zkBugs Evaluation Results

Table 1: Tool Performance Summary

Tool	TP	FN	Timeout	Failure	Total	Median Time (s)
circomspect	1	34	0	0	35	0.03
circom_civer	10	2	15	8	35	2.17
picus	7	9	11	8	35	2.39
ecneproject	21	9	3	2	35	12.01
zkfuzz	18	7	9	1	35	0.73
TOTAL	57	61	38	19	175	2.20

Table 2: Execution Time Statistics

Tool	Total	Min (s)	Max (s)	Median (s)	Mean (s)	NR-Timeout
circomspect	35	0.01	0.42	0.03	0.10	0
circom_civer	12	0.03	552.60	2.17	138.19	15
picus	24	1.41	337.26	2.39	38.03	11
ecneproject	30	9.23	178.97	12.01	17.99	3
zkfuzz	25	0.01	410.56	0.73	34.07	9

Table 3: Bug-Tool Matrix (by Bug ID)

Bug ID	circomspect	circom_civer	picus	ecneproject	zkfuzz
1	FN	TP	Failure	TP*	TP*
2	FN	Timeout	Timeout	TP*	TP*
3	FN	Timeout	Failure	TP*	TP*
4	FN	Timeout	Timeout	TP*	TP*
5	FN	Timeout	Timeout	Timeout	FN
6	FN	Timeout	FN	Timeout	Failure
7	FN	Timeout	Failure	Timeout	FN
8	TP*	Timeout	Timeout	TP*	Timeout
9	FN	TP	TP*	Failure	TP*
10	FN	TP	TP*	TP*	TP*
11	FN*	FN	FN*	FN*	FN*
12	FN	Timeout	Timeout	TP*	Timeout
13	FN	Timeout	FN	FN	TP*
14	FN	FN	FN	FN	Timeout
15	FN	Timeout	Failure	TP*	TP*
16	FN	Timeout	Timeout	FN	Timeout
17	FN	TP*	Failure	TP*	TP*
18	FN	TP*	Failure	TP*	TP*
19	FN	TP*	Failure	TP*	TP*
20	FN	Timeout	TP*	TP*	TP*
21	FN	TP	TP*	TP*	TP*
22	FN	TP	TP*	TP*	TP*
23	FN	Timeout	TP*	TP*	TP*
24	FN	TP	Timeout	TP*	FN
25	FN	Timeout	Timeout	TP*	Timeout
26	FN	Timeout	Timeout	TP*	TP*
27	FN	Failure	Timeout	TP*	Timeout
28	FN	Failure	FN*	FN*	FN*
29	FN	Failure	FN*	Failure	FN*
30	FN	Failure	FN	FN	FN
31	FN	Failure	Failure	FN	Timeout
32	FN	Failure	Timeout	TP*	Timeout
33	FN	Failure	FN	FN	Timeout
34	FN	Failure	FN	FN	TP*
35	FN	TP	TP*	TP*	TP*

