Cardano-Semaphore Trusted Setup Phase 2.

Process overview

The objective of the ceremony was to derive the public keys necessary for constructing the Zero-Knowledge proofs used in the Cardano-Semaphore protocol.

The ceremony involved **20** participants and began on November 18th, 2024, concluding on December 20th 2024. Participation was announced open to the public on X, and coordination was facilitated through a dedicated Discord server.

To ensure the authenticity of contributors, their identities were verified through direct messages or, when necessary, via video calls. Ten contributors who did not respond to our messages could not be fully verified; however, a record of their social media accounts was included.

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.

Coordinator

Coordinator name	Juan Magán Valero.
Email address:	jmaganvalero@gmail.com

Participants

Participant 1°	Juan Magán Valero.
Email address	jmaganvalero@gmail.com
Github account	jmagan
Twitter account	DoItWLovelace

Wallet address	n/a

Participant 2°	Agustín Salinas H.
Email address	librenotgratis@tuta.io
Github account	AgustinBadi
Twitter account	modp_
Wallet address	n/a

Participant 3°	Fernando Gonzalez
Email address	
Github account	pescantao9
Twitter account	feeer2011
Wallet address	

Participant 4°	Sergio Nicolas Chouhy
Email address	sergiochouhy@gmail.com
Github account	schouhy
Twitter account	schouhy
Wallet address	addr1qxm84n5ryh206cpwq9gc6vjl6kq040k5tw3cysz3mkhaq95z6r06cuazrswp2fq7n6y3h9h3jpfv9y9sutwfvr78s5gs9gswln

Participant 5°	Agustín Garassino.
Email address	

Github account	
Twitter account	
Wallet address	

Participant 6°	Chino Cribioli
Email address	echinoc40@gmail.com
Github account	ChinoCribioli
Twitter account	0xRocketRaccon
Wallet address	addr1qx0vk7fl8mzhh9sc7twmcly3297a6qfz6rwzplpcqhhqhzalckr2p8myxzvaen43yvd4zl7wjp7zcu8256hn6mqt7xvsfqnwu7

Participant 7°	Alejandro Tomás Grosso
Email address	tgrosso@eryx.co
Github account	atgrosso
Twitter account	atomgrosso
Wallet address	addr1qxyttz69yn7fe2cz4etzswxuyuf5ssxz9nuwd9rawlh9th8g6h4y75eadsamafu0nmp3j9257756k7am076s97zelq2s30eh72

Participant 8°	marlon poaires
Email address	
Github account	uawaaN
Twitter account	gostshark
Wallet address	

Participant 9°	agustina verdile
Email address	
Github account	vaipytiQ6
Twitter account	agusagusver
Wallet address	

Participant 10°	Carlo Giambiagi Ferrari
Email address	cgferrari@gmail.com
Github account	carlogf
Twitter account	CgferrariFerr
Wallet address	addr1qxys73sqrwhlk8whk8mcmkstqrjnnrrrdedehy5v7z5us5u4x3tnaqmpc2sk0pxvrx974xlph7v97ndt2lsak2f3psssl56z2e

Participant 11°	Dav Can
Email address	adarules@protonmail.com
Github account	bnchk
Twitter account	IbisNodes
Wallet address	addr1q9ysf6fnlr0qg46x3x8j8dhzn3r2fhfw0l34tca5zlkvnga73vr75xknjt53ac2tdcl5093q6yxj9v7thx7mvluwux2s8kjfr0

Participant 12°	Gilles BERNARD
Email address	gillesstargate@yahoo.fr
Github account	GillesGaelBERNARD
Twitter account	Gilles51405099

Wallet address	addr1qxjxk7c0y8qpu92hd97qwwxgk06cyjnkzgd6h4qwkll0cmtcuzvwqyykmgtuuzgzf370atfv2veh20520y0wv26ttghqpp6zx4

Participant 13°	Ash Can
Email address	schnoomoo@gmail.com
Github account	schnoomoo
Twitter account	w3_future
Wallet address	addr1qypwtfzfn3v8vg5xuwd3r92y4f4g670uuswfs2wmzesta88pas09r70l494qk2j3hpfdlrpfw2nsdhglc7mc72cqprdqrt0drw

Participant 14°	Declan McLaren
Email address	arrenclan@mail.com
Github account	sobrelacallew9
Twitter account	Mujammilkhan7
Wallet address	

Participant 15°	unknown
Email address	
Github account	granonasag
Twitter account	kashifazadkhan
Wallet address	

Participant 16°	**Unknown**
Email address	

Github account	poganjenaTR
Twitter account	
Wallet address	

Participant 17°	**Unknown**
Email address	
Github account	alnash
Twitter account	berkay_ak1
Wallet address	

Participant 18°	**Unknown**
Email address	
Github account	KevinLarsson6
Twitter account	Valezhca
Wallet address	

Participant 19°	**Unknown**
Email address	
Github account	Ydlxz
Twitter account	amandaesidney
Wallet address	

Participant 20°	**Unknown**
Email address	

Github account	byncnittyvM
Twitter account	wormyking
Wallet address	

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/transcript

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.

Outputs: Public keys

The resulting keys of the process can be found in the following link:

https://github.com/Modulo-P/Cardano-Semaphore/blob/main/keys/semaphore_final.zkey

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

Conclusions

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