CAIRO SECURITY CLAN

HYPERLANE UPDATE

SECURITY ASSESMENT REPORT

JUNE 2025

Prepared for

HYPERLANE XYZ

Contents

1 About Cairo Security Clan

Cairo Security Clan is a leading force in the realm of blockchain security, dedicated to fortifying the foundations of the digital age. As pioneers in the field, we specialize in conducting meticulous smart contract security audits, ensuring the integrity and reliability of decentralized applications built on blockchain technology.

At Cairo Security Clan, we boast a multidisciplinary team of seasoned professionals proficient in blockchain security, cryptography, and software engineering. With a firm commitment to excellence, our experts delve into every aspect of the Web3 ecosystem, from foundational layer protocols to application-layer development. Our comprehensive suite of services encompasses smart contract audits, formal verification, and real-time monitoring, offering unparalleled protection against potential vulnerabilities.

Our team comprises industry veterans and scholars with extensive academic backgrounds and practical experience. Armed with advanced methodologies and cutting-edge tools, we scrutinize and analyze complex smart contracts with precision and rigor. Our track record speaks volumes, with a plethora of published research papers and citations, demonstrating our unwavering dedication to advancing the field of blockchain security.

At Cairo Security Clan, we prioritize collaboration and transparency, fostering meaningful partnerships with our clients. We believe in a customer-oriented approach, engaging stakeholders at every stage of the auditing process. By maintaining open lines of communication and soliciting client feedback, we ensure that our solutions are tailored to meet the unique needs and objectives of each project.

Beyond our core services, Cairo Security Clan is committed to driving innovation and shaping the future of blockchain technology. As active contributors to the ecosystem, we participate in the development of emerging technologies such as Starknet, leveraging our expertise to build robust infrastructure and tools. Through strategic guidance and support, we empower our partners to navigate the complexities of the blockchain landscape with confidence and clarity.

In summary, Cairo Security Clan stands at the forefront of blockchain security, blending technical prowess with a client-centric ethos to deliver unparalleled protection and peace of mind in an ever-evolving digital landscape. Join us in safeguarding the future of decentralized finance and digital assets with confidence and conviction.

2 Disclaimer

Disclaimer Limitations of this Audit:

This report is based solely on the materials and documentation provided by you to Cairo Security Clan for the specific purpose of conducting the security review outlined in the Summary of Audit and Scoped Files. The findings presented here may not be exhaustive and may not identify all potential vulnerabilities. Cairo Security Clan provides this review and report on an "as-is" and "as-available" basis. You acknowledge that your use of this report, including any associated services, products, protocols, platforms, content, and materials, occurs entirely at your own risk.

Inherent Risks of Blockchain Technology:

Blockchain technology remains in its developmental stage and is inherently susceptible to unknown risks and vulnerabilities. This review is specifically focused on the smart contract code and does not extend to the compiler layer, programming language elements beyond the reviewed code, or other potential security risks outside the code itself.

Report Purpose and Reliance:

This report should not be construed as an endorsement of any specific project or team, nor does it guarantee the absolute security of the audited smart contracts. No third party should rely on this report for any purpose, including making investment or purchasing decisions.

Liability Disclaimer:

To the fullest extent permitted by law, Cairo Security Clan disclaims all liability associated with this report, its contents, and any related services and products arising from your use. This includes, but is not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Third-Party Products and Services:

Cairo Security Clan does not warrant, endorse, guarantee, or assume responsibility for any products or services advertised by third parties within this report, nor for any open-source or third-party software, code, libraries, materials, or information linked to, referenced by, or accessible through this report, its content, and related services and products. This includes any hyperlinked websites, websites or applications appearing on advertisements, and Cairo Security Clan will not be responsible for monitoring any transactions between you and third-party providers. It is recommended that you exercise due diligence and caution when considering any third-party products or services, just as you would with any purchase or service through any medium.

Disclaimer of Advice:

FOR THE AVOIDANCE OF DOUBT, THIS REPORT, ITS CONTENT, ACCESS, AND/OR USE, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHOULD NOT BE CONSIDERED OR RELIED UPON AS FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER PROFESSIONAL ADVICE.

3   Executive Summary

This document presents the security review performed by Cairo Security Clan on the Starknet implementation of Hyperlane protocol.

Hyperlane is the first permissionless interoperability layer that enables smart contract developers to send arbitrary data between blockchains. By leveraging Hyperlane, developers can move tokens, execute function calls, and build interchain applications that are accessible to users across any blockchain. Users interact with the protocol through on-chain mailbox smart contracts, which handle the sending and receiving of interchain messages. With its modular security model, Hyperlane allows applications to choose and configure their own Interchain Security Modules (ISMs), giving them full control over how their cross-chain communications are secured. Learn more from docs.

The audit was performed using

- manual analysis of the codebase,

- automated analysis tools,

- simulation of the smart contract,

- analysis of edge test cases

2 points of attention, where 0 is classified as Critical, 0 is classified as High, 0 is classified as Medium, 0 is classified as Low, 0 is classified as Informational, 1 is classified as Best Practices and 1 is classified as Undetermined. The issues are summarized in Fig. 1.

This document is organized as follows.   Section 1 About Cairo Security Clan. Section 2 Disclaimer. Section 3 Executive Summary. Section 4 Summary of Audit. Section 5 Risk Classification. Section 6 Issues by Severity Levels. Section 7 Test Evaluation.