* = *manually analyzed*

Table 4: Bug ID to Name Mapping

ID	Bug Name
1	daira_hopwood_darkforest_v0_3_missing_bit_length_check
2	hashcloak_data_are_not_fully_verified_during_state_update
3	kobi_gurkan_mimc_hash_assigned_but_not_constrained
4	leastauthority_previously_correct_ownership_proof_disabled_via_code_changes
5	trailofbits_incorrect_handling_of_point_doubling_can_allow_signature_forgery
6	trailofbits_prover_can_lock_user_funds_by_including_ill-formed_bigints_in_public_key_commitment
7	trailofbits_prover_can_lock_user_funds_by_supplying_non-reduced_Y_values_to_G1BigIntToSignFlag
8	trailofbits_unsafe_use_of_num2bits_in_multiple_circuits
9	veridise_arrayxor_is_under_constrained
10	veridise_decoder_accepting_bogus_output_signal
11	veridise_incorrect_initialization_in_membership_circuits
12	veridise_missing_range_checks_in_bigmod
13	veridise_missing_range_checks_on_comparison_circuits
14	veridise_no_zero_value_validation
15	veridise_template_CoreVerifyPubkeyG1_does_not_perform_input_validation_simplified
16	veridise_underconstrained_circuit_allows_invalid_comparison
17	veridise_underconstrained_outputs_in_bitElementMulAny
18	veridise_underconstrained_outputs_in_window4
19	veridise_underconstrained_outputs_in_windowmulfix
20	veridise_underconstrained_points_in_edwards2Montgomery
21	veridise_underconstrained_points_in_montgomery2Edwards
22	veridise_underconstrained_points_in_montgomeryAdd
23	veridise_underconstrained_points_in_montgomeryDouble
24	veridise_zero_padding_for_sha256_in_ExpandMessageXMD_is_vulnerable_to_an_overflow
25	yacademy_input_signal_s_is_not_constrained_in_eff_ecdsa_circom
26	yacademy_under_constrained_circuits_compromising_the_soundness_of_the_system
27	zksecurity_an_attacker_can_craft_a_fake_non_inclusion_proof_for_a_given_key_due_to_an_aliasing_bug_in_the_smt_verifier
28	zksecurity_big_integer_zero_check_is_not_sound
29	zksecurity_exclusion_check_of_forbidden_countries_is_unsound_and_incomplete_due_to_incorrect_indexing
30	zksecurity_forbidden_country_check_bypass_via_packed_byte_overflow
31	zksecurity_missing_boolean_constraints_in_the_merkle_tree_path_leads_to_an_attacker_being_able_to_craft_a_fake_merkle_proof_for_an_arbitrary_l
32	zksecurity_missing_byte_range_checks_allows_packed_data_pollution
33	zksecurity_second_pre_image_attacks_on_packbytesandposeidon_may_be_used_to_register_arbitrary_passports_and_dsc_certificates
34	zksecurity_the_registration_and_disclosure_circuits_lack_range_checks_for_the_input_indices
35	zksecurity_unsound_left_rotation

Table 5: Execution Times per Bug (by Bug ID, in seconds)

Bug ID	circomspect	circom_civer	picus	ecneproject	zkfuzz
1	0.05	0.20	7.11	11.56	0.03
2	0.38	—	—	178.97	64.29
3	0.01	7.13	6.32	11.96	0.04
4	0.21	—	—	11.76	0.73
5	0.10	—	—	—	28.42
6	0.31	—	2.91	—	1.20
7	0.42	—	2.23	—	6.71
8	0.02	500.22	—	15.26	—
9	0.03	0.09	2.23	10.55	0.01
10	0.02	0.03	1.68	11.78	0.23
11	0.02	0.07	1.59	10.83	11.37
12	0.04	—	—	13.74	—
13	0.04	502.58	2.61	13.02	112.00
14	0.20	2.20	2.75	12.60	—
15	0.38	503.24	2.20	11.09	0.63
16	0.02	556.74	—	13.22	—
17	0.01	552.60	81.98	11.05	0.53
18	0.04	537.33	337.16	11.02	0.10
19	0.03	509.30	337.26	11.16	11.70
20	0.02	500.13	2.36	10.64	1.51
21	0.01	0.04	1.41	9.23	0.08
22	0.01	2.13	1.78	11.63	0.01
23	0.01	526.83	2.22	12.80	0.05
24	0.02	29.08	—	11.90	410.56
25	0.02	—	—	12.32	—
26	0.02	—	—	11.97	0.11
27	0.22	—	—	16.38	—
28	0.04	—	2.42	13.75	24.60
29	0.03	—	1.63	13.79	83.79
30	0.01	—	1.46	12.05	86.89
31	0.24	—	104.29	13.65	—
32	0.24	—	—	17.42	—
33	0.23	—	2.59	13.03	—
34	0.01	—	1.61	12.54	0.04
35	0.02	25.17	2.89	11.32	7.29