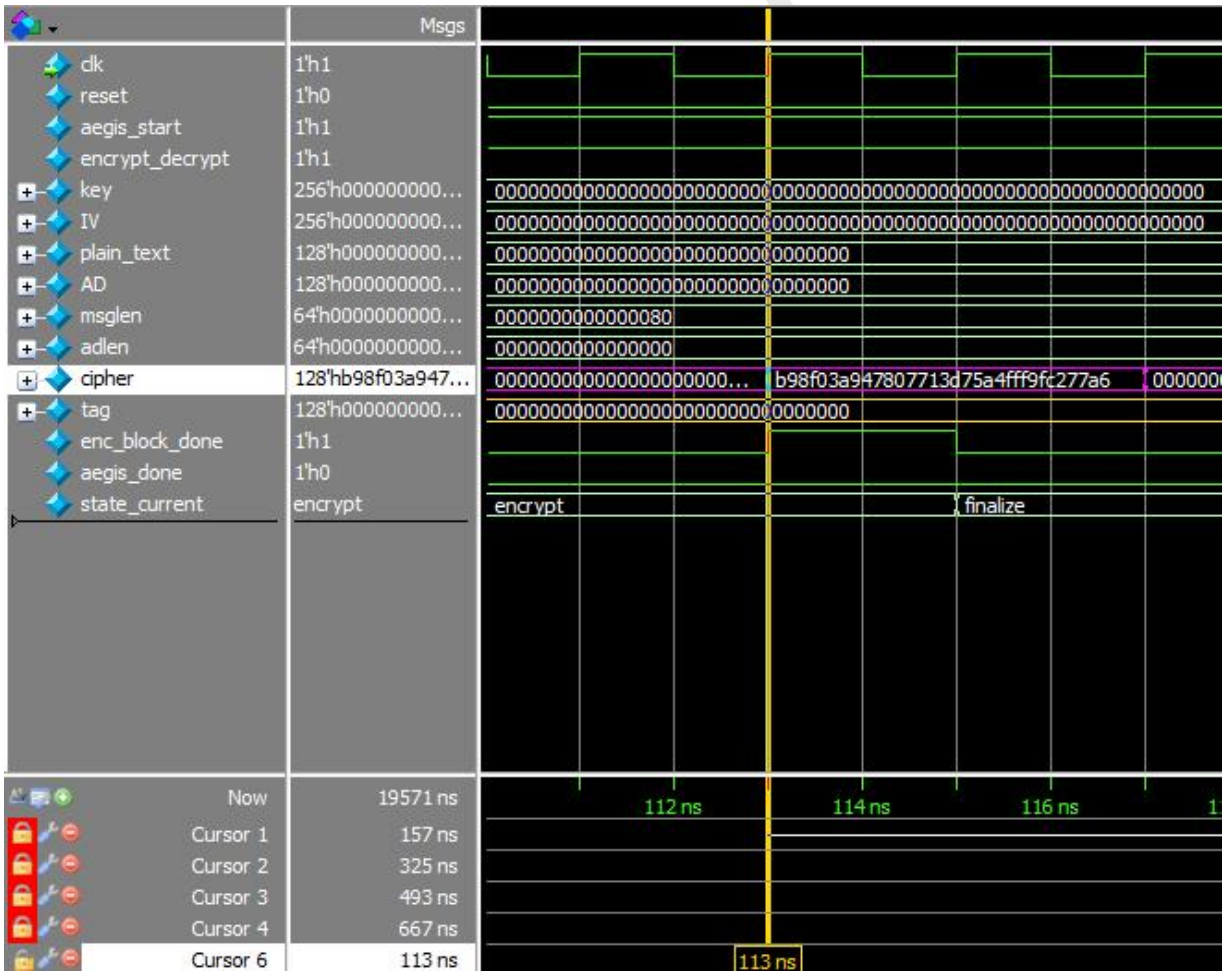
1. AEGIS Paper Reference Cases Validation

To better understand AEGIS Encryption algorithm, refer to AEGIS explanation.