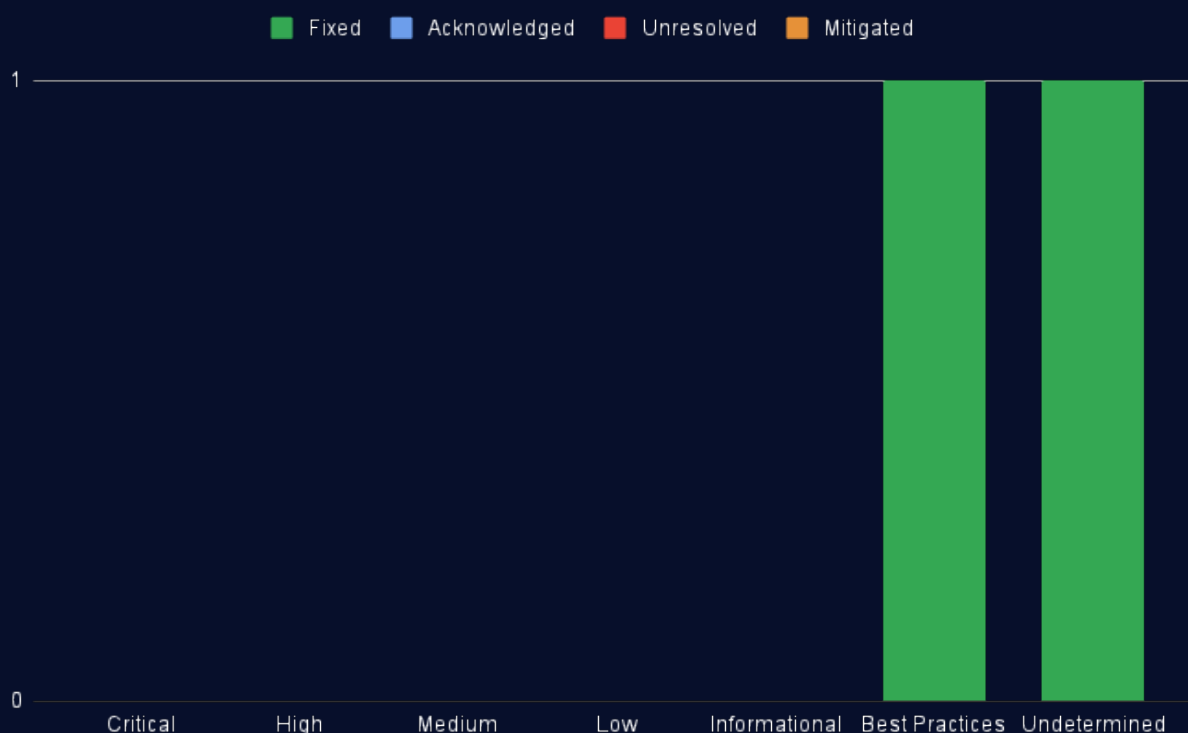**Fig 1: Distribution of issues: Critical** (0), **High** (0), **Medium** (0), **Low** (0), **Informational** (0), **Best Practices** (1), **Undetermined** (1). **Distribution of status: Fixed** (2), **Acknowledged** (0), **Mitigated** (0), **Unresolved** (0).

4 Summary of Audit

Audit Type	Security Review of Difference Between Commits
Cairo Version (cairo Folder)	2.6.3
Final Report	09/06/2025
Repository	astraly-labs/hyperlane_starknet
Initial Commit Hash	717d5feae7bd4c633e93b81f50b8848c92581a57
Difference Between Hashes	717d5fe...bf65048
Documentation	Website documentation
Test Suite Assessment	High

4.1 Scoped Files

	Contracts
1	cairo/crates/contracts/src/client/router_component.cairo
2	cairo/crates/contracts/src/lib.cairo
3	cairo/crates/token/src/extensions/hyp_erc20_vault.cairo

4.2 Issues

	Findings	Severity	Update
1	Inconsistent mutability in owner component reference	Best Practices	Fixed
2	Inconsistent asset-to-share conversion in transfer functions	Undetermined	Fixed

5   Risk Classification

The risk rating methodology used by Cairo Security Clan follows the principles established by the CVSS risk rating methodology. The severity of each finding is determined by two factors: **Likelihood** and **Impact**.

Likelihood measures how likely an attacker will uncover and exploit the finding. This factor will be one of the following values:

a) **High**: The issue is trivial to exploit and has no specific conditions that need to be met;

b) **Medium**: The issue is moderately complex and may have some conditions that need to be met;

c) **Low**: The issue is very complex and requires very specific conditions to be met.

When defining the likelihood of a finding, other factors are also considered. These can include but are not limited to Motive, opportunity, exploit accessibility, ease of discovery, and ease of exploit.

Impact is a measure of the damage that may be caused if an attacker exploits the finding. This factor will be one of the following values:

a) **High**: The issue can cause significant damage such as loss of funds or the protocol entering an unrecoverable state;

b) **Medium**: The issue can cause moderate damage such as impacts that only affect a small group of users or only a particular part of the protocol;

c) **Low**: The issue can cause little to no damage such as bugs that are easily recoverable or cause unexpected interactions that cause minor inconveniences.

When defining the impact of a finding other factors are also considered. These can include but are not limited to Data/state integrity, loss of availability, financial loss, and reputation damage. After defining the likelihood and impact of an issue, the severity can be determined according to the table below.

		Likelihood		
		High	**Medium**	**Low**
Impact	**High**	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Info/Best Practices

To address issues that do not fit a High/Medium/Low severity, Cairo Security Clan also uses three more finding severities: **Informational**, **Best Practices** and **Gas**

a) **Informational** findings do not pose any risk to the application, but they carry some information that the audit team intends to formally pass to the client;

b) **Best Practice** findings are used when some piece of code does not conform with smart contract development best practices;

c) **Gas** findings are used when some piece of code uses more gas than it should be or have some functions that can be removed to save gas.

