MantaPay Trusted Setup Protocol Specification
v0.0.0

Francisco Hernandez, Todd Norton [*]

September 21, 2022

Abstract

We describe the protocol for the MantaPay trusted setup ceremony to generate prover and verifier keys for Groth16 ZK-SNARK proofs.

Contents

[*] ordered alphabetically.

1 Context

The context is this. Definitely gonna cite Groth16 [1] at some point.

1.1 Groth16 Protocol

1.2 MPC Parameter Generation

1.3 Phase Structure

2 Scope

The scope is this

3 Definitions

Definition 3.0.1 (Circuit)**.** A circuit is . . .

4 Requirements

4.1 Goals

4.2 Non-Goals

5 Design

5.1 Ceremony Protocol

5.2 Server State Machine

5.3 Client State Machine

6 References

References

[1] Jens Groth. On the size of pairing-based non-interactive arguments. In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 305–326. Springer, 2016.