Chapter 1

Trusted Setup and ceremony plan

This chapter will provide an overview of what a trusted setup entails and its importance in Zero-Knowledge proof systems like Groth16. In this part we will detail the steps involved in organizing a trusted setup ceremony, including the roles of participants and how the process generates the cryptographic keys necessary for secure proof generation. Additionally, security considerations will be detailed, such as the requirement for participants to properly discard their secret inputs (toxic waste) and the potential risks if the process is compromised. The chapter will highlight how these elements contribute to the overall security of the system.

1.1 What is a trusted setup?

The Semaphore protocol relies on a Zero-Knowledge proof system known as Groth16. To securely generate proofs using this system, a preliminary step known as a "setup" must be performed. This setup is done through a Multi-Party Computation (MPC) ceremony, which aims to generate two essential cryptographic components: the *prover key* and the *verification key*. These keys are critical for ensuring that the proofs created by the protocol are valid and secure.

To complete the trusted setup requires participation from multiple parties. Each participant takes turns to provide a random input to the process, so the randomness is secuentially provided by the different parties during the ceremony. This randomness must be kept secret by each participant. Once a participant has contributed their randomness, they are required to discard it, as retaining or revealing it could compromise the entire system. For this reason, the discarded randomness is referred to as *toxic waste*. The security of the ceremony depends on at least one participant properly discarding their toxic waste. As long as one member securely destroys their secret input, the integrity of the setup remains

intact. However, if all participants collude and retain or share their randomness, the integrity of the ceremony is compromised. In such a scenario, malicious actors could generate seemingly valid but fraudulent proofs. This would allow users to bypass the security measures of any system that relies on the Groth-16 scheme, effectively undermining its trustworthiness. Therefore, the ceremony requires a significant numbers of contributors, where the possibility of collusion lowers when newer contributors join the ceremony.

1.2 Ceremony phases

The Semaphore protocol setup consists of two phases: the Powers of Tau and a Circuit-Specific setup. Both phases are crucial for securely generating the cryptographic material required to create and verify proofs in the Groth-16 scheme.

1.2.1 Phase I: Powers of Tau

The first phase, called *Powers of Tau*, is a universal setup process that generates reusable parameters for different circuits or applications using zk-SNARKs. This phase relies on an MPC ceremony where multiple participants contribute randomness in sequence. Each participant takes the result from the previous participant, adds their own secret randomness, and passes the updated result to the next. As in all MPC processes, the security of this phase depends on at least one participant discarding their secret input, or *toxic waste*. If even a single participant behaves honestly, the final parameters remain secure. On the contrary, if all participants collude and keep their secret randomness, it could compromise the integrity of the parameters, leading to the possibility of malicious proofs.

1.2.2 Phase II: Circuit-specific phase

Once the Powers of Tau phase is completed, the setup moves to the Circuit-Specific phase. In this phase, the parameters from the Powers of Tau are adapted for a specific circuit or application. The goal is to generate the *prover key* and *verification key*, which are essential for constructing and verifying proofs tailored to that specific circuit. Similar to the previous phase, this process is carried out through an MPC ceremony where multiple participants inject randomness into the circuit-specific parameters. Again, each participant must discard their toxic waste to ensure the security of the system. If even one participant acts honestly, the setup remains secure. However, if all participants collude, they could manipulate the circuit-specific parameters, enabling them to produce fraudulent proofs and potentially undermining the trustworthiness of any system built on top of the circuit.

1.3 Plan for Semaphore Trusted Setup Ceremony

The Semaphore protocol requires a trusted setup ceremony to ensure the security of its cryptographic system. The PSE.DEV group has already conducted a trusted setup ceremony for their 3rd version, which we plan to port to our implementation of Semaphore. However, it is original setup only supports Zero-Knowledge proofs using the BN254 elliptic curve, which is incompatible with the BLS12-381 elliptic curve cryptographic supported by Cardano. This difference in elliptic curves means that we cannot simply reuse the existing trusted setup: A completely new setup has to be executed again, in order to generate a new set of cryptographic parameters compatible with the elliptic curves used in Cardano. To ensure the successful completion of the trusted setup for Semaphore, we will follow a structured plan that accommodates the transition from the original BN254 curve to Cardano's BLS12-381 curve. Below are the steps for coordinating the ceremony, covering both logistical and cryptographic aspects:

1.3.1 Initial Preparations

Objective: Perform the trusted setup for Semaphore on the BLS12-381 curve, since the previous setup on the BN254 curve is cryptographically incompatible with Cardano.

Team Coordination: Our team will act as the coordinator for the ceremony, ensuring smooth communication between participants, software setup, and results management.

Software: We will use the software *poti0n*, developed by the PSE dev group, to manage the ceremony. This software will handle the cryptographic computations, manage participant inputs, and ensure transparency in the process.

1.3.2 Participant Selection

Target Group: We will invite between 15 and 20 participants for the ceremony. To ensure security and diversity, the group will consist at least of:

- **10 paid participants** funded by the proposal.
- **voluntary participants.** who will contribute ad-honorem to the ceremony.

Selection Criteria: Participants selected will be independent from the Modulo-p team. The only requirement for participants is basic terminal usage and comply with the minimal hardware specifications to run the setup. We aim to have a mix of cryptographers, developers, and community members to prevent any risk of collusion.

1.3.3 Ceremony Coordination

Role Assignment: The participants will be divided into groups, with each participant contributing randomness sequentially to the ceremony.

Coordinator Role: As coordinators, we will:

- Set up the initial parameters.
- Provide the infraestructure means to distribute challenge files to each participant.
- Collect their response files.
- Ensure proper cryptographic attestation for each contribution.
- Maintain a public record of the entire process.

1.3.4 Ceremony Execution

Step 1: Generate Initial Parameters Using the poti0n software, the ceremony begins by generating the initial parameters for the cryptographic curve BLS12-381.

Step 2: Multi-Party Contributions Each participant receives the challenge file and injects their secret randomness. Their response is submitted back, signed with a cryptographic attestation.

Step 3: Toxic Waste Handling Participants must destroy their secret inputs after contributing to ensure the security of the ceremony.

Step 4: Verification and Public Transcript As the process completes, the coordinator will verify the responses and compile the public transcript, which includes the full set of challenge files, response files, and signed attestations. This ensures that the process can be audited by anyone.

1.3.5 Security Considerations

Honest Participation The ceremony is secure as long as at least one participant discards their toxic waste. Even if multiple participants collude, as long as one behaves honestly, the entire process remains secure.

Transparency: The public transcript will be made available for review by any interested party, enabling external verification of the ceremony's integrity.

Fraud Prevention: If all participants collude to retain their toxic waste, the ceremony could be compromised. Thus, careful selection and diversity among participants are essential to avoid such risks.

1.3.6 Post-Ceremony Steps

Public Announcement: Once the ceremony is completed and verified, a document with key information about the ceremony and the public transcript will be shared with the community, including all contributions and details of the process. This transcript will contain all the cryptographic elements needed for public verification.

Public Testimony: Each participant will share a post on social networks, declaring their participation in the ceremony and verifying their honest contribution. These posts will include evidence of their involvement, such as timestamps or signed messages, and potentially a brief explanation of their role in the process. This step enhances transparency and encourages broader community trust.

Auditing and Validation (optionally): Cryptographic experts and the wider community will be invited to audit the transcript. This allows independent verification of the ceremony's correctness, ensuring that no party had the ability to influence the outcome improperly. Participants and observers can use the public transcript to check that all contributions were valid and that the secrets were appropriately discarded

This plan ensures the trusted setup for Semaphore on the Cardano blockchain is secure, transparent, and verifiable.