Continuous Integration Meets Cryptographic Artifacts: Building Reliable and Reproducible Research

OPTIMIST 2025

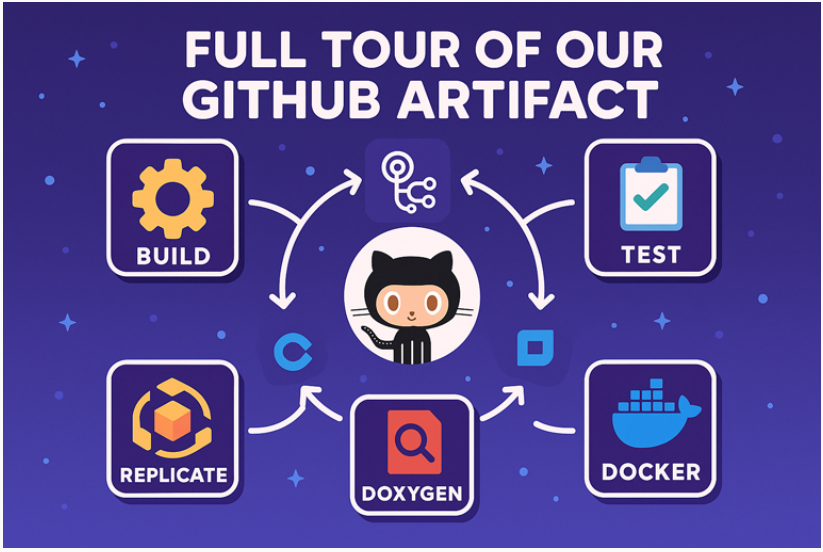
Jesús-Javier Chi-Domínguez [1], Eduardo Ochoa-Jimenez [1], Ricardo-Neftalí Pontaza-Rodas[1]

[1] Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE

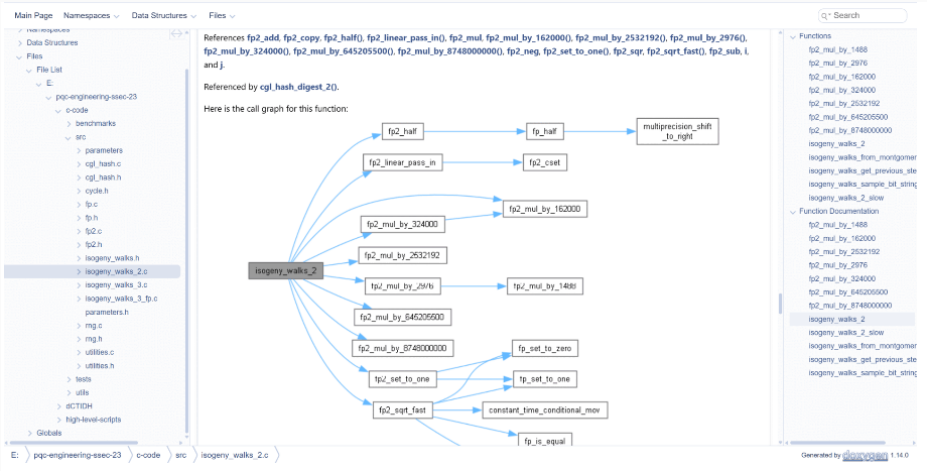
{jesus.dominguez,eduardo.ochoa,ricardo.pontaza}@tii.ae