6 Issues by Severity Levels

6.1 Best Practices

6.1.1 Inconsistent mutability in owner component reference

File(s): cairo/crates/contracts/src/client/router_component.cairo

Description: The function `unenroll_remote_router()` uses a mutable reference to the Owner component (`get_dep_component_mut!(ref self, Owner)`) while similar functions use immutable references (`get_dep_component!(@self, Owner)`). Since the component is only used for the `assert_only_owner()` check and isn't modified, this inconsistency introduces potential bugs.

```
fn unenroll_remote_router(ref self: ComponentState<TContractState>, domain: u32) {
    let mut ownable_comp = get_dep_component_mut!(ref self, Owner); // @audit mutable
    ownable_comp.assert_only_owner();

    self._unenroll_remote_router(domain);
}

fn unenroll_remote_routers(ref self: ComponentState<TContractState>, domains: Array<u32>) {
    let ownable_comp = get_dep_component!(@self, Owner); // @audit immutable
    ownable_comp.assert_only_owner();
    let domains_len = domains.len();
    let mut i = 0;
    while i < domains_len {
        self._unenroll_remote_router(*domains.at(i));
        i += 1;
    }
}
```

Recommendation(s): Consider changing the mutable reference to an immutable one to maintain consistency across similar functions.

Status: Fixed

Update from the client: Fixed in PR #18

6.2   Undetermined

6.2.1   Inconsistent asset-to-share conversion in transfer functions

File(s): `cairo/crates/token/src/extensions/hyp_erc20_vault.cairo`

Description: There is an inconsistency in how the contract handles asset-to-share conversions between the `transfer()` and `transfer_-from()` functions.

```
1  fn transfer(ref self: ContractState, recipient: ContractAddress, amount: u256) -> bool {
2      self.erc20.transfer(recipient, self.assets_to_shares(amount));
3      true
4  }
5
6  fn transfer_from(
7      ref self: ContractState,
8      sender: ContractAddress,
9      recipient: ContractAddress,
10     amount: u256
11 ) -> bool {
12     self.erc20.transfer_from(sender, recipient, amount)
13 }
```

The function `transfer()` applies a conversion using `self.assets_to_shares(amount)` while the function `transfer_from()` does not apply any conversion. Due to lack of time, the full impact of this inconsistency has not been clearly investigated.

Recommendation(s): Consider reviewing the intended behavior for all transfer functions and ensure consistent handling of asset-to-share conversions across all related functions. Either all functions should convert amounts to shares before transfer, or none should, depending on the contract's intended behavior.

Status: Fixed

Update from the client: Fixed in PR #16

7   Test Evaluation

7.1   Compilation Output

```
 1  scarb build
 2      Updating git repository https://github.com/openzeppelin/cairo-contracts
 3      Updating git repository https://github.com/foundry-rs/starknet-foundry
 4    Compiling lib(contracts) contracts v0.0.6 (hyperlane/cairo/crates/contracts/Scarb.toml)
 5    Compiling starknet-contract(contracts) contracts v0.0.6 (hyperlane/cairo/crates/contracts/Scarb.toml)
 6    Compiling lib(mocks) mocks v0.0.6 (hyperlane/cairo/crates/mocks/Scarb.toml)
 7    Compiling starknet-contract(mocks) mocks v0.0.6 (hyperlane/cairo/crates/mocks/Scarb.toml)
 8    Compiling lib(token) token v0.0.1 (hyperlane/cairo/crates/token/Scarb.toml)
 9    Compiling starknet-contract(token) token v0.0.1 (hyperlane/cairo/crates/token/Scarb.toml)
10     Finished release target(s) in 3 minutes
```