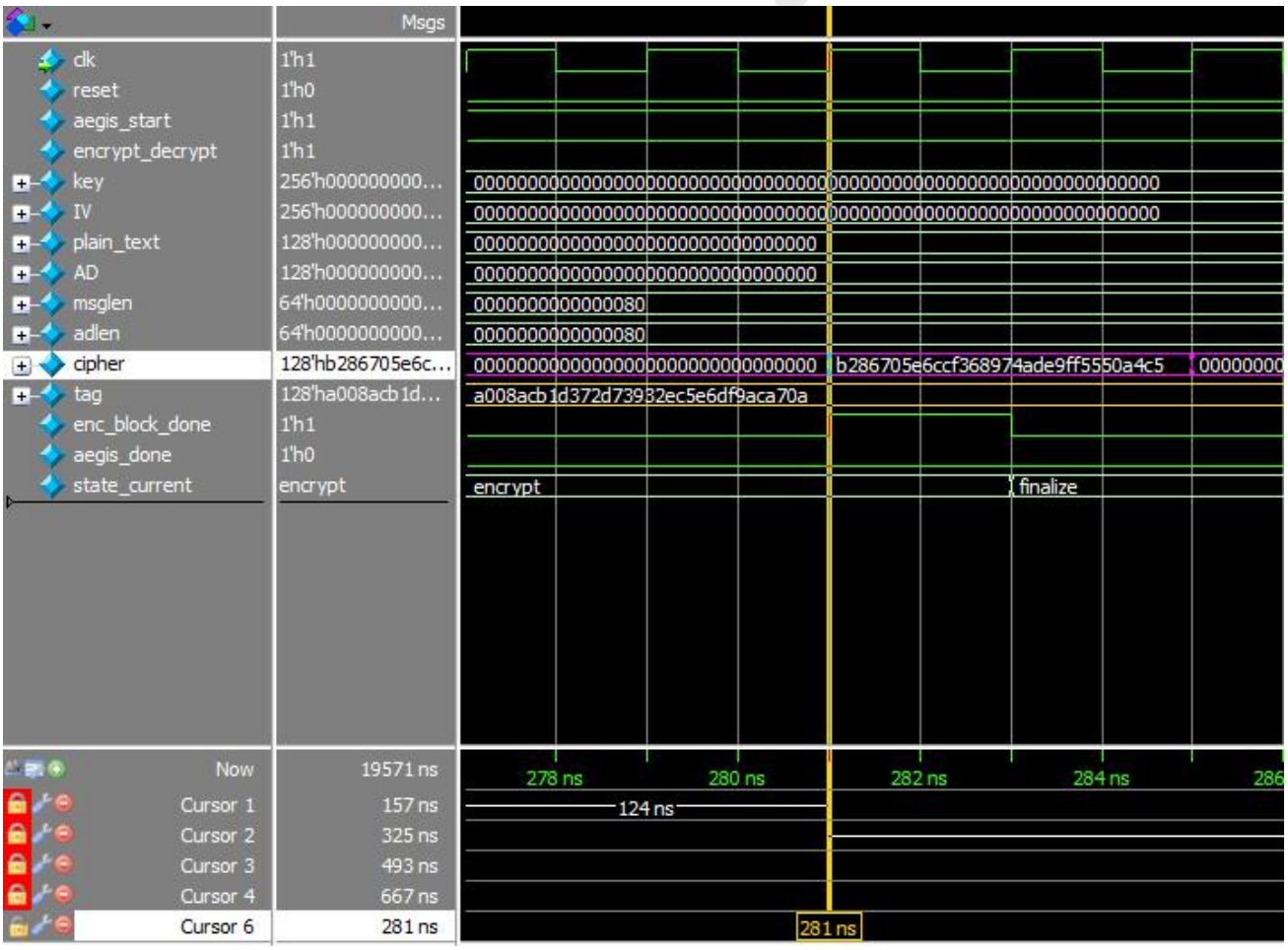
Case 1:

