



Security Review For Privacy Cash



Private Best Efforts Audit Contest Prepared For:
Lead Security Expert:
Date Audited:

Privacy Cash
LZ_security
November 13 - November 17, 2025

Introduction

Privacy Cash is a compliant privacy pool on Solana. The contest is on auditing the ZK circuit, Solana programs and key crypto/encryption primitives used in the product, to ensure the protocol logic is sound.

Scope

Repository: Privacy-Cash/privacy-cash

Audited Commit: d2711c1f1f1deebe61278a8d3033ded85629e09e

Final Commit: b62c1e733cfc43616f945de86be7b415c0ca2def

Files:

- anchor/programs/zkcash/src/errors.rs
- anchor/programs/zkcash/src/groth16.rs
- anchor/programs/zkcash/src/lib.rs
- anchor/programs/zkcash/src/merkle_tree.rs
- anchor/programs/zkcash/src/utils.rs
- circuits/keypair.circom
- circuits/merkleProof.circom
- circuits/transaction2.circom
- circuits/transaction.circom

Final Commit Hash

b62c1e733cfc43616f945de86be7b415c0ca2def

Findings

Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.

Issues Found

High	Medium
0	0

Issues Not Fixed and Not Acknowledged

High	Medium
0	0

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.