7.2   Tests Output

```
 1  snforge test
 2    Compiling lib(contracts) contracts v0.0.6 (/home/boreas/hyperlane/cairo/crates/contracts/Scarb.toml)
 3    Compiling starknet-contract(contracts) contracts v0.0.6 (/home/boreas/hyperlane/cairo/crates/contracts/Scarb.
      toml)
 4    Compiling lib(mocks) mocks v0.0.6 (/home/boreas/hyperlane/cairo/crates/mocks/Scarb.toml)
 5    Compiling starknet-contract(mocks) mocks v0.0.6 (/home/boreas/hyperlane/cairo/crates/mocks/Scarb.toml)
 6    Compiling lib(token) token v0.0.1 (/home/boreas/hyperlane/cairo/crates/token/Scarb.toml)
 7    Compiling starknet-contract(token) token v0.0.1 (/home/boreas/hyperlane/cairo/crates/token/Scarb.toml)
 8     Finished release target(s) in 3 minutes
 9
10
11  Collected 144 test(s) from contracts package
12  Running 10 test(s) from src/
13  [PASS] contracts::utils::keccak256::tests::test_reverse_endianness (gas: ~2)
14  [PASS] contracts::utils::keccak256::tests::test_u64_word_size (gas: ~6)
15  [PASS] contracts::utils::keccak256::tests::test_down_bytes (gas: ~1)
16  [PASS] contracts::libs::aggregation_ism_metadata::test::test_aggregation_ism_has_metadata (gas: ~14)
17  [PASS] contracts::utils::keccak256::tests::test_up_bytes (gas: ~68)
18  [PASS] contracts::libs::message::tests::test_append_u128_to_byte_array (gas: ~21)
19  [PASS] contracts::libs::aggregation_ism_metadata::test::test_aggregation_ism_metadata (gas: ~37)
20  [PASS] contracts::hooks::libs::standard_hook_metadata::tests::test_standard_hook_metadata_default_value (gas:
         ~49)
21  [PASS] contracts::hooks::libs::standard_hook_metadata::tests::test_standard_hook_metadata (gas: ~106)
22  [PASS] contracts::utils::keccak256::tests::test_compute_keccak (gas: ~457)
23  Running 134 test(s) from tests/
24  [PASS] tests::libs::test_rate_limited::test_should_panic_when_validate_consume_filled_levels_when_exceeding_limit
         (gas: ~308)
25  [PASS] tests::isms::test_messageid_multisig::test_message_id_multisig_module_type (gas: ~296)
26  [PASS] tests::isms::test_aggregation::test_aggregation_initialize_with_too_many_modules (gas: ~267)
27
28  Success data:
29      0x526573756c743a3a756e77726170206661696c65642e ('Result::unwrap failed.')
30
31  [PASS] tests::isms::test_aggregation::test_aggregation_module_type (gas: ~361)
32  [PASS] tests::test_mailbox::test_set_required_hook_fails_if_not_owner (gas: ~1112)
33  [PASS] tests::test_validator_announce::test_digest_computation (gas: ~596)
34  [PASS] tests::test_mailbox::test_set_default_hook_fails_if_not_owner (gas: ~1112)
35  [PASS] tests::test_mailbox::test_dispatch_with_two_fee_hook_fails_if_greater_than_required_and_lower_than_default
         (gas: ~2176)
36  [PASS] tests::test_mailbox::test_local_domain (gas: ~1112)
37  [PASS] tests::test_validator_announce::test_announce_fails_if_wrong_signer (gas: ~2349)
38  [PASS] tests::test_mailbox::test_dispatch_with_two_fee_hook (gas: ~2332)
39  [PASS] tests::test_validator_announce::test_announce_fails_if_replay (gas: ~2804)
40  [PASS] tests::hooks::test_protocol_fee::test_set_protocol_fee_fails_if_higher_than_max (gas: ~427)
41  [PASS] tests::test_mailbox::test_set_default_ism (gas: ~1118)
42  [PASS] tests::isms::test_messageid_multisig::test_message_id_multisig_verify_with_empty_metadata (gas: ~556)
43  [PASS] tests::hooks::test_protocol_fee::test_set_beneficiary (gas: ~429)
44  [PASS] tests::test_mailbox::test_transfer_ownership (gas: ~1119)
45  [PASS] tests::hooks::test_domain_routing_hook::test_transfer_routing_fee_insufficient_balance (gas: ~2117)
```

```
46  [PASS] tests::hooks::test_domain_routing_hook::test_domain_routing_hook_type (gas: ~1472)
47  [PASS] tests::isms::test_aggregation::test_setup_aggregation_with_null_module_address (gas: ~230)
48
49  Success data:
50      0x526573756c743a3a756e77726170206661696c65642e ('Result::unwrap failed.')
51
52  [PASS] tests::isms::test_messageid_multisig::test_message_id_multisig_verify_with_4_valid_signatures (gas: ~3662)
53  [PASS] tests::hooks::test_domain_routing_hook::test_supports_metadata_for_domain_routing_hook (gas: ~1472)
54  [PASS] tests::hooks::test_domain_routing_hook::test_domain_rounting_set_hook (gas: ~1539)
55  [PASS] tests::hooks::test_protocol_fee::test_set_beneficiary_fails_if_not_owner (gas: ~426)
56  [PASS] tests::isms::test_messageid_multisig::test_message_id_multisig_verify_with_insufficient_valid_signatures (
           gas: ~4400)
57  [PASS] tests::isms::test_messageid_multisig::
           test_message_id_multisig_verify_with_4_valid_signatures_fails_if_duplicate_signatures (gas: ~4216)
58  [PASS] tests::test_mailbox::test_dispatch_with_protocol_fee_hook_fails_if_provided_fee_lower_than_required_fee (
           gas: ~2050)
59  [PASS] tests::isms::test_aggregation::test_get_modules (gas: ~363)
60  [PASS] tests::test_validator_announce::test_double_announce (gas: ~1034)
61  [PASS] tests::hooks::test_domain_routing_hook::test_set_hook_fails_if_not_owner (gas: ~1472)
62  [PASS] tests::hooks::test_protocol_fee::test_collect_protocol_fee (gas: ~1001)
63  [PASS] tests::hooks::test_protocol_fee::test_collect_protocol_fee_fails_if_insufficient_balance (gas: ~917)