Inputs	Size (bits)	Paper values
msglen	64	128
plain_text	128	0
adlen	64	0
AD	128	0
key	256	0
IV	256	0
Outputs	**Size (bits)**	**Paper values**
cipher	128	b98f03a947807713d75a4fff9fc277a6
tag	128	a008acb1d372d73932ec5e6df9aca70a



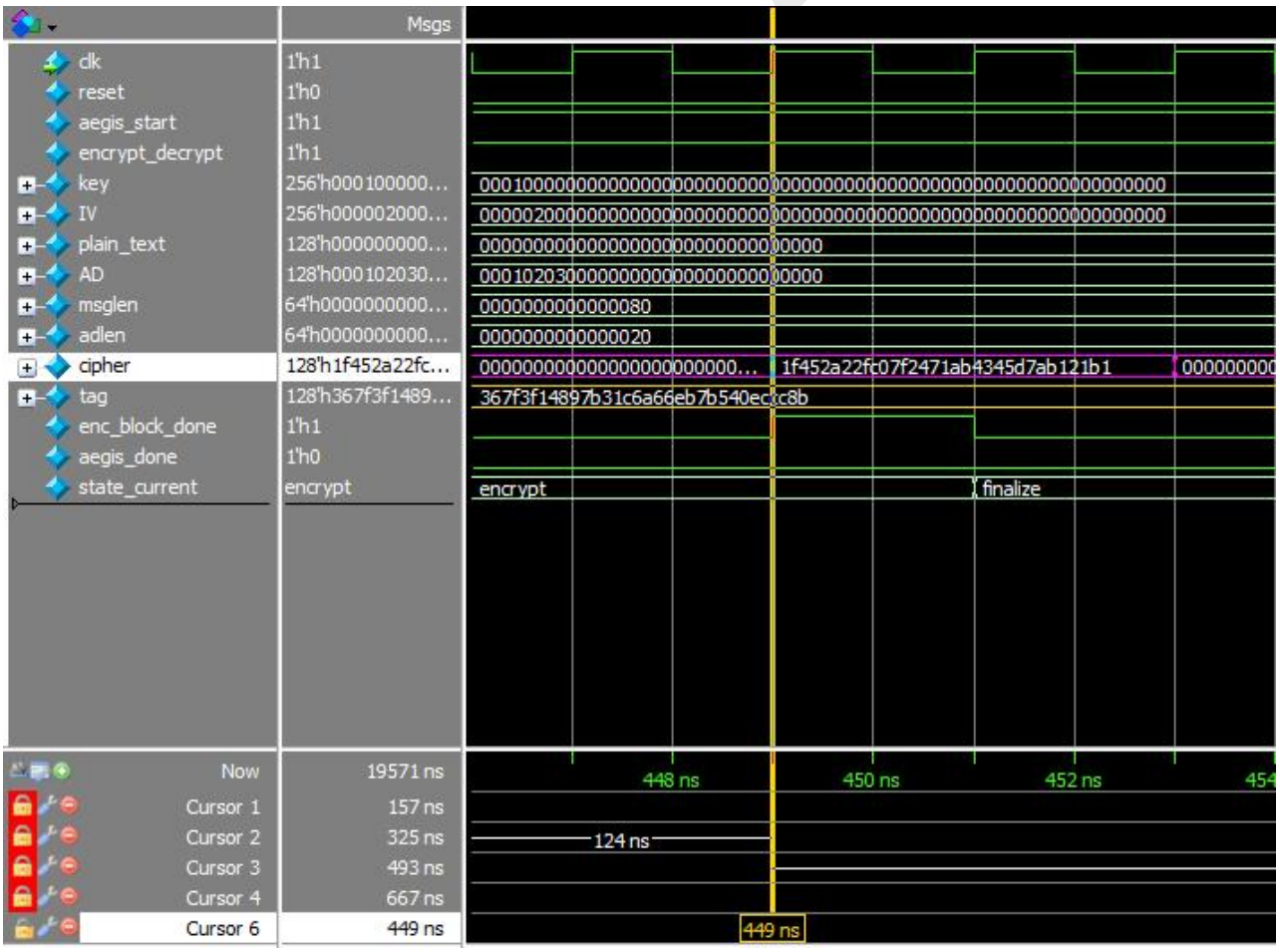
Case 2:

Inputs	Size (bits)	Paper values
msglen	64	128
plain_text	128	0
adlen	64	128
AD	128	0
key	256	0
IV	256	0
Outputs	**Size (bits)**	**Paper values**
cipher	128	b286705e6ccf368974ade9ff5550a4c5
tag	128	367f3f14897b31c6a66eb7b540eccc8b



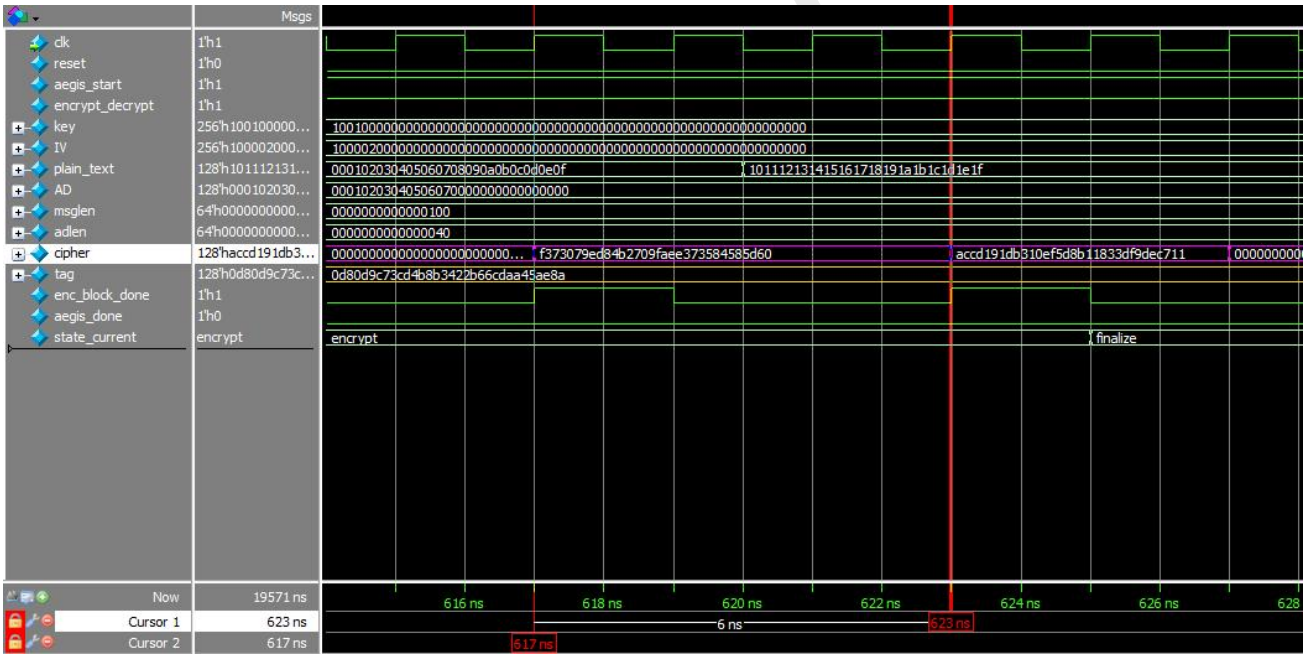
Case 3:

Inputs	Size (bits)	Paper values
msglen	64	128
plain_text	128	0
adlen	64	32
AD	128	0x00010203_0000000000000000…
key	256	0x0001_0000000000000000000…
IV	256	0x000002_000000000000000000…
Outputs	Size (bits)	Paper values
cipher	128	1f452a22fc07f2471ab4345d7ab121b1
tag	128	0d80d9c73cd4b8b3422b66cdaa45ae8a