September 14, 2025

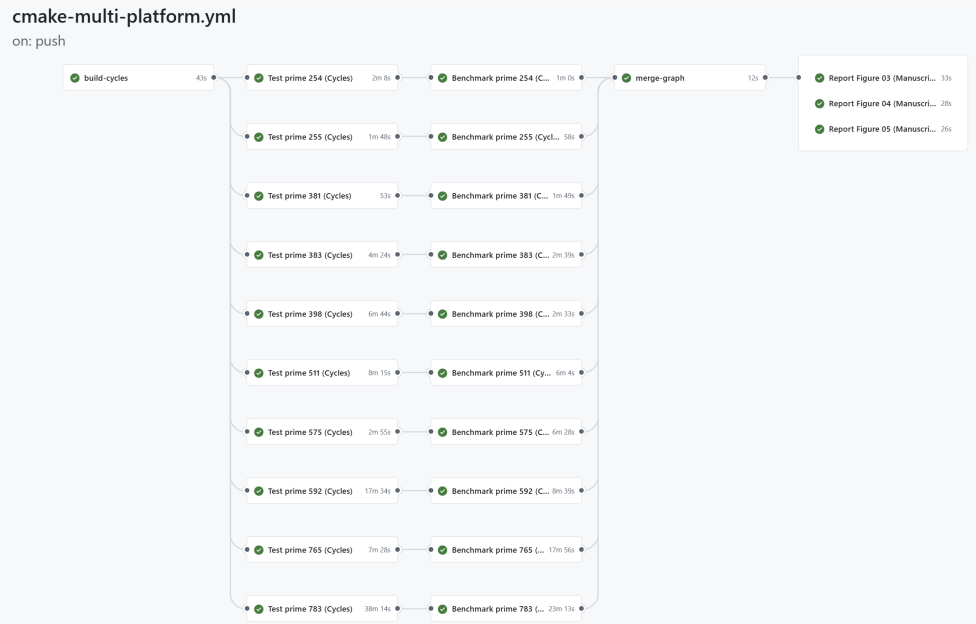
Technology Innovation Institute


FULL TOUR OF OUR
GITHUB ARTIFACT
BUILD
TEST
REPLICATE
DOXYGEN
DOCKER

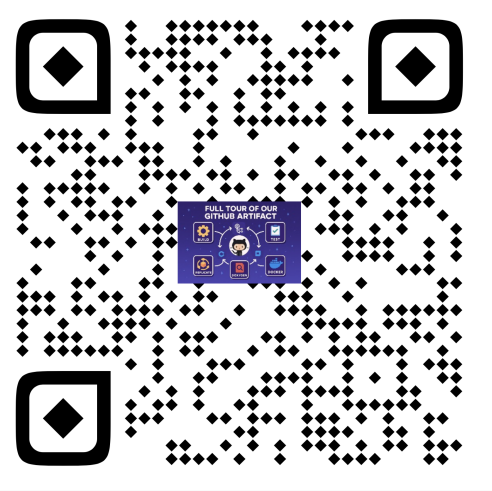
Doxygen


Main Page
Namespaces
Data Structures
Files
Search
Data Structures
Files
File List
E:
pqc-engineering-ssec-23
c-code
benchmarks
src
parameters
cgl_hash.c
cgl_hash.h
cycle.h
fp.c
fp.h
fp2.c
fp2.h
isogeny_walks.h
isogeny_walks_2.c
isogeny_walks_3.c
isogeny_walks_3_fp.c
parameters.h
rng.c
rng.h
utilities.c
utilities.h
tests
utils
dCTIDH
high-level-scripts
Globals
References fp2_add, fp2_copy, fp2_half(), fp2_linear_pass_in(), fp2_mul, fp2_mul_by_162000(), fp2_mul_by_2532192(), fp2_mul_by_2976(), fp2_mul_by_324000(), fp2_mul_by_645205500(), fp2_mul_by_8748000000(), fp2_neg, fp2_set_to_one(), fp2_sqr, fp2_sqrt_fast(), fp2_sub, i, and j.
Referenced by cgl_hash_digest_2().
Here is the call graph for this function:
fp2_half
fp_half
multiprecision_shift_to_right
fp2_linear_pass_in
fp2_cset
fp2_mul_by_162000
fp2_mul_by_324000
fp2_mul_by_2532192
isogeny_walks_2
fp2_mul_by_2976
fp2_mul_by_1488
fp2_mul_by_645205500
fp2_mul_by_8748000000
fp2_set_to_zero
fp2_set_to_one
fp_set_to_one
fp2_sqrt_fast
constant_time_conditional_mov
fp_is_equal
Functions
fp2_mul_by_1488
fp2_mul_by_2976
fp2_mul_by_162000
fp2_mul_by_324000
fp2_mul_by_2532192
fp2_mul_by_645205500
fp2_mul_by_8748000000
isogeny_walks_2
isogeny_walks_from_montgomer
isogeny_walks_get_previous_ste
isogeny_walks_sample_bit_string
isogeny_walks_2_slow
Function Documentation
fp2_mul_by_1488
fp2_mul_by_162000
fp2_mul_by_2532192
fp2_mul_by_2976
fp2_mul_by_324000
fp2_mul_by_645205500
fp2_mul_by_8748000000
isogeny_walks_2
isogeny_walks_2_slow
isogeny_walks_from_montgomer
isogeny_walks_get_previous_ste
isogeny_walks_sample_bit_string
E:
pqc-engineering-ssec-23
c-code
src
isogeny_walks_2.c
Generated by
1.14.0

Pipeline GitHub actions



Thank you



Guided Tour of our Artifact