64  [PASS] tests::test_validator_announce::test_announce (gas: ~2808)
65  [PASS] tests::isms::test_default_ism::test_verify_noop_ism (gas: ~105)
66  [PASS] tests::test_mailbox::test_process (gas: ~2190)
67  [PASS] tests::isms::test_default_ism::test_pause_unpause_pausable_ism (gas: ~173)
68  [PASS] tests::hooks::test_protocol_fee::test_quote_dispatch (gas: ~432)
69  [PASS] tests::isms::test_default_ism::test_unpause_pausable_ism_fails_if_not_owner (gas: ~167)
70  [PASS] tests::hooks::test_protocol_fee::test_post_dispatch_fails_if_invalid_variant (gas: ~432)
71  [PASS] tests::isms::test_default_ism::test_verify_pausable_ism (gas: ~170)
72  [PASS] tests::isms::test_default_ism::test_pause_pausable_ism_fails_if_not_owner (gas: ~167)
73  [PASS] tests::hooks::test_protocol_fee::test_supports_metadata (gas: ~443)
74  [PASS] tests::isms::test_aggregation::test_aggregation_verify (gas: ~3333)
75  [PASS] tests::test_mailbox::test_set_required_hook (gas: ~1118)
76  [PASS] tests::hooks::test_protocol_fee::test_quote_dispatch_fails_if_invalid_variant (gas: ~431)
77  [PASS] tests::routing::test_default_fallback_routing_ism::test_initialize (gas: ~1812)
78  [PASS] tests::isms::test_default_ism::test_veriy_pausable_ism_fails_if_paused (gas: ~236)
79  [PASS] tests::isms::test_merkleroot_multisig::test_set_validators (gas: ~363)
80  [PASS] tests::hooks::test_merkle_tree_hook::test_post_dispatch_fails_if_invalid_variant (gas: ~1414)
81  [PASS] tests::test_mailbox::test_dispatch_with_protocol_fee_hook_fails_if_user_balance_lower_than_fee_amount (gas
           : ~2051)
82  [PASS] tests::routing::test_default_fallback_routing_ism::test_initialize_fails_if_module_is_zero (gas: ~1669)
83  [PASS] tests::isms::test_default_ism::test_verify_trusted_relayer_ism (gas: ~2601)
84  [PASS] tests::hooks::test_domain_routing_hook::hook_set_for_destination_quote_dispatch (gas: ~2475)
85  [PASS] tests::hooks::test_domain_routing_hook::test_transfer_routing_fee_insufficient_allowance (gas: ~2119)
86  [PASS] tests::routing::test_default_fallback_routing_ism::test_initialize_fails_if_length_mismatch (gas: ~1409)
87  [PASS] tests::isms::test_merkleroot_multisig::test_set_validators_fails_if_null_validator (gas: ~294)
88
89  Success data:
90      0x526573756c743a3a756e77726170206661696c65642e ('Result::unwrap failed.')
91
92  [PASS] tests::routing::test_default_fallback_routing_ism::test_initialize_fails_if_caller_not_owner (gas: ~1409)
93  [PASS] tests::routing::test_default_fallback_routing_ism::test_remove_domain (gas: ~1743)
94  [PASS] tests::isms::test_merkleroot_multisig::test_set_threshold (gas: ~297)
95  [PASS] tests::isms::test_merkleroot_multisig::test_merkle_root_multisig_module_type (gas: ~296)
96  [PASS] tests::routing::test_default_fallback_routing_ism::get_default_module (gas: ~1413)
97  [PASS] tests::hooks::test_merkle_tree_hook::test_merkle_tree_hook_type (gas: ~1407)
98  [PASS] tests::hooks::test_merkle_tree_hook::test_supports_metadata (gas: ~1425)
99  [PASS] tests::routing::test_default_fallback_routing_ism::test_remove_domain_fails_if_domain_not_found (gas:
           ~1804)
100 [PASS] tests::hooks::test_merkle_tree_hook::test_post_dispatch (gas: ~2141)
101 [PASS] tests::hooks::test_merkle_tree_hook::test_post_dispatch_fails_if_message_not_dispatching (gas: ~1532)
102 [PASS] tests::routing::test_default_fallback_routing_ism::test_set_domain_and_module (gas: ~1949)
103 [PASS] tests::isms::test_merkleroot_multisig::test_merkleroot_ism_metadata (gas: ~1430)
104 [PASS] tests::routing::test_default_fallback_routing_ism::test_set_domain_and_module_fails_if_caller_is_not_owner
           (gas: ~1409)
105 [PASS] tests::hooks::test_domain_routing_hook::hook_not_set_for_destination_should_fail (gas: ~1541)
106 [PASS] tests::routing::test_default_fallback_routing_ism::test_remove_domain_module_check (gas: ~1747)
107 [PASS] tests::isms::test_messageid_multisig::test_set_validators (gas: ~363)
108 [PASS] tests::hooks::test_domain_routing_hook::test_set_hook_array_fails_if_not_owner (gas: ~1473)
109 [PASS] tests::isms::test_messageid_multisig::test_set_threshold (gas: ~296)
```

```
110  [PASS] tests::isms::test_merkleroot_multisig::test_merkle_root_multisig_verify_with_empty_metadata (gas: ~556)
111  [PASS] tests::hooks::test_domain_routing_hook::test_domain_rounting_set_hook_array (gas: ~1675)
112  [PASS] tests::routing::test_default_fallback_routing_ism::test_remove_domain_fails_if_caller_not_owner (gas:
        ~1409)
113  [PASS] tests::hooks::test_merkle_tree_hook::test_count (gas: ~1408)
114  [PASS] tests::hooks::test_merkle_tree_hook::test_quote_dispatch (gas: ~1414)
115  [PASS] tests::isms::test_messageid_multisig::test_set_validators_fails_if_null_validator (gas: ~294)
116
117  Success data:
118      0x526573756c743a3a756e77726170206661696c65642e ('Result::unwrap failed.')
119
120  [PASS] tests::hooks::test_domain_routing_hook::test_post_dispatch_insufficient_fee (gas: ~1971)
121  [PASS] tests::isms::test_messageid_multisig::test_message_id_ism_metadata (gas: ~263)