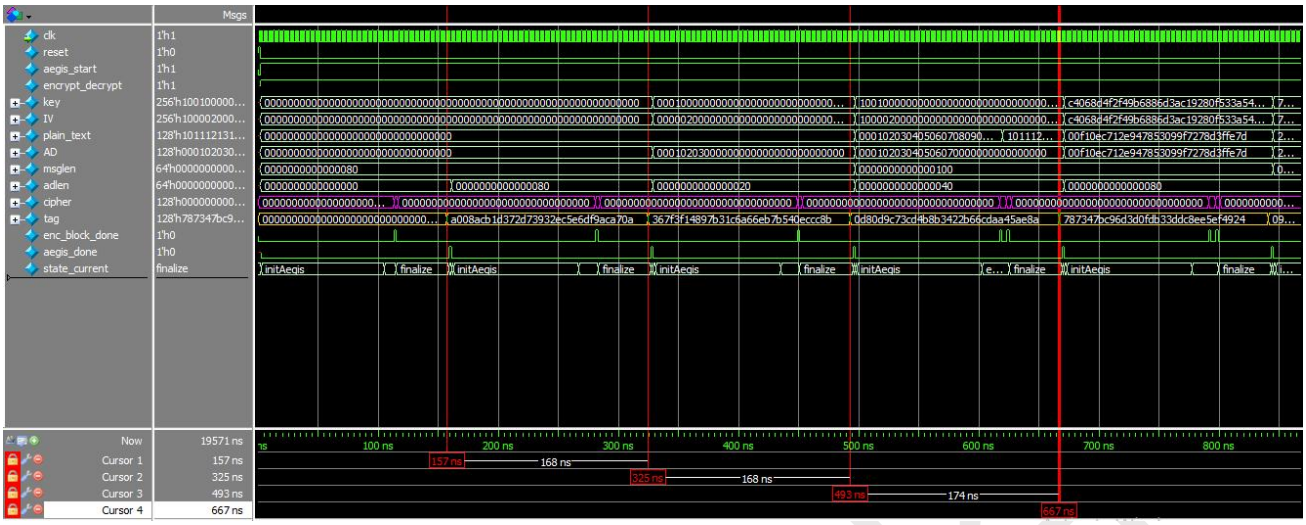


Case 4:

Inputs	Size (bits)	Paper values
msglen	64	256
plain_text	128x2	0x000102030405060708090a0b0c0d0e0f 0x101112131415161718191a1b1c1d1e1f
adlen	64	64
AD	128	0x0001020304050607_000000000…
key	256	0x10002_000000000000000000…
IV	256	0x000002_000000000000000000…
Outputs	**Size (bits)**	**Paper values**
cipher	128x2	0xf373079ed84b2709faee373584585d60 0xaccd191db310ef5d8b11833df9dec711
tag	128	0x787347bc96d3d0fdb33ddc8ee5ef4924



