Cardano-Semaphore Trusted Setup Test Document

Process overview

The objective of this experiment is to test the ceremony software, and have a simulation of how the ceremony would be.

The software used is based on an instance of the p0tion software. This software provides the means to coordinate and contribute to the ceremony. First, we created a package of the software required to contribute, and published it to the npm registry as @modulo-p/phase2cli. Then, set up the ceremony in an AWS instance and ran the ceremony with 1 one coordinator and three contributions. Since we now are just two members in the modulo-p team, we repeated a contribution with the same participant. In a production ceremony this is not good practice to have duplicate participants, however since this is a simulation ceremony to test the software, to have a virtual third contributor it doesn't represent any inconvenience to the process itself. We could accomplish the ceremony and derive the public keys correctly.

Participants

- **Coordinator:** Juan Magán Valero (jmagan-24716625).
- **Contributor 1:** Juan Magán Valero
- **Contributor 2:** Agustín Salinas (AgustinBadi-52472400).
- **Contributor 3 (Virtual):** Juan Magán Valero.

Verification transcript for semaphore circuit Phase 2 contribution.

The software generates a transcript file which details the participants and its contributions. A new transcript file is generated at each contribution, the outputs of this process can be found in this link:

https://github.com/Modulo-P/Cardano-Semaphore/tree/main/docs/Ceremony/test_outputs/transcripts

Taking in account the final transcript which sums up the whole process. The coordinator is specified at the start of the document, along with each participant's contribution digest and an ID based on its Github profile. The transcript shows a digest of the circuit, which is the circuit that we are using in our prototype. The final contributor has to generate a beacon to finalize the ceremony.

Coordinator (jmagan-24716625)

Circuit Hash:

fc05fe32 90faee66 6c48733a 1fb35d55

61d6bb9a 2e2de081 a27accbc 14d69722

e05bdbe4 6055d700 1472e4eb e1877951

b3719fb5 47a419da b41c5b66 99051aa4

---

contribution #3 jmagan-24716625:

24c6f893 9d94eb6a 1d670da5 f5adf362

7f8f0264 c7fb720c d0bf4537 89654b8e

691dd347 2bc6ef1d 476a0003 8d682f94

e885383a 318bc1de b3a6aa73 704cac03

Beacon generator:
c60b464076d4060865e08bdfcf386f05d45ec0d57799d071e92f0240f6bb91e5

Beacon iterations Exp: 10

---

contribution #2 AgustinBadi-52472400:

5a6a3ae7 15a18196 37c706e7 493c232c

548ee122 530a4b66 f62b39d5 4c293c83

1523c620 a49f6128 0cb3bfb0 7da818b8

edb2f0de cea702c7 1aaff028 cf93df99

---

contribution #1 jmagan-24716625:

```
            ec9071bc 8e091428 07cdc68e 723f3179

            4b983450 cbd5937a 1c1c0773 3ff9da83

            2b4e2fd1 eb7037f9 5aca782c a409a71a

            184cddce 9110224e 0ac1083b e0785b68

-------------------------

ZKey Ok!
```

Outputs: Public keys

Also the ceremony generates the corresponding keys at each step of the process. In the following link it can be found the keys generated at each contribution step, along with the keys derived at the close in a json format:

https://github.com/Modulo-P/Cardano-Semaphore/tree/main/docs/Ceremony/test_outputs/contributions

These keys are the public values that are used by Semaphore protocol to build the Zero-Knowledge proofs.

Conclusions

We could successfully conduct the simulation ceremony and derive a set of public keys to be used for the Semaphore protocol.