122  [PASS] tests::hooks::test_domain_routing_hook::hook_set_for_destination_post_dispatch (gas: ~2669)
123  [PASS] tests::hooks::test_merkle_tree_hook::test_quote_dispatch_fails_if_invalid_variant (gas: ~1413)
124  [PASS] tests::hooks::test_protocol_fee::test_hook_type (gas: ~425)
125  [PASS] tests::routing::test_default_fallback_routing_ism::test_module_type (gas: ~1408)
126  [PASS] tests::routing::test_domain_routing_ism::test_verify (gas: ~4221)
127  [PASS] tests::routing::test_domain_routing_ism::test_remove_domain_check_module (gas: ~501)
128  [PASS] tests::isms::test_merkleroot_multisig::test_merkle_root_multisig_verify_with_4_valid_signatures (gas:
        ~9088)
129  [PASS] tests::routing::test_domain_routing_ism::test_remove_domain_fails_if_domain_not_found (gas: ~563)
130  [PASS] tests::test_mailbox::test_dispatch (gas: ~1702)
131  [PASS] tests::test_mailbox::test_dispatch_with_protocol_fee_hook (gas: ~2196)
132  [PASS] tests::routing::test_domain_routing_ism::test_set_domain_and_module (gas: ~708)
133  [PASS] tests::routing::test_domain_routing_ism::get_module_fails_if_origin_not_found (gas: ~167)
134  [PASS] tests::routing::test_domain_routing_ism::test_initialize (gas: ~571)
135  [PASS] tests::isms::test_merkleroot_multisig::
        test_merkle_root_multisig_verify_with_4_valid_signatures_fails_if_duplicate_signatures (gas: ~9638)
136  [PASS] tests::routing::test_domain_routing_ism::test_initialize_fails_if_caller_not_owner (gas: ~168)
137  [PASS] tests::routing::test_domain_routing_ism::test_remove_domain_fails_if_caller_not_owner (gas: ~168)
138  [PASS] tests::routing::test_domain_routing_ism::test_set_domain_and_module_fails_if_caller_is_not_owner (gas:
        ~168)
139  [PASS] tests::routing::test_domain_routing_ism::test_module_type (gas: ~167)
140  [PASS] tests::routing::test_domain_routing_ism::test_remove_domain (gas: ~503)
141  [PASS] tests::routing::test_domain_routing_ism::test_route_ism (gas: ~569)
142  [PASS] tests::routing::test_domain_routing_ism::test_initialize_fails_if_length_mismatch (gas: ~169)
143  [PASS] tests::routing::test_domain_routing_ism::test_initialize_fails_if_module_is_zero (gas: ~429)
144  [PASS] tests::routing::test_domain_routing_ism::test_route_ism_fails_if_origin_not_found (gas: ~562)
145  [PASS] tests::routing::test_default_fallback_routing_ism::test_verify (gas: ~5450)
146  [PASS] tests::libs::test_rate_limited::test_should_consume_filled_level_and_emit_events (gas: ~312)
147  [PASS] tests::libs::test_rate_limited::test_should_decreases_limit_within_same_day (gas: ~400)
148  [PASS] tests::isms::test_merkleroot_multisig::test_merkle_root_multisig_verify_with_insufficient_valid_signatures
        (gas: ~10252)
149  [PASS] tests::hooks::test_merkle_tree_hook::test_insert_node_into_merkle_tree_hook (gas: ~13494)
150  [PASS] tests::test_mailbox::test_set_default_ism_fails_if_not_owner (gas: ~1112)
151  [PASS] tests::test_mailbox::test_process_fails_if_destination_domain_does_not_match_local_domain (gas: ~1304)
152  [PASS] tests::test_mailbox::test_owner (gas: ~1112)
153  [PASS] tests::libs::test_rate_limited::test_should_panic_when_current_level_when_capacity_is_zero (gas: ~241)
154  [PASS] tests::libs::test_rate_limited::test_replenishes_within_same_day (gas: ~383)
155  [PASS] tests::libs::test_rate_limited::test_ctor_should_panic_when_low_capacity (gas: ~101)
156
157  Success data:
158      0x526573756c743a3a756e77726170206661696c65642e ('Result::unwrap failed.')
159
160  [PASS] tests::routing::test_default_fallback_routing_ism::test_route_ism (gas: ~1817)
161  [PASS] tests::libs::test_rate_limited::test_should_sets_new_limit (gas: ~308)
162  [PASS] tests::test_mailbox::test_process_fails_if_already_delivered (gas: ~2386)
163  [PASS] tests::test_mailbox::test_dispatch_with_protocol_fee_hook_fails_if_insufficient_allowance (gas: ~2052)
164  [PASS] tests::libs::test_rate_limited::test_should_panic_when_max_not_set (gas: ~241)
165  [PASS] tests::libs::test_enumerable_map::test_initialize_empty_map (gas: ~102)
166  [PASS] tests::hooks::test_protocol_fee::test_set_protocol_fee (gas: ~430)
167  [PASS] tests::test_mailbox::test_process_fails_if_version_mismatch (gas: ~1303)
168  [PASS] tests::hooks::test_protocol_fee::test_set_protocol_fee_fails_if_not_owner (gas: ~426)
169  [PASS] tests::libs::test_enumerable_map::test_fuzz_set (runs: 256, gas: {max: ~438, min: ~310, mean: ~437.00, std
        deviation: ~8.92})
170  [PASS] tests::test_mailbox::test_set_default_hook (gas: ~1118)
171  [PASS] tests::libs::test_rate_limited::test_should_return_curreny_filled_level_any_time (runs: 256, gas: {max:
        ~302, min: ~301, mean: ~301.00, std deviation: ~0.72})
```

```
172  [PASS] tests::libs::test_rate_limited::test_should_reset_limit_when_duration_exceeds (runs: 256, gas: {max: ~380,
         min: ~380, mean: ~380.00, std deviation: ~0.00})
173  [PASS] tests::libs::test_enumerable_map::test_fuzz_should_remove (runs: 256, gas: {max: ~190, min: ~126, mean:
         ~189.00, std deviation: ~4.06})
174  [PASS] tests::libs::test_rate_limited::test_should_panic_when_caller_not_owner_when_set_limits (runs: 256, gas: {