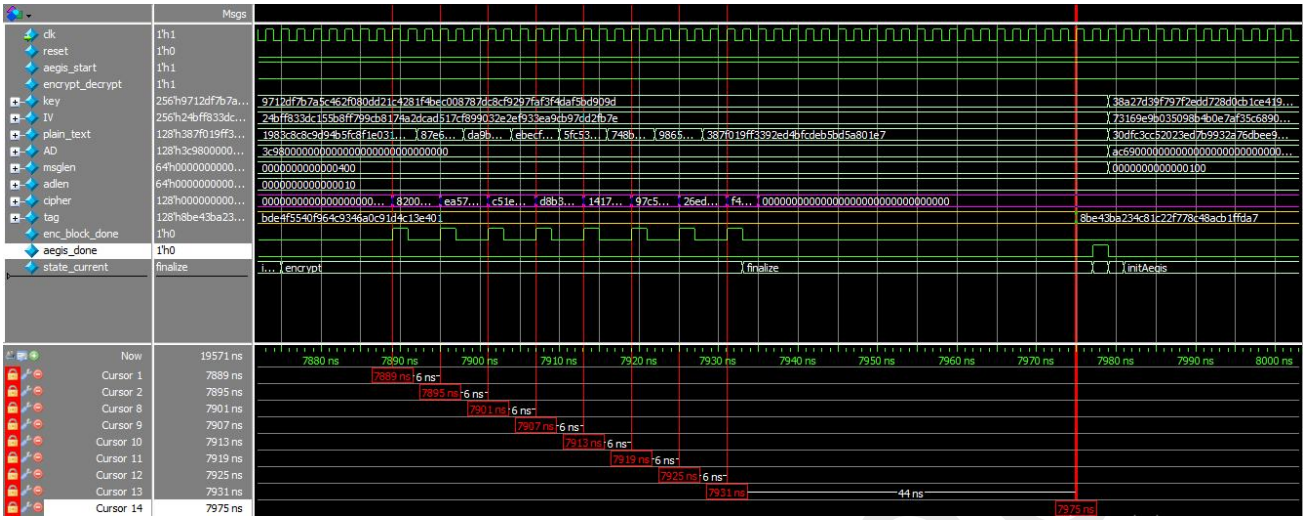
The tag in the four cases:




```
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/test.sv(44) @ 0: uvm_test_top [run_phase] Reset Asserted
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/test.sv(46) @ 2: uvm_test_top [run_phase] Reset De-asserted
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/test.sv(50) @ 2: uvm_test_top [run_phase] main sequence Starts
# CipheredText: b98f03a947807713d75a4fff9fc277a6
#
#
#
# Tag: a008acb1d372d73932ec5e6df9aca70a
#
#
#
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(87) @ 160: uvm_test_top.env.sb [run_phase] Encryption of 1 msg blocks Succeeded!
#
# CipheredText: b286705e6ccf368974ade9ff5550a4c5
#
#
#
# Tag: 367f3f14897b31c6a66eb7b540eccc8b
#
#
#
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(87) @ 328: uvm_test_top.env.sb [run_phase] Encryption of 1 msg blocks Succeeded!
# CipheredText: 1f452a22fc07f2471ab4345d7ab121b1
#
#
#
# Tag: 0d80d9c73cd4b8b3422b66cdaa45ae8a
#
#
#
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(87) @ 496: uvm_test_top.env.sb [run_phase] Encryption of 1 msg blocks Succeeded!
#
# CipheredText: f373079ed84b2709faee373584585d60
#
#               accd191db310ef5d8b11833df9dec711
#
#
#
# Tag: 787347bc96d3d0fdb33ddc8ee5ef4924
#
#
#
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(87) @ 670: uvm_test_top.env.sb [run_phase] Encryption of 2 msg blocks Succeeded!
```

Random Case:

Encryption of (8x128-bit/8 blocks) of plain text




```
# CipheredText: 8200a64df21132f17efb603b48487434
#
#               ea57173e1bec662762154d418fa98818
#
#               c51e455d89396eb936e59a7cd8dd06bc
#
#               d8b3c90ab2dd98e852eac6a46f39d400
#
#               14176ce68f9a1bf7de1bf754ad4ae376
#
#               97c54e9fc99b7a84937bb24b637e4e94
#
#               26edcc7c435f7abd1907372da41b3f0d
#
#               f49242b35e541ae9e9d9f6ad4c4b79a4
#
#
#
# Tag: 8be43ba234c81c22f778c48acb1ffda7
#
#
#
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(87) @ 7978: uvm_test_top.env.sb [run_phase] Encryption of 8 msg blocks Succeeded!
```

QuestaSim transcript:

After the Encryption on the 4 cases of the paper + 100 other random cases, the questasim transcript which shows the error/correct counts after comparing RTL outputs with golden outputs generated by the C++ AEGIS function:

```
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/test.sv(52) @ 19571: uvm_test_top [run_phase] main sequence Ends
# UVM_INFO verilog_src/uvm-1.1d/src/base/uvm_objection.svh(1267) @ 19571: reporter [TEST_DONE] 'run' phase is ready to proceed to the 'extract' phase
# UVM_INFO U:/AYMAN/DIGITAL/1.Verification/Final Course Projects/AEGIS_UVM/scoreboard.sv(97) @ 19571: uvm_test_top.env.sb [report_phase] At time 19571: Simulation Ends and Error Count= 0,
# Correct Count= 104
#
# --- UVM Report Summary ---
#
# ** Report counts by severity
# UVM_INFO :  113
# UVM_WARNING :    0
# UVM_ERROR :    0
# UVM_FATAL :    0
# ** Report counts by id
# [Questa UVM]     2
# [RNTST]     1
# [TEST_DONE]     1
# [report_phase]     1
# [run_phase]   108
# ** Note: $finish    : C:/questasim64_2021.1/win64/../verilog_src/uvm-1.1d/src/base/uvm_root.svh(430)
#    Time: 19571 ns  Iteration: 63  Instance: /top
```

2. Functional Coverage Report

NOTE: The UVM environment tests only the **Encryption** process of the AEGIS RTL design.

Covergroup instance \/AEGIS_coverage_pkg::AEGIS_coverage::cvr_grp				
	100.00%	100	-	Covered
covered/total bins:	25	25	-	
missing/total bins:	0	25	-	
% Hit:	100.00%	100	-	
Coverpoint plain_text_patterns_cp	100.00%	100	-	Covered
covered/total bins:	3	3	-	
missing/total bins:	0	3	-	
% Hit:	100.00%	100	-	
bin all_ones	7	1	-	Covered
bin all_zeros	16	1	-	Covered
bin alternating_bits	35	1	-	Covered
default bin random	397		-	Occurred
Coverpoint AD_patterns_cp	100.00%	100	-	Covered
covered/total bins:	3	3	-	
missing/total bins:	0	3	-	
% Hit:	100.00%	100	-	
bin all_ones	1	1	-	Covered
bin all_zeros	4	1	-	Covered
bin alternating_bits	2	1	-	Covered
default bin random	97		-	Occurred
Coverpoint key_patterns_cp	100.00%	100	-	Covered
covered/total bins:	3	3	-	
missing/total bins:	0	3	-	
% Hit:	100.00%	100	-	
bin all_ones	2	1	-	Covered
bin all_zeros	5	1	-	Covered
bin alternating_bits	3	1	-	Covered
default bin random	94		-	Occurred

Coverpoint IV_patterns_cp	100.00%	100	-	Covered
covered/total bins:	3	3	-	
missing/total bins:	0	3	-	
% Hit:	100.00%	100	-	
bin all_ones	1	1	-	Covered
bin all_zeros	5	1	-	Covered
bin alternating_bits	5	1	-	Covered
default bin random	93		-	Occurred
Coverpoint msglen_patterns_cp	100.00%	100	-	Covered
covered/total bins:	8	8	-	
missing/total bins:	0	8	-	
% Hit:	100.00%	100	-	
bin one_block	11	1	-	Covered
bin two_blocks	14	1	-	Covered
bin three_blocks	19	1	-	Covered
bin four_blocks	12	1	-	Covered
bin five_blocks	12	1	-	Covered
bin six_blocks	10	1	-	Covered
bin seven_blocks	17	1	-	Covered
bin eight_blocks	9	1	-	Covered
Coverpoint adlen_patterns_cp	100.00%	100	-	Covered
covered/total bins:	5	5	-	
missing/total bins:	0	5	-	
% Hit:	100.00%	100	-	
bin block8	15	1	-	Covered
bin block16	10	1	-	Covered
bin block32	10	1	-	Covered
bin block64	19	1	-	Covered
bin block128	49	1	-	Covered