         max: ~299, min: ~299, mean: ~299.00, std deviation: ~0.00})
175  [PASS] tests::libs::test_rate_limited::test_should_never_return_gt_max_limit (runs: 256, gas: {max: ~382, min:
         ~318, mean: ~378.00, std deviation: ~3.89})
176  [PASS] tests::libs::test_enumerable_map::test_fuzz_contains (runs: 256, gas: {max: ~427, min: ~102, mean:
         ~265.00, std deviation: ~161.99})
177  [PASS] tests::libs::test_enumerable_map::test_fuzz_get_keys (runs: 256, gas: {max: ~715, min: ~587, mean:
         ~713.00, std deviation: ~12.57})
178  Tests: 144 passed, 0 failed, 0 skipped, 0 ignored, 0 filtered out
179  Fuzzer seed: 15800759655720481905
180
181
182  Collected 0 test(s) from mocks package
183  Running 0 test(s) from src/
184  Tests: 0 passed, 0 failed, 0 skipped, 0 ignored, 0 filtered out
185
186
187  Collected 61 test(s) from token package
188  Running 0 test(s) from src/
189  Running 61 test(s) from tests/
190  [PASS] tests::hyp_erc20::common::test_hyp_erc20_setup (gas: ~1)
191  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_total_supply (gas: ~6124)
192  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_decimals (gas: ~6124)
193  [PASS] tests::hyp_erc20::hyp_fiat_token_test::test_fiat_token_handle (gas: ~7240)
194  [PASS] tests::hyp_erc20::hyp_erc20_collateral_test::test_remote_transfer_invalid_allowance (gas: ~7217)
195
196  Success data:
197     0x45524332303a20696e73756666696369656e7420616c6c6f77616e6365 ('ERC20: insufficient allowance')
198
199  [PASS] tests::hyp_erc20::hyp_xerc20_test::test_handle (gas: ~7552)
200  [PASS] tests::hyp_erc20::hyp_erc20_collateral_test::test_remote_transfer (gas: ~8884)
201  [PASS] tests::hyp_erc20::hyp_erc20_collateral_test::test_remote_transfer_with_custom_gas_config (gas: ~8818)
202  [PASS] tests::hyp_erc20::hyp_xerc20_test::test_remote_transfer (gas: ~9240)
203  [PASS] tests::hyp_erc20::hyp_erc20_lockbox_test::test_remote_transfer_with_custom_gas_config (gas: ~9865)
204  [PASS] tests::hyp_erc20::hyp_erc20_lockbox_test::test_erc20_lockbox_transfer (gas: ~9930)
205  [PASS] tests::hyp_erc20::hyp_xerc20_test::test_erc20_remote_transfer_with_custom_gas_config (gas: ~9106)
206  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_local_transfer (gas: ~6204)
207  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_remote_transfer_invalid_amount (gas: ~6126)
208
209  Success data:
210     0x45524332303a20696e73756666696369656e742062616c616e6365 ('ERC20: insufficient balance')
211
212  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_remote_transfer (gas: ~8127)
213  [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_remote_transfer_with_custom_gas_config (gas: ~8062)
214  [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_cyclic_transfers (gas: ~22901)
215  [PASS] tests::hyp_erc20::hyp_fiat_token_test::test_fiat_token_remote_transfer (gas: ~8886)
216  [PASS] tests::hyp_erc20::hyp_fiat_token_test::test_fiat_token_remote_transfer_with_custom_gas_config (gas: ~8821)
217  [PASS] tests::hyp_erc20::hyp_erc20_lockbox_test::test_erc20_lockbox_approval (gas: ~8207)
218  [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_remote_transfer_rebase_after (gas: ~16507)
219  [PASS] tests::hyp_erc20::hyp_erc20_collateral_test::test_erc20_remote_transfer_collateral_with_hook_specified (
         runs: 256, gas: {max: ~9165, min: ~9027, mean: ~9164.00, std deviation: ~8.62})
220  [PASS] tests::hyp_erc721::common::test_erc721_setup (gas: ~8610)
221  [PASS] tests::hyp_erc721::hyp_erc721_collateral_test::test_erc721_collateral_remote_transfer (gas: ~12626)
222  [PASS] tests::hyp_erc721::hyp_erc721_uri_storage_test::
         test_erc721_uri_storage_remote_transfer_with_hook_specified (runs: 256, gas: {max: ~13812, min: ~13674, mean:
         ~13811.00, std deviation: ~8.62})
223  [PASS] tests::hyp_erc721::hyp_erc721_collateral_test::
         test_erc721_collateral_remote_transfer_revert_invalid_token_id (gas: ~10839)
224
225  Success data:
226     0x4552433732313a20696e76616c696420746f6b656e204944 ('ERC721: invalid token ID')
227
228  [PASS] tests::hyp_erc721::hyp_erc721_collateral_test::test_erc721_collateral_remote_transfer_revert_unowned (gas:
         ~10912)
229
230  Success data:
```

```
231        0x4552433732313a20756e617574686f72697a65642063616c6c6572 ('ERC721: unauthorized caller')

232

233   [PASS] tests::hyp_erc721::hyp_erc721_collateral_test::test_erc721__collateral_remote_transfer_with_hook_specified
            (runs: 256, gas: {max: ~12773, min: ~12635, mean: ~12772.00, std deviation: ~8.62})
234   [PASS] tests::hyp_erc721::hyp_erc721_collateral_uri_storage_test::
            test_erc721_collateral_uri_storage_remote_transfer_revert_burned (gas: ~12863)
235   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_total_supply (gas: ~8938)
236   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_owner_of (gas: ~8938)
237   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_local_transfer_invalid_token_id (gas: ~8939)

238

239   Success data:
240        0x4552433732313a20696e76616c696420746f6b656e204944 ('ERC721: invalid token ID')

241

242   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_local_transfer (gas: ~9013)
243   [PASS] tests::hyp_erc721::hyp_erc721_collateral_uri_storage_test::
            test_erc721_collateral_uri_storage_remote_transfer_with_hook_specified (runs: 256, gas: {max: ~13010, min:
            ~12872, mean: ~13009.00, std deviation: ~8.62})
244   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_remote_transfer (runs: 256, gas: {max: ~12001, min:
            ~11560, mean: ~11787.00, std deviation: ~220.39})
245   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_remote_transfer_revert_unowned (gas: ~10346)

246

247   Success data:
248        "Caller␣is␣not␣owner"

249

250   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_remote_transfer_revert_invalid_token_id (gas: ~9957)

251

252   Success data:
253        0x4552433732313a20696e76616c696420746f6b656e204944 ('ERC721: invalid token ID')

254

255   [PASS] tests::hyp_erc721::hyp_erc721_test::test_erc721_remote_transfer_with_hook_specified (runs: 256, gas: {max:
            ~12147, min: ~11568, mean: ~11900.00, std deviation: ~219.14})
256   [PASS] tests::hyp_erc721::hyp_erc721_uri_storage_test::test_erc721_uri_storage_remote_transfer (gas: ~13666)
257   [PASS] tests::hyp_erc721::hyp_erc721_uri_storage_test::test_erc721_uri_storage_remote_transfer_revert_burned (gas
            : ~13667)

258

259   Success data:
260        0x4552433732313a20696e76616c696420746f6b656e204944 ('ERC721: invalid token ID')

261

262   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_erc4626_vault_deposit_remote_transfer_sweep_excess_shares_multiple_deposit (runs: 256, gas: {max:
            ~12865, min: ~12865, mean: ~12865.00, std deviation: ~0.00})
263   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_collateral_domain (gas: ~11910)
264   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_erc4626_vault_deposit_remote_transfer_sweep_excess_shares_12312 (runs: 256, gas: {max: ~11101, min:
            ~11101, mean: ~11101.00, std deviation: ~0.00})
265   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_fuzz_erc4626_vault_deposit_remote_transfer_withdraw_less_shares (runs: 256, gas: {max: ~11211, min:
            ~11211, mean: ~11211.00, std deviation: ~0.00})
266   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_fuzz_erc4626_vault_deposit_remote_transfer_withdraws_from_vault (runs: 256, gas: {max: ~11215, min:
            ~10957, mean: ~11213.00, std deviation: ~16.12})
267   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_fuzz_erc4626_vault_deposit_remote_transfer_sweep_revert_non_owner (runs: 256, gas: {max: ~11242, min:
            ~11242, mean: ~11242.00, std deviation: ~0.00})

268

269   Success data:
270        0x43616c6c6572206973206e6f7420746865206f776e6572 ('Caller is not the owner')

271

272   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_rebase_with_transfer (gas: ~16583)
273   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_withdrawal_without_yield (gas: ~16388)
274   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_synthetic_transfers_with_rebase (gas: ~16661)
275   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_withdrawal_with_yield (gas: ~16530)
276   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_withdrawal_after_yield (gas: ~18568)
277   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_withdrawal_after_drawdown (gas: ~18424)
278   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_withdrawal_in_flight (gas: ~20876)
279   [PASS] tests::vault_extensions::hyp_erc20_vault_test::test_exchange_rate_set_only_by_collateral (gas: ~20697)
280   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
            test_fuzz_erc4626_vault_deposit_remote_transfer_deposits_into_vault (runs: 256, gas: {max: ~9641, min: ~9256,
            mean: ~9639.00, std deviation: ~24.02})
```

```
281   [PASS] tests::vault_extensions::hyp_erc20_collateral_vault_deposit_test::
           test_fuzz_erc4626_vault_deposit_remote_transfer_sweep_no_excess_shares (runs: 256, gas: {max: ~9664, min:
           ~9279, mean: ~9662.00, std deviation: ~24.02})
282   [PASS] tests::hyp_erc20::hyp_erc20_lockbox_test::test_erc20_lockbox_handle (gas: ~8251)
283   [PASS] tests::hyp_erc20::hyp_xerc20_test::test_erc20_remote_transfer_with_hook_specified (runs: 256, gas: {max:
           ~9520, min: ~9381, mean: ~9519.00, std deviation: ~8.68})
284   [PASS] tests::hyp_erc20::hyp_erc20_test::test_erc20_remote_transfer_with_hook_specified (runs: 256, gas: {max:
           ~8476, min: ~8336, mean: ~8475.00, std deviation: ~8.74})
285   [PASS] tests::hyp_erc20::hyp_erc20_lockbox_test::test_erc20_lockbox_remote_transfer_with_hook_specified (runs:
           256, gas: {max: ~10212, min: ~10073, mean: ~10211.00, std deviation: ~8.68})
286   [PASS] tests::hyp_erc20::hyp_fiat_token_test::test_fiat_token_remote_transfer_with_hook_specified (runs: 256, gas
           : {max: ~9170, min: ~9032, mean: ~9169.00, std deviation: ~8.62})
287   Tests: 61 passed, 0 failed, 0 skipped, 0 ignored, 0 filtered out
288   Fuzzer seed: 13597663669351